



# **Cisco IOS IP Routing Protocols Configuration Guide**

Release 12.4

## **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Customer Order Number: DOC-7817481=  
Text Part Number: 78-17481-01



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.



## **About Cisco IOS Software Documentation for Release 12.4**    **xlv**

Documentation Objectives	<b>xlv</b>
Audience	<b>xlv</b>
Documentation Organization for Cisco IOS Release 12.4	<b>xlvi</b>
Document Conventions	<b>lii</b>
Obtaining Documentation	<b>liii</b>
Cisco.com	<b>liii</b>
Product Documentation DVD	<b>liv</b>
Ordering Documentation	<b>liv</b>
Documentation Feedback	<b>liv</b>
Cisco Product Security Overview	<b>lv</b>
Reporting Security Problems in Cisco Products	<b>lv</b>
Obtaining Technical Assistance	<b>lvi</b>
Cisco Technical Support & Documentation Website	<b>lvi</b>
Submitting a Service Request	<b>lvi</b>
Definitions of Service Request Severity	<b>lvii</b>
Obtaining Additional Publications and Information	<b>lvii</b>

## **Using Cisco IOS Software for Release 12.4**    **lix**

Understanding Command Modes	<b>lix</b>
Getting Help	<b>lx</b>
Example: How to Find Command Options	<b>lxi</b>
Using the no and default Forms of Commands	<b>lxiv</b>
Saving Configuration Changes	<b>lxiv</b>
Filtering Output from the show and more Commands	<b>lxv</b>
Finding Additional Feature Support Information	<b>lxv</b>

---

## **PART 1: BGP**

### **BGP Features Roadmap**    **3**

### **Cisco BGP Overview**    **11**

Contents	<b>11</b>
Prerequisites for Cisco BGP	<b>11</b>

Restrictions for Cisco BGP	11
Information About Cisco BGP	12
BGP Version 4 Functional Overview	12
BGP Autonomous Systems	13
Classless Interdomain Routing	14
Multiprotocol BGP	14
Benefits of Using Multiprotocol BGP Versus BGP	14
Multiprotocol BGP Extensions for IP Multicast	15
NLRI Configuration CLI	17
Cisco BGP Address Family Model	17
IPv4 Address Family	19
IPv6 Address Family	20
CLNS Address Family	20
VPNv4 Address Family	20
Where to Go Next	21
Additional References	21
Related Documents	21
Standards	21
MIBs	22
RFCs	22
Technical Assistance	22
<b>Configuring a Basic BGP Network</b>	<b>23</b>
Contents	23
Prerequisites for Configuring a Basic BGP Network	23
Restrictions for Configuring a Basic BGP Network	24
Information About Configuring a Basic BGP Network	24
BGP Version 4	24
BGP-Speaker and Peer Relationships	25
BGP Peer Session Establishment	25
Cisco Implementation of BGP Global and Address Family Configuration Commands	26
BGP Session Reset	27
BGP Route Aggregation	28
BGP Peer Groups	28
Peer Groups and BGP Update Messages	28
BGP Update Group	29
Peer Templates	29
How to Configure a Basic BGP Network	30
Configuring a BGP Routing Process	30



BGP Router ID	31
Examples	33
Troubleshooting Tips	33
Configuring a BGP Peer	33
Prerequisites	33
Restrictions	34
Examples	35
Troubleshooting Tips	37
What To Do Next	37
Configuring a BGP Peer for the IPv4 VRF Address Family	37
Prerequisites	38
Troubleshooting Tips	41
Customizing a BGP Peer	41
Restrictions	41
Examples	44
Monitoring and Maintaining Basic BGP	45
Routing Policy Change Management	46
Configuring Inbound Soft-Reconfiguration When Route Refresh Capability is Missing	47
Resetting and Displaying Basic BGP Information	50
Aggregating Route Prefixes Using BGP	52
Redistributing a Static Aggregate Route Into BGP	52
Configuring Conditional Aggregate Routes Using BGP	53
Suppressing and Unsuppressing Advertising Aggregated Routes Using BGP	55
Suppressing Inactive Route Advertisement Using BGP	56
Conditionally Advertising BGP Routes	58
Originating BGP Routes	60
Advertising a Default Route Using BGP	60
Conditionally Injecting BGP Routes	62
Originating BGP Routes Using Backdoor Routes	66
Configuring a BGP Peer Group	68
Restrictions	68
Configuring Peer Session Templates	70
Inheritance in Peer Templates	70
Configuring a Basic Peer Session Template	71
Configuring Peer Session Template Inheritance with the inherit peer-session Command	74
Configuring Peer Session Template Inheritance with the neighbor inherit peer-session Command	76
Configuring Peer Policy Templates	78
Configuring Basic Peer Policy Templates	78
Restrictions	79

Configuring Peer Policy Template Inheritance with the inherit peer-policy Command	81
Configuring Peer Policy Template Inheritance with the neighbor inherit peer-policy Command	83
Monitoring and Maintaining BGP Dynamic Update Groups	85
BGP Dynamic Update Group Configuration	85
Configuration Examples for Configuring a Basic BGP Network	87
Configuring a BGP Process and Customizing Peers: Example	87
NLRI to AFI Configuration: Example	88
BGP Soft Reset: Examples	90
Aggregating Prefixes Using BGP: Examples	90
Configuring a BGP Peer Group: Example	91
Configuring Peer Session Templates: Examples	91
Configuring Peer Policy Templates: Examples	92
Monitoring and Maintaining BGP Dynamic Update Peer-Groups: Examples	93
Where to Go Next	94
Additional References	94
Related Documents	94
Standards	94
MIBs	95
RFCs	95
Technical Assistance	95
Feature Information for Configuring a Basic BGP Network	96
<b>Connecting to a Service Provider Using External BGP</b>	<b>99</b>
Contents	99
Prerequisites for Connecting to a Service Provider Using External BGP	100
Restrictions for Connecting to a Service Provider Using External BGP	100
Information About Connecting to a Service Provider Using External BGP	100
External BGP Peering	101
BGP Attributes	102
BGP Multipath Support	103
Multihoming	104
Transit Versus Nontransit Traffic	104
BGP Policy Configuration	105
BGP Communities	105
Extended Communities	106
Administrative Distance	107
BGP Route Map Policy Lists	107
How to Connect to a Service Provider Using External BGP	108

Influencing Inbound Path Selection	108
Influencing Inbound Path Selection by Modifying the AS-path Attribute	108
Influencing Inbound Path Selection by Setting the MED Attribute	112
Influencing Outbound Path Selection	116
Influencing Outbound Path Selection Using the Local_Pref Attribute	116
Filtering Outbound BGP Route Prefixes	119
Prerequisites	119
Restrictions	119
Configuring BGP Peering with ISPs	122
Configuring Multihoming with Two ISPs	122
Multihoming with a Single ISP	126
Configuring Multihoming to Receive the Full Internet Routing Table	131
Configuring BGP Policies	134
Filtering BGP Prefixes with Prefix Lists	135
Filtering BGP Prefixes with AS-path Filters	138
Filtering Traffic Using Community Lists	140
Filtering Traffic Using Extended Community Lists	144
Filtering Traffic Using a BGP Route Map Policy List	147
Filtering Traffic Using BGP Route Map Continue Clauses	150
Configuration Examples for Connecting to a Service Provider Using External BGP	154
Influencing Inbound Path Selection: Examples	154
Influencing Outbound Path Selection: Examples	156
Filtering BGP Prefixes with Prefix Lists: Examples	157
Filtering BGP Prefixes Using a Single Prefix List	157
Filtering BGP Prefixes Using a Group of Prefixes	157
Adding or Deleting Prefix List Entries	158
Filtering Traffic Using Community Lists: Examples	158
Filtering Traffic Using AS-path Filters: Example	159
Filtering Traffic Using a BGP Route Map: Example	159
Filtering Traffic Using a BGP Route Map Continue Clause: Example	160
Where to Go Next	160
Additional References	161
Related Documents	161
Standards	161
MIBs	161
RFCs	161
Technical Assistance.	162
Feature Information for Connecting to a Service Provider Using External BGP	162

<b>Configuring Internal BGP Features</b>	<b>167</b>
Configuring Internal BGP Features	167
Configuring a Routing Domain Confederation	168
Configuring a Route Reflector	168
Adjusting BGP Timers	172
Configuring the Router to Consider a Missing MED as Worst Path	172
Configuring the Router to Consider the MED to Choose a Path from Subautonomous System Paths	172
Configuring the Router to Use the MED to Choose a Path in a Confederation	173
Configuring Route Dampening	173
Minimizing Flapping	174
Understanding Route Dampening Terms	174
Enabling Route Dampening	175
Monitoring and Maintaining BGP Route Dampening	175
Internal BGP Feature Configuration Examples	176
BGP Confederation Configurations with Route Maps Example	176
BGP Confederation Examples	177
<b>BGP Link Bandwidth</b>	<b>179</b>
Contents	179
Prerequisites for BGP Link Bandwidth	180
Restrictions for BGP Link Bandwidth	180
Information About BGP Link Bandwidth	180
BGP Link Bandwidth Overview	180
Link Bandwidth Extended Community Attribute	181
Benefits of the BGP Link Bandwidth Feature	181
How to Configure BGP Link Bandwidth	181
Configuring BGP Link Bandwidth	181
Verifying BGP Link Bandwidth Configuration	183
Configuration Examples for BGP Link Bandwidth	183
BGP Link Bandwidth Configuration Example	184
Verifying BGP Link Bandwidth	186
Where to Go Next	187
Additional References	187
Related Documents	187
Standards	188
MIBs	188
RFCs	188
Technical Assistance	188

Command Reference	189
<b>iBGP Multipath Load Sharing</b>	<b>191</b>
Feature Overview	191
Benefits	193
Restrictions	193
Related Features and Technologies	194
Related Documents	194
Supported Platforms	194
Supported Standards, MIBs, and RFCs	195
Configuration Tasks	195
Configuring iBGP Multipath Load Sharing	195
Verifying iBGP Multipath Load Sharing	196
Monitoring and Maintaining iBGP Multipath Load Sharing	198
Configuration Examples	198
Non-MPLS Topology Example	199
MPLS VPN Topology Example	199
Command Reference	200
<b>BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN</b>	<b>201</b>
Contents	202
Prerequisites for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN	202
Restrictions for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN	202
Information About BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN	203
Multipath Load Sharing Between eBGP and iBGP	203
eBGP and iBGP Multipath Load Sharing in a BGP MPLS Network	204
eBGP and iBGP Multipath Load Sharing With Route Reflectors	205
Benefits of Multipath Load Sharing for Both eBGP and iBGP	205
How to Configure BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN	205
Configuring Multipath Load Sharing for Both eBGP and iBGP	206
Verifying Multipath Load Sharing for Both eBGP and iBGP	207
Configuration Examples for the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN Feature	208
eBGP and iBGP Multipath Load Sharing Configuration Example	208
eBGP and iBGP Multipath Load Sharing Verification Examples	209
Where to Go Next	210
Additional References	210
Related Documents	210
Standards	210

MIBs	211
RFCs	211
Technical Assistance	211
Command Reference	211

## **BGP Hide Local-Autonomous System 213**

Contents	213
Prerequisites for BGP Hide Local-Autonomous System	214
Restrictions for BGP Hide Local-Autonomous System	214
Information About BGP Hide Local-Autonomous System	214
Changing the Autonomous System Number in a BGP Network	214
Configuring the BGP Hide Local-Autonomous System Feature	214
Benefits of the BGP Hide Local-Autonomous System Feature	215
How to Configure BGP Hide Local-Autonomous System	215
Configuring BGP to Not Prepend the Local Autonomous System Number to Routes Learned From External Peers	215
Configuring the no-prepend Keyword	215
Restrictions	216
Examples	217
What to Do Next	217
Verifying the Configuration of the BGP Hide Local-Autonomous Feature	217
Additional References	218
Related Documents	218
Standards	218
MIBs	218
RFCs	218
Technical Assistance	219
Command Reference	219

## **BGP 4 MIB Support for per-Peer Received Routes 221**

Feature Overview	221
BGP 4 per-Peer Received Routes Table Elements and Objects	222
MIB Tables and Objects	222
AFIs and SAFIs	223
Network Address Prefix Descriptions for the NLRI Field	224
Benefits	225
Restrictions	225
Related Features and Technologies	225
Related Documents	225
Supported Platforms	225

Supported Standards, MIBs, and RFCs	226
Configuration Tasks	226
Configuration Examples	227
Command Reference	227
Glossary	228
<b>BGP Policy Accounting</b>	<b>229</b>
Feature Overview	229
<b>BGP Policy Accounting</b>	<b>229</b>
Feature Overview	229
Benefits	230
Related Features and Technologies	230
Related Documents	231
Supported Platforms	231
Supported Standards, MIBs, and RFCs	232
Prerequisites	232
Configuration Tasks	233
Specifying the Match Criteria for BGP Policy Accounting	233
Classifying the IP Traffic and Enabling BGP Policy Accounting	234
Verifying BGP Policy Accounting	234
Monitoring and Maintaining BGP Policy Accounting	235
Configuration Examples	236
Specifying the Match Criteria for BGP Policy Accounting Example	236
Classifying the IP Traffic and Enabling BGP Policy Accounting Example	236
Command Reference	237
Glossary	237
<b>BGP Nonstop Forwarding (NSF) Awareness</b>	<b>239</b>
Contents	239
Prerequisites for BGP Nonstop Forwarding Awareness	240
Restrictions for BGP Nonstop Forwarding Awareness	240
Information About BGP Nonstop Forwarding Awareness	240
Cisco NSF Routing and Forwarding Operation	240
Cisco Express Forwarding	241
BGP Graceful Restart	241
BGP NSF Awareness	242
How to Configure BGP Nonstop Forwarding Awareness	243
Configuring BGP Nonstop Forwarding Awareness	243

BGP Graceful Restart	243
Troubleshooting Tips	244
What to do next	245
Configuring BGP NSF Awareness Timers	245
BGP NSF Awareness Timers	245
What to do next	246
Verifying the Configuration of BGP Nonstop Forwarding Awareness	247
Configuration Examples for Nonstop Forwarding	247
Configuring BGP NSF Awareness Example	248
Configuring the Restart Time for BGP NSF Awareness	248
Configuring the Stalepath Time for BGP NSF Awareness	248
Verifying BGP NSF Awareness	248
Where to Go Next	249
Additional References	249
Related Documents	249
Standards	250
MIBs	250
RFCs	250
Technical Assistance	251
Command Reference	251
<b>BGP Restart Session After Max-Prefix Limit</b>	<b>253</b>
Contents	253
Prerequisites for Restart Session After Max-Prefix Limit	254
Restrictions for Restart Session After Max-Prefix Limit	254
Information About Restart Session After Max-Prefix Limit	254
Prefix Limits and Peering Sessions	254
Reestablishing Sessions After the Maximum Prefix Limit	254
How to Configure the Restart Session After Max-Prefix Limit feature	255
Configuring a Router to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded	255
Reestablishing Peering Sessions	255
Restrictions	255
Troubleshooting Tips	257
What to Do Next	257
Verifying that a Router is Configured to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded	257
Configuration Examples for the Restart Session After Max-Prefix Limit feature	258
Restart Session After Max-Prefix Limit Configuration Example	258



Restart Session After Max-Prefix Limit Verification Example	258
Additional References	260
Related Documents	260
Standards	260
MIBs	260
RFCs	261
Technical Assistance	261
Command Reference	261
<b>BGP Cost Community</b>	<b>263</b>
Contents	263
Prerequisites for the BGP Cost Community Feature	264
Restrictions for the BGP Cost Community Feature	264
Information About the BGP Cost Community Feature	264
BGP Cost Community Overview	264
How the BGP Cost Community Influences the Best Path Selection Process	265
Cost Community Support for Aggregate Routes and Multipaths	266
Influencing Route Preference in a Multi-Exit IGP Network	266
BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links	267
How to Configure the BGP Cost Community Feature	267
Configuring the BGP Cost Community	268
Verifying the Configuration of the BGP Cost Community	269
Troubleshooting Tips	269
Configuration Examples for the BGP Cost Community Feature	270
BGP Cost Community Configuration Example	270
BGP Cost Community Verification Examples	270
Where to Go Next	272
Additional References	272
Related Documents	272
Standards	272
MIBs	272
RFCs	272
Technical Assistance	273
Command Reference	273
<b>Loadsharing IP Packets Over More Than Six Parallel Paths</b>	<b>275</b>
Contents	275
Restrictions for Loadsharing IP Packets Over More Than Six Parallel Paths	275
Loadsharing IP Packets Over More Than Six Parallel Paths Overview	276

Additional References	276
Related Documents	276
MIBs	276
RFCs	277
Technical Assistance	277
Command Reference	277

## **BGP Policy Accounting Output Interface Accounting** 279

Contents	279
Prerequisites for BGP PA Output Interface Accounting	280
Information About BGP PA Output Interface Accounting	280
BGP PA Output Interface Accounting	280
Benefits of BGP PA Output Interface Accounting	281
How to Configure BGP PA Output Interface Accounting	281
Specifying the Match Criteria for BGP PA	282
Classifying the IP Traffic and Enabling BGP PA	283
Verifying BGP Policy Accounting	285
Configuration Examples for BGP PA Output Interface Accounting	288
Specifying the Match Criteria for BGP Policy Accounting: Example	288
Classifying the IP Traffic and Enabling BGP Policy Accounting: Example	288
Where to Go Next	289
Additional References	289
Related Documents	289
Standards	289
MIBs	290
RFCs	290
Technical Assistance	290
Command Reference	290
Glossary	291

## **Regex Engine Performance Enhancement** 293

Contents	293
Prerequisites for Regex Engine Performance Enhancement	294
Information About Regex Engine Performance Enhancement	294
Regular Expression Overview	294
Default Regular Expression Engine	294
New Regular Expression Engine Selection	294
How to Change the Regular Expression Engine	295
Selecting the New Regular Expression Engine	295

Prerequisites	295
Examples	296
Additional References	296
Related Documents	296
Standards	296
MIBs	297
RFCs	297
Technical Assistance	297
Command Reference	297
<b>BGP MIB Support Enhancements</b>	<b>299</b>
Contents	299
Prerequisites for BGP MIB Support Enhancements	300
Restrictions for BGP MIB Support Enhancements	300
BGP MIB Support Enhancements Overview	300
BGP FSM Transition Change Support	300
BGP Route Received Route Support	301
BGP Prefix Threshold Notification Support	301
VPNv4 Unicast Address Family Route Support	301
How to Enable BGP MIB Support on a Router	302
Configuration Examples for BGP MIB Support Enhancements	303
Configuring BGP MIB Support Enhancements: Example	303
Verifying BGP MIB Support Enhancements: Example	303
Where to Go Next	303
Additional References	303
Related Documents	303
Standards	303
MIBs	304
RFCs	304
Technical Assistance	304
Command Reference	304
<b>BGP Support for TTL Security Check</b>	<b>305</b>
Contents	305
Prerequisites for BGP Support for TTL Security Check	306
Restrictions for BGP Support for TTL Security Check	306
Information About BGP Support for TTL Security Check	306
BGP Support for TTL Security Check Feature Overview	307
Configuring the TTL Security Check for BGP Peering Sessions	307

Configuring the TTL Security Check for Multihop BGP Peering Sessions	307
Benefits of the BGP Support for TTL Security Check Feature	308
How to Secure BGP Sessions with the BGP Support for TTL Security Check Feature	308
Configuring the TTL-Security Check	308
Prerequisites	308
Restrictions	308
Examples	309
What to Do Next	310
Verifying the TTL-Security Check Configuration	310
Configuration Examples for the BGP Support for TTL Security Check Feature	311
Configuring the TTL-Security Check: Example	311
Verifying the TTL-Security Check Configuration: Example	311
Additional References	313
Related Documents	313
Standards	313
MIBs	314
RFCs	314
Technical Assistance	314
Command Reference	314
<b>BGP Support for Dual AS Configuration for Network AS Migrations</b>	<b>315</b>
Contents	315
Prerequisites for BGP Support for Dual AS Configuration for Network AS Migrations	316
Restrictions for BGP Support for Dual AS Configuration for Network AS Migrations	316
Information About BGP Support for Dual AS Configuration for Network AS Migrations	316
How to Configure Autonomous System Migration	317
Configuring Dual-AS Peering for Network Migration	317
Confederations, Individual Peering Sessions and Peer Groupings are Supported	317
Ingress Filtering can be Applied to Minimize the Possibility of Routing Loop Creation	317
Restrictions	317
Verifying Autonomous System Number Configuration	320
Configuration Examples for Autonomous-System Migration	321
Dual-AS Configuration: Example	321
Dual-AS Confederation Configuration: Example	322
Replace-AS Configuration: Example	322
Additional References	322
Related Documents	322
Standards	322
MIBs	323

RFCs	323
Technical Assistance	323
Command Reference	323
<b>BGP Support for IP Prefix Import from Global Table into a VRF Table</b>	<b>325</b>
Contents	325
Prerequisites for BGP Support for IP Prefix Import from Global Table into a VRF Table	326
Restrictions for BGP Support for IP Prefix Import from Global Table into a VRF Table	326
Information About BGP Support for IP Prefix Import from Global Table into a VRF Table	326
Importing IPv4 Prefixes into a VRF	326
Black Hole Routing	327
Classifying Global Traffic	327
How to Import IP Prefixes from Global Table into a VRF Table	327
Defining IPv4 IP Prefixes to Import	327
What to Do Next	328
Creating the VRF and the Import Route Map	328
MPLS and Route Target Configuration is not Required	328
Import Actions	329
New Syslog Message	329
Restrictions	329
What to Do Next	331
Filtering on the Ingress Interface	331
Unicast Reverse Path Forwarding	331
What to Do Next	332
Verifying Global IP Prefix Import	332
Configuration Examples for Importing IP Prefixes from the Global Table into a VRF Table	334
Configuring Global IP Prefix Import: Example	334
Verifying Global IP Prefix Import: Example	334
Additional References	335
Related Documents	335
Standards	336
MIBs	336
RFCs	336
Technical Assistance	336
Command Reference	337
<b>BGP Support for Fast Peering Session Deactivation</b>	<b>339</b>
Contents	339
Prerequisites for BGP Support for Next-Hop Address Tracking	340

Restrictions for BGP Support for Fast Peering Session Deactivation	340
Information About BGP Support for Fast Peering Session Deactivation	340
BGP Hold Timer	340
BGP Fast Peering Session Deactivation	340
How to Configure Fast Peering Session Deactivation	340
Configuring Fast Session Deactivation for a BGP Neighbor	341
Aggressively Dampen IGP Routes	341
Configuration Examples for BGP Fast Peering Session Deactivation	342
Configuring BGP Fast Peering Session Deactivation: Example	342
Where to Go Next	342
Additional References	342
Related Documents	343
Standards	343
MIBs	343
RFCs	343
Technical Assistance	343
Command Reference	344
<b>BGP Support for Next-Hop Address Tracking</b>	<b>345</b>
Contents	345
Prerequisites for BGP Support for Next-Hop Address Tracking	346
Restrictions for BGP Support for Next-Hop Address Tracking	346
Information About BGP Support for Next-Hop Address Tracking	346
Default BGP Scanner Behavior	346
BGP Support for Next-Hop Address Tracking	346
How to Configure BGP Next-Hop Address Tracking	346
Disabling BGP Next-Hop Address Tracking	347
Adjusting the Delay Interval for BGP Next-Hop Address Tracking	348
Configuration Examples for BGP Next-Hop Address Tracking	349
Enabling and Disabling BGP Next-Hop Address Tracking: Example	349
Adjusting the Delay Interval for BGP Next-Hop Address Tracking: Example	350
Where to Go Next	350
Additional References	350
Related Documents	350
Standards	350
MIBs	351
RFCs	351
Technical Assistance	351

Command Reference 351

## **BGP Multicast Inter-AS (IAS) VPN 353**

Contents 353

How to Configure an MDT Address Family Session in BGP 354

Configuring the MDT Address Family in BGP 354

Supported Policy 354

Prerequisites 354

Restrictions 354

Clearing IPv4 MDT Peering Sessions in BGP 355

Displaying Information about IPv4 MDT Sessions in BGP 356

Configuration Examples for the MDT Address Family 357

Configuring an IPv4 MDT Address-Family Session: Example 357

Additional References 357

Related Documents 357

Standards 357

MIBs 358

RFCs 358

Technical Assistance 358

Command Reference 358

---

## **PART 2: EIGRP**

### **Configuring EIGRP 361**

The Cisco EIGRP Implementation 361

EIGRP Configuration Task List 363

Enabling EIGRP 363

Making the Transition from IGRP to EIGRP 364

Logging EIGRP Neighbor Adjacency Changes 364

Configuring the Percentage of Link Bandwidth Used 364

Adjusting the EIGRP Metric Weights 364

Mismatched K Values 365

The Goodbye Message 366

Applying Offsets to Routing Metrics 366

Disabling Route Summarization 366

Configuring Summary Aggregate Addresses 367

Configuring Floating Summary Routes 367

Configuring EIGRP Route Authentication 369

Configuring EIGRP Protocol-Independent Parameters 370

Adjusting the Interval Between Hello Packets and the Hold Time 370

Disabling Split Horizon	371
Configuring EIGRP Stub Routing	372
Dual-Homed Remote Topology	373
EIGRP Stub Routing Configuration Task List	376
Configuring EIGRP Stub Routing	376
Verifying EIGRP Stub Routing	376
Monitoring and Maintaining EIGRP	377
EIGRP Configuration Examples	377
Route Summarization Example	377
Route Authentication Example	378
Stub Routing Example	379
<b>EIGRP Nonstop Forwarding (NSF) Awareness</b>	<b>381</b>
Contents	381
Prerequisites for EIGRP Nonstop Forwarding Awareness	382
Restrictions for EIGRP Nonstop Forwarding Awareness	382
Information About EIGRP Nonstop Forwarding Awareness	382
Cisco NSF Routing and Forwarding Operation	382
Cisco Express Forwarding	383
EIGRP Nonstop Forwarding Awareness	383
EIGRP NSF Capable and NSF Aware Interoperation	384
Non-NSF Aware EIGRP Neighbors	384
EIGRP NSF Route-Hold Timers	384
How to Modify and Maintain EIGRP Nonstop Forwarding Awareness	385
Adjusting NSF Route-Hold Timers	385
Route-Hold Timers	385
Troubleshooting Tips	386
Monitoring EIGRP NSF Debug Events and Notifications	386
Debug Commands	386
Verifying the Local Configuration of EIGRP NSF Awareness	387
Configuration Examples for EIGRP Nonstop Forwarding Awareness	388
EIGRP Route-Hold Timer Configuration Example	388
Monitoring EIGRP NSF Debug Events and Notifications Configuration Example	388
Verifying Local Configuration of EIGRP NSF Awareness	388
Additional References	389
Related Documents	389
Standards	389
MIBs	389
RFCs	389



Technical Assistance	390
Command Reference	390
<b>MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge</b>	<b>391</b>
Contents	391
Prerequisites for MPLS VPN Support for EIGRP Between PE and CE	392
Restrictions for MPLS VPN Support for EIGRP Between PE and CE	392
Information About MPLS VPN Support for EIGRP Between PE and CE	392
MPLS VPN Support for EIGRP	392
EIGRP Extended Community Attributes	394
Benefits of MPLS VPN Support for EIGRP	395
How to Configure an MPLS VPN Using EIGRP	395
Configuring the VRF for the EIGRP MPLS VPN	395
Creating a VRF	395
Prerequisites	395
Restrictions	396
What to Do Next	397
Configuring EIGRP Redistribution in the MPLS VPN	397
Creating the MPLS VPN	397
Prerequisites	398
Restrictions	398
Troubleshooting Tips	400
What to Do Next	400
Configuring the PE Routers to Support the EIGRP MPLS VPN	401
Basic BGP Configuration	401
Prerequisites	401
Verifying the VPN Configuration	403
Verifying PE-to-PE Connectivity	404
Verifying EIGRP VRF Configuration	405
Configuration Examples for the EIGRP MPLS VPN	405
EIGRP MPLS VPN Configuration Example	406
BGP Network Configuration Example	406
EIGRP Redistribution Example	406
EIGRP MPLS VPN Verification Examples	406
Verifying Route Distinguisher and MPLS Configuration Example	407
Verifying PE-to-PE Connectivity Example	407
Verifying EIGRP VRF Configuration Example	409
Where to Go Next	409
Additional References	410

Related Documents	410
Standards	410
MIBs	410
RFCs	411
Technical Assistance	411
Command Reference	411
<b>EIGRP MPLS VPN PE-CE Site of Origin (SoO)</b>	<b>413</b>
Contents	413
Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin (SoO)	414
Restrictions for EIGRP MPLS VPN PE-CE Site of Origin (SoO)	414
Information About EIGRP MPLS VPN PE-CE Site of Origin (SoO)	414
EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Overview	414
Site of Origin (SoO) Support for Back Door Links	415
Router Interoperation with the Site of Origin (SoO) Extended Community	415
Redistributing BGP VPN Routes that Carry the Site of Origin (SoO) into EIGRP	416
BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies	416
Benefits of the EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Feature	417
How to Configure EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support	417
Configuring the Site of Origin (SoO) Extended Community	417
Prerequisites	417
Examples	420
What to Do Next	420
Verifying the Configuration of the SoO Extended Community	420
Examples	421
Where to Go Next	421
Additional References	422
Related Documents	422
Standards	422
MIBs	422
RFCs	422
Technical Assistance	423
Command Reference	423
Glossary	424
<b>EIGRP Route Map Support</b>	<b>425</b>
Contents	425
How to Configure EIGRP Route Map Support	426
Configuring EIGRP Metrics	426

Verifying EIGRP Metrics	427
Configuration Examples for EIGRP Route Map Support	429
EIGRP Route Metric Configuration: Example	429
Additional References	429
Related Documents	429
Standards	429
MIBs	430
RFCs	430
Technical Assistance	430
Command Reference	430
<b>EIGRP Prefix Limit Support</b>	<b>431</b>
Contents	431
Prerequisites for EIGRP Prefix Limit Support	432
Restrictions for EIGRP Prefix Limit Support	432
Information About EIGRP Prefix Limit Support	432
Misconfigured VPN Peers	432
EIGRP Prefix Limit Support Overview	433
Warning-Only Mode	433
Restart, Reset, and Dampening Timers and Counters	434
Supported Only Under the IPv4 VRF Address Family	434
Configuring the Maximum Number of Prefix Accepted from Peering Sessions	435
Inherited Timer Values	435
Prerequisites	435
Restrictions	435
Troubleshooting Tips	438
Configuring the Maximum Number of Prefixes Learned Through Redistribution	438
Inherited Timer Values	438
Prerequisites	438
Restrictions	438
Troubleshooting Tips	440
Configuring the Maximum Prefix Limit for an EIGRP Process	440
Inherited Timer Values	440
Prerequisites	441
Restrictions	441
Troubleshooting Tips	443
Verifying the EIGRP Maximum Prefix Limit Configuration	443
Example	444
Configuration Examples for Configuring the Maximum Prefix Limit	444

Configuring the Maximum Prefix Limit for a Single Peer: Example	444
Configuring the Maximum Prefix Limit for All Peers: Example	444
Configuring the Maximum Prefix Limit for Redistributed Routes: Example	445
Configuring the Maximum Prefix Limit for an EIGRP Process: Example	445
Additional References	445
Related Documents	445
Standards	446
MIBs	446
RFCs	446
Technical Assistance	446
Command Reference	447
<b>EIGRP SNMP Support</b>	<b>449</b>
Contents	449
Prerequisites for EIGRP SNMP Support	449
Restrictions for EIGRP SNMP Support	450
Information About EIGRP SNMP Support	450
EIGRP SNMP Support Overview	450
EIGRP VPN Table	450
EIGRP Traffic Statistics Table	451
EIGRP Topology Table	452
EIGRP Neighbor Table	453
EIGRP Interface Table	454
EIGRP Notifications	455
How to Enable EIGRP SNMP Support	455
Configuration Examples for Enabling EIGRP SNMP Support	456
EIGRP SNMP Support Configuration: Example	457
EIGRP SNMP Support Verification: Example	457
Additional References	457
Related Documents	457
Standards	457
MIBs	458
RFCs	458
Technical Assistance	458
Command Reference	458

## PART 3: INTEGRATED IS-IS

### Configuring Integrated IS-IS 461

#### IS-IS Configuration Task List 461

Enabling IS-IS and Assigning Areas 461

Enabling IP Routing for an Area on an Interface 463

#### IS-IS Interface Parameters Configuration Task List 463

Configuring IS-IS Link-State Metrics 464

Setting the Advertised Hello Interval 464

Setting the Advertised CSNP Interval 464

Setting the Retransmission Interval 465

Setting the LSP Transmissions Interval 465

Setting the Retransmission Throttle Interval 465

Setting the Hello Multiplier 466

Specifying Designated Router Election 466

Specifying the Interface Circuit Type 466

Assigning a Password for an Interface 466

Limiting LSP Flooding 467

Blocking Flooding on Specific Interfaces 467

Configuring Mesh Groups 467

#### Miscellaneous IS-IS Parameters Configuration Task List 468

Generating a Default Route 468

Specifying the System Type 468

Configuring IS-IS Authentication Passwords 469

Summarizing Address Ranges 469

Setting the Overload Bit 469

Changing the Routing Level for an Area 470

Tuning LSP Interval and Lifetime 470

Customizing IS-IS Throttling of LSP Generation, SPF Calculation, and PRC 471

Partial Route Computation (PRC) 471

Benefits of Throttling IS-IS LSP Generation, SPF Calculation, and PRC 471

How Throttling of IS-IS LSP Generation, SPF Calculation, and PRC Works 471

Modifying the Output of show Commands 472

#### Monitoring IS-IS 473

#### IS-IS Configuration Examples 473

Enabling IS-IS Configuration Example 473

Multiarea IS-IS Configuration for CLNS Network Example 474

IS-IS Throttle Timers Example 475

## **Integrated IS-IS Point-to-Point Adjacency over Broadcast Media 477**

Feature Overview	477
Benefits	477
Restrictions	478
Related Features and Technologies	478
Related Documents	478
Supported Platforms	478
Supported Standards, MIBs, and RFCs	479
Prerequisites	479
Configuration Tasks	479
Configuring Point-to-Point Adjacency over Broadcast Media	480
Configuration Example	480
Command Reference	480

## **IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication 481**

Contents	482
Prerequisites for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	482
Information About IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	482
IS-IS HMAC-MD5 Authentication	483
Benefits of IS-IS HMAC-MD5 Authentication	483
Benefits of IS-IS Clear Text Authentication	483
How to Configure IS-IS HMAC-MD5 Authentication or Enhanced Clear Text Authentication	483
Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time	484
Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance	484
Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface	486
Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication	488
Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for the IS-IS Instance	488
Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for an IS-IS Interface	490
Migrating from Old Clear Text Authentication to the New Clear Text Authentication	492
Migrating from Old Clear Text Authentication to the New Clear Text Authentication for the IS-IS Instance	492
Migrating from Old Clear Text Authentication to the New Clear Text Authentication for an IS-IS Interface	494
Configuration Examples for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication	496
Configuring IS-IS HMAC-MD5 Authentication Example	496
Configuring IS-IS Clear Text Authentication Example	497
Additional References	497

Related Documents	497
MIBs	498
RFCs	498
Technical Assistance	498
Command Reference	499
<b>Integrated IS-IS Nonstop Forwarding (NSF) Awareness</b>	<b>501</b>
Contents	501
Information About IS-IS NSF Awareness	501
Benefits of IS-IS NSF Awareness	502
Additional References	502
Related Documents	502
Standards	502
MIBs	503
RFCs	503
Technical Assistance	503
Command Reference	503
<b>IS-IS Incremental SPF</b>	<b>505</b>
Contents	505
Prerequisites for IS-IS Incremental SPF	505
Information About IS-IS Incremental SPF	506
Benefits of IS-IS Incremental SPF	506
How to Enable IS-IS Incremental SPF	506
Enabling Incremental SPF	506
Configuration Examples for IS-IS Incremental SPF	507
Incremental SPF: Example	507
Additional References	508
Related Documents	508
Standards	508
MIBs	508
RFCs	508
Technical Assistance	509
Command Reference	509
<b>IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements</b>	<b>511</b>
Contents	511
Prerequisites for IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements	512
Information About IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements	512

Convergence	512
Two Alternative Methods to Reduce IS-IS Convergence Time	512
Small-Scale Method to Reduce IS-IS Convergence Time	513
Large-Scale Method to Reduce IS-IS Convergence Time	513
Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements	513
How to Exclude Connected IP Prefixes from IS-IS LSP Advertisements	513
Excluding Connected IP Prefixes on a Small Scale	513
Excluding Connected IP Prefixes on a Large Scale	515
Configuration Examples of IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements	517
Excluding Connected IP Prefixes on a Small Scale: Example	518
Excluding Connected IP Prefixes on a Large Scale: Example	518
Where to Go Next	518
Additional References	519
Related Documents	519
Standards	519
MIBs	519
RFCs	519
Technical Assistance	520
Command Reference	520
<b>IS-IS Support for Route Tags</b>	<b>521</b>
Contents	521
Prerequisites to Using IS-IS Route Tags	521
Information About IS-IS Route Tags	522
Benefits of IS-IS Route Tags	522
IS-IS Route Tag Characteristics	522
IS-IS Route Leaking Based on a Route Tag	523
How to Use IS-IS Route Tags	523
Tagging IS-IS Routes	523
Prerequisites	523
Tagging Routes for Networks Directly Connected to an Interface	523
Tagging Routes Using a Route Map	525
Tagging a Summary Address	528
Using the Tag to Set Values and/or Redistribute Routes	529
Prerequisites	529
Configuration Examples for IS-IS Support for Route Tags	532
Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them: Example	532



Redistributing IS-IS Routes Using a Route-Map: Example	533
Tagging a Summary Address and Applying a Route Map: Example	533
Filtering and Redistributing IS-IS Routes Using an Access List and a Route Map: Example	534
Additional References	535
Related Documents	535
MIBs	536
Technical Assistance	536
Command Reference	536
Integrated IS-IS Global Default Metric	537
Contents	537
Prerequisites for Integrated IS-IS Global Default Metric	537
Restrictions for Integrated IS-IS Global Default Metric	538
Information About Integrated IS-IS Global Default Metric	538
Benefits of Using the Integrated IS-IS Global Default Metric Feature	538
How to Configure the Integrated IS-IS Global Default Metric Feature	538
Changing the Global IS-IS IPv4 Default Metric for IPv4 Networks	538
Changing the Global IS-IS IPv6 Default Metric for IPv6 Networks	540
Configuration Examples for the Integrated IS-IS Global Default Metric Feature	541
Setting a Global Default Metric for IPv4: Example	542
Setting a Global Default Metric for IPv6: Example	544
Additional References	545
Related Documents	545
Standards	546
MIBs	546
RFCs	546
Technical Assistance	546
Command Reference	546
<b>Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters</b>	<b>547</b>
Contents	547
Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	548
Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	548
Benefits of Using the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature	548
How to Configure Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters	549
Shutting Down the IS-IS Protocol in Interface Mode	549

Shutting Down the IS-IS Protocol and Maintaining IS-IS Configuration Parameters in Router Mode 550

Configuration Examples for the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature 551

Shutting Down the IS-IS Protocol in Interface Mode: Example 551

Shutting Down the IS-IS Protocol in Router Mode: Example 552

Additional References 552

Related Documents 553

Standards 553

MIBs 553

RFCs 553

Technical Assistance 553

Command Reference 554

## **IS-IS Caching of Redistributed Routes 555**

Contents 555

Information About IS-IS Caching of Redistributed Routes 556

Benefits of Caching of Redistributed Routes 556

How to Use the IS-IS Caching of Redistributed Routes Feature 556

Monitoring the IS-IS Caching of Redistributed Routes Feature 556

Additional References 557

Related Documents 557

Standards 557

MIBs 557

RFCs 557

Technical Assistance 558

Command Reference 558

## **IS-IS Fast-Flooding of LSPs Using the fast-flood Command 559**

Contents 559

Information About IS-IS Fast-Flooding of LSPs Using the fast-flood Command 560

Benefits of Fast-Flooding 560

How to Use the IS-IS Fast-Flooding of LSPs Using the fast-flood Command Feature 560

Enabling Fast-Flooding 560

Additional References 561

Related Documents 561

Standards 562

MIBs 562

RFCs 562

Technical Assistance 562

Command Reference 562

---

## PART 4: ODR

### Configuring On-Demand Routing 565

- On-Demand Routing Configuration Task List 566
  - Enabling ODR 566
  - Filtering ODR Information 567
  - Redistributing ODR Information into the Dynamic Routing Protocol of the Hub 567
  - Reconfiguring CDP or ODR Timers 567
  - Using ODR with Dialer Mappings 568
- 

## PART 5: OSPF

### Configuring OSPF 571

- The Cisco OSPF Implementation 571
- OSPF Configuration Task List 572
- Enabling OSPF 573
- Configuring OSPF Interface Parameters 573
- Configuring OSPF over Different Physical Networks 574
  - Configuring Your OSPF Network Type 574
  - Configuring Point-to-Multipoint, Broadcast Networks 575
  - Configuring OSPF for Nonbroadcast Networks 575
- Configuring OSPF Area Parameters 576
- Configuring OSPF NSSA 577
  - Implementation Considerations 578
- Configuring Route Summarization Between OSPF Areas 578
- Configuring Route Summarization When Redistributing Routes into OSPF 578
- Creating Virtual Links 579
- Generating a Default Route 579
- Configuring Lookup of DNS Names 580
- Forcing the Router ID Choice with a Loopback Interface 580
- Controlling Default Metrics 580
- Changing the OSPF Administrative Distances 581
- Configuring OSPF on Simplex Ethernet Interfaces 581
- Configuring Route Calculation Timers 581
- Configuring OSPF over On-Demand Circuits 582
  - Implementation Considerations 583

Logging Neighbors Going Up or Down	583
Changing the LSA Group Pacing	583
Original LSA Behavior	584
LSA Group Pacing With Multiple Timers	584
Blocking OSPF LSA Flooding	585
Reducing LSA Flooding	586
Ignoring MOSPF LSA Packets	586
Displaying OSPF Update Packet Pacing	587
Monitoring and Maintaining OSPF	587
OSPF Configuration Examples	589
OSPF Point-to-Multipoint Example	589
OSPF Point-to-Multipoint, Broadcast Example	591
OSPF Point-to-Multipoint, Nonbroadcast Example	592
Variable-Length Subnet Masks Example	592
OSPF Routing and Route Redistribution Examples	593
Basic OSPF Configuration Examples	593
Basic OSPF Configuration Example for Internal Router, ABR, and ASBRs	593
Complex Internal Router, ABR, and ASBRs Example	594
Complex OSPF Configuration for ABR Examples	597
Route Map Examples	598
Changing OSPF Administrative Distance Example	601
OSPF over On-Demand Routing Example	601
LSA Group Pacing Example	603
Block LSA Flooding Example	603
Ignore MOSPF LSA Packets Example	603
<b>OSPF ABR Type 3 LSA Filtering</b>	<b>605</b>
Feature Overview	605
Benefits	606
Restrictions	606
Related Features and Technologies	606
Supported Platforms	606
Supported Standards, MIBs, and RFCs	607
Configuration Tasks	607
Configuring OSPF ABR Type 3 LSA Filtering	608
Verifying OSPF ABR Type 3 LSA Filtering	608
Monitoring and Maintaining OSPF ABR Type 3 LSA Filtering	609
Configuration Examples	609

Command Reference	609
<b>OSPF Stub Router Advertisement</b>	<b>611</b>
Feature Overview	612
Allowing Routing Tables to Converge	612
Configuring a Graceful Shutdown	612
Benefits	613
Related Features and Technologies	613
Supported Platforms	613
Supported Standards, MIBs, and RFCs	614
Configuration Tasks	615
Configuring Advertisement on Startup	615
Configuring Advertisement Until Routing Tables Converge	615
Configuring Advertisement for a Graceful Shutdown	616
Verifying the Advertisement of a Maximum Metric	616
Monitoring and Maintaining OSPF Stub Router Advertisement	618
Configuration Examples	619
Advertisement on Startup Example	619
Advertisement Until Routing Tables Converge Example	619
Graceful Shutdown Example	619
Command Reference	619
<b>OSPF Update Packet-Pacing Configurable Timers</b>	<b>621</b>
Feature Overview	621
Benefits	622
Restrictions	622
Related Features and Technologies	622
Supported Platforms	622
Supported Standards, MIBs, and RFCs	623
Configuration Tasks	624
Configuring OSPF Packet-Pacing Timers	624
Verifying OSPF Packet-Pacing Timers	625
Troubleshooting Tips	625
Monitoring and Maintaining OSPF Packet-Pacing Timers	626
Configuration Examples	626
Flood Pacing Example	626
Retransmission Pacing Example	626
Group Pacing Example	626
Command Reference	627

**OSPF Sham-Link Support for MPLS VPN 629**

- Feature Overview 629
  - Using OSPF in PE-CE Router Connections 629
  - Using a Sham-Link to Correct OSPF Backdoor Routing 630
  - Sham-Link Configuration Example 633
  - Benefits 635
  - Restrictions 636
  - Related Features and Technologies 636
  - Related Documents 636
- Supported Platforms 636
- Supported Standards, MIBs, and RFCs 638
- Prerequisites 638
- Configuration Tasks 638
  - Creating a Sham-Link 638
  - Verifying Sham-Link Creation 639
- Monitoring and Maintaining a Sham-Link 640
- Configuration Examples 640
- Command Reference 640
- Glossary 641

**OSPF Retransmissions Limit 643**

- Feature Overview 643
  - Benefits 643
  - Restrictions 644
  - Related Features and Technologies 644
- Supported Platforms 644
- Configuration Tasks 645
  - Setting OSPF Retransmission Limits 646
- Command Reference 646

**OSPF Support for Multi-VRF on CE Routers 647**

- Contents 648
- Information About OSPF Support for Multi-VRF on CE Routers 648
  - Benefits of OSPF Multi-VRF Support 648
- How to Configure OSPF Support for Multi-VRF on CE Routers 649
  - Configuring the Multi-VRF Capability for OSPF Routing 649
  - Verifying the OSPF Multi-VRF Configuration 650
- Configuration Examples for OSPF Support for Multi-VRF on CE Routers 650
  - Configuring the Multi-VRF Capability Example 650

Verifying the OSPF Multi-VRF Configuration Example	651
Additional References	651
Related Documents	651
Standards	651
MIBs	652
RFCs	652
Technical Assistance	652
Command Reference	653
Glossary	654
<b>OSPF Nonstop Forwarding (NSF) Awareness</b>	<b>655</b>
Contents	655
Information About OSPF NSF Awareness	655
Benefits of OSPF NSF Awareness	656
How to Control OSPF NSF Awareness	656
Setting the OSPF Resynchronization Timeout Timer	656
Prerequisites	656
Disabling OSPF NSF Awareness	657
Configuration Examples for OSPF NSF Awareness	658
Setting OSPF Resynchronization Timeout Example	658
Displaying OSPF Neighbor NSF Information	659
Additional References	659
Related Documents	659
Standards	660
MIBs	660
RFCs	660
Technical Assistance	661
Command Reference	661
<b>OSPF Forwarding Address Suppression in Translated Type-5 LSAs</b>	<b>663</b>
Contents	663
Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs	664
Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs	664
Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs	664
When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs	664
How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs	665
Suppressing OSPF Forwarding Address in Translated Type-5 LSAs	665
Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs	667
Suppressing OSPF Forwarding Address in Translated Type-5 LSAs Example	667

Additional References	667
Related Documents	667
Standards	667
MIBs	668
RFCs	668
Technical Assistance	668
Command Reference	669

## **OSPF Inbound Filtering Using Route Maps with a Distribute List 671**

Contents	671
Prerequisites	672
Information About OSPF Inbound Filtering Using Route Maps with a Distribute List	672
Benefits of OSPF Route Map-Based Filtering	672
How to Configure OSPF Inbound Filtering Using Route Maps	673
Configuring OSPF Route Map-Based Filtering	673
Configuration Examples for OSPF Inbound Filtering Using Route Maps with a Distribute List	674
OSPF Route Map-Based Filtering Example	675
Additional References	675
Related Documents	675
Standards	675
MIBs	676
RFCs	676
Technical Assistance	676
Command Reference	676

## **OSPF Shortest Path First Throttling 677**

Contents	677
Information About OSPF SPF Throttling	678
Shortest Path First Calculations	678
How to Configure OSPF SPF Throttling	679
Configuring OSPF SPF Throttling	679
Verifying SPF Throttle Values	680
Configuration Examples for OSPF SPF Throttling	681
Throttle Timers Example	681
Additional References	682
Related Documents	682
Standards	682
MIBs	682
RFCs	683



Technical Assistance	683
Command Reference	683
<b>OSPF Support for Fast Hello Packets</b>	<b>685</b>
Contents	685
Prerequisites for OSPF Support for Fast Hello Packets	686
Information About OSPF Support for Fast Hello Packets	686
OSPF Hello Interval and Dead Interval	686
OSPF Fast Hello Packets	686
Benefits of OSPF Fast Hello Packets	687
How to Configure OSPF Fast Hello Packets	687
Configure OSPF Fast Hello Packets	687
Configuration Examples for OSPF Support of Fast Hello Packets	688
OSPF Fast Hello Packets Example	689
Additional References	689
Related Documents	689
Standards	689
MIBs	689
RFCs	690
Technical Assistance	690
Command Reference	690
<b>OSPF Incremental SPF</b>	<b>691</b>
Contents	691
Prerequisites for OSPF Incremental SPF	691
Information About OSPF Incremental SPF	692
Benefits of OSPF Incremental SPF	692
How to Enable OSPF Incremental SPF	692
Enabling Incremental SPF	692
Configuration Examples for OSPF Incremental SPF	693
Incremental SPF: Example	693
Additional References	694
Related Documents	694
Standards	694
MIBs	694
RFCs	694
Technical Assistance	695
Command Reference	695

**OSPF Limit on Number of Redistributed Routes 697**

Contents 697

Prerequisites for OSPF Limit on Number of Redistributed Routes 697

Information About OSPF Limit on Number of Redistributed Routes 698

Benefits of OSPF Limit on Number of Redistributed Routes 698

How to Limit OSPF Redistributed Routes or Receive Warning About Number of OSPF Redistributed Routes 698

Limiting the Number of OSPF Redistributed Routes 698

Requesting a Warning About the Number of Routes Redistributed into OSPF 700

Configuration Examples for OSPF Limit on Number of Redistributed Routes 701

OSPF Limit on Number of Redistributed Routes: Example 701

Requesting a Warning About the Number of Redistributed Routes: Example 702

Additional References 702

Related Documents 702

Standards 702

MIBs 702

RFCs 703

Technical Assistance 703

Command Reference 703

**OSPF Link-State Advertisement (LSA) Throttling 705**

Contents 705

Prerequisites for OSPF LSA Throttling 705

Information About OSPF LSA Throttling 706

Benefits of OSPF LSA Throttling 706

How OSPF LSA Throttling Works 706

How to Customize OSPF LSA Throttling 706

Customizing OSPF LSA Throttling 706

Configuration Examples for OSPF LSA Throttling 709

OSPF LSA Throttling: Example 709

Additional References 709

Related Documents 709

Standards 709

MIBs 709

RFCs 710

Technical Assistance 710

Command Reference 710

## **OSPF Support for Unlimited Software VRFs per Provider Edge Router 711**

Contents 711

Prerequisites for OSPF Support for Unlimited Software VRFs per Provider Edge Router 712

Restrictions for OSPF Support for Unlimited Software VRFs per Provider Edge Router 712

Information About OSPF Support for Unlimited Software VRFs per Provider Edge Router 712

Benefits of Having Unlimited Software VRFs per PE Router 712

How to Configure the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature 713

Configuring and Verifying Unlimited Software VRFs per Provider Edge Router 713

Configuration Examples for the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature 714

Configuring the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature:  
Example 714

Verifying the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature:  
Example 714

Additional References 715

Related Documents 715

Standards 715

MIBs 716

RFCs 716

Technical Assistance 716

Command Reference 716

Glossary 717

## **OSPF Area Transit Capability 719**

Contents 719

Information About OSPF Area Transit Capability 720

How the OSPF Area Transit Capability Feature Works 720

How to Disable OSPF Area Transit Capability 720

Disabling OSPF Area Transit Capability on an Area Border Router 720

Additional References 721

Related Documents 721

Standards 721

MIBs 722

RFCs 722

Technical Assistance 722

Command Reference 722

## **OSPF Link-Local Signaling Per-Interface Basis 723**

Contents 723

Information About OSPF per-Interface Link-Local Signaling	724
Benefits of the OSPF Per-Interface Link-Local Signaling Feature	724
How to Configure the OSPF per-Interface Link-Local Signaling Feature	724
Turning Off LLS on a per-Interface Basis	724
What to Do Next	725
Configuration Examples for the OSPF per-Interface Link-Local Signaling Feature	726
Configuring and Verifying the OSPF per-Interface Link-Local Signaling Feature: Example	726
Additional References	727
Related Documents	727
Standards	727
MIBs	728
RFCs	728
Technical Assistance	728
Command Reference	728
<b>OSPF Link-State Database Overload Protection</b>	<b>729</b>
Contents	729
Prerequisites for OSPF Link-State Database Overload Protection	730
Information About OSPF Link-State Database Overload Protection	730
Benefits of Using OSPF Link-State Database Overload Protection	730
How OSPF Link-State Database Overload Protection Works	730
How to Configure the OSPF Link-State Database Overload Protection Feature	730
Limiting the Number of Self-Generating LSAs for an OSPF Process	731
Verifying the Number of Nonself-Generated LSAs on a Router	732
Configuration Examples for the OSPF Link-State Database Overload Protection Feature	733
Setting a Limit for LSA Generation: Example	733
Additional References	734
Related Documents	734
Standards	734
MIBs	734
RFCs	735
Technical Assistance	735
Command Reference	735
Glossary	736

---

## PART 6: PROTOCOL-INDEPENDENT ROUTING

<b>Configuring IP Routing Protocol-Independent Features</b>	<b>739</b>
Protocol-Independent Feature Task List	739

Using Variable-Length Subnet Masks	740
Configuring Static Routes	740
Specifying Default Routes	741
Specifying a Default Network	741
Understanding Gateway of Last Resort	742
Changing the Maximum Number of Paths	742
Configuring Multi-Interface Load Splitting	743
Redistributing Routing Information	743
Understanding Supported Metric Translations	745
Filtering Routing Information	746
Preventing Routing Updates Through an Interface	746
Configuring Default Passive Interfaces	747
Controlling the Advertising of Routes in Routing Updates	748
Controlling the Processing of Routing Updates	748
Filtering Sources of Routing Information	748
Enabling Policy Routing	749
Enabling Fast-Switched Policy Routing	751
Enabling Local Policy Routing	752
Enabling NetFlow Policy Routing	752
Managing Authentication Keys	754
Monitoring and Maintaining the IP Network	755
Clearing Routes from the IP Routing Table	755
Displaying System and Network Statistics	755
IP Routing Protocol-Independent Configuration Examples	756
Variable-Length Subnet Mask Example	756
Overriding Static Routes with Dynamic Protocols Example	757
Administrative Distance Examples	757
Static Routing Redistribution Example	758
EIGRP Redistribution Examples	758
RIP and EIGRP Redistribution Examples	759
Simple Redistribution Example	759
Complex Redistribution Example	759
OSPF Routing and Route Redistribution Examples	760
Basic OSPF Configuration Examples	760
Internal Router, ABR, and ASBRs Configuration Example	762
Complex OSPF Configuration Example	764
Default Metric Values Redistribution Example	766
Route Map Examples	766
Passive Interface Examples	768

Default Passive Interface Example	768
Policy Routing Example	769
Policy Routing with CEF Example	769
Key Management Examples	770
<b>IP Event Dampening</b>	<b>773</b>
Contents	773
Restrictions for IP Event Dampening	774
Information About IP Event Dampening	774
IP Event Dampening Overview	774
Interface State Change Events	775
Suppress Threshold	775
Half-Life Period	775
Reuse Threshold	775
Maximum Suppress Time	775
Affected Components	776
Route Types	776
Supported Protocols	777
Network Deployments	777
Benefits of IP Event Dampening	778
How to Configure IP Event Dampening	778
Enabling IP Event Dampening	778
Verifying IP Event Dampening	779
Configuration Examples for IP Event Dampening	780
Configuring IP Event Dampening: Example	780
Verifying IP Event Dampening: Example	781
Additional References	781
Related Documents	781
Standards	781
MIBs	782
RFCs	782
Technical Assistance	782
Command Reference	782
Glossary	783
<b>PBR Support for Multiple Tracking Options</b>	<b>785</b>
Contents	785
Information About PBR Support for Multiple Tracking Options	786
Object Tracking	786

PBR Support for Multiple Tracking Options Feature Design	786
How to Configure PBR Support for Multiple Tracking Options	786
Configuring PBR Support for Multiple Tracking Options	786
Configuration Examples for PBR Support for Multiple Tracking Options	789
PBR Support for Multiple Tracking Options: Example	789
Additional References	790
Related Documents	790
Standards	790
MIBs	790
RFCs	791
Technical Assistance	791
Command Reference	791
<b>PBR Recursive Next Hop</b>	<b>793</b>
Contents	793
How to Configure PBR Recursive Next Hop	794
Setting the Recursive Next-Hop IP Address	794
Prerequisites	794
Restrictions	794
Verifying the Recursive Next-Hop Configuration	796
Configuration Examples for PBR Recursive Next Hop	796
Recursive Next-Hop IP Address: Example	796
Additional References	797
Related Documents	797
MIBs	797
Technical Assistance	797
Command Reference	797

---

## **PART 7: RIP**

<b>Configuring Routing Information Protocol</b>	<b>801</b>
RIP Configuration Task List	802
Enabling RIP	802
Allowing Unicast Updates for RIP	803
Applying Offsets to Routing Metrics	803
Adjusting Timers	803
Specifying a RIP Version	804
Enabling RIP Authentication	805
RIP Route Summarization	805

Restrictions to RIP Route Summarization	807
Configuring Route Summarization on an Interface	807
Verifying IP Route Summarization	807
Disabling Automatic Route Summarization	808
Disabling the Validation of Source IP Addresses	808
Enabling or Disabling Split Horizon	809
Configuring Interpacket Delay	810
Connecting RIP to a WAN	810
RIP Configuration Examples	811
Route Summarization Examples	811
Example 1: Correct Configuration	811
Example 2: Incorrect Configuration	812
Split Horizon Examples	812
Example 1	812
Example 2	812
Address Family Timers Example	814





# About Cisco IOS Software Documentation for Release 12.4

---

This chapter describes the objectives, audience, organization, and conventions of Cisco IOS software documentation. It also provides sources for obtaining documentation, technical assistance, and additional publications and information from Cisco Systems. It contains the following sections:

- [Documentation Objectives, page xlv](#)
- [Audience, page xlv](#)
- [Documentation Organization for Cisco IOS Release 12.4, page xlvi](#)
- [Document Conventions, page lii](#)
- [Obtaining Documentation, page liii](#)
- [Documentation Feedback, page liv](#)
- [Cisco Product Security Overview, page lv](#)
- [Obtaining Technical Assistance, page lvi](#)
- [Obtaining Additional Publications and Information, page lvii](#)

## Documentation Objectives

Cisco IOS software documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

## Audience

The Cisco IOS software documentation set is intended primarily for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS software commands necessary to perform particular tasks. The Cisco IOS software documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS software release.

# Documentation Organization for Cisco IOS Release 12.4

The Cisco IOS Release 12.4 documentation set consists of the configuration guide and command reference pairs listed in [Table 1](#) and the supporting documents listed in [Table 2](#). The configuration guides and command references are organized by technology. For the configuration guides:

- Some technology documentation, such as that for DHCP, contains features introduced in Releases 12.2T and 12.3T and, in some cases, Release 12.2S. To assist you in finding a particular feature, a roadmap document is provided.
- Other technology documentation, such as that for OSPF, consists of a chapter and accompanying Release 12.2T and 12.3T feature documents.



## Note

In some cases, information contained in Release 12.2T and 12.3T feature documents augments or supersedes content in the accompanying documentation. Therefore it is important to review all feature documents for a particular technology.

[Table 1](#) lists the Cisco IOS Release 12.4 configuration guides and command references.

**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
<b>IP</b>	
<a href="#">Cisco IOS IP Addressing Services Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Addressing Services Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS IP Application Services Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Application Services Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS IP Mobility Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Mobility Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS IP Multicast Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Multicast Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide.

**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
<a href="#">Cisco IOS IP Switching Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP Switching Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS IPv6 Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IPv6 Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Optimized Edge Routing Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Optimized Edge Routing Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide.
<b>Security and VPN</b>	
<a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Security Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide.
<b>QoS</b>	
<a href="#">Cisco IOS Quality of Service Solutions Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide.
<b>LAN Switching</b>	
<a href="#">Cisco IOS LAN Switching Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS LAN Switching Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide.
<b>Multiprotocol Label Switching (MPLS)</b>	
<a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide.
<b>Network Management</b>	
<a href="#">Cisco IOS IP SLAs Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS IP SLAs Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide.

**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
<a href="#">Cisco IOS NetFlow Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS NetFlow Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Network Management Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Network Management Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol, configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide.
<b>Voice</b>	
<a href="#">Cisco IOS Voice Configuration Library</a> , Release 12.4 <a href="#">Cisco IOS Voice Command Reference</a> , Release 12.4	The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library.
<b>Wireless/Mobility</b>	
<a href="#">Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Mobile Wireless Home Agent Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Mobile Wireless Home Agent Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide.

**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
<a href="#">Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Mobile Wireless Radio Access Networking Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide.
<b>Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)</b>	
<a href="#">Cisco IOS Broadband and DSL Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Broadband and DSL Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Service Selection Gateway Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Service Selection Gateway Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide.
<b>Dial—Access</b>	
<a href="#">Cisco IOS Dial Technologies Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Dial Technologies Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS VPDN Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS VPDN Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Virtual Private Dialup Networks (VPDNs), including information about Layer 2 tunneling protocols, client-initiated VPDN tunneling, NAS-initiated VPDN tunneling, and multihop VPDN. The command reference provides detailed information about the commands used in the configuration guide.
<b>Asynchronous Transfer Mode (ATM)</b>	
<a href="#">Cisco IOS Asynchronous Transfer Mode Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Asynchronous Transfer Mode Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide.
<b>WAN</b>	
<a href="#">Cisco IOS Wide-Area Networking Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Wide-Area Networking Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide.

**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
<b>System Management</b>	
<a href="#">Cisco IOS Configuration Fundamentals Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Configuration Fundamentals Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Interface and Hardware Component Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Interface and Hardware Component Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide.
<b>IBM Technologies</b>	
<a href="#">Cisco IOS Bridging and IBM Networking Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Bridging Command Reference</a> , Release 12.4 <a href="#">Cisco IOS IBM Networking Command Reference</a> , Release 12.4	<p>The configuration guide is a task-oriented guide to configuring:</p> <ul style="list-style-type: none"> <li>• Bridging features, including transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM).</li> <li>• IBM network features, including data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA Frame Relay Access, Advanced Peer-to-Peer Networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</li> </ul> <p>The two command references provide detailed information about the commands used in the configuration guide.</p>
<b>Additional and Legacy Protocols</b>	
<a href="#">Cisco IOS AppleTalk Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS AppleTalk Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS DECnet Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS DECnet Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS ISO CLNS Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS ISO CLNS Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide.



**Table 1** Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
<a href="#">Cisco IOS Novell IPX Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Novell IPX Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide.
<a href="#">Cisco IOS Terminal Services Configuration Guide</a> , Release 12.4 <a href="#">Cisco IOS Terminal Services Command Reference</a> , Release 12.4	The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide.

Table 2 lists the documents and resources that support the Cisco IOS Release 12.4 software configuration guides and command references.

**Table 2** Cisco IOS Release 12.4 Supporting Documents and Resources

Document Title	Description
<a href="#">Cisco IOS Master Commands List</a> , Release 12.4	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4 command references.
<a href="#">Cisco IOS New, Modified, Replaced, and Removed Commands</a> , Release 12.4	A listing of all the new, modified, replaced and removed commands since Cisco IOS Release 12.3, grouped by Release 12.3T maintenance release and ordered alphabetically within each group.
<a href="#">Cisco IOS New and Modified Commands</a> , Release 12.3	A listing of all the new, modified, and replaced commands since Cisco IOS Release 12.2, grouped by Release 12.2T maintenance release and ordered alphabetically within each group.
<a href="#">Cisco IOS System Messages, Volume 1 of 2</a> <a href="#">Cisco IOS System Messages, Volume 2 of 2</a>	Listings and descriptions of Cisco IOS system messages. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software.
<a href="#">Cisco IOS Debug Command Reference</a> , Release 12.4	An alphabetical listing of the <b>debug</b> commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines.
<a href="#">Release Notes</a> , Release 12.4	A description of general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.
<a href="#">Internetworking Terms and Acronyms</a>	Compilation and definitions of the terms and acronyms used in the internetworking industry.

**Table 2** Cisco IOS Release 12.4 Supporting Documents and Resources (continued)

Document Title	Description
RFCs	RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>
MIBs	MIBs are used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## Document Conventions

Within Cisco IOS software documentation, the term *router* is generally used to refer to a variety of Cisco products (for example, routers, access servers, and switches). Routers, access servers, and other networking devices that support Cisco IOS software are shown interchangeably within examples. These products are used only for illustrative purposes; that is, an example that shows one product does not necessarily indicate that other products are not supported.

The Cisco IOS documentation set uses the following conventions:

Convention	Description
^ or Ctrl	The ^ and Ctrl symbols represent the Control key. For example, the key combination ^D or Ctrl-D means hold down the Control key while you press the D key. Keys are indicated in capital letters but are not case sensitive.
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting an SNMP community string to <i>public</i> , do not use quotation marks around the string or the string will include the quotation marks.

Command syntax descriptions use the following conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter literally as shown.
<i>italics</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional element (keyword or argument).
	A vertical line indicates a choice within an optional or required set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a vertical line indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a vertical line indicate a required choice.



Nested sets of square brackets or braces indicate optional or required choices within optional or required elements. For example:

Convention	Description
[x {y   z}]	Braces and a vertical line within square brackets indicate a required choice within an optional element.

Examples use the following conventions:

Convention	Description
screen	Examples of information displayed on the screen are set in Courier font.
<b>bold screen</b>	Examples of text that you must enter are set in Courier bold font.
< >	Angle brackets enclose text that is not printed to the screen, such as passwords, and are used in contexts in which the italic document convention is not available, such as ASCII text.
!	An exclamation point at the beginning of a line indicates a comment line. (Exclamation points are also displayed by the Cisco IOS software for certain processes.)
[ ]	Square brackets enclose default responses to system prompts.

The following conventions are used to attract the attention of the reader:



#### Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



#### Note

Means *reader take note*. Notes contain suggestions or references to material not covered in the manual.



#### Timesaver

Means the *described action saves time*. You can save time by performing the action described in the paragraph.

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation and technical support at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at [tech-doc-store-mkpl@external.cisco.com](mailto:tech-doc-store-mkpl@external.cisco.com) or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

The link on this page has the current PGP key ID in use.

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://cisoiq.texterity.com/cisoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>



## Using Cisco IOS Software for Release 12.4

---

This chapter provides tips for understanding and configuring Cisco IOS software using the command-line interface (CLI). It contains the following sections:

- [Understanding Command Modes, page lix](#)
- [Getting Help, page lx](#)
- [Using the no and default Forms of Commands, page lxiv](#)
- [Saving Configuration Changes, page lxiv](#)
- [Filtering Output from the show and more Commands, page lxv](#)
- [Finding Additional Feature Support Information, page lxv](#)

For an overview of Cisco IOS software configuration, see the [Cisco IOS Configuration Fundamentals Configuration Guide](#).

For information on the conventions used in the Cisco IOS software documentation set, see the “[About Cisco IOS Software Documentation for Release 12.4](#)” chapter.

## Understanding Command Modes

You use the CLI to access Cisco IOS software. Because the CLI is divided into many different modes, the commands available to you at any given time depend on the mode that you are currently in. Entering a question mark (?) at the CLI prompt allows you to obtain a list of commands available for each command mode.

When you log in to a Cisco device, the device is initially in user EXEC mode. User EXEC mode contains only a limited subset of commands. To have access to all commands, you must enter privileged EXEC mode by entering the **enable** command and a password (when required). From privileged EXEC mode you have access to both user EXEC and privileged EXEC commands. Most EXEC commands are used independently to observe status or to perform a specific function. For example, **show** commands are used to display important status information, and **clear** commands allow you to reset counters or interfaces. The EXEC commands are not saved when the software reboots.

Configuration modes allow you to make changes to the running configuration. If you later save the running configuration to the startup configuration, these changed commands are stored when the software is rebooted. To enter specific configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and a variety of other modes, such as protocol-specific modes.

ROM monitor mode is a separate mode used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode.

Table 1 describes how to access and exit various common command modes of the Cisco IOS software. It also shows examples of the prompts displayed for each mode.

**Table 1 Accessing and Exiting Command Modes**

Command Mode	Access Method	Prompt	Exit Method
User EXEC	Log in.	Router>	Use the <b>logout</b> command.
Privileged EXEC	From user EXEC mode, use the <b>enable</b> command.	Router#	To return to user EXEC mode, use the <b>disable</b> command.
Global configuration	From privileged EXEC mode, use the <b>configure terminal</b> command.	Router(config)#	To return to privileged EXEC mode from global configuration mode, use the <b>exit</b> or <b>end</b> command.
Interface configuration	From global configuration mode, specify an interface using an <b>interface</b> command.	Router(config-if)#	To return to global configuration mode, use the <b>exit</b> command. To return to privileged EXEC mode, use the <b>end</b> command.
ROM monitor	From privileged EXEC mode, use the <b>reload</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	>	To exit ROM monitor mode, use the <b>continue</b> command.

For more information on command modes, see the “Using the Cisco IOS Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

## Getting Help

Entering a question mark (?) at the CLI prompt displays a list of commands available for each command mode. You can also get a list of keywords and arguments associated with any command by using the context-sensitive help feature.

To get help specific to a command mode, a command, a keyword, or an argument, use one of the following commands:

Command	Purpose
<b>help</b>	Provides a brief description of the help system in any command mode.
<i>abbreviated-command-entry?</i>	Provides a list of commands that begin with a particular character string. (No space between command and question mark.)
<i>abbreviated-command-entry</i> <Tab>	Completes a partial command name.



Command	Purpose
<code>?</code>	Lists all commands available for a particular command mode.
<code>command ?</code>	Lists the keywords or arguments that you must enter next on the command line. (Space between command and question mark.)

## Example: How to Find Command Options

This section provides an example of how to display syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (?) at the configuration prompt or after entering part of a command followed by a space. The Cisco IOS software displays a list and brief description of available keywords and arguments. For example, if you were in global configuration mode and wanted to see all the keywords or arguments for the **arap** command, you would type **arap ?**.

The <cr> symbol in command help output stands for “carriage return.” On older keyboards, the carriage return key is the Return key. On most modern keyboards, the carriage return key is the Enter key. The <cr> symbol at the end of command help output indicates that you have the option to press **Enter** to complete the command and that the arguments and keywords in the list preceding the <cr> symbol are optional. The <cr> symbol by itself indicates that no more arguments or keywords are available and that you must press **Enter** to complete the command.

[Table 2](#) shows examples of how you can use the question mark (?) to assist you in entering commands. The table steps you through configuring an IP address on a serial interface on a Cisco 7206 router that is running Cisco IOS Release 12.0(3).

**Table 2**     *How to Find Command Options*

Command	Comment
Router> <b>enable</b> Password: <password> Router#	Enter the <b>enable</b> command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to Router#.
Router# <b>configure terminal</b> Enter configuration commands, one per line. End with CNTL/Z. Router(config)#	Enter the <b>configure terminal</b> privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to Router(config)#.

**Table 2**     *How to Find Command Options (continued)*

Command	Comment
<pre>Router(config)# <b>interface serial</b> ? &lt;0-6&gt;      Serial interface number Router(config)# <b>interface serial 4</b> ? / Router(config)# <b>interface serial 4/</b> ? &lt;0-3&gt;      Serial interface number Router(config)# <b>interface serial 4/0</b> ? &lt;cr&gt; Router(config)# <b>interface serial 4/0</b> Router(config-if)#</pre>	<p>Enter interface configuration mode by specifying the serial interface that you want to configure using the <b>interface serial</b> global configuration command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter the serial interface slot number and port number, separated by a forward slash.</p> <p>When the &lt;cr&gt; symbol is displayed, you can press <b>Enter</b> to complete the command.</p> <p>You are in interface configuration mode when the prompt changes to Router(config-if)#.</p>
<pre>Router(config-if)# ? Interface configuration commands: . . . ip                Interface Internet Protocol config commands keepalive         Enable keepalive lan-name          LAN Name command llc2              LLC2 Interface Subcommands load-interval     Specify interval for load calculation for an                   interface locaddr-priority  Assign a priority group logging           Configure logging for interface loopback          Configure internal loopback on an interface mac-address       Manually set interface MAC address mls               mls router sub/interface commands mpoa              MPOA interface configuration commands mtu               Set the interface Maximum Transmission Unit (MTU) netbios           Use a defined NETBIOS access list or enable                   name-caching no                Negate a command or set its defaults nrzi-encoding     Enable use of NRZI encoding ntp               Configure NTP . . . Router(config-if)#</pre>	<p>Enter ? to display a list of all the interface configuration commands available for the serial interface. This example shows only some of the available interface configuration commands.</p>

**Table 2**     *How to Find Command Options (continued)*

Command	Comment
<pre>Router(config-if)# ip ? Interface IP configuration subcommands:   access-group      Specify access control for packets   accounting         Enable IP accounting on this interface   address           Set the IP address of an interface   authentication     authentication subcommands   bandwidth-percent Set EIGRP bandwidth limit   broadcast-address  Set the broadcast address of an interface   cgmp              Enable/disable CGMP   directed-broadcast Enable forwarding of directed broadcasts   dvmrp             DVMRP interface commands   hello-interval     Configures IP-EIGRP hello interval   helper-address     Specify a destination address for UDP broadcasts   hold-time          Configures IP-EIGRP hold time   .   .   .</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.</p> <p>Enter ? to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p>
<pre>Router(config-if)# ip Router(config-if)# ip address ?   A.B.C.D           IP address   negotiated         IP Address negotiated over PPP Router(config-if)# ip address</pre>	<p>Enter the command that you want to configure for the interface. This example uses the <b>ip address</b> command.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP address or the <b>negotiated</b> keyword.</p> <p>A carriage return (&lt;cr&gt;) is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>
<pre>Router(config-if)# ip address 172.16.0.1 ?   A.B.C.D           IP subnet mask Router(config-if)# ip address 172.16.0.1</pre>	<p>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>A &lt;cr&gt; is not displayed; therefore, you must enter additional keywords or arguments to complete the command.</p>

**Table 2**    *How to Find Command Options (continued)*

Command	Comment
Router(config-if)# <b>ip address 172.16.0.1 255.255.255.0 ?</b> secondary                      Make this IP address a secondary address <cr>	Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.
Router(config-if)# <b>ip address 172.16.0.1 255.255.255.0</b>	Enter ? to display what you must enter next on the command line. In this example, you can enter the <b>secondary</b> keyword, or you can press <b>Enter</b> .  A <cr> is displayed; you can press <b>Enter</b> to complete the command, or you can enter another keyword.
Router(config-if)# <b>ip address 172.16.0.1 255.255.255.0</b> Router(config-if)#	In this example, Enter is pressed to complete the command.

## Using the no and default Forms of Commands

Almost every configuration command has a **no** form. In general, use the **no** form to disable a function. Use the command without the **no** keyword to reenable a disabled function or to enable a function that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, use the **no ip routing** command; to reenable IP routing, use the **ip routing** command. The Cisco IOS software command reference publications provide the complete syntax for the configuration commands and describe what the **no** form of a command does.

Configuration commands can also have a **default** form, which returns the command settings to the default values. Most commands are disabled by default, so in such cases using the **default** form has the same result as using the **no** form of the command. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** form of the command enables the command and sets the variables to their default values. The Cisco IOS software command reference publications describe the effect of the **default** form of a command if the command functions differently than the **no** form.

## Saving Configuration Changes

Use the **copy system:running-config nvram:startup-config** command or the **copy running-config startup-config** command to save your configuration changes to the startup configuration so that the changes will not be lost if the software reloads or a power outage occurs. For example:

```
Router# copy system:running-config nvram:startup-config
Building configuration...
```

It might take a minute or two to save the configuration. After the configuration has been saved, the following output appears:

```
[OK]
Router#
```

On most platforms, this task saves the configuration to NVRAM. On the Class A flash file system platforms, this task saves the configuration to the location specified by the CONFIG\_FILE environment variable. The CONFIG\_FILE variable defaults to NVRAM.

## Filtering Output from the show and more Commands

You can search and filter the output of **show** and **more** commands. This functionality is useful if you need to sort through large amounts of output or if you want to exclude output that you need not see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (**|**); one of the keywords **begin**, **include**, or **exclude**; and a regular expression on which you want to search or filter (the expression is case-sensitive):

*command | {begin | include | exclude} regular-expression*

The output matches certain lines of information in the configuration file. The following example illustrates how to use output modifiers with the **show interface** command when you want the output to include only lines in which the expression “protocol” appears:

```
Router# show interface | include protocol
```

```
FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

For more information on the search and filter functionality, see the “Using the Cisco IOS Command-Line Interface” chapter in the *Cisco IOS Configuration Fundamentals Configuration Guide*.

## Finding Additional Feature Support Information

If you want to use a specific Cisco IOS software feature, you will need to determine in which Cisco IOS software images that feature is supported. Feature support in Cisco IOS software images depends on three main factors: the software version (called the “Release”), the hardware model (the “Platform” or “Series”), and the “Feature Set” (collection of specific features designed for a certain network environment). Although the Cisco IOS software documentation set documents feature support information for Release 12.4 as a whole, it does not generally provide specific hardware and feature set information.

To determine the correct combination of Release (software version), Platform (hardware version), and Feature Set needed to run a particular feature (or any combination of features), use Feature Navigator.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Software features may also have additional limitations or restrictions. For example, a minimum amount of system memory may be required. Or there may be known issues for features on certain platforms that have not yet been resolved (called “Caveats”). For the latest information about these limitations, see the release notes for the appropriate Cisco IOS software release. Release notes provide detailed installation instructions, new feature descriptions, system requirements, limitations and restrictions, caveats, and troubleshooting information for a particular software release.





## **Part 1: BGP**









# BGP Features Roadmap

This roadmap lists the features documented in the *Cisco BGP Implementation Configuration Guide* and maps them to the modules in which they appear.

## Roadmap History

This roadmap was first published on May 2, 2005, and last updated on May 2, 2005.

## Feature and Release Support

**Table 3** lists BGP feature support for the following Cisco IOS software release trains:

- [Cisco IOS Release 12.0S](#)
- [Cisco IOS Release 12.2S](#)
- [Cisco IOS Releases 12.2T, 12.3, and 12.3T](#)

Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or a later release appear in the table. *Not all features may be supported in your Cisco IOS software release.*

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

**Table 3** lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3**     **Supported BGP Features**

Release	Feature Name	Feature Description	Where Documented
<b>Cisco IOS Release 12.0S</b>			
12.0(24)S	BGP Configuration Using Peer Templates	The BGP Configuration Using Peer Templates feature introduces a new mechanism that groups distinct neighbor configurations for Border Gateway Protocol (BGP) neighbors that share policies. Configuration templates provide an alternative to peer group configuration and overcome some of the limitations of peer groups.	<a href="#">Configuring a Basic BGP Network</a>

**Table 3**    **Supported BGP Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.0(24)S	BGP Dynamic Update Peer Groups	The BGP Dynamic Update Peer Groups feature introduces a new algorithm that dynamically calculates and optimizes update groups of neighbors that share the same outbound policies and can share the same update messages. In previous versions of Cisco IOS software, BGP update messages were grouped based on peer group configurations. This method of grouping updates limited outbound policies and specific-session configurations. The BGP Dynamic Update Peer Group feature separates update group replication from peer group configuration, which improves convergence time and flexibility of neighbor configuration.	<a href="#">Configuring a Basic BGP Network</a>
12.0(24)S	BGP Route-Map Continue	The BGP Route-Map Continue feature introduces the continue clause to BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.0(22)S	BGP Conditional Route Injection	The BGP Conditional Route Injection feature allows you to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.	<a href="#">Configuring a Basic BGP Network</a>
12.0(22)S	BGP Hybrid CLI	The BGP Hybrid CLI feature simplifies the migration of BGP networks and existing configurations from the network layer reachability information (NLRI) format to the address family identifier (AFI) format. This new functionality allows the network operator to configure commands in the AFI format and save these command configurations to existing NLRI formatted configurations. The feature provides the network operator with the capability to take advantage of new features and provides support for migration from the NLRI format to the AFI format.	<a href="#">Configuring a Basic BGP Network</a>
12.0(22)S	BGP Increased Support of Numbered AS-Path Access Lists to 500	The BGP Increased Support of Numbered AS-Path Access Lists to 500 feature increases the maximum number of autonomous systems access lists that can be configured using the <b>ip as-path access-list</b> command from 199 to 500.	<a href="#">Connecting to a Service Provider Using External BGP</a>

**Table 3** *Supported BGP Features (continued)*

Release	Feature Name	Feature Description	Where Documented
12.0(22)S	BGP Prefix-Based Outbound Route Filtering	The BGP Prefix-Based Outbound Route Filtering feature uses BGP outbound route filtering (ORF) send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the number of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.0(22)S	BGP Route-Map Policy List Support	The BGP Route-Map Policy List Support feature introduces new functionality to BGP route maps. This feature adds the capability for a network operator to group route map match clauses into named lists called policy lists. A policy list functions like a macro. When a policy list is referenced in a route map, all of the match clauses are evaluated and processed as if they had been configured directly in the route map. This enhancement simplifies the configuration of BGP routing policy in medium-size and large networks because a network operator can preconfigure policy lists with groups of match clauses and then reference these policy lists within different route maps. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.0(31)S	BGP Route-Map Continue	The BGP Route-Map Continue feature introduces the continue clause to BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map.  Continue clauses are supported in outbound route maps only in Cisco IOS Release 12.0(31)S and later releases.	<a href="#">Connecting to a Service Provider Using External BGP</a>
<b>Cisco IOS Release 12.2S</b>			
12.2(25)S	BGP Support for Named Extended Community Lists	The BGP Support for Named Extended Community Lists feature introduces the ability to configure extended community lists using names in addition to the existing numbered format.	<a href="#">Connecting to a Service Provider Using External BGP</a>

**Table 3**    *Supported BGP Features (continued)*

Release	Feature Name	Feature Description	Where Documented
12.2(25)S	BGP Support for Sequenced Entries in Extended Community Lists	The BGP Support for Sequenced Entries in Extended Community Lists feature introduces automatic sequencing of individual entries in BGP extended community lists. This feature also introduces the ability to remove or resequence extended community list entries without deleting the entire existing extended community list.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(18)S	BGP Configuration Using Peer Templates	The BGP Configuration Using Peer Templates feature introduces a new mechanism that groups distinct neighbor configurations for BGP neighbors that share policies. Configuration templates provide an alternative to peer group configuration and overcome some of the limitations of peer groups.	<a href="#">Configuring a Basic BGP Network</a>
12.2(18)S	BGP Dynamic Update Peer Groups	The BGP Dynamic Update Peer Groups feature introduces a new algorithm that dynamically calculates and optimizes update groups of neighbors that share outbound policies and can share update messages. In previous versions of Cisco IOS software, BGP update messages were grouped based on peer-group configurations. This method of grouping updates limited outbound policies and specific-session configurations. The BGP Dynamic Update Peer Groups feature separates update group replication from peer group configuration, which improves convergence time and flexibility of neighbor configuration.	<a href="#">Configuring a Basic BGP Network</a>
12.2(18)S	BGP Increased Support of Numbered AS-Path Access Lists to 500	The BGP Increased Support of Numbered AS-Path Access Lists to 500 feature increases the maximum number of autonomous systems access lists that can be configured using the <b>ip as-path access-list</b> command from 199 to 500.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(18)S	BGP Route-Map Continue	The BGP Route-Map Continue feature introduces the continue clause to BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map.  Continue clauses are supported in outbound route maps only in Cisco IOS Release 12.0(31)S and later releases.	<a href="#">Connecting to a Service Provider Using External BGP</a>

**Table 3**     *Supported BGP Features (continued)*

Release	Feature Name	Feature Description	Where Documented
12.2(18)S	BGP Route-Map Policy List Support	The BGP Route-Map Policy List Support feature introduces new functionality to BGP route maps. This feature adds the capability for a network operator to group route map match clauses into named lists called policy lists. A policy list functions like a macro. When a policy list is referenced in a route map, all of the match clauses are evaluated and processed as if they had been configured directly in the route map. This enhancement simplifies the configuration of BGP routing policy in medium-size and large networks because a network operator can preconfigure policy lists with groups of match clauses and then reference these policy lists within different route maps. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(14)S	BGP Conditional Route Injection	The BGP Conditional Route Injection feature allows you to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.	<a href="#">Configuring a Basic BGP Network</a>
12.2(14)S	BGP Prefix-Based Outbound Route Filtering	The BGP Prefix-Based Outbound Route Filtering feature uses BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the number of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.	<a href="#">Connecting to a Service Provider Using External BGP</a>
<b>Cisco IOS Releases 12.2T, 12.3, and 12.3T</b>			
12.3(11)T	BGP Support for Named Extended Community Lists	The BGP Support for Named Extended Community Lists feature introduces the ability to configure extended community lists using names in addition to the existing numbered format.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.3(11)T	BGP Support for Sequenced Entries in Extended Community Lists	The BGP Support for Sequenced Entries in Extended Community Lists feature introduces automatic sequencing of individual entries in BGP extended community lists. This feature also introduces the ability to remove or resequence extended community list entries without deleting the entire existing extended community list.	<a href="#">Connecting to a Service Provider Using External BGP</a>

**Table 3**    *Supported BGP Features (continued)*

Release	Feature Name	Feature Description	Where Documented
12.3(4)T	BGP Configuration Using Peer Templates	The BGP Configuration Using Peer Templates feature introduces a new mechanism that groups distinct neighbor configurations for BGP neighbors that share policies. Configuration templates provide an alternative to peer group configuration and overcome some of the limitations of peer groups.	<a href="#">Configuring a Basic BGP Network</a>
12.3(4)T	BGP Dynamic Update Peer Groups	The BGP Dynamic Update Peer Groups feature introduces a new algorithm that dynamically calculates and optimizes update groups of neighbors that share outbound policies and can share update messages. In previous versions of Cisco IOS software, BGP update messages were grouped based on peer group configurations. This method of grouping updates limited outbound policies and specific-session configurations. The BGP Dynamic Update Peer Groups feature separates update group replication from peer group configuration, which improves convergence time and flexibility of neighbor configuration.	<a href="#">Configuring a Basic BGP Network</a>
12.3(2)T	BGP Route-Map Continue	The BGP Route-Map Continue feature introduces the continue clause to BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(15)T	BGP Hybrid CLI	The BGP Hybrid CLI feature simplifies the migration of BGP networks and existing configurations from the NLRI format to the AFI format. This new functionality allows the network operator to configure commands in the AFI format and save these command configurations to existing NLRI formatted configurations. The feature provides the network operator with the capability to take advantage of new features and provides support for migration from the NLRI format to the AFI format.	<a href="#">Configuring a Basic BGP Network</a>
12.2(15)T	BGP Increased Support of Numbered AS-Path Access Lists to 500	The BGP Increased Support of Numbered AS-Path Access Lists to 500 feature increases the maximum number of autonomous systems access lists that can be configured using the <b>ip as-path access-list</b> command from 199 to 500.	<a href="#">Connecting to a Service Provider Using External BGP</a>

**Table 3**     *Supported BGP Features (continued)*

Release	Feature Name	Feature Description	Where Documented
12.2(15)T	BGP Route-Map Policy List Support	The BGP Route-Map Policy List Support feature introduces new functionality to BGP route maps. This feature adds the capability for a network operator to group route map match clauses into named lists called policy lists. A policy list functions like a macro. When a policy list is referenced in a route map, all of the match clauses are evaluated and processed as if they had been configured directly in the route map. This enhancement simplifies the configuration of BGP routing policy in medium-size and large networks because a network operator can preconfigure policy lists with groups of match clauses and then reference these policy lists within different route maps. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(8)T	BGP Named Community Lists	The BGP Named Community Lists feature introduces a new type of community list called the named community list. The BGP Named Community Lists feature allows the network operator to assign meaningful names to community lists and increases the number of community lists that can be configured. A named community list can be configured with regular expressions and with numbered community lists. All rules of numbered communities apply to named community lists except that there is no limitation on the number of community attributes that can be configured for a named community list.	<a href="#">Connecting to a Service Provider Using External BGP</a>
12.2(4)T	BGP Conditional Route Injection	The BGP Conditional Route Injection feature allows you to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.	<a href="#">Configuring a Basic BGP Network</a>
12.2(4)T	BGP Prefix-Based Outbound Route Filtering	The BGP Prefix-Based Outbound Route Filtering feature uses BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the number of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.	<a href="#">Connecting to a Service Provider Using External BGP</a>







## Cisco BGP Overview

---

Border Gateway Protocol (BGP) is an interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems). The Cisco IOS software implementation of BGP version 4 includes multiprotocol extensions to allow BGP to carry routing information for IP multicast routes and multiple Layer 3 protocol address families including IP Version 4 (IPv4), IP Version 6 (IPv6), Virtual Private Networks version 4 (VPNv4), and Connectionless Network Services (CLNS). This module contains conceptual material to help you understand how BGP is implemented in Cisco IOS software.

### Module History

This module was first published on May 2, 2005, and last updated on March 16, 2006.

### Finding Feature Information in This Module

Your Cisco IOS software release may not support all features.

## Contents

- [Prerequisites for Cisco BGP, page 11](#)
- [Restrictions for Cisco BGP, page 11](#)
- [Information About Cisco BGP, page 12](#)
- [Where to Go Next, page 21](#)
- [Additional References, page 21](#)

## Prerequisites for Cisco BGP

This document assumes knowledge of CLNS, IPv4, IPv6, multicast, VPNv4, and Interior Gateway Protocols (IGPs). The amount of knowledge required for each technology is dependent on your deployment.

## Restrictions for Cisco BGP

A router that runs Cisco IOS software can be configured to run only one BGP routing process and to be a member of only one BGP autonomous system. However, a BGP routing process and autonomous system can support multiple concurrent BGP address family and subaddress family configurations.

# Information About Cisco BGP

To deploy and configure BGP in your network you should understand the following concepts:

- [BGP Version 4 Functional Overview, page 12](#)
- [BGP Autonomous Systems, page 13](#)
- [Classless Interdomain Routing, page 14](#)
- [Multiprotocol BGP, page 14](#)
- [Benefits of Using Multiprotocol BGP Versus BGP, page 14](#)
- [Multiprotocol BGP Extensions for IP Multicast, page 15](#)
- [NLRI Configuration CLI, page 17](#)
- [Cisco BGP Address Family Model, page 17](#)
- [IPv4 Address Family, page 19](#)
- [IPv6 Address Family, page 20](#)
- [CLNS Address Family, page 20](#)
- [VPNv4 Address Family, page 20](#)

## BGP Version 4 Functional Overview

BGP is an interdomain routing protocol designed to provide loop-free routing links between organizations. BGP is designed to run over a reliable transport protocol; it uses TCP (Port 179) as the transport protocol because TCP is a connection-oriented protocol. The destination TCP port is assigned 179, and the local port assigned a random port number. Cisco IOS software supports BGP version 4 and it is this version that has been used by Internet Service Providers to help build the Internet. RFC 1771 introduced and discussed a number of new BGP features to allow the protocol to scale for Internet use. RFC 2858 introduced multiprotocol extensions to allow BGP to carry routing information for IP multicast routes and multiple Layer 3 protocol address families including IPv4, IPV6, and CLNS.

BGP is mainly used to connect a local network to an external network to gain access to the Internet or to connect to other organizations. When connecting to an external organization, external BGP (eBGP) peering sessions are created. Although BGP is referred to as an exterior gateway protocol (EGP) many networks within an organization are becoming so complex that BGP can be used to simplify the internal network used within the organization. BGP peers within the same organization exchange routing information through internal BGP (iBGP) peering sessions. For more details about configuring BGP peer sessions and other tasks to build a basic BGP network, see the [“Configuring a Basic BGP Network”](#) module.

BGP uses a path-vector routing algorithm to exchange network reachability information with other BGP speaking networking devices. Network reachability information is exchanged between BGP peers in routing updates. Network reachability information contains the network number, path specific attributes, and the list of autonomous system numbers that a route must transit through to reach a destination network. This list is contained in the AS-path attribute. BGP prevents routing loops by rejecting any routing update that contains the local autonomous system number because this indicates that the route has already travelled through that autonomous system and a loop would therefore be created. The BGP path-vector routing algorithm is a combination of the distance-vector routing algorithm and the AS-path loop detection.

BGP selects a single path, by default, as the best path to a destination host or network. The best path selection algorithm analyzes path attributes to determine which route is installed as the best path in the BGP routing table. Each path carries well-known mandatory, well-known discretionary, and optional transitive attributes that are used in BGP best path analysis. Cisco IOS software provides the ability to influence BGP path selection by altering some of these attributes using the command-line interface (CLI.) BGP path selection can also be influenced through standard BGP policy configuration. For more details about using BGP to influence path selection and configuring BGP policies to filter traffic, see the [“Connecting to a Service Provider Using External BGP”](#) module.

BGP can be used to help manage complex internal networks by interfacing with Interior Gateway Protocols (IGPs). Internal BGP can help with issues such as scaling the existing IGPs to match the traffic demands while maintaining network efficiency. For more details about configuring advanced BGP features including tasks to configure iBGP peering sessions, see the [“Configuring Advanced BGP Features”](#) module.

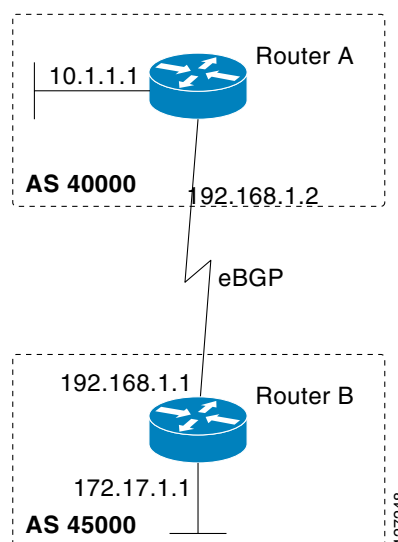
## BGP Autonomous Systems

An autonomous system is a network controlled by a single technical administration entity. BGP autonomous systems are used to divide global external networks into individual routing domains where local routing policies are applied. This organization simplifies routing domain administration and simplifies consistent policy configuration. Consistent policy configuration is important to allow BGP to efficiently process routes to destination networks.

Each routing domain can support multiple routing protocols. However, each routing protocol is administrated separately. Other routing protocols can dynamically exchange routing information with BGP through redistribution. Separate BGP autonomous systems dynamically exchange routing information through eBGP peering sessions. BGP peers within the same autonomous system exchange routing information through iBGP peering sessions.

[Figure 1](#) illustrates two routers in separate autonomous systems that can be connected using BGP. Router A and Router B are Internet service provider (ISP) routers in separate routing domains that use public autonomous system numbers. These routers carry traffic across the Internet. Router A and Router B are connected through eBGP peering sessions.

**Figure 1** *BGP Topology with Two Autonomous Systems*



Each public autonomous system that directly connects to the Internet is assigned a unique number that identifies both the BGP routing process and the autonomous system (a number from 1 to 64511). Private autonomous system numbers are in the range from 64512 to 65534 (65535 is reserved for special use). Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

**Note**

Autonomous system number assignment for public and private networks is governed by the Internet Assigned Number Authority (IANA). For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, refer to the following URL: <http://www.iana.org/>

## Classless Interdomain Routing

BGP version 4 supports classless interdomain routing (CIDR). CIDR eliminates classful network boundaries, providing more efficient usage of the IPv4 address space. CIDR provides a method to reduce the size of routing tables by configuring aggregate routes (or supernets). CIDR processes a prefix as an IP address and bit mask (bits are processed from left to right) to define each network. A prefix can represent a network, subnetwork, supernet, or single host route. For example, using classful IP addressing, the IP address 192.168.2.1 is defined as a single host in the Class C network 192.168.2.0. Using CIDR the IP address can be shown as 192.168.2.1/16, which defines a network (or supernet) of 192.168.0.0. CIDR is enabled by default for all routing protocols in Cisco IOS software. Enabling CIDR affects how packets are forwarded but it does not change the operation of BGP.

## Multiprotocol BGP

Cisco IOS software supports multiprotocol BGP extensions as defined in RFC 2858. The extensions introduced in this RFC allow BGP to carry routing information for multiple network layer protocols including CLNS, IPv4, IPv6, and VPNv4. These extensions are backward compatible to enable routers that do not support multiprotocol extensions to communicate with those routers that do support multiprotocol extensions. Multiprotocol BGP carries routing information for multiple network layer protocols and IP multicast routes. BGP carries different sets of routes depending on the protocol. For example, BGP can carry one set of routes for IPv4 unicast routing, one set of routes for IPv4 multicast routing, and one set of routes for MPLS VPNv4 routes.

**Note**

A multiprotocol BGP network is backwards compatible with a BGP network but BGP peers that do not support multiprotocol extensions cannot forward routing information, such as address family identifier information, that the multiprotocol extensions carry.

## Benefits of Using Multiprotocol BGP Versus BGP

In complex networks with multiple network layer protocols, multiprotocol BGP must be used. In less complex networks we recommend using multiprotocol BGP because it offers the following benefits:

- All of the BGP commands and routing policy capabilities of BGP can be applied to multiprotocol BGP.
- A network can carry routing information for multiple network layer protocol address families (for example, IP Version 4 or VPN Version 4) as specified in RFC 1700, *Assigned Numbers*.
- A network can support incongruent unicast and multicast topologies.
- A multiprotocol BGP network is backward compatible because the routers that support the multiprotocol extensions can interoperate with routers that do not support the extensions.

In summary, multiprotocol BGP support for multiple network layer protocol address families provides a flexible and scalable infrastructure that allows you to define independent policy and peering configurations on a per-address family basis.

## Multiprotocol BGP Extensions for IP Multicast

The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) feature to build data distribution trees. Multiprotocol BGP is useful when you want a link dedicated to multicast traffic, perhaps to limit which resources are used for which traffic. For example, you want all multicast traffic exchanged at one network access point (NAP). Multiprotocol BGP allows you to have a unicast routing topology different from a multicast routing topology that allows you more control over your network and resources.

In BGP, the only way to perform interdomain multicast routing is to use the BGP infrastructure that is in place for unicast routing. If the routers are not multicast-capable, or there are differing policies about where multicast traffic should flow, multicast routing cannot be supported without multiprotocol BGP.

A multicast routing protocol, such as PIM, uses both the multicast and unicast BGP database to source the route, perform Reverse Path Forwarding (RPF) lookups for multicast-capable sources, and build a multicast distribution tree (MDT). The multicast table is the primary source for the router, but if the route is not found in the multicast table then the unicast table is searched. Although multicast can be performed with unicast BGP, multicast BGP routes allow an alternative topology to be used for RPF.

It is possible to configure BGP peers that exchange both unicast and multicast Network Layer Reachability Information (NLRI) where multiprotocol BGP routes can be redistributed into BGP. Multiprotocol extensions, however, will be ignored by any peers that do not support multiprotocol BGP. When PIM builds a multicast distribution tree through a unicast BGP network (because the route through the unicast network is the most attractive), the RPF check may fail, preventing the MDT from being built. If the unicast network runs multiprotocol BGP, peering can be configured using the appropriate multicast address family. The multicast address family configuration enables multiprotocol BGP to carry the multicast information and the RPF lookup will succeed.

[Figure 2](#) illustrates a simple example of unicast and multicast topologies that are incongruent; these topologies cannot exchange information without implementing multiprotocol BGP. Autonomous systems 100, 200, and 300 are each connected to two NAPs that are FDDI rings. One is used for unicast peering (and therefore the exchanging of unicast traffic). The Multicast Friendly Interconnect (MFI) ring is used for multicast peering (and therefore the exchanging of multicast traffic). Each router is unicast- and multicast-capable.

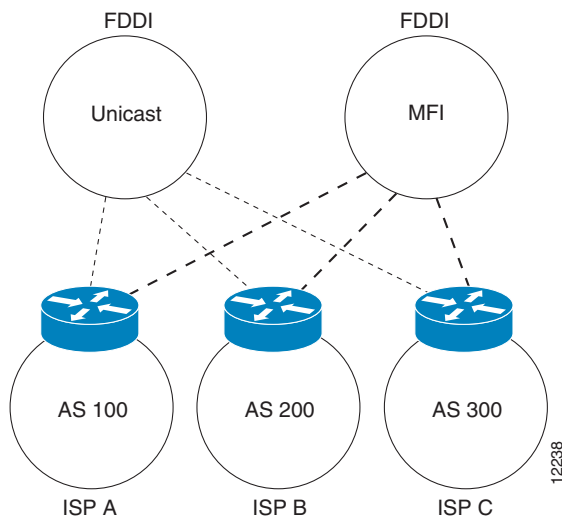
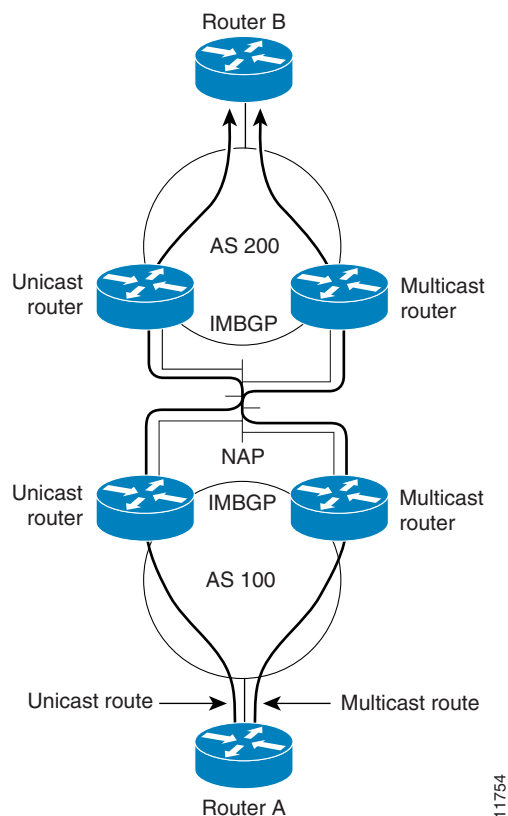
**Figure 2** *Incongruent Unicast and Multicast Routes*

Figure 3 is a topology of unicast-only routers and multicast-only routers. The two routers on the left are unicast-only routers (that is, they do not support or are not configured to perform multicast routing). The two routers on the right are multicast-only routers. Routers A and B support both unicast and multicast routing. The unicast-only and multicast-only routers are connected to a single NAP.

In Figure 3, only unicast traffic can travel from Router A to the unicast routers to Router B and back. Multicast traffic could not flow on that path, because multicast routing is not configured on the unicast routers and therefore the BGP routing table does not contain any multicast routes. On the multicast routers, multicast routes are enabled and BGP builds a separate routing table to hold the multicast routes. Multicast traffic uses the path from Router A to the multicast routers to Router B and back.

Figure 3 illustrates a multiprotocol BGP environment with a separate unicast route and multicast route from Router A to Router B. Multiprotocol BGP allows these routes to be noncongruent. Both of the autonomous systems must be configured for internal multiprotocol BGP in the figure.

**Figure 3 Multicast BGP Environment**

For more information about IP multicast, see the “Configuring IP Multicast” configuration library.

## NLRI Configuration CLI

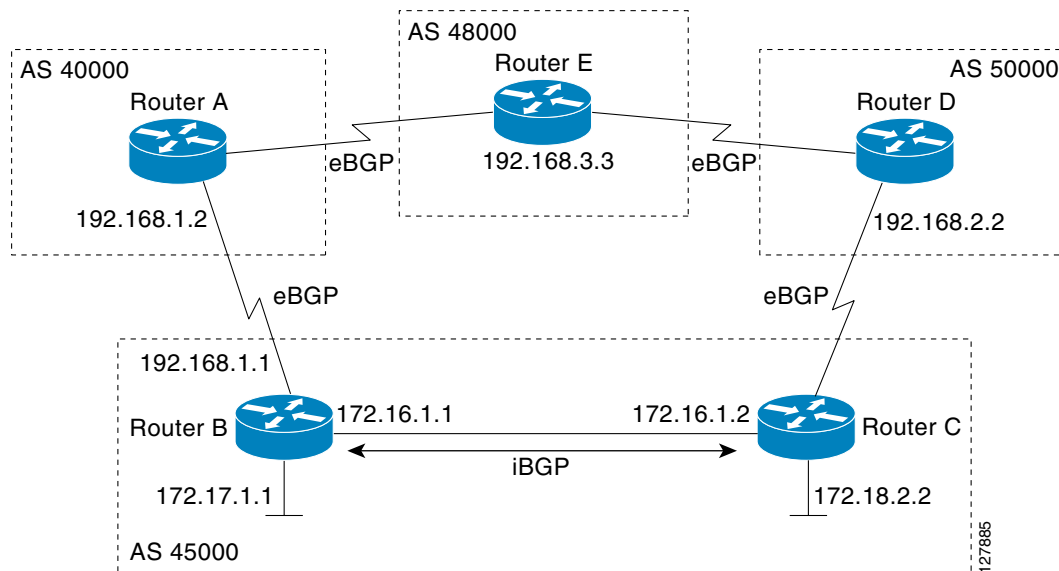
BGP was designed to carry only unicast IPv4 routing information. BGP configuration used the Network Layer Reachability Information (NLRI) format CLI in Cisco IOS software. The NLRI format offers only limited support for multicast routing information and does not support multiple network layer protocols. We do not recommend using NLRI format CLI for BGP configuration. Using the BGP hybrid CLI feature you can configure commands in the address family VPNv4 format and save these command configurations without modifying an existing NLRI formatted configuration. If you want to use other address family configurations such as IPv4 unicast or multicast, then you must upgrade the configuration using the **bgp upgrade-cli** command. For more details about using BGP hybrid CLI command, see the “Configuring a Basic BGP Network” module. See the “Multiprotocol BGP” and “Cisco BGP Address Family Model” concepts for more information about address family configuration format and the limitations of the NLRI CLI format.

## Cisco BGP Address Family Model

The Cisco BGP address family identifier (AFI) model was introduced with multiprotocol BGP and is designed to be modular and scalable, and to support multiple AFI and subsequent address family identifier (SAFI) configurations. Networks are increasing in complexity and many companies are now using BGP to connect to many autonomous systems, as shown in the network topology in Figure 4. Each

of the separate autonomous systems shown in Figure 4 may be running several routing protocols such as Multiprotocol Label Switching (MPLS) and IPv6 and require both unicast and multicast routes to be transported via BGP.

**Figure 4** *BGP Network Topology for Multiple Address Families*



The Cisco BGP AFI model introduced new command-line interface (CLI) commands supported by a new internal structure. Multiprotocol BGP carries routing information for multiple network layer protocols and IP multicast routes. This routing information is carried in the AFI model as appended BGP attributes (multiprotocol extensions). Each address family maintains a separate BGP database, which allows you to configure BGP policy on per-address family basis. SAFI configurations are subsets of the parent AFI. SAFIs can be used to refine BGP policy configurations.

The AFI model was created because of scalability limitations of the NLRI format. A router that is configured in NLRI format has IPv4 unicast but limited multicast capabilities. Networks that are configured in the NLRI format have the following limitations:

- No support for AFI and SAFI configuration information. Many new BGP (and other protocols such as MPLS) features are supported only in AFI and SAFI configuration modes and cannot be configured in NLRI configuration modes.
- No support for IPv6. A router that is configured in the NLRI format cannot establish peering with an IPv6 neighbor.
- Limited support for multicast interdomain routing and incongruent multicast and unicast topologies. In the NLRI format, not all configuration options are available and there is no support for VPNv4. The NLRI format configurations can be more complex than configurations that support the AFI model. If the routers in the infrastructure do not have multicast capabilities, or if policies differ as to where multicast traffic is configured to flow, multicast routing cannot be supported.

The AFI model in multiprotocol BGP supports multiple AFIs and SAFIs, all NLRI-based commands and policy configurations, and is backward compatible with routers that support only the NLRI format. A router that is configured using the AFI model has the following features:

- AFI and SAFI information and configurations are supported. A router that is configured using the AFI model can carry routing information for multiple network layer protocol address families (for example, IPv4 and IPv6).



- AFI configuration is similar in all address families, making the CLI syntax easier to use than the NLRI format syntax.
- All BGP routing policy capabilities and commands are supported.
- Congruent unicast and multicast topologies that have different policies (BGP filtering configurations) are supported, as are incongruent multicast and unicast topologies.
- CLNS is supported.
- Interoperation between routers that support only the NLRI format (AFI-based networks are backward compatible) is supported. This includes both IPv4 unicast and multicast NLRI peers.
- Virtual Private Networks (VPNs) and VPN routing and forwarding (VRF) instances are supported. Unicast IPv4 for VRFs can be configured from a specific address family IPv4 VRF; this configuration update is integrated into the BGP VPNv4 database.

Within a specific address family configuration mode, the question mark (?) online help function can be used to display supported commands. The BGP commands supported in address family configuration mode configure the same functionality as the BGP commands supported in router configuration mode; however, the BGP commands in router configuration mode configure functionality only for the IPv4 unicast address prefix. To configure BGP commands and functionality for other address family prefixes (for example, the IPv4 multicast or IPv6 unicast address prefixes), you must enter address family configuration mode for those address prefixes.

The BGP address family model consists of four address families in Cisco IOS software; IPv4, IPv6, CLNS, and VPNv4. Within the IPv4 and IPv6 address families SAFIs such as Multicast Distribution Tree (MDT), tunnel, and VRF exist. [Table 4](#) shows the list of SAFIs supported by Cisco IOS software. To ensure compatibility between networks running all types of AFI and SAFI configuration, we recommend configuring BGP on Cisco IOS devices using the multiprotocol BGP address family model.

**Table 4** SAFIs supported by Cisco IOS software

SAFI field value	Description	Reference
1	NLRI used for unicast forwarding.	RFC 2858
2	NLRI used for multicast forwarding.	RFC 2858
3	NLRI used for both unicast and multicast forwarding.	RFC 2858
4	NLRI with MPLS labels.	RFC 3107
64	Tunnel SAFI.	draft-nalawade-kapoor-tunnel-safi -01.txt
65	Virtual Private LAN Service (VPLS).	—
66	BGP MDT SAFI	draft-nalawade-idr-mdt-safi-00.txt
128	MPLS-labeled VPN address	RFC-ietf-l3vpn-rfc2547bis-03.txt

## IPv4 Address Family

The IPv4 address family is used to identify routing sessions for protocols such as BGP that use standard IP version 4 address prefixes. Unicast or multicast address prefixes can be specified within the IPv4 address family. Routing information for address family IPv4 unicast is advertised by default when a BGP peer is configured unless the advertisement of unicast IPv4 information is explicitly turned off.

VRF instances can also be associated with IPv4 AFI configuration mode commands.

In Cisco IOS Release 12.0(28)S the tunnel SAFI was introduced to support multipoint tunneling IPv4 routing sessions. The tunnel SAFI is used to advertise the tunnel endpoints and the SAFI specific attributes that contain the tunnel type and tunnel capabilities. Redistribution of tunnel endpoints into the BGP IPv4 tunnel SAFI table occurs automatically when the tunnel address family is configured. However, peers need to be activated under the tunnel address family before the sessions can exchange tunnel information.

In Cisco IOS Release 12.0(29)S the multicast distribution tree (MDT) SAFI was introduced to support multicast VPN architectures. The MDT SAFI is a transitive multicast capable connector attribute that is defined as an IPv4 address family in BGP. The MDT address family session operates as a SAFI under the IPv4 multicast address family, and is configured on provider edge (PE) routers to establish VPN peering sessions with customer edge (CE) routers that support inter-AS multicast VPN peering sessions.

## IPv6 Address Family

The IPv6 address family is used to identify routing sessions for protocols such as BGP that use standard IPv6 address prefixes. Unicast or multicast address prefixes can be specified within the IPv6 address family.



### Note

Routing information for address family IPv4 unicast is advertised by default when you configure a BGP peer unless you explicitly turn off the advertisement of unicast IPv4 information.

## CLNS Address Family

The CLNS address family is used to identify routing sessions for protocols such as BGP that use standard network service access point (NSAP) address prefixes. Unicast address prefixes are the default when NSAP address prefixes are configured.

CLNS routes are used in networks where CLNS addresses are configured. This is typically a telecommunications Data Communications Network (DCN). Peering is established using IP addresses, but update messages contain CLNS routes.

## VPNv4 Address Family

The VPNv4 multicast address family is used to identify routing sessions for protocols such as BGP that use standard VPN Version 4 address prefixes. Unicast address prefixes are the default when VPNv4 address prefixes are configured. VPNv4 routes are the same as IPv4 routes, but VPNv4 routes have a route descriptor (RD) prepended that allows replication of prefixes. It is possible to associate every different RD with a different VPN. Each VPN needs its own set of prefixes.

Companies use an IP VPN as the foundation for deploying or administering value-added services including applications and data hosting network commerce, and telephony services to business customers.

In private LANs, IP-based intranets have fundamentally changed the way companies conduct their business. Companies are moving their business applications to their intranets to extend over a WAN. Companies are also addressing the needs of their customers, suppliers, and partners by using extranets (an intranet that encompasses multiple businesses). With extranets, companies reduce business process

costs by facilitating supply-chain automation, electronic data interchange (EDI), and other forms of network commerce. To take advantage of this business opportunity, service providers must have an IP VPN infrastructure that delivers private network services to businesses over a public infrastructure.

VPNs, when used with MPLS, allow several sites to transparently interconnect through a service provider's network. One service provider network can support several different IP VPNs. Each of these appears to its users as a private network, separate from all other networks. Within a VPN, each site can send IP packets to any other site in the same VPN. Each VPN is associated with one or more VPN VRFs. The router maintains a separate routing and Cisco Express Forwarding (CEF) table for each VRF. This prevents information from being sent outside the VPN and allows the same subnet to be used in several VPNs without causing duplicate IP address problems. The router using BGP distributes the VPN routing information using the BGP extended communities.

The VPN address space is isolated from the global address space by design. BGP distributes reachability information for VPN-IPv4 prefixes for each VPN using the VPNv4 multiprotocol extensions to ensure that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

RFC 3107 specifies how to add label information to multiprotocol BGP address families using a SAFI. The Cisco IOS implementation of MPLS uses RFC 3107 to provide support for sending IPv4 routes with a label. VPNv4 routes implicitly have a label associated with each route.

## Where to Go Next

Proceed to the “Configuring a Basic BGP Network” module.

## Additional References

The following sections provide references related to configuring BGP.

## Related Documents

Related Topic	Document Title
BGP commands	<a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a> , Release 12.4
Roadmap of BGP features	<a href="#">“BGP Features Roadmap”</a>
Configuring basic BGP tasks	<a href="#">“Configuring a Basic BGP Network”</a> module
Configuring BGP to connect to a service provider	<a href="#">“Connecting to a Service Provider Using External BGP”</a> module
Configuring advanced BGP features	<a href="#">“Configuring Advanced BGP Features”</a> chapter of the <i>Cisco IOS IP Routing Configuration Guide</i> , Release 12.4

## Standards

Standard	Title
MDT SAFI	<a href="#">MDT SAFI</a>

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>CISCO-BGP4-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 1700	<i>Assigned Numbers</i>
RFC 1771	<i>A Border Gateway Protocol 4 (BGP-4)</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>
RFC 3107	<i>Carrying Label Information in BGP-4</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>



## Configuring a Basic BGP Network

---

This module describes the basic configuration tasks to configure a basic Border Gateway Protocol (BGP) network. BGP is an interdomain routing protocol designed to provide loop-free routing between organizations. The Cisco IOS implementation of the neighbor and address family commands is explained. This module also contains tasks to configure and customize BGP peers, configure BGP route aggregation, configure BGP route origination, configure BGP backdoor routes, and configure BGP peer groups, configure peer session templates, and configure update groups.

### Module History

This module was first published on May 2, 2005 and last updated on June 19, 2006.

### Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Configuring a Basic BGP Network”](#) section on page 96.

## Contents

- [Prerequisites for Configuring a Basic BGP Network](#), page 23
- [Restrictions for Configuring a Basic BGP Network](#), page 24
- [Information About Configuring a Basic BGP Network](#), page 24
- [How to Configure a Basic BGP Network](#), page 30
- [Configuration Examples for Configuring a Basic BGP Network](#), page 87
- [Where to Go Next](#), page 94
- [Additional References](#), page 94
- [Feature Information for Configuring a Basic BGP Network](#), page 96

## Prerequisites for Configuring a Basic BGP Network

Before configuring basic BGP tasks you should be familiar with the [“Cisco BGP Overview”](#) module.

# Restrictions for Configuring a Basic BGP Network

A router that runs Cisco IOS software can be configured to run only one BGP routing process and to be a member of only one BGP autonomous system. However, a BGP routing process and autonomous system can support multiple address family configurations.

## Information About Configuring a Basic BGP Network

To configure a basic BGP network you should understand the following concepts:

- [BGP Version 4, page 24](#)
- [BGP-Speaker and Peer Relationships, page 25](#)
- [BGP Peer Session Establishment, page 25](#)
- [Cisco Implementation of BGP Global and Address Family Configuration Commands, page 26](#)
- [BGP Session Reset, page 27](#)
- [BGP Route Aggregation, page 28](#)
- [BGP Peer Groups, page 28](#)
- [Peer Groups and BGP Update Messages, page 28](#)
- [BGP Update Group, page 29](#)
- [Peer Templates, page 29](#)

## BGP Version 4

Border Gateway Protocol (BGP) is an interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems). The Cisco IOS software implementation of BGP version 4 includes multiprotocol extensions to allow BGP to carry routing information for IP multicast routes and multiple Layer 3 protocol address families including IP Version 4 (IPv4), IP Version 6 (IPv6), Virtual Private Networks version 4 (VPNv4), and Connectionless Network Services (CLNS).

BGP is mainly used to connect a local network to an external network to gain access to the Internet or to connect to other organizations. When connecting to an external organization, external BGP (eBGP) peering sessions are created. Although BGP is referred to as an exterior gateway protocol (EGP) many networks within an organization are becoming so complex that BGP can be used to simplify the internal network used within the organization. BGP peers within the same organization exchange routing information through internal BGP (iBGP) peering sessions.

**Note**

BGP requires more configuration than other routing protocols and the effects of any configuration changes must be fully understood. Incorrect configuration can create routing loops and negatively impact normal network operation.

## BGP-Speaker and Peer Relationships

A BGP-speaking router does not discover another BGP-speaking device automatically. A network administrator usually manually configures the relationships between BGP-speaking routers. A peer device is a BGP-speaking router that has an active TCP connection to another BGP-speaking device. This relationship between BGP devices is often referred to as a neighbor but, as this can imply the idea that the BGP devices are directly connected with no other router in between, the term neighbor will be avoided whenever possible in this document. A BGP speaker is the local router and a peer is any other BGP-speaking network device.

When a TCP connection is established between peers, each BGP peer initially exchanges all its routes—the complete BGP routing table—with the other peer. After this initial exchange only incremental updates are sent when there has been a topology change in the network, or when a routing policy has been implemented or modified. In the periods of inactivity between these updates, peers exchange special messages called keepalives.

A BGP autonomous system is a network controlled by a single technical administration entity. Peer routers are called external peers when they are in different autonomous systems and internal peers when they are in the same autonomous system. Usually, external peers are adjacent and share a subnet; internal peers may be anywhere in the same autonomous system.

For more details about external BGP peers, see the [“Connecting to a Service Provider Using External BGP”](#) module. For more details about internal BGP peers, see the [“Configuring Internal BGP Features”](#) chapter of the BGP section of the *Cisco IOS IP Routing Configuration Guide*, Release 12.4.

## BGP Peer Session Establishment

When a BGP routing process establishes a peering session with a peer it goes through the following state changes:

- **Idle**—Initial state the BGP routing process enters when the routing process is enabled or when the router is reset. In this state, the router waits for a start event, such as a peering configuration with a remote peer. After the router receives a TCP connection request from a remote peer, the router initiates another start event to wait for a timer before starting a TCP connection to a remote peer. If the router is reset then the peer is reset and the BGP routing process returns to the Idle state.
- **Connect**—The BGP routing process detects that a peer is trying to establish a TCP session with the local BGP speaker.
- **Active**—In this state, the BGP routing process tries to establish a TCP session with a peer router using the ConnectRetry timer. Start events are ignored while the BGP routing process is in the Active state. If the BGP routing process is reconfigured or if an error occurs, the BGP routing process will release system resources and return to an Idle state.
- **OpenSent**—The TCP connection is established and the BGP routing process sends an OPEN message to the remote peer, and transitions to the OpenSent state. The BGP routing process can receive other OPEN messages in this state. If the connection fails, the BGP routing process transitions to the Active state.
- **OpenReceive**—The BGP routing process receives the OPEN message from the remote peer and waits for an initial keepalive message from the remote peer. When a keepalive message is received, the BGP routing process transitions to the Established state. If a notification message is received, the BGP routing process transitions to the Idle state. If an error or configuration change occurs that affects the peering session, the BGP routing process sends a notification message with the Finite State Machine (FSM) error code and then transitions to the Idle state.

- **Established**—The initial keepalive is received from the remote peer. Peering is now established with the remote neighbor and the BGP routing process starts exchanging update message with the remote peer. The hold timer restarts when an update or keepalive message is received. If the BGP process receives an error notification, it will transition to the Idle state.

## Cisco Implementation of BGP Global and Address Family Configuration Commands

The address family model for configuring BGP is based on splitting apart the configuration for each address family. All commands that are independent of the address family are grouped together at the beginning (highest level) of the configuration, and these are followed by separate submodes for commands specific to each address family (with the exception that commands relating to IPv4 unicast can also be entered at the beginning of the configuration). When a network operator configures BGP, the flow of BGP configuration categories is represented by the following bullets in order:

- **Global configuration**—configuration that is applied to BGP in general, rather than to specific neighbors. For example, the **network**, **redistribute**, and **bgp bestpath** commands.
- **Address family-dependent configuration**—configuration that applies to a specific address family such as policy on an individual neighbor.

The relationship between BGP global and BGP address family-dependent configuration categories is shown in [Table 5](#).

**Table 5** Relationships between BGP Configuration Categories

BGP Configuration Category	Configuration Sets Within Category
Global address family-independent	One set of global address family-independent configurations
Address family-dependent	One set of global address family-dependent configurations per address family



### Note

Address family configuration must be entered within the address family submode to which it applies.

The following is an example of BGP configuration statements showing the grouping of global address family-independent and address family-dependent commands.

```
router bgp <AS>
 ! AF independent part
 neighbor <ip-address> <command> ! Session config; AF independent
 address-family ipv4 unicast
 ! AF dependant part
 neighbor <ip-address> <command> ! Policy config; AF dependant
 exit-address-family
 address-family ipv4 multicast
 ! AF dependant part
 neighbor <ip-address> <command> ! Policy config; AF dependant
 exit-address-family
 address-family ipv4 unicast vrf <vrf-name>
 ! VRF specific AS independent commands
 ! VRF specific AS dependant commands
 neighbor <ip-address> <command> ! Session config; AF independent
```



```
neighbor <ip-address> <command> ! Policy config; AF dependant
exit-address-family !
```

The following example shows actual BGP commands that match the BGP configuration statements in the previous example:

```
router bgp 45000
router-id 172.17.1.99
bgp log-neighbor-changes
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.3.2 remote-as 50000
address-family ipv4 unicast
neighbor 192.168.1.2 activate
network 172.17.1.0 mask 255.255.255.0
exit-address-family
address-family ipv4 multicast
neighbor 192.168.3.2 activate
neighbor 192.168.3.2 advertisement-interval 25
network 172.16.1.0 mask 255.255.255.0
exit-address-family
address-family ipv4 vrf vpn1
neighbor 192.168.3.2 activate
network 172.21.1.0 mask 255.255.255.0
exit-address-family
```

In Cisco IOS Releases 12.0(22)S, 12.2(15)T, and later releases the **bgp upgrade-cli** command simplifies the migration of BGP networks and existing configurations from the network layer reachability information (NLRI) format to the address family format. Network operators can configure commands in the address family identifier (AFI) format and save these command configurations to existing NLRI formatted configurations. The BGP hybrid command-line interface (CLI) does not add support for complete AFI and NLRI integration because of the limitations of the NLRI format. For complete support of AFI commands and features, we recommend upgrading existing NLRI configurations with the **bgp upgrade-cli** command. For a configuration example of migrating BGP configurations from the NLRI format to the address family format, see the [“NLRI to AFI Configuration: Example”](#) section on page 88.

## BGP Session Reset

Whenever there is a change in the routing policy due to a configuration change, BGP peering sessions must be reset using the **clear ip bgp** command. Cisco IOS software support the following three mechanisms to reset BGP peering sessions:

- *Hard reset*—A hard reset tears down the specified peering sessions including the TCP connection and deletes routes coming from the specified peer.
- *Soft reset*—A soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.
- *Dynamic inbound soft reset*—The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh must first be advertised through BGP capability negotiation between peers. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

In Cisco IOS Release 12.3(14)T the **bgp soft-reconfig-backup** command was introduced to configure BGP to perform inbound soft reconfiguration for peers that do not support the route refresh capability. The configuration of this command allows you to configure BGP to store updates (soft reconfiguration) only as necessary. Peers that support the route refresh capability are unaffected by the configuration of this command.

## BGP Route Aggregation

BGP peers store and exchange routing information and the amount of routing information increases as more BGP speakers are configured. The use of route aggregation reduces the amount of information involved. Aggregation is the process of combining the attributes of several different routes so that only a single route is advertised. Aggregate prefixes use the classless interdomain routing (CIDR) principle to combine contiguous networks into one classless set of IP addresses that can be summarized in routing tables. Fewer routes now need to be advertised.

Two methods are available in BGP to implement route aggregation. You can redistribute an aggregated route into BGP or you can use a form of conditional aggregation. Basic route redistribution involves creating an aggregate route and then redistributing the routes into BGP. Conditional aggregation involves creating an aggregate route and then advertising or suppressing the advertising of certain routes on the basis of route maps, autonomous system set path (AS-SET) information, or summary information.

In Cisco IOS Release 12.2(25)S the **bgp suppress-inactive** command was introduced to configure BGP to not advertise inactive routes to any BGP peer. A BGP routing process can advertise routes that are not installed in the routing information database (RIB) to BGP peers by default. A route that is not installed into the RIB is an inactive route. Inactive route advertisement can occur, for example, when routes are advertised through common route aggregation. Inactive route advertisements can be suppressed to provide more consistent data forwarding.

## BGP Peer Groups

Often, in a BGP network, many neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into BGP peer groups to simplify configuration and, more importantly, to make configuration updates more efficient. When you have many peers, this approach is highly recommended.

## Peer Groups and BGP Update Messages

In Cisco IOS software releases prior to Release 12.0(24)S, 12.2(18)S, or 12.3(4)T, BGP update messages were grouped based on peer group configurations. This method of grouping neighbors for BGP update message generation reduced the amount of system processing resources needed to scan the routing table. This method, however, had the following limitations:

- All neighbors that shared peer group configuration also had to share outbound routing policies.

- All neighbors had to belong to the same peer group and address family. Neighbors configured in different address families could not belong to different peer groups.

These limitations existed to balance optimal update generation and replication against peer group configuration. These limitations could cause the network operator to configure smaller peer groups, which reduced the efficiency of update message generation and limited the scalability of neighbor configuration.

## BGP Update Group

The introduction of the BGP (dynamic) update group in Cisco IOS Releases 12.0(24)S, 12.2(18)S, or 12.3(4)T provides a different type of BGP peer grouping from existing BGP peer groups. Existing peer groups are not affected but peers with the same outbound policy configured that are not members of a current peer group can be grouped into an update group. The members of this update group will use the same update generation engine. When BGP update groups are configured an algorithm dynamically calculates the BGP update group membership based on outbound policies. Optimal BGP update message generation occurs automatically and independently. BGP neighbor configuration is no longer restricted by outbound routing policies, and update groups can belong to different address families.

## Peer Templates

To address some of the limitations of peer groups such as configuration management, BGP peer templates were introduced to support the BGP update group configuration.

A peer template is a configuration pattern that can be applied to neighbors that share policies. Peer templates are reusable and support inheritance, which allows the network operator to group and apply distinct neighbor configurations for BGP neighbors that share policies. Peer templates also allow the network operator to define very complex configuration patterns through the capability of a peer template to inherit a configuration from another peer template.

There are two types of peer templates:

- Peer session templates are used to group and apply the configuration of general session commands that are common to all address family and NLRI configuration modes.
- Peer policy templates are used to group and apply the configuration of commands that are applied within specific address families and NLRI configuration modes.

Peer templates improve the flexibility and enhance the capability of neighbor configuration. Peer templates also provide an alternative to peer group configuration and overcome some limitations of peer groups. BGP peer routers using peer templates also benefit from automatic update group configuration. With the configuration of the BGP peer templates and the support of the BGP dynamic update peer groups, the network operator no longer needs to configure peer groups in BGP and the network can benefit from improved configuration flexibility and faster convergence.



### Note

The configuration of BGP peer templates does not conflict with or restrict peer group configuration and peer groups are still supported in Cisco IOS Releases that support BGP peer templates. However, a BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from peer templates.

# How to Configure a Basic BGP Network

Configuring a basic BGP network consists of a few required tasks and many optional tasks. A BGP routing process must be configured and BGP peers must be configured, preferably using the address family configuration model. If the BGP peers are part of a VPN network then the BGP peers must be configured using the IPv4 VRF address family task. The other tasks in the following list are optional:

- [Configuring a BGP Routing Process, page 30](#)
- [Configuring a BGP Peer, page 33](#)
- [Configuring a BGP Peer for the IPv4 VRF Address Family, page 37](#)
- [Customizing a BGP Peer, page 41](#)
- [Monitoring and Maintaining Basic BGP, page 45](#)
- [Aggregating Route Prefixes Using BGP, page 52](#)
- [Originating BGP Routes, page 60](#)
- [Configuring a BGP Peer Group, page 68](#)
- [Configuring Peer Session Templates, page 70](#)
- [Configuring Peer Policy Templates, page 78](#)
- [Monitoring and Maintaining BGP Dynamic Update Groups, page 85](#)

## Configuring a BGP Routing Process

Perform this task to configure a BGP routing process. You must perform the required steps at least once to enable BGP. The optional steps here allow you to configure additional features in your BGP network. Several of the features, such as logging neighbor resets and immediate reset of a peer when its link goes down, are enabled by default but are presented here to enhance your understanding of how your BGP network operates.

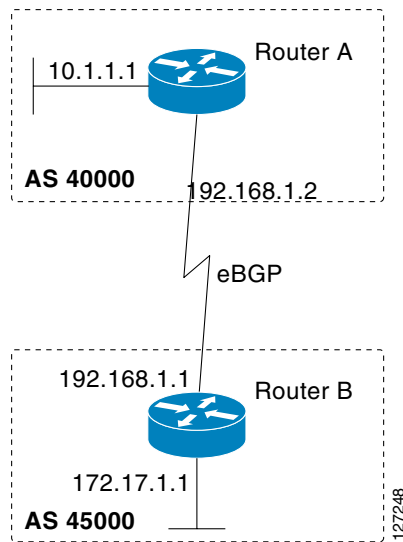
**Note**

---

A router that runs Cisco IOS software can be configured to run only one BGP routing process and to be a member of only one BGP autonomous system. However, a BGP routing process and autonomous system can support multiple concurrent BGP address family and subaddress family configurations.

---

The configuration in this task is done at Router A in [Figure 5](#) and would need to be repeated with appropriate changes to the IP addresses (for example, at Router B) to fully achieve a BGP process between the two routers. No address family is configured here for the BGP routing process so routing information for the IPv4 unicast address family is advertised by default.

**Figure 5** BGP Topology with Two Autonomous Systems

## BGP Router ID

BGP uses a router ID to identify BGP-speaking peers. The BGP router ID is 32-bit value that is often represented by an IPv4 address. By default, the Cisco IOS software sets the router ID to the IPv4 address of a loopback interface on the router. If no loopback interface is configured on the router, then the software chooses the highest IPv4 address configured to a physical interface on the router to represent the BGP router ID. The BGP router ID must be unique to the BGP peers in a network.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
5. **bgp router-id** *ip-address*
6. **timers bgp** *keepalive holdtime*
7. **bgp fast-external-fallover**
8. **bgp log-neighbor-changes**
9. **end**
10. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Configures a BGP routing process, and enters router configuration mode for the specified routing process. <ul style="list-style-type: none"> <li>Use the <i>autonomous-system-number</i> argument to specify an integer, from 0 and 65534, that identifies the router to other BGP speakers.</li> </ul>
Step 4	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router)# network 10.1.1.0 mask 255.255.255.0	(Optional) Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 5	<b>bgp router-id</b> <i>ip-address</i>  <b>Example:</b> Router(config-router)# bgp router-id 10.1.1.99	(Optional) Configures a fixed 32-bit router ID as the identifier of the local router running BGP. <ul style="list-style-type: none"> <li>Use the <i>ip-address</i> argument to specify a unique router ID within the network.</li> </ul> <b>Note</b> Configuring a router ID using the <b>bgp router-id</b> command resets all active BGP peering sessions.
Step 6	<b>timers bgp</b> <i>keepalive holdtime</i>  <b>Example:</b> Router(config-router)# timers bgp 70 120	(Optional) Sets BGP network timers. <ul style="list-style-type: none"> <li>Use the <i>keepalive</i> argument to specify the frequency, in seconds, with which the software sends keepalive messages to its BGP peer. By default, the keepalive timer is set to 60 seconds.</li> <li>Use the <i>holdtime</i> argument to specify the interval, in seconds, after not receiving a keepalive message that the software declares a BGP peer dead. By default, the holdtime timer is set to 180 seconds.</li> </ul>
Step 7	<b>bgp fast-external-fallover</b>  <b>Example:</b> Router(config-router)# bgp fast-external-fallover	(Optional) Enables the automatic resetting of BGP sessions. <ul style="list-style-type: none"> <li>By default, the BGP sessions of any directly adjacent external peers are reset if the link used to reach them goes down.</li> </ul>

	Command or Action	Purpose
Step 8	<b>bgp log-neighbor-changes</b>  <b>Example:</b> Router(config-router)# bgp log-neighbor-changes	(Optional) Enables logging of BGP neighbor status changes (up or down) and neighbor resets. <ul style="list-style-type: none"> <li>Use this command for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.</li> </ul>
Step 9	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 10	<b>show ip bgp [network] [network-mask]</b>  <b>Example:</b> Router# show ip bgp	(Optional) Displays the entries in the BGP routing table.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.

## Examples

The following sample output from the **show ip bgp** command shows the BGP routing table for Router A in [Figure 5](#) after this task has been configured on Router A. You can see an entry for the network 10.1.1.0 that is local to this autonomous system.

```

BGP table version is 12, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop              Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0           32768 i

```

## Troubleshooting Tips

Use the **ping** command to check basic network connectivity between the BGP routers.

## Configuring a BGP Peer

Perform this task to configure BGP between two IPv4 routers (peers). The address family configured here is the default IPv4 unicast address family and the configuration is done at Router A in [Figure 5 on page 31](#). Remember to perform this task for any neighbor routers that are to be BGP peers.

## Prerequisites

Perform the “[Configuring a BGP Routing Process](#)” task before you perform this task.

## Restrictions

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only IPv4 unicast address prefixes. To exchange other address prefix types, such as IPv6 prefixes, neighbors must also be activated using the **neighbor activate** command in address family configuration mode for the other prefix types, such as IPv6 prefixes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor ip-address remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf vrf-name**]
6. **neighbor ip-address activate**
7. **end**
8. **show ip bgp** [*network*] [*network-mask*]
9. **show ip bgp neighbors** [*neighbor-address*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor ip-address remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.1 remote-as 45000	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.



	Command or Action	Purpose
Step 5	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<b>neighbor ip-address activate</b>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.1 activate	Enables the neighbor to exchange prefixes for the IPv4 unicast address family with the local router.
Step 7	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode and enters privileged EXEC mode.
Step 8	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp	(Optional) Displays the entries in the BGP routing table.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 9	<b>show ip bgp neighbors</b> [ <i>neighbor-address</i> ]  <b>Example:</b> Router(config-router-af)# show ip bgp neighbors 192.168.2.2	(Optional) Displays information about the TCP and BGP connections to neighbors.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.

## Examples

The following sample output from the **show ip bgp** command shows the BGP routing table for Router A in [Figure 5 on page 31](#) after this task has been configured on Router A and Router B. You can now see an entry for the network 172.17.1.0 in autonomous system 45000.

```

BGP table version is 13, local router ID is 10.1.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0              0         32768 i
*> 172.17.1.0/24    192.168.1.1          0              0 45000 i

```

The following sample output from the **show ip bgp neighbors** command shows information about the TCP and BGP connections to the BGP neighbor 192.168.1.1 of Router A in [Figure 5 on page 31](#) after this task has been configured on Router A:

```
BGP neighbor is 192.168.1.1, remote AS 45000, external link
BGP version 4, remote router ID 172.17.1.99
BGP state = Established, up for 00:06:55
Last read 00:00:15, last write 00:00:15, hold time is 120, keepalive intervals
Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtimes
Neighbor capabilities:
  Route refresh: advertised and received (old & new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

              Sent          Rcvd
Opens:          1            1
Notifications:  0            0
Updates:        1            2
Keepalives:     13           13
Route Refresh:  0            0
Total:          15           16
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP table version 13, neighbor version 13/0
Output queue size : 0
Index 1, Offset 0, Mask 0x2
1 update-group member

              Sent          Rcvd
Prefix activity:  ----      ----
Prefixes Current:      1            1 (Consumes 52 bytes)
Prefixes Total:       1            1
Implicit Withdraw:     0            0
Explicit Withdraw:     0            0
Used as bestpath:      n/a          1
Used as multipath:     n/a          0

              Outbound      Inbound
Local Policy Denied Prefixes:  -----
AS_PATH loop:                  n/a          1
Bestpath from this peer:        1          n/a
Total:                          1            1
Number of NLRI's in the update sent: max 0, min 0

Connections established 1; dropped 0
Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.1.2, Local port: 179
Foreign host: 192.168.1.1, Foreign port: 37725

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
```

```
Event Timers (current time is 0x12F4F2C):
Timer      Starts    Wakeups    Next
Retrans      14         0         0x0
TimeWait      0         0         0x0
AckHold     13         8         0x0
SendWnd       0         0         0x0
KeepAlive     0         0         0x0
GiveUp        0         0         0x0
PmtuAger      0         0         0x0
DeadWait      0         0         0x0
```

```
iss: 165379618 snduna: 165379963 sndnxt: 165379963 sndwnd: 16040
irs: 3127821601 rcvnxt: 3127821993 rcvwnd: 15993 delrcvwnd: 391

SRTT: 254 ms, RTTO: 619 ms, RTV: 365 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 20 (out of order: 0), with data: 15, total data bytes: 391
Sent: 22 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 04
```

## Troubleshooting Tips

Use the **ping** command to verify basic network connectivity between the BGP routers.

## What To Do Next

If you have BGP peers in a VPN, proceed to the next task. If you do not have BGP peers in a VPN, proceed to the [“Customizing a BGP Peer” section on page 41](#).

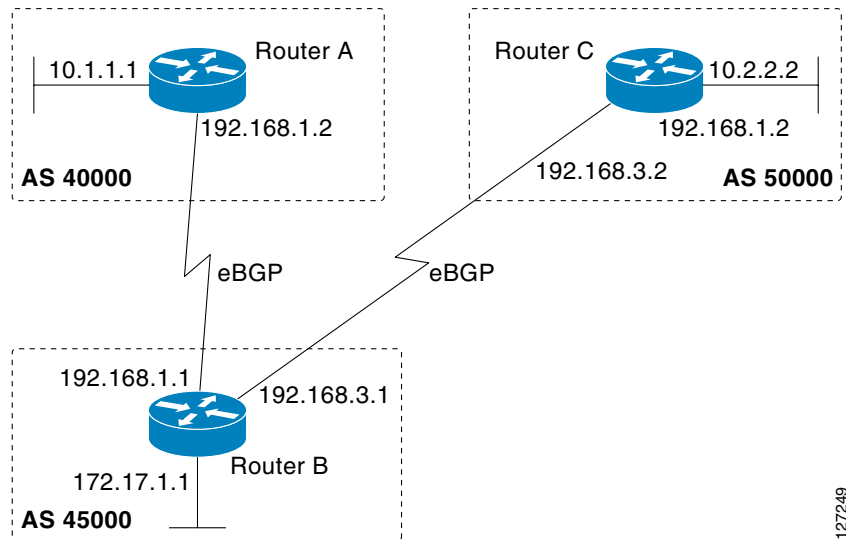
## Configuring a BGP Peer for the IPv4 VRF Address Family

Perform this optional task to configure BGP between two IPv4 routers (peers) that must exchange IPv4 VRF information because they exist in a VPN. The address family configured here is the IPv4 VRF address family and the configuration is done at Router B in [Figure 6](#) with the neighbor 192.168.3.2 at Router E in autonomous system 50000. Remember to perform this task for any neighbor routers that are to be BGP IPv4 VRF address family peers.



### Note

This task does not show the complete configuration required for VPN routing. For some complete example configurations see the [“Additional References” section on page 94](#).

**Figure 6** BGP Topology for IPv4 VRF Address Family

## Prerequisites

Perform the “[Configuring a BGP Routing Process](#)” task before you perform this task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **rd route-distinguisher**
5. **route-target {import | multicast | both} route-target-ext-community**
6. **exit**
7. **router bgp autonomous-system-number**
8. **address-family ipv4 [unicast | multicast | vrf vrf-name]**
9. **neighbor ip-address remote-as autonomous-system-number**
10. **neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [restart restart-interval] [warning-only]**
11. **neighbor ip-address activate**
12. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip vrf vrf-name</b>  <b>Example:</b> Router(config)# ip vrf vpn1	Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>Use the <i>vrf-name</i> argument to specify a name to be assigned to the VRF.</li> </ul>
Step 4	<b>rd route-distinguisher</b>  Router(config-vrf)# rd 45000:5	Creates routing and forwarding tables and specifies the default route distinguisher for a VPN. <ul style="list-style-type: none"> <li>Use the <i>route-distinguisher</i> argument to add an 8-byte value to an IPv4 prefix to create a unique VPN IPv4 prefix.</li> </ul>
Step 5	<b>route-target {import   multicast   both}</b> <b>route-target-ext-community</b>  Router(config-vrf)# route-target both 45000:100	Creates a route target extended community for a VRF. <ul style="list-style-type: none"> <li>Use the <b>import</b> keyword to import routing information from the target VPN extended community.</li> <li>Use the <b>export</b> keyword to export routing information to the target VPN extended community.</li> <li>Use the <b>both</b> keyword to import both import and export routing information to the target VPN extended community.</li> <li>Use the <i>route-target-ext-community</i> argument to add the route target extended community attributes to the VRF's list of import, export, or both (import and export) route target extended communities.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-vrf)# exit	Exits VRF configuration mode and enters global configuration mode.
Step 7	<b>router bgp autonomous-system-number</b>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.

	Command or Action	Purpose
Step 8	<p><b>address-family</b> <b>ipv4</b> [<b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b> Router(config-router)# address-family ipv4 vrf vpn1</p>	<p>Specifies the IPv4 address family and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>Use the <b>unicast</b> keyword to specify the IPv4 unicast address family. By default, the router is placed in configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>Use the <b>multicast</b> keyword to specify IPv4 multicast address prefixes.</li> <li>Use the <b>vrf</b> keyword and <i>vrf-name</i> argument to specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 9	<p><b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i></p> <p><b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 remote-as 45000</p>	<p>Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.</p>
Step 10	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>maximum-prefix</b> <i>maximum</i> [<i>threshold</i>] [<b>restart</b> <i>restart-interval</i>] [<b>warning-only</b>]</p> <p><b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 maximum-prefix 10000 warning-only</p>	<p>Controls how many prefixes can be received from a neighbor.</p> <ul style="list-style-type: none"> <li>Use the <i>maximum</i> argument to specify the maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.</li> <li>Use the <i>threshold</i> argument to specify an integer representing a percentage of the maximum prefix limit at which the router starts to generate a warning message.</li> <li>Use the <b>warning-only</b> keyword to allow the router to generate a log message when the maximum prefix limit is exceeded, instead of terminating the peering session.</li> </ul>
Step 11	<p><b>neighbor</b> <i>ip-address</i> <b>activate</b></p> <p><b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 activate</p>	<p>Enables the neighbor to exchange prefixes for the IPv4 VRF address family with the local router.</p>
Step 12	<p><b>end</b></p> <p><b>Example:</b> Router(config-router-af)# end</p>	<p>Exits address family configuration mode and enters privileged EXEC mode.</p>

## Troubleshooting Tips

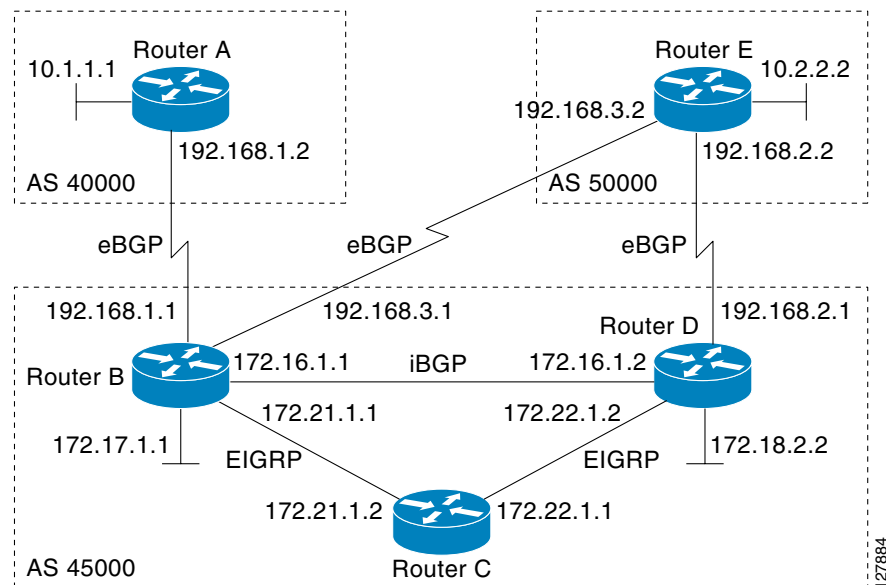
Use the **ping** command to verify basic network connectivity between the BGP routers and use the **show ip vrf** command to verify that the VRF instance has been created.

## Customizing a BGP Peer

Perform this task to customize your BGP peers. Although many of the steps in this task are optional, this task demonstrates how the neighbor and address family configuration command relationships work. Using the example of the IPv4 multicast address family, neighbor address family-independent commands are configured before the IPv4 multicast address family is configured. Commands that are address family-dependent are then configured and the **exit address-family** command is shown. An optional step shows how to disable a neighbor.

The configuration in this task is done at Router B in Figure 7 and would need to be repeated with appropriate changes to the IP addresses, for example, at Router E to fully configure a BGP process between the two routers.

**Figure 7** BGP Peer Topology



## Restrictions

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only IPv4 unicast address prefixes. To exchange other address prefix types, such as IPv6 prefixes, neighbors must also be activated using the **neighbor activate** command in address family configuration mode for the other prefix types, such as IPv6 prefixes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router bgp** *autonomous-system-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*
7. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
8. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*
11. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]
12. **exit-address-family**
13. **neighbor** {*ip-address* | *peer-group-name*} **shutdown**
14. **end**
15. **show ip bgp ipv4 multicast** [*command*]
16. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regexp* | **dampened-routes** | **received** *prefix-filter*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>no bgp default ipv4-unicast</b>  <b>Example:</b> Router(config-router)# no bgp default ipv4-unicast	Disables the IPv4 unicast address family for the BGP routing process.  <b>Note</b> Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session configured with the <b>neighbor remote-as</b> router configuration command unless you configure the <b>no bgp default ipv4-unicast</b> router configuration command before configuring the <b>neighbor remote-as</b> command. Existing neighbor configurations are not affected.



	Command or Action	Purpose
Step 5	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>description</b> <i>text</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 description finance	(Optional) Associates a text description with the specified neighbor.
Step 7	<b>address-family</b> <b>ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 multicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 8	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0	(Optional) Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 9	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 activate	Enables the exchange of information with a BGP neighbor.
Step 10	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>advertisement-interval</b> <i>seconds</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 advertisement-interval 25	(Optional) Sets the minimum interval between the sending of BGP routing updates.

	Command or Action	Purpose
Step 11	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>default-originate</b> [ <b>route-map</b> <i>map-name</i> ]  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 default-originate	(Optional) Permits a BGP speaker—the local router—to send the default route 0.0.0.0 to a peer for use as a default route.
Step 12	<b>exit-address-family</b>  <b>Example:</b> Router(config-router-af)# exit-address-family	Exits address family configuration mode and enters router configuration mode.
Step 13	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>shutdown</b>  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 shutdown	(Optional) Disables a BGP peer or peer group.  <b>Note</b> If you perform this step you will not be able to run either of the subsequent <b>show</b> command steps because you have disabled the neighbor.
Step 14	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 15	<b>show ip bgp ipv4 multicast</b> [ <i>command</i> ]  <b>Example:</b> Router# show ip bgp ipv4 multicast	(Optional) Displays IPv4 multicast database-related information.  <ul style="list-style-type: none"> <li>Use the <i>command</i> argument to specify any multiprotocol BGP command that is supported. To see the supported commands, use the ? prompt on the CLI.</li> </ul>
Step 16	<b>show ip bgp neighbors</b> [ <i>neighbor-address</i> ] [ <b>received-routes</b>   <b>routes</b>   <b>advertised-routes</b>   <b>paths</b> <i>regex</i>   <b>dampened-routes</b>   <b>received prefix-filter</b> ]  <b>Example:</b> Router# show ip bgp neighbors 192.168.3.2	(Optional) Displays information about the TCP and BGP connections to neighbors.

## Examples

The following sample output from the **show ip bgp ipv4 multicast** command shows BGP IPv4 multicast information for Router B in [Figure 7 on page 41](#) after this task has been configured on Router B and Router E. Note that the networks local to each router that were configured under IPv4 multicast address family appear in the output table.

```
BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```

Network          Next Hop           Metric LocPrf Weight Path
*> 10.2.2.0/24    192.168.3.2         0             0 50000 i
*> 172.17.1.0/24  0.0.0.0             0             32768 i
```

The following partial sample output from the **show ip bgp neighbors** command for neighbor 192.168.3.2 shows general BGP information and specific BGP IPv4 multicast address family information about the neighbor. The command was entered on Router B in [Figure 7 on page 41](#) after this task has been configured on Router B and Router E.

```
BGP neighbor is 192.168.3.2, remote AS 50000, external link
Description: finance
  BGP version 4, remote router ID 10.2.2.99
  BGP state = Established, up for 01:48:27
  Last read 00:00:26, last write 00:00:26, hold time is 120, keepalive intervals
  Configured hold time is 120,keepalive interval is 70 seconds, Minimum holdtimes
  Neighbor capabilities:
    Route refresh: advertised and received (old & new)
    Address family IPv4 Unicast: advertised
    Address family IPv4 Multicast: advertised and received
!
For address family: IPv4 Multicast
  BGP table version 3, neighbor version 3/0
  Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
    Uses NEXT_HOP attribute for MBGP NLRI's

Prefix activity:
      Sent      Rcvd
-----
Prefixes Current:      1      1 (Consumes 48 bytes)
Prefixes Total:        1      1
Implicit Withdraw:      0      0
Explicit Withdraw:      0      0
Used as bestpath:      n/a      1
Used as multipath:      n/a      0

Local Policy Denied Prefixes:
      Outbound  Inbound
-----
Bestpath from this peer:      1      n/a
Total:                        1      0
Number of NLRI's in the update sent: max 0, min 0
Minimum time between advertisement runs is 25 seconds

Connections established 8; dropped 7
Last reset 01:48:54, due to User reset
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 192.168.3.1, Local port: 13172
Foreign host: 192.168.3.2, Foreign port: 179
!
```

## Monitoring and Maintaining Basic BGP

The tasks in this section are concerned with the resetting and display of information about basic BGP processes and peer relationships. Once you have defined two routers to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you may have to reset BGP connections for the configuration change to take effect.

- [Configuring Inbound Soft-Reconfiguration When Route Refresh Capability is Missing, page 47](#)
- [Resetting and Displaying Basic BGP Information, page 50](#)

## Routing Policy Change Management

Routing policies for a peer include all the configurations for elements such as route map, distribute list, prefix list, and filter list that may impact inbound or outbound routing table updates. Whenever there is a change in the routing policy, the BGP session must be soft cleared, or soft reset, for the new policy to take effect. Performing inbound reset enables the new inbound policy configured on the router to take effect. Performing outbound reset causes the new local outbound policy configured on the router to take effect without resetting the BGP session. As a new set of updates is sent during outbound policy reset, a new inbound policy of the neighbor can also take effect. This means that after changing inbound policy you must do an inbound reset on the local router or an outbound reset on the peer router. Outbound policy changes require an outbound reset on the local router or an inbound reset on the peer router.

There are two types of reset, hard reset and soft reset. [Table 6](#) lists their advantages and disadvantages.

**Table 6** Advantages and Disadvantages of Hard and Soft Resets

Type of Reset	Advantages	Disadvantages
Hard reset	No memory overhead.	The prefixes in the BGP, IP, and Forwarding Information Base (FIB) tables provided by the neighbor are lost. Not recommended.
Outbound soft reset	No configuration, no storing of routing table updates.	Does not reset inbound routing table updates.
Dynamic inbound soft reset	Does not clear the BGP session and cache.  Does not require storing of routing table updates, and has no memory overhead.	Both BGP routers must support the route refresh capability (in Cisco IOS Release 12.1 and later releases).  <b>Note</b> Does not reset outbound routing table updates.
Configured inbound soft reset (uses the <b>neighbor soft-reconfiguration</b> router configuration command)	Can be used when both BGP routers do not support the automatic route refresh capability.  In Cisco IOS Release 12.3(14)T the <b>bgp soft-reconfig-backup</b> command was introduced to configure inbound soft reconfiguration for peers that do not support the route refresh capability.	Requires preconfiguration.  Stores all received (inbound) routing policy updates without modification; is memory-intensive.  Recommended only when absolutely necessary, such as when both BGP routers do not support the automatic route refresh capability.  <b>Note</b> Does not reset outbound routing table updates.

Once you have defined two routers to be BGP neighbors, they will form a BGP connection and exchange routing information. If you subsequently change a BGP filter, weight, distance, version, or timer, or make a similar configuration change, you must reset BGP connections for the configuration change to take effect.

A soft reset updates the routing table for inbound and outbound routing updates. Cisco IOS Release 12.1 and later releases support soft reset without any prior configuration. This soft reset allows the dynamic exchange of route refresh requests and routing information between BGP routers, and the subsequent readvertisement of the respective outbound routing table. There are two types of soft reset:

- When soft reset is used to generate inbound updates from a neighbor, it is called dynamic inbound soft reset.
- When soft reset is used to send a new set of updates to a neighbor, it is called outbound soft reset.

To use soft reset without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session. Routers running Cisco IOS releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** router configuration command. Clearing the BGP session in this way will have a negative impact upon network operations and should be used only as a last resort.

## Configuring Inbound Soft-Reconfiguration When Route Refresh Capability is Missing

Perform this task to configure inbound soft reconfiguration using the **bgp soft-reconfig-backup** command for BGP peers that do not support the route refresh capability. BGP Peers that support the route refresh capability are unaffected by the configuration of this command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp log-neighbor-changes**
5. **bgp soft-reconfig-backup**
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration** [**inbound**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. Repeat Steps 6 through 8 for every peer that is to be configured with soft-reconfiguration inbound.
10. **exit**
11. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
12. **set local-preference** *number-value*
13. **end**
14. **show ip bgp neighbors** [*neighbor-address*]
15. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>bgp log-neighbor-changes</b>  <b>Example:</b> Router(config-router)# bgp log-neighbor-changes	Enables logging of BGP neighbor resets.
Step 5	<b>bgp soft-reconfig-backup</b>  <b>Example:</b> Router(config-router)# bgp soft-reconfig-backup	Configures a BGP speaker to perform inbound soft reconfiguration for peers that do not support the route refresh capability. <ul style="list-style-type: none"> <li>This command is used to configure BGP to perform inbound soft reconfiguration for peers that do not support the route refresh capability. The configuration of this command allows you to configure BGP to store updates (soft reconfiguration) only as necessary. Peers that support the route refresh capability are unaffected by the configuration of this command.</li> </ul>
Step 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>soft-reconfiguration</b> [ <i>inbound</i> ]  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 soft-reconfiguration inbound	Configures the Cisco IOS software to start storing updates. <ul style="list-style-type: none"> <li>All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.</li> </ul>
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <i>in</i>   <i>out</i> }  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 route-map LOCAL in	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named LOCAL will be applied to incoming routes.</li> </ul>

	Command or Action	Purpose
Step 9	Repeat Steps 6 through 8 for every peer that is to be configured with soft-reconfiguration inbound.	—
Step 10	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 11	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <b>sequence-number</b> ]  <b>Example:</b> Router(config)# route-map LOCAL permit 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"><li>In this example, a route map named LOCAL is created.</li></ul>
Step 12	<b>set local-preference</b> <i>number-value</i>  <b>Example:</b> Router(config-route-map)# set local-preference 200	Specifies a preference value for the autonomous system path. <ul style="list-style-type: none"><li>In this example, the local preference value is set to 200.</li></ul>
Step 13	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 14	<b>show ip bgp neighbors</b> [ <i>neighbor-address</i> ]  <b>Example:</b> Router(config-router-af)# show ip bgp neighbors 192.168.1.2	(Optional) Displays information about the TCP and BGP connections to neighbors.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4T.
Step 15	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp	(Optional) Displays the entries in the BGP routing table.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4T.

## Examples

The following partial output from the **show ip bgp neighbors** command shows information about the TCP and BGP connections to the BGP neighbor 192.168.2.1. This peer supports route refresh.

```
BGP neighbor is 192.168.1.2, remote AS 40000, external link
Neighbor capabilities:
  Route refresh: advertised and received(new)
```

The following partial output from the **show ip bgp neighbors** command shows information about the TCP and BGP connections to the BGP neighbor 192.168.3.2. This peer does not support route refresh so the soft-reconfig inbound paths for BGP peer 192.168.3.2 will be stored because there is no other way to update any inbound policy updates.

```
BGP neighbor is 192.168.3.2, remote AS 50000, external link
Neighbor capabilities:
  Route refresh: advertised
```

The following sample output from the **show ip bgp** command shows the entry for the network 172.17.1.0. Both BGP peers are advertising 172.17.1.0/24 but only the received-only path is stored for 192.168.3.2.

```
BGP routing table entry for 172.17.1.0/24, version 11
Paths: (3 available, best #3, table Default-IP-Routing-Table, RIB-failure(4))
Flag: 0x820
  Advertised to update-groups:
    1
50000
  192.168.3.2 from 192.168.3.2 (172.17.1.0)
    Origin incomplete, metric 0, localpref 200, valid, external
50000, (received-only)
  192.168.3.2 from 192.168.3.2 (172.17.1.0)
    Origin incomplete, metric 0, localpref 100, valid, external
40000
  192.168.1.2 from 192.168.1.2 (172.16.1.0)
    Origin incomplete, metric 0, localpref 200, valid, external, best
```

## Resetting and Displaying Basic BGP Information

Perform this task to reset and display information about basic BGP processes and peer relationships.

### SUMMARY STEPS

1. **enable**
2. **clear ip bgp** { \* | *ip-address* | *peer-group-name* } [soft [in | out]]
3. **show ip bgp** [*network-address*] [*network-mask*] [longer-prefixes] [prefix-list *prefix-list-name* | route-map *route-map-name*] [shorter prefixes *mask-length*]
4. **show ip bgp neighbors** [*neighbor-address*] [received-routes | routes | advertised-routes | paths regexp | dampened-routes | received *prefix-filter*]
5. **show ip bgp paths**
6. **show ip bgp summary**

### DETAILED STEPS

#### Step 1 enable

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

#### Step 2 clear ip bgp { \* | *ip-address* | *peer-group-name* } [soft [in | out]]

This command is used to clear and reset BGP neighbor sessions. Specific neighbors or peer groups can be cleared by using the *ip-address* and *peer-group-name* arguments. If no argument is specified, this command will clear and reset all BGP neighbor sessions.



**Note** The **clear ip bgp \*** command also clears all the internal BGP structures which makes it useful as a troubleshooting tool.

The following example clears and resets all the BGP neighbor sessions. In Cisco IOS Release 12.2(25)S and later releases, the syntax is **clear ip bgp all**.



```
RouterA# clear ip bgp *
```

**Step 3** **show ip bgp** [*network-address*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]

This command is used to display all the entries in the BGP routing table. The following example displays BGP routing table information for the 10.1.1.0 network:

```
Router# show ip bgp 10.1.1.0 255.255.255.0
BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  40000
    192.168.1.2 from 192.168.1.2 (10.1.1.99)
      Origin IGP, metric 0, localpref 100, valid, external, best
```

**Step 4** **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regex* | **dampened-routes** | **received prefix-filter**]

This command is used to display information about the TCP and BGP connections to neighbors.

The following example displays the routes that were advertised from Router B in [Figure 6 on page 38](#) to its BGP neighbor 192.168.3.2 on Router E:

```
Router# show ip bgp neighbors 192.168.3.2 advertised-routes
BGP table version is 3, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 40000 i
*> 172.17.1.0/24    0.0.0.0                  0             32768 i

Total number of prefixes 2
```

**Step 5** **show ip bgp paths**

This command is used to display all the BGP paths in the database. The following example displays BGP path information for Router B in [Figure 7 on page 41](#):

```
Router# show ip bgp paths
Address      Hash Refcount Metric Path
0x2FB5DB0    0        5        0 i
0x2FB5C90    1        4        0 i
0x2FB5C00   1361        2        0 50000 i
0x2FB5D20   2625        2        0 40000 i
```

**Step 6** **show ip bgp summary**

This command is used to display the status of all BGP connections. The following example displays BGP routing table information for Router B in [Figure 7 on page 41](#):

```
Router# show ip bgp summary
BGP router identifier 172.17.1.99, local AS number 45000
BGP table version is 3, main routing table version 3
2 network entries using 234 bytes of memory
2 path entries using 104 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
```

```

BGP using 882 total bytes of memory
BGP activity 14/10 prefixes, 16/12 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
192.168.1.2    4 40000    667    672      3    0    0 00:03:49      1
192.168.3.2    4 50000    468    467      0    0    0 00:03:49 (NoNeg)

```

---

## Aggregating Route Prefixes Using BGP

BGP peers exchange information about local networks but this can quickly lead to large BGP routing tables. CIDR enables the creation of aggregate routes (or *supernets*) to minimize the size of routing tables. Smaller BGP routing tables can reduce the convergence time of the network and improve network performance. Aggregated routes can be configured and advertised using BGP. Some aggregations advertise only summary routes and other methods of aggregating routes allow more specific routes to be forwarded. Aggregation applies only to routes that exist in the BGP routing table. An aggregated route is forwarded if at least one more specific route of the aggregation exists in the BGP routing table. Perform one of the following tasks to aggregate routes within BGP:

- [Redistributing a Static Aggregate Route Into BGP, page 52](#)
- [Configuring Conditional Aggregate Routes Using BGP, page 53](#)
- [Suppressing and Unsuppressing Advertising Aggregated Routes Using BGP, page 55](#)
- [Suppressing Inactive Route Advertisement Using BGP, page 56](#)
- [Conditionally Advertising BGP Routes, page 58](#)

## Redistributing a Static Aggregate Route Into BGP

Use this task to redistribute a static aggregate route into BGP. A static aggregate route is configured and then redistributed into the BGP routing table. The static route must be configured to point to interface null 0 and the prefix should be a superset of known BGP routes. When a router receives a BGP packet it will use the more specific BGP routes. If the route is not found in the BGP routing table, then the packet will be forwarded to null 0 and discarded.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask* { *ip-address* | *interface-type interface-number* [*ip-address*] } [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
4. **router bgp** *autonomous-system-number*
5. **redistribute static**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]}</i> [distance] [name] [ <b>permanent</b>   <b>track</b> <i>number</i> ] [ <b>tag</b> <i>tag</i> ]  <b>Example:</b> Router(config)# ip route 172.0.0.0 255.0.0.0 null 0	Creates a static route.
Step 4	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 5	<b>redistribute static</b>  <b>Example:</b> Router(config-router)# redistribute static	Redistributes routes into the BGP routing table.
Step 6	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

## Configuring Conditional Aggregate Routes Using BGP

Use this task to create an aggregate route entry in the BGP routing table when at least one specific route falls into the specified range. The aggregate route is advertised as originating from your autonomous system.

### AS-SET Generation

AS-SET information can be generated when BGP routes are aggregated using the **aggregate-address** command. The path advertised for such a route is an AS-SET consisting of all the elements, including the communities, contained in all the paths that are being summarized. If the AS-PATHs to be aggregated are identical, only the AS-PATH is advertised. The ATOMIC-AGGREGATE attribute, set by default for the **aggregate-address** command, is not added to the AS-SET.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **aggregate-address** *address mask* [**as-set**]
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>aggregate-address</b> <i>address mask</i> [ <b>as-set</b> ]  <b>Example:</b> Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 as-set	Creates an aggregate entry in a BGP routing table. <ul style="list-style-type: none"> <li>A specified route must exist in the BGP table.</li> <li>Use the <b>aggregate-address</b> command with no keywords to create an aggregate entry if any more-specific BGP routes are available that fall in the specified range.</li> <li>Use the <b>as-set</b> keyword to specify that the path advertised for this route is an AS-SET. Do not use the <b>as-set</b> keyword when aggregating many paths because this route is withdrawn and updated every time the reachability information for the aggregated route changes.</li> </ul> <b>Note</b> Only partial syntax is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 5	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.

## Suppressing and Unsuppressing Advertising Aggregated Routes Using BGP

Use this task to create an aggregate route, suppress the advertisement of routes using BGP, and subsequently unsuppress the advertisement of routes. Routes that are suppressed are not advertised to any neighbors, but it is possible to unsuppress routes that were previously suppressed to specific neighbors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **aggregate-address** *address mask* [**summary-only**]  
or  
**aggregate-address** *address mask* [**suppress-map** *map-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *map-name*
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.

	Command or Action	Purpose
Step 5	<p><b>aggregate-address</b> <i>address mask</i> [<b>summary-only</b>] or <b>aggregate-address</b> <i>address mask</i> [<b>suppress-map</b> <i>map-name</i>]</p> <p><b>Example:</b> Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 summary-only or Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1</p>	<p>Creates an aggregate route.</p> <ul style="list-style-type: none"> <li>Use the optional <b>summary-only</b> keyword to create the aggregate route (for example, 10.*.*) and also suppresses advertisements of more-specific routes to all neighbors.</li> <li>Use the optional <b>suppress-map</b> keyword to create the aggregate route but suppress advertisement of specified routes. Routes that are suppressed are not advertised to any neighbors. You can use the <b>match</b> clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists <b>match</b> clauses are supported.</li> </ul> <p><b>Note</b> Only partial syntax is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</p>
Step 6	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>unsuppress-map</b> <i>map-name</i></p> <p><b>Example:</b> Router(config-router)# neighbor 192.168.1.2 unsuppress map1</p>	<p>(Optional) Selectively advertises routes previously suppressed by the <b>aggregate-address</b> command.</p> <ul style="list-style-type: none"> <li>In this example, the routes previously suppressed in Step 5 are advertised to neighbor 192.168.1.2.</li> </ul>
Step 7	<p><b>exit</b></p> <p><b>Example:</b> Router(config-router)# exit</p>	<p>Exits router configuration mode and enters global configuration mode.</p>

## Suppressing Inactive Route Advertisement Using BGP

Perform this task to suppress the advertisement of inactive routes by BGP. In Cisco IOS Release 12.2(25)S the **bgp suppress-inactive** command was introduced to configure BGP to not advertise inactive routes to any BGP peer. A BGP routing process can advertise routes that are not installed in the RIB to BGP peers by default. A route that is not installed into the RIB is an inactive route. Inactive route advertisement can occur, for example, when routes are advertised through common route aggregation.

Inactive route advertisements can be suppressed to provide more consistent data forwarding. This feature can be configured on a per IPv4 address family basis. For example, when specifying the maximum number of routes that can be configured in a VRF with the **maximum routes** global configuration command, you also suppress inactive route advertisement to prevent inactive routes from being accepted into the VRF after route limit has been exceeded.

### Prerequisites

This task assumes that BGP is enabled and peering has been established.

### Restrictions

Inactive route suppression can be configured only under the IPv4 address family or under a default IPv4 general session.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** { **ipv4** [**mdt** | **multicast** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**] }
5. **bgp suppress-inactive**
6. **end**
7. **show ip bgp rib-failure**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode, and creates a BGP routing process.
Step 4	<b>address-family</b> { <b>ipv4</b> [ <b>mdt</b>   <b>multicast</b>   <b>unicast</b> [ <b>vrf</b> <i>vrf-name</i> ]   <b>vrf</b> <i>vrf-name</i> ]   <b>vpnv4</b> [ <b>unicast</b> ] }  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Enter address family configuration mode to configure BGP peers to accept address family specific configurations. <ul style="list-style-type: none"> <li>The example creates an IPv4 unicast address family session.</li> </ul>
Step 5	<b>bgp suppress-inactive</b>  <b>Example:</b> Router(config-router-af)# bgp suppress-inactive	Suppresses BGP advertising of inactive routes. <ul style="list-style-type: none"> <li>BGP advertises inactive routes by default.</li> <li>Entering the <b>no</b> form of this command reenables the advertisement of inactive routes.</li> </ul>
Step 6	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode and enters privileged EXEC mode.
Step 7	<b>show ip bgp rib-failure</b>  <b>Example:</b> Router# show ip bgp rib-failure	(Optional) Displays BGP routes that are not installed in the RIB.

## Examples

The following example shows output from the **show ip bgp rib-failure** command displaying routes that are not installed in the RIB. The output shows that the displayed routes were not installed because a route or routes with a better administrative distance already exist in the RIB.

```
Router# show ip bgp rib-failure
```

Network	Next Hop	RIB-failure	RIB-NH Matches
10.1.15.0/24	10.1.35.5	Higher admin distance	n/a
10.1.16.0/24	10.1.15.1	Higher admin distance	n/a

## Conditionally Advertising BGP Routes

Perform this task to conditionally advertise selected BGP routes. The routes or prefixes that will be conditionally advertised are defined in two route maps, an advertise map and an exist map or nonexist map. The route map associated with the exist map or nonexist map specifies the prefix that the BGP speaker will track. The route map associated with the advertise map specifies the prefix that will be advertised to the specified neighbor when the condition is met. When an exist map is configured, the condition is met when the prefix exists in both the advertise map and the exist map. When a nonexist map is configured, the condition is met when the prefix exists in the advertise map but does not exist in the nonexist map. If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur. These routes are referenced from an access list or an IP prefix list.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** *ip-address* **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*}
6. **exit**
7. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
8. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
9. Repeat Steps 7 and 8 for every prefix to be tracked.
10. **exit**
11. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]
12. Repeat Step 11 for every access list to be created.
13. **exit**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 5	<b>neighbor</b> <i>ip-address</i> <b>advertise-map</b> <i>map-name</i> { <b>exist-map</b> <i>map-name</i>   <b>non-exist-map</b> <i>map-name</i> }  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 advertise-map map1 exist-map map2	Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 7	<b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <b>sequence-number</b> ]  <b>Example:</b> Router(config)# route-map map1 permit 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named map1 is created.</li> </ul>
Step 8	<b>match ip address</b> { <i>access-list-number</i> [ <i>access-list-number...</i>   <i>access-list-name...</i> ]   <i>access-list-name</i> [ <i>access-list-number...</i>   <i>access-list-name</i> ]   <b>prefix-list</b> <i>prefix-list-name</i> [ <i>prefix-list-name...</i> ]}  <b>Example:</b> Router(config-route-map)# match ip address 1	Configures the route map to match a prefix that is permitted by a standard access list, an extended access list, or a prefix list. <ul style="list-style-type: none"> <li>In this example, the route map is configured to match a prefix permitted by access list 1.</li> </ul>
Step 9	Repeat Steps 7 and 8 for every prefix to be tracked.	—

	Command or Action	Purpose
Step 10	<b>exit</b>  <b>Example:</b> Router(config-route-map)# exit	Exits route map configuration mode and enters global configuration mode.
Step 11	<b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ] [ <b>log</b> ]  <b>Example:</b> Router(config)# access-list 1 permit 172.17.0.0	Configures a standard access list. <ul style="list-style-type: none"><li>In this example, access list 1 permits advertising of the 172.17.0.0. prefix depending on other conditions set by the <b>neighbor advertise-map</b> command.</li></ul>
Step 12	Repeat Step 11 for every access list to be created.	—
Step 13	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 14	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.

## Originating BGP Routes

Route aggregation is useful to minimize the size of the BGP table but there are situations when you want to add more specific prefixes to the BGP table. Route aggregation can hide more specific routes. Using the **network** command as shown in “[Configuring a BGP Routing Process](#)” section on page 30 originates routes and the following optional tasks originate BGP routes for the BGP table for different situations.

- [Advertising a Default Route Using BGP](#), page 60
- [Conditionally Injecting BGP Routes](#), page 62
- [Originating BGP Routes Using Backdoor Routes](#), page 66

## Advertising a Default Route Using BGP

Perform this task to advertise a default route to BGP peers. The default route is locally originated. A default route can be useful to simplify configuration or to prevent the router from using too many system resources. If the router is peered with an Internet service provider (ISP), the ISP will carry full routing tables, so configuring a default route into the ISP network saves resources at the local router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*]
4. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]

5. **match ip address** {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}
6. **exit**
7. **router bgp** *autonomous-system-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]
9. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip prefix-list</b> <i>list-name</i> [ <b>seq</b> <i>seq-value</i> ] ( <b>deny</b> <i>network/length</i>   <b>permit</b> <i>network/length</i> ) [ <b>ge</b> <i>ge-value</i> ] [ <b>le</b> <i>le-value</i> ]  <b>Example:</b> Router(config)# ip prefix-list DEFAULT permit 10.1.1.0/24	Configures an IP prefix list. <ul style="list-style-type: none"> <li>In this example, prefix list DEFAULT permits advertising of the 10.1.1.0/24. prefix depending on a match set by the <b>match ip address</b> command.</li> </ul>
Step 4	<b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <b>sequence-number</b> ]  <b>Example:</b> Router(config)# route-map ROUTE	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named ROUTE is created.</li> </ul>
Step 5	<b>match ip address</b> { <i>access-list-number</i> [ <i>access-list-number...</i>   <i>access-list-name...</i> ]   <i>access-list-name</i> [ <i>access-list-number...</i>   <i>access-list-name</i> ]   <b>prefix-list</b> <i>prefix-list-name</i> [ <i>prefix-list-name...</i> ]}  <b>Example:</b> Router(config-route-map)# match ip address prefix-list DEFAULT	Configures the route map to match a prefix that is permitted by a standard access list, an extended access list, or a prefix list. <ul style="list-style-type: none"> <li>In this example, the route map is configured to match a prefix permitted by prefix list DEFAULT.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-route-map)# exit	Exits route map configuration mode and enters global configuration mode.
Step 7	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode for the specified routing process.

	Command or Action	Purpose
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>default-originate</b> [ <b>route-map</b> <i>map-name</i> ]  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 default-originate	(Optional) Permits a BGP speaker—the local router—to send the default route 0.0.0.0 to a peer for use as a default route.
Step 9	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.

## Troubleshooting Tips

Use the **show ip route** command on the receiving BGP peer (not on the local router) to verify that the default route has been set. In the output, verify that a line similar to the following showing the default route 0.0.0.0 is present:

```
B*    0.0.0.0/0 [20/0] via 192.168.1.2, 00:03:10
```

## Conditionally Injecting BGP Routes

Use this task to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.

### Conditional BGP Route Injection

Routes that are advertised through the BGP are commonly aggregated to minimize the number of routes that are used and reduce the size of global routing tables. However, common route aggregation can obscure more specific routing information that is more accurate but not necessary to forward packets to their destinations. Routing accuracy is obscured by common route aggregation because a prefix that represents multiple addresses or hosts over a large topological area cannot be accurately reflected in a single route. Cisco IOS software provides several methods in which you can originate a prefix into BGP. The existing methods include redistribution and using the **network** or **aggregate-address** command. These methods assume the existence of more specific routing information (matching the route to be originated) in either the routing table or the BGP table.

BGP conditional route injection allows you to originate a prefix into a BGP routing table without the corresponding match. This feature allows more specific routes to be generated based on administrative policy or traffic engineering information in order to provide more specific control over the forwarding of packets to these more specific routes, which are injected into the BGP routing table only if the configured conditions are met. Enabling this feature will allow you to improve the accuracy of common route aggregation by conditionally injecting or replacing less specific prefixes with more specific prefixes. Only prefixes that are equal to or more specific than the original prefix may be injected. BGP conditional route injection is enabled with the **bgp inject-map exist-map** command and uses two route maps (inject map and exist map) to install one (or more) more specific prefixes into a BGP routing table. The exist-map specifies the prefixes that the BGP speaker will track. The inject map defines the prefixes that will be created and installed into the local BGP table.

## Prerequisites

This task assumes that the IGP is already configured for the BGP peers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp inject-map** *inject-map-name* **exist-map** *exist-map-name* [**copy-attributes**]
5. **exit**
6. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
7. **match ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}]
8. **match ip route-source** { *access-list-number* | *access-list-name* } [*access-list-number...* | *access-list-name...*]
9. **exit**
10. **route-map** *map-tag* [**permit** | **deny**] [**sequence-number**]
11. **set ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}]
12. **set community** { *community-number* [**additive**] [*well-known-community*] | **none** }
13. **exit**
14. **ip prefix-list** *list-name* [**seq** *seq-value*] { **deny** *network/length* | **permit** *network/length* } [**ge** *ge-value*] [**le** *le-value*]
15. Repeat Step 14 for every prefix list to be created.
16. **exit**
17. **show ip bgp injected-paths**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode for the specified routing process.

	Command or Action	Purpose
Step 4	<b>bgp inject-map</b> <i>inject-map-name</i> <b>exist-map</b> <i>exist-map-name</i> [ <b>copy-attributes</b> ]  <b>Example:</b> Router(config-router)# bgp inject-map ORIGINATE exist-map LEARNED_PATH	Specifies the inject map and the exist map for conditional route injection. <ul style="list-style-type: none"> <li>Use the <b>copy-attributes</b> keyword to specify that the injected route inherit the attributes of the aggregate route.</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 6	<b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map LEARNED_PATH permit 10	Configures a route map and enters route map configuration mode.
Step 7	<b>match ip address</b> { <i>access-list-number</i> [ <i>access-list-number...</i>   <i>access-list-name</i> [ <i>access-list-number...</i>   <i>access-list-name</i> ]   <b>prefix-list</b> <i>prefix-list-name</i> [ <i>prefix-list-name...</i> ]}  <b>Example:</b> Router(config-route-map)# match ip address prefix-list SOURCE	Specifies the aggregate route to which a more specific route will be injected. <ul style="list-style-type: none"> <li>In this example, the prefix list named SOURCE is used to redistribute the source of the route.</li> </ul>
Step 8	<b>match ip route-source</b> { <i>access-list-number</i>   <i>access-list-name</i> } [ <i>access-list-number...</i>   <i>access-list-name...</i> ]  <b>Example:</b> Router(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE	Specifies the match conditions for redistributing the source of the route. <ul style="list-style-type: none"> <li>In this example, the prefix list named ROUTE_SOURCE is used to redistribute the source of the route.</li> </ul> <p><b>Note</b> The route source is the neighbor address that is configured with the <b>neighbor remote-as</b> command. The tracked prefix must come from this neighbor in order for conditional route injection to occur.</p>
Step 9	<b>exit</b>  <b>Example:</b> Router(config-route-map)# exit	Exits route map configuration mode and enters global configuration mode.
Step 10	<b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map ORIGINATE permit 10	Configures a route map and enters route map configuration mode.

	Command or Action	Purpose
Step 11	<pre>set ip address {access-list-number [access-list-number...   access-list-name...]   access-list-name [access-list-number...   access-list-name]   prefix-list prefix-list-name [prefix-list-name...]}</pre> <p><b>Example:</b> Router(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES</p>	<p>Specifies the routes to be injected.</p> <ul style="list-style-type: none"> <li>In this example, the prefix list named <code>originated_routes</code> is used to redistribute the source of the route.</li> </ul>
Step 12	<pre>set community {community-number [additive] [well-known-community]   none}</pre> <p><b>Example:</b> Router(config-route-map)# set community 14616:555 additive</p>	Sets the BGP community attribute of the injected route.
Step 13	<pre>exit</pre> <p><b>Example:</b> Router(config-route-map)# exit</p>	Exits route map configuration mode and enters global configuration mode.
Step 14	<pre>ip prefix-list list-name [seq seq-value] {deny network/length   permit network/length} [ge ge-value] [le le-value]</pre> <p><b>Example:</b> Router(config)# ip prefix-list SOURCE permit 10.1.1.0/24</p>	<p>Configures a prefix list.</p> <ul style="list-style-type: none"> <li>In this example, the prefix list named <code>SOURCE</code> is configured to permit routes from network <code>10.1.1.0/24</code>.</li> </ul>
Step 15	Repeat Step 14 for every prefix list to be created.	—
Step 16	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode and returns to privileged EXEC mode.
Step 17	<pre>show ip bgp injected-paths</pre> <p><b>Example:</b> Router# show ip bgp injected-paths</p>	(Optional) Displays information about injected paths.

## Examples

The following sample output is similar to the output that will be displayed when the **show ip bgp injected-paths** command is entered:

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 172.16.0.0        10.0.0.2              0 ?
*> 172.17.0.0/16     10.0.0.2              0 ?
```

## Troubleshooting Tips

BGP conditional route injection is based on the injection of a more specific prefix into the BGP routing table when a less specific prefix is present. If conditional route injection is not working properly, verify the following:

- If conditional route injection is configured but does not occur, verify the existence of the aggregate prefix in the BGP routing table. The existence (or not) of the tracked prefix in the BGP routing table can be verified with the **show ip bgp** command.
- If the aggregate prefix exists but conditional route injection does not occur, verify that the aggregate prefix is being received from the correct neighbor and the prefix list identifying that neighbor is a /32 match.
- Verify the injection (or not) of the more specific prefix using the **show ip bgp injected-paths** command.
- Verify that the prefix that is being injected is not outside of the scope of the aggregate prefix.

Ensure that the inject route map is configured with the **set ip address** command and not the **match ip address** command.

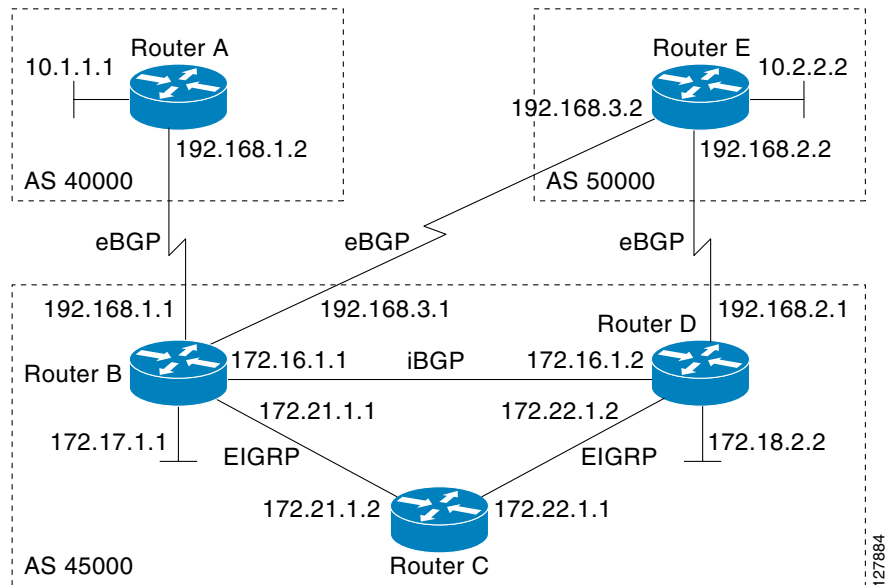
## Originating BGP Routes Using Backdoor Routes

Use this task to indicate to border routers which networks are reachable using a backdoor route. A backdoor network is treated the same as a local network except that it is not advertised.

### BGP Backdoor Routes

In a BGP network topology with two border routers using eBGP to communicate to a number of different autonomous systems, using eBGP to communicate between the two border routers may not be the most efficient routing method. In [Figure 8](#) Router C as a BGP speaker will receive a route to Router D through eBGP but this route will traverse a number of other autonomous systems. Router C and Router D are also connected through an Enhanced Interior Gateway Routing Protocol (EIGRP) network (any IGP can be used here) and this route has a shorter path. EIGRP routes, however, have a default administrative distance of 90 and eBGP routes have a default administrative distance of 20 so BGP will prefer the eBGP route. Changing the default administrative distances is not recommended because changing the administrative distance may lead to routing loops. To cause BGP to prefer the EIGRP route you can use the **network backdoor** command. BGP treats the network specified by the network backdoor command as a locally assigned network, except that it does not advertise the specified network in BGP updates. In [Figure 8](#) this means that Router C will communicate to Router D using the shorter EIGRP route instead of the longer eBGP route.



**Figure 8** BGP Backdoor Route Topology

## Prerequisites

This task assumes that the IGP—EIGRP in this example—is already configured for the BGP peers. The configuration is done at Router C in [Figure 8](#) and the BGP peer is Router D.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **network** *ip-address* **backdoor**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>router</b> <b>bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 172.22.1.2 remote-as 45000	Adds the IP address of the neighbor in the specified autonomous system to the multiprotocol BGP neighbor table of the local router.
Step 5	<b>network</b> <i>ip-address</i> <b>backdoor</b>  <b>Example:</b> Router(config-router)# network 172.21.1.0 backdoor	Indicates a network that is reachable through a backdoor route.
Step 6	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

## Configuring a BGP Peer Group

This task explains how to configure a BGP peer group. Often, in a BGP speaker, many neighbors are configured with the same update policies (that is, the same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and, more importantly, to make updating more efficient. When you have many peers, this approach is highly recommended.

The three steps to configure a BGP peer group, described in the following task, are as follows:

- Creating the peer group
- Assigning options to the peer group
- Making neighbors members of the peer group

You can disable a BGP peer or peer group without removing all the configuration information using the **neighbor shutdown** router configuration command.

## Restrictions

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only IPv4 unicast address prefixes. To exchange other address prefix types, such as IPv6 prefixes, neighbors must also be activated using the **neighbor activate** command in address family configuration mode for the other prefix types.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router** *bgp* *autonomous-system-number*
4. **neighbor** *peer-group-name* **peer-group**
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **peer-group** *peer-group-name*
7. **address-family** *ipv4* [*unicast* | *multicast* | *vrf vrf-name*]
8. **neighbor** *peer-group-name* **activate**
9. **neighbor** *ip-address* **peer-group** *peer-group-name*
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router</b> <i>bgp</i> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> <i>peer-group-name</i> <b>peer-group</b>  <b>Example:</b> Router(config-router)# neighbor fingroup peer-group	Creates a BGP peer group.
Step 5	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.1 remote-as 45000	Adds the IP address of the neighbor in the specified autonomous system to the multiprotocol BGP neighbor table of the local router.
Step 6	<b>neighbor</b> <i>ip-address</i> <b>peer-group</b> <i>peer-group-name</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.1 peer-group fingroup	Assigns the IP address of a BGP neighbor to a peer group.

	Command or Action	Purpose
Step 7	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 multicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. This is the default.</li> <li>The <b>multicast</b> keyword specifies that IPv4 multicast address prefixes will be exchanged.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify that IPv4 VRF instance information will be exchanged.</li> </ul>
Step 8	<b>neighbor peer-group-name activate</b>  <b>Example:</b> Router(config-router-af)# neighbor fingroup activate	Enables the neighbor to exchange prefixes for the IPv4 address family with the local router. <p><b>Note</b> By default, neighbors that are defined using the <b>neighbor remote-as</b> command in router configuration mode exchange only unicast address prefixes. To allow BGP to exchange other address prefix types, such as multicast that is configured in this example, neighbors must also be activated using the <b>neighbor activate</b> command.</p>
Step 9	<b>neighbor ip-address peer-group peer-group-name</b>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.1 peer-group fingroup	Assigns the IP address of a BGP neighbor to a peer group.
Step 10	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode and returns to global configuration mode.

## Configuring Peer Session Templates

The following tasks create and configure a peer session template:

- [Configuring a Basic Peer Session Template, page 71](#)
- [Configuring Peer Session Template Inheritance with the inherit peer-session Command, page 74](#)
- [Configuring Peer Session Template Inheritance with the neighbor inherit peer-session Command, page 76](#)

## Inheritance in Peer Templates

The inheritance capability is a key component of peer template operation. Inheritance in a peer template is similar to node and tree structures commonly found in general computing, for example, file and directory trees. A peer template can directly or indirectly inherit the configuration from another peer template. The directly inherited peer template represents the tree in the structure. The indirectly inherited peer template represents a node in the tree. Because each node also supports inheritance, branches can be created that apply the configurations of all indirectly inherited peer templates within a chain back to the directly inherited peer template or the source of the tree. This structure eliminates the need to repeat configuration statements that are commonly reapplied to groups of neighbors because

common configuration statements can be applied once and then indirectly inherited by peer templates that are applied to neighbor groups with common configurations. Configuration statements that are duplicated separately within a node and a tree are filtered out at the source of the tree by the directly inherited template. A directly inherited template will overwrite any indirectly inherited statements that are duplicated in the directly inherited template.

Inheritance expands the scalability and flexibility of neighbor configuration by allowing you to chain together peer templates configurations to create simple configurations that inherit common configuration statements or complex configurations that apply very specific configuration statements along with common inherited configurations. Specific details about configuring inheritance in peer session templates and peer policy templates are provided in the following sections.

## Configuring a Basic Peer Session Template

Perform this task to create a basic peer session template with general BGP routing session commands that can be applied to many neighbors using one of the next two tasks.



### Note

The commands in Step 5 and 6 are optional and could be replaced with any supported general session commands.

### Peer Session Templates

Peer session templates are used to group and apply the configuration of general session commands to groups of neighbors that share session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template. The following general session commands are supported by peer session templates:

- **description**
- **disable-connected-check**
- **ebgp-multihop**
- **exit peer-session**
- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplifies the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

Peer session templates support direct and indirect inheritance. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template.

**Note**

If you attempt to configure more than one inherit statement with a single peer session template, an error message will be displayed.

This behavior allows a BGP neighbor to directly inherit only one session template and indirectly inherit up to seven additional peer session templates. This allows you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer session template and the configurations from up to seven indirectly inherited peer session templates. Inherited peer session configurations are evaluated first and applied starting with the last node in the branch and ending with the directly applied peer session template configuration at the root of the tree. The directly applied peer session template will have priority over inherited peer session template configurations. Any configuration statements that are duplicated in inherited peer session templates will be overwritten by the directly applied peer session template. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template. The following examples illustrate the use of this feature.

In the following example, the general session command **remote-as 1** is applied in the peer session template named SESSION-TEMPLATE-ONE:

```
template peer-session SESSION-TEMPLATE-ONE
  remote-as 1
exit peer-session
```

Peer session templates support only general session commands. BGP policy configuration commands that are configured only for a specific address family or NLRI configuration mode are configured with peer policy templates.

## Restrictions

The following restrictions apply to the peer session templates:

- A peer session template can directly inherit only one session template, and each inherited session template can also contain one indirectly inherited session template. So, a neighbor or neighbor group can be configured with only one directly applied peer session template and seven additional indirectly inherited peer session templates.
- A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **remote-as** *autonomous-system-number*
6. **timers** *keepalive-interval hold-time*
7. **exit peer-session**

8. **end**
9. **show ip bgp template peer-session** [*session-template-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>template peer-session</b> <i>session-template-name</i>  <b>Example:</b> Router(config-router)# template peer-session INTERNAL-BGP	Enters session-template configuration mode and creates a peer session template.
Step 5	<b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router-stmp)# remote-as 202	(Optional) Configures peering with a remote neighbor in the specified autonomous system.  <b>Note</b> Any supported general session command can be used here. For a list of the supported commands, see the <a href="#">“Peer Session Templates” section on page 71</a> .
Step 6	<b>timers</b> <i>keepalive-interval hold-time</i>  <b>Example:</b> Router(config-router-stmp)# timers 30 300	(Optional) Configures BGP keepalive and hold timers. <ul style="list-style-type: none"> <li>The hold time must be at least twice the keepalive time.</li> </ul> <b>Note</b> Any supported general session command can be used here. For a list of the supported commands, see the <a href="#">“Peer Session Templates” section on page 71</a> .
Step 7	<b>exit peer-session</b>  <b>Example:</b> Router(config-router-stmp)# exit peer-session	Exits session-template configuration mode and enters router configuration mode.

	Command or Action	Purpose
Step 8	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 9	<b>show ip bgp template peer-session</b> [ <i>session-template-name</i> ]  <b>Example:</b> Router#> show ip bgp template peer-session	Displays locally configured peer session templates. <ul style="list-style-type: none"> <li>The output can be filtered to display a single peer policy template with the <i>session-template-name</i> argument. This command also supports all standard output modifiers.</li> </ul>

## What to Do Next

After the peer session template is created, the configuration of the peer session template can be inherited or applied by another peer session template with the **inherit peer-session** or **neighbor inherit peer-session** command.

## Configuring Peer Session Template Inheritance with the **inherit peer-session** Command

This task configures peer session template inheritance with the **inherit peer-session** command. It creates and configures a peer session template and allows it to inherit a configuration from another peer session template.



### Note

The commands in Steps 5 and 6 are optional and could be replaced with any supported general session commands.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-session** *session-template-name*
5. **description** *text-string*
6. **update-source** *interface-type interface-number*
7. **inherit peer-session** *session-template-name*
8. **exit peer-session**
9. **end**
10. **show ip bgp template peer-session** [*session-template-name*]



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> autonomous-system-number  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>template peer-session</b> session-template-name  <b>Example:</b> Router(config-router)# template peer-session CORE1	Enter session-template configuration mode and creates a peer session template.
Step 5	<b>description</b> text-string  <b>Example:</b> Router(config-router-stmp)# description CORE-123	(Optional) Configures a description. <ul style="list-style-type: none"> <li>The text string can be up to 80 characters.</li> </ul> <b>Note</b> Any supported general session command can be used here. For a list of the supported commands, see the <a href="#">“Peer Session Templates” section on page 71</a> .
Step 6	<b>update-source</b> interface-type interface-number  <b>Example:</b> Router(config-router-stmp)# update-source loopback 1	(Optional) Configures a router to select a specific source or interface to receive routing table updates. <ul style="list-style-type: none"> <li>The example uses a loopback interface. The advantage to this configuration is that the loopback interface is not as susceptible to the effects of a flapping interface.</li> </ul> <b>Note</b> Any supported general session command can be used here. For a list of the supported commands, see the <a href="#">“Peer Session Templates” section on page 71</a> .
Step 7	<b>inherit peer-session</b> session-template-name  <b>Example:</b> Router(config-router-stmp)# inherit peer-session INTERNAL-BGP	Configures this peer session template to inherit the configuration of another peer session template. <ul style="list-style-type: none"> <li>The example configures this peer session template to inherit the configuration from INTERNAL-BGP. This template can be applied to a neighbor, and the configuration INTERNAL-BGP will be applied indirectly. No additional peer session templates can be directly applied. However, the directly inherited template can contain up to seven indirectly inherited peer session templates.</li> </ul>

	Command or Action	Purpose
Step 8	<b>exit peer-session</b>  <b>Example:</b> Router(config-router-stmp)# exit peer-session	Exits session-template configuration mode and enters router configuration mode.
Step 9	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 10	<b>show ip bgp template peer-session</b> [session-template-name]  <b>Example:</b> Router#> show ip bgp template peer-session	Displays locally configured peer session templates. <ul style="list-style-type: none"> <li>The output can be filtered to display a single peer policy template with the optional <i>session-template-name</i> argument. This command also supports all standard output modifiers.</li> </ul>

## What to Do Next

After the peer session template is created, the configuration of the peer session template can be inherited or applied by another peer session template with the **inherit peer-session** or **neighbor inherit peer-session** command.

## Configuring Peer Session Template Inheritance with the neighbor inherit peer-session Command

This task configures a router to send a peer session template to a neighbor to inherit the configuration from the specified peer session template with the **neighbor inherit peer-session** command. Use the following steps to send a peer session template configuration to a neighbor to inherit:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor ip-address remote-as** *autonomous-system-number*
5. **neighbor ip-address inherit peer-session** *session-template-name*
6. **exit**
7. **show ip bgp template peer-session** [*session-template-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> autonomous-system-number  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>neighbor</b> ip-address <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router)# neighbor 172.16.0.1 remote-as 202	Configures a peering session with the specified neighbor. <ul style="list-style-type: none"> <li>The explicit <b>remote-as</b> statement is required for the neighbor inherit statement in Step 5 to work. If a peering is not configured, the specified neighbor in Step 5 will not accept the session template.</li> </ul>
Step 5	<b>neighbor</b> ip-address <b>inherit peer-session</b> session-template-name  <b>Example:</b> Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1	Sends a peer session template to a neighbor so that the neighbor can inherit the configuration. <ul style="list-style-type: none"> <li>The example configures a router to send the peer session template named CORE1 to the 172.16.0.1 neighbor to inherit. This template can be applied to a neighbor, and if another peer session template is indirectly inherited in CORE1, the indirectly inherited configuration will also be applied. No additional peer session templates can be directly applied. However, the directly inherited template can also inherit up to seven additional indirectly inherited peer session templates.</li> </ul>
Step 6	<b>end</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters privileged EXEC mode.
Step 7	<b>show ip bgp template peer-session</b> [session-template-name]  <b>Example:</b> Router#> show ip bgp template peer-session	Displays locally configured peer session templates. <ul style="list-style-type: none"> <li>The output can be filtered to display a single peer policy template with the optional <i>session-template-name</i> argument. This command also supports all standard output modifiers.</li> </ul>

## What to Do Next

After the peer session template is created, the configuration of the peer session template can be inherited or applied by another peer session template with the **inherit peer-session** or **neighbor inherit peer-session** command.

## Configuring Peer Policy Templates

The following tasks create and configure a peer policy template:

- [Configuring Basic Peer Policy Templates, page 78](#)
- [Configuring Peer Policy Template Inheritance with the `inherit peer-policy` Command, page 81](#)
- [Configuring Peer Policy Template Inheritance with the `neighbor inherit peer-policy` Command, page 83](#)

### Configuring Basic Peer Policy Templates

Perform this task to create a basic peer policy template with BGP policy configuration commands that can be applied to many neighbors using one of the next two tasks.

**Note**

The commands in Steps 5 through 8 are optional and could be replaced with any supported BGP policy configuration commands.

#### Peer Policy Templates

Peer policy templates are used to group and apply the configuration of commands that are applied within specific address families and NLRI configuration mode. Peer policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address families or NLRI configuration modes are configured in a peer policy template. The following BGP policy commands are supported by peer policy templates:

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**
- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**

- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

Peer policy templates are used to configure BGP policy commands that are configured for neighbors that belong to specific address families and NLRI configuration modes. Like peer session templates, peer policy templates are configured once and then applied to many neighbors through the direct application of a peer policy template or through inheritance from peer policy templates. The configuration of peer policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Like peer session templates, a peer policy template supports inheritance. However, there are minor differences. A directly applied peer policy template can directly or indirectly inherit configurations from up to seven peer policy templates. So, a total of eight peer policy templates can be applied to a neighbor or neighbor group. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number and ending with the highest sequence number. However, there is a difference; a peer policy template will not collapse like a route map. Every sequence is evaluated, and if a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.

The directly applied peer policy template and the inherit statement with the highest sequence number will always have priority and be applied last. Commands that are reapplied in subsequent peer templates will always overwrite the previous values. This behavior is designed to allow you to apply common policy configurations to large neighbor groups and specific policy configurations only to certain neighbors and neighbor groups without duplicating individual policy configuration commands.

Peer policy templates support only policy configuration commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

The configuration of peer policy templates simplifies and improves the flexibility of BGP configuration. A specific policy can be configured once and referenced many times. Because a peer policy supports up to eight levels of inheritance, very specific and very complex BGP policies can also be created.

## Restrictions

The following restrictions apply to the peer policy templates:

- A peer policy template can directly or indirectly inherit up to eight peer policy templates.
- A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **send-community** [**both** | **extended** | **standard**]
6. **maximum-prefix** *prefix-limit* [*threshold*] [**restart** *restart-interval* | **warning-only**]

7. **weight** *weight-value*
8. **prefix-list** *prefix-list-name* {**in** | **out**}
9. **exit peer-policy**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>template peer-policy</b> <i>policy-template-name</i>  <b>Example:</b> Router(config-router)# template peer-policy GLOBAL	Enters policy-template configuration mode and creates a peer policy template.
Step 5	<b>send-community</b> [ <b>both</b>   <b>extended</b>   <b>standard</b> ]  <b>Example:</b> Router(config-router-ptmp)# send community	(Optional) Configures the router to send the community attribute or the extended community attribute or both the community and extended community attribute.  <b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a> .
Step 6	<b>maximum-prefix</b> <i>prefix-limit</i> [ <i>threshold</i> ] [ <b>restart</b> <i>restart-interval</i>   <b>warning-only</b> ]  <b>Example:</b> Router(config-router-ptmp)# maximum-prefix 10000	(Optional) Configures the maximum number of prefixes that a neighbor will accept from this peer.  <b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a> .
Step 7	<b>weight</b> <i>weight-value</i>  <b>Example:</b> Router(config-router-ptmp)# weight 300	(Optional) Sets the default weight for routes that are sent from this neighbor.  <b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a> .

	Command or Action	Purpose
Step 8	<pre>prefix-list prefix-list-name {in   out}</pre> <p><b>Example:</b>  Router(config-router-ptmp)# prefix-list NO-MARKETING in</p>	<p>(Optional) Filters prefixes that are received by the router or sent from the router.</p> <ul style="list-style-type: none"> <li>The prefix list in the example filters inbound internal addresses.</li> </ul> <p><b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a>.</p>
Step 9	<pre>exit peer-policy</pre> <p><b>Example:</b>  Router(config-router-ptmp)# exit peer-policy</p>	Exits policy-template configuration mode and enters router configuration mode.

## What to Do Next

After the peer policy template is created, the configuration of the peer policy template can be inherited or applied by another peer policy template with the **inherit peer-policy** or **neighbor inherit peer-policy** command.

## Configuring Peer Policy Template Inheritance with the inherit peer-policy Command

This task configures peer policy template inheritance with the **inherit peer-policy** command. It creates and configure a peer policy template and allows it to inherit a configuration from another peer policy template.



### Note

The commands in Steps 5 and 6 are optional and could be replaced with any supported BGP policy configuration commands.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **template peer-policy** *policy-template-name*
5. **route-map** *map-name* {in | out}
6. **filter-list** *as-path-list* {in | out}
7. **inherit peer-policy** *policy-template-name* *sequence-number*
8. **exit peer-policy**
9. **end**
10. **show ip bgp template peer-policy** [*policy-template-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>template peer-policy</b> <i>policy-template-name</i>  <b>Example:</b> Router(config-router)# template peer-policy NETWORK-A	Enter policy-template configuration mode and creates a peer policy template.
Step 5	<b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router-ptmp)# route-map SET-COMMUNITY in	(Optional) Applies the specified route map to inbound or outbound routes.  <b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a> .
Step 6	<b>filter-list</b> <i>as-path-list</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router-ptmp)# filter-list 202 in	(Optional) Creates a filter list and applies it to inbound or outbound routes.  <b>Note</b> Any supported BGP policy configuration command can be used here. For a list of the supported commands, see the <a href="#">“Peer Policy Templates” section on page 78</a> .



	Command or Action	Purpose
Step 7	<b>inherit peer-policy</b> <i>policy-template-name</i> <i>sequence-number</i>  <b>Example:</b> Router(config-router-ptmp)# inherit peer-policy GLOBAL 10	Configures the peer policy template to inherit the configuration of another peer policy template. <ul style="list-style-type: none"> <li>The <i>sequence-number</i> argument sets the order in which the peer policy template is evaluated. Like a route map sequence number, the lowest sequence number is evaluated first.</li> <li>The example configures this peer policy template to inherit the configuration from GLOBAL. If the template created in these steps is applied to a neighbor, the configuration GLOBAL will also be inherited and applied indirectly. Up to six additional peer policy templates can be indirectly inherited from GLOBAL for a total of eight directly applied and indirectly inherited peer policy templates.</li> <li>This template in the example will be evaluated first if no other templates are configured with a lower sequence number.</li> </ul>
Step 8	<b>exit peer-policy</b>  <b>Example:</b> Router(config-router-ptmp)# exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
Step 9	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 10	<b>show ip bgp template peer-policy</b> <i>[policy-template-name]</i>  <b>Example:</b> Router#> show ip bgp template peer-policy	Displays locally configured peer policy templates. <ul style="list-style-type: none"> <li>The output can be filtered to display a single peer policy template with the <i>policy-template-name</i> argument. This command also supports all standard output modifiers.</li> </ul>

## Configuring Peer Policy Template Inheritance with the neighbor inherit peer-policy Command

This task configures a router to send a peer policy template to a neighbor to inherit with the **neighbor inherit peer-policy** command. Use the following steps to send a peer policy template configuration to a neighbor to inherit:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** *ip-address* **inherit peer-policy** *policy-template-name*

7. **end**
8. **show ip bgp template peer-policy** *[policy-template-name]*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 101	Enters router configuration mode and creates a BGP routing process.
Step 4	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 10.0.0.1 remote-as 202	Configures a peering session with the specified neighbor. <ul style="list-style-type: none"> <li>The explicit <b>remote-as</b> statement is required for the neighbor inherit statement in Step 5 to work. If a peering is not configured, the specified neighbor in Step 5 will not accept the session template.</li> </ul>
Step 5	<b>address-family</b> <b>ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Enter address family configuration mode to configure a neighbor to accept address family-specific command configurations.
Step 6	<b>neighbor</b> <i>ip-address</i> <b>inherit peer-policy</b> <i>policy-template-name</i>  <b>Example:</b> Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy GLOBAL	Sends a peer policy template to a neighbor so that the neighbor can inherit the configuration. <ul style="list-style-type: none"> <li>The example configures a router to send the peer policy template named GLOBAL to the 10.0.0.1 neighbor to inherit. This template can be applied to a neighbor, and if another peer policy template is indirectly inherited from GLOBAL, the indirectly inherited configuration will also be applied. Up to seven additional peer policy templates can be indirectly inherited from GLOBAL.</li> </ul>

	Command or Action	Purpose
Step 7	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode and enters privileged EXEC mode.
Step 8	<b>show ip bgp template peer-policy</b> [ <i>policy-template-name</i> ]  <b>Example:</b> Router#> show ip bgp template peer-policy	Displays locally configured peer policy templates. <ul style="list-style-type: none"> <li>The output can be filtered to display a single peer policy template with the <i>policy-template-name</i> argument. This command also supports all standard output modifiers.</li> </ul>

## What to Do Next

After the peer policy template is created, the configuration of the peer policy template can be inherited or applied by another peer policy template. For more details about peer policy inheritance see the [“Configuring Peer Policy Template Inheritance with the inherit peer-policy Command”](#) task or the [“Configuring Peer Policy Template Inheritance with the neighbor inherit peer-policy Command”](#) task.

# Monitoring and Maintaining BGP Dynamic Update Groups

Use this task to clear and display information about the processing of dynamic BGP update groups. The performance of BGP update message generation is improved with the use of BGP update groups. With the configuration of the BGP peer templates and the support of the dynamic BGP update groups, the network operator no longer needs to configure peer groups in BGP and can benefit from improved configuration flexibility and system performance. For more information about using BGP peer templates, see the [“Configuring Peer Session Templates”](#) section and the [“Configuring Peer Policy Templates”](#) section.

## BGP Dynamic Update Group Configuration

In Cisco IOS Release 12.0(24)S, 12.2(18)S, and 12.3(4)T a new algorithm was introduced that dynamically calculates and optimizes update groups of neighbors that share the same outbound policies and can share the same update messages. No configuration is required to enable the BGP dynamic update group and the algorithm runs automatically. When a change to outbound policy occurs, the router automatically recalculates update group memberships and applies the changes by triggering an outbound soft reset after a 3-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp ip-address soft out** command. For the best optimization of BGP update group generation, we recommend that the network operator keeps outbound routing policy the same for neighbors that have similar outbound policies.

## SUMMARY STEPS

1. **enable**
2. **clear ip bgp update-group** [*index-group* | *ip-address*]
3. **show ip bgp replication** [*index-group* | *ip-address*]
4. **show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

## DETAILED STEPS

**Step 1**    **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

**Step 2**    **clear ip bgp update-group** [*index-group* | *ip-address*]

This command is used to clear BGP update membership and recalculate BGP update groups. Specific update groups can be cleared by using the *index-group* argument. The range of update group index numbers is from 1 to 4294967295. Specific neighbors can be cleared by using the *ip-address* argument. If no argument is specified, this command will clear and recalculate all BGP update groups.

The following example clears the membership of neighbor 10.0.0.1 from an update group:

```
Router# clear ip bgp update-group 10.0.0.1
```

**Step 3**    **show ip bgp replication** [*index-group* | *ip-address*]

This command displays BGP update group replication statistics. Specific update group replication statistics can be displayed by using the *index-group* argument. The range of update group index numbers is from 1 to 4294967295. Specific update group replication statistics can be displayed by using the *ip-address* argument. If no argument is specified, this command will display replication statistics for all update groups.

The following example displays update group replication information for all BGP neighbors:

```
Router# show ip bgp replication
```

```
BGP Total Messages Formatted/Enqueued : 0/0
```

Index	Type	Members	Leader	MsgFmt	MsgRepl	Csize	Qsize
1	internal	1	10.4.9.21	0	0	0	0
2	internal	2	10.4.9.5	0	0	0	0

**Step 4**    **show ip bgp update-group** [*index-group* | *ip-address*] [**summary**]

This command is used to display information about BGP update groups. Information about specific update group statistics can be displayed by using the *index-group* argument. The range of update group index numbers is from 1 to 4294967295. Information about specific update groups can be displayed by using the *ip-address* argument. If no argument is specified, this command will display statistics for all update groups. Summary information can be displayed by using the **summary** keyword.

The following example displays update group information for all neighbors:

```
Router# show ip bgp update-group
```

```
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRI in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
```

```
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
  Number of NLRI in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
```

```
Has 2 members:  
10.4.9.5 10.4.9.8
```

---

## Troubleshooting Tips

Use the **debug ip bgp groups** command to display information about the processing of BGP update groups. Information can be displayed for all update groups, an individual update group, or a specific BGP neighbor. The output of this command can be very verbose. This command should not be deployed in a production network unless you are troubleshooting a problem.

# Configuration Examples for Configuring a Basic BGP Network

This section contains the following examples:

- [Configuring a BGP Process and Customizing Peers: Example, page 87](#)
- [NLRI to AFI Configuration: Example, page 88](#)
- [BGP Soft Reset: Examples, page 90](#)
- [Aggregating Prefixes Using BGP: Examples, page 90](#)
- [Configuring a BGP Peer Group: Example, page 91](#)
- [Configuring Peer Session Templates: Examples, page 91](#)
- [Configuring Peer Policy Templates: Examples, page 92](#)
- [Monitoring and Maintaining BGP Dynamic Update Peer-Groups: Examples, page 93](#)

## Configuring a BGP Process and Customizing Peers: Example

The following example shows the configuration for Router B in [Figure 7 on page 41](#) with a BGP process configured with two neighbor peers (at Router A and at Router E) in separate autonomous systems. IPv4 unicast routes are exchanged with both peers and IPv4 multicast routes are exchanged with the BGP peer at Router E.

### Router B

```
router bgp 45000  
  bgp router-id 172.17.1.99  
  no bgp default ipv4-unicast  
  bgp log-neighbor-changes  
  timers bgp 70 120  
  neighbor 192.168.1.2 remote-as 40000  
  neighbor 192.168.3.2 remote-as 50000  
  neighbor 192.168.3.2 description finance  
  !  
  address-family ipv4  
    neighbor 192.168.1.2 activate  
    neighbor 192.168.3.2 activate  
    no auto-summary  
    no synchronization  
    network 172.17.1.0 mask 255.255.255.0  
  exit-address-family  
  !  
  address-family ipv4 multicast  
    neighbor 192.168.3.2 activate
```

```
neighbor 192.168.3.2 advertisement-interval 25
no auto-summary
no synchronization
network 172.17.1.0 mask 255.255.255.0
exit-address-family
```

## NLRI to AFI Configuration: Example

The following example upgrades an existing router configuration file in the NLRI format to the AFI format and set the router CLI to use only commands in the AFI format:

```
router bgp 60000
  bgp upgrade-cli
```

The **show running-config** command can be used in privileged EXEC mode to verify that an existing router configuration file has been upgraded from the NLRI format to the AFI format. The following sections provide sample output from a router configuration file in the NLRI format, and the same router configuration file after it has been upgraded to the AFI format with the **bgp upgrade-cli** command in router configuration mode.

- [Router Configuration File in NLRI Format Prior to Upgrading](#)
- [Router Configuration File in AFI Format After Upgrading](#)



### Note

After a router has been upgraded from the AFI format to the NLRI format with the **bgp upgrade-cli** command, NLRI commands will no longer be accessible or configurable.

### Router Configuration File in NLRI Format Prior to Upgrading

The following sample output is from the **show running-config** command in privileged EXEC mode. The sample output shows a router configuration file, in the NLRI format, prior to upgrading to the AFI format with the **bgp upgrade-cli** command. The sample output is filtered to show only the affected portion of the router configuration.

```
Router# show running-config | begin bgp
router bgp 101
  no synchronization
  bgp log-neighbor-changes
  neighbor 10.1.1.1 remote-as 505 nlri unicast multicast
  no auto-summary
!
ip default-gateway 10.4.9.1
ip classless
!
!
route-map REDISTRIBUTE-MULTICAST permit 10
  match ip address prefix-list MULTICAST-PREFIXES
  set nlri multicast
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
  match ip address prefix-list UNICAST-PREFIXES
  set nlri unicast
!
!
!
line con 0
line aux 0
```

```
line vty 0 4
  password PASSWORD
  login
!
end
```

### Router Configuration File in AFI Format After Upgrading

The following sample output shows the router configuration file after it has been upgraded to the AFI format. The sample output is filtered to show only the affected portion of the router configuration file.

```
Router# show running-config | begin bgp

router bgp 101
  bgp log-neighbor-changes
  neighbor 10.1.1.1 remote-as 505
  no auto-summary
  !
  address-family ipv4 multicast
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
  !
  address-family ipv4
  neighbor 10.1.1.1 activate
  no auto-summary
  no synchronization
  exit-address-family
  !
ip default-gateway 10.4.9.1
ip classless
!
!
route-map REDISTRIBUTE-MULTICAST_mcast permit 10
  match ip address prefix-list MULTICAST-PREFIXES
!
route-map REDISTRIBUTE-MULTICAST permit 10
  match ip address prefix-list MULTICAST-PREFIXES
!
route-map MULTICAST-PREFIXES permit 10
!
route-map REDISTRIBUTE-UNICAST permit 20
  match ip address prefix-list UNICAST-PREFIXES
!
!
!
line con 0
line aux 0
line vty 0 4
  password PASSWORD
  login
!
end
```

## BGP Soft Reset: Examples

The following examples show two ways to reset the connection for BGP peer 192.168.1.1.

### Dynamic Inbound Soft Reset Example

The following example shows the **clear ip bgp 192.168.1.1 soft in** EXEC command used to initiate a dynamic soft reconfiguration in the BGP peer 192.168.1.1. This command requires that the peer support the route refresh capability.

```
clear ip bgp 192.168.1.1 soft in
```

### Inbound Soft Reset Using Stored Information Example

The following example shows how to enable inbound soft reconfiguration for the neighbor 192.168.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is performed later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 192.168.1.1 remote-as 200
 neighbor 192.168.1.1 soft-reconfiguration inbound
```

The following example clears the session with the neighbor 192.168.1.1:

```
clear ip bgp 192.168.1.1 soft in
```

## Aggregating Prefixes Using BGP: Examples

The following examples show how you can use aggregate routes in BGP either by redistributing an aggregate route into BGP or by using the BGP conditional aggregation routing feature.

In the following example, the **redistribute static** router configuration command is used to redistribute aggregate route 10.0.0.0:

```
ip route 10.0.0.0 255.0.0.0 null 0
!
router bgp 100
 redistribute static
```

The following configuration shows how to create an aggregate entry in the BGP routing table when at least one specific route falls into the specified range. The aggregate route will be advertised as coming from your autonomous system and has the atomic aggregate attribute set to show that information might be missing. (By default, atomic aggregate is set unless you use the **as-set** keyword in the **aggregate-address** router configuration command.)

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0
```

The following example shows how to create an aggregate entry using the same rules as in the previous example, but the path advertised for this route will be an AS-SET consisting of all elements contained in all paths that are being summarized:

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 as-set
```

The following example shows how to create the aggregate route for 10.0.0.0 and also suppress advertisements of more specific routes to all neighbors:

```
router bgp 100
 aggregate-address 10.0.0.0 255.0.0.0 summary-only
```



The following example, starting in global configuration mode, configures BGP to not advertise inactive routes:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# bgp suppress-inactive
Router(config-router-af)# end
```

The following example configures a maximum route limit in the VRF named red and configures BGP to not advertise inactive routes through the VRF named RED:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 50000:10
Router(config-vrf)# maximum routes 1000 10
Router(config-vrf)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# bgp suppress-inactive
Router(config-router-af)# end
```

## Configuring a BGP Peer Group: Example

The following example shows how to use an address family to configure a peer group so that all members of the peer group are both unicast- and multicast-capable:

```
router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.3.2 remote-as 50000
address-family ipv4 unicast
neighbor mygroup peer-group
neighbor 192.168.1.2 peer-group mygroup
neighbor 192.168.3.2 peer-group mygroup

router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.3.2 remote-as 50000
address-family ipv4 multicast
neighbor mygroup peer-group
neighbor 192.168.1.2 peer-group mygroup
neighbor 192.168.3.2 peer-group mygroup
neighbor 192.168.1.2 activate
neighbor 192.168.3.2 activate
```

## Configuring Peer Session Templates: Examples

The following example creates a peer session template named INTERNAL-BGP in session-template configuration mode:

```
router bgp 101
template peer-session INTERNAL-BGP
remote-as 202
timers 30 300
exit-peer-session
```

The following example creates a peer session template named CORE1. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
template peer-session CORE1
description CORE-123
update-source loopback 1
```

```
inherit peer-session INTERNAL-BGP
exit-peer-session
```

The following example configures the 172.16.0.1 neighbor to inherit the CORE1 peer session template. The 172.16.0.1 neighbor will also indirectly inherit the configuration from the peer session template named INTERNAL-BGP. The explicit **remote-as** statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
router bgp 101
 neighbor 172.16.0.1 remote-as 202
 neighbor 172.16.0.1 inherit peer-session CORE1
```

## Configuring Peer Policy Templates: Examples

The following example creates a peer policy template named GLOBAL in policy-template configuration mode:

```
router bgp 101
 template peer-policy GLOBAL
 send-community
 weight 1000
 maximum-prefix 10000
 prefix-list no-marketing in
 exit-peer-policy
```

The following example creates a peer policy template named PRIMARY-IN in policy-template configuration mode:

```
template peer-policy PRIMARY-IN
 prefix-list ALLOW-PRIMARY-A in
 route-map SET-LOCAL in
 weight 2345
 default-originate
 exit-peer-policy
```

The following example creates a peer policy template named CUSTOMER-A. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
template peer-policy CUSTOMER-A
 route-map SET-COMMUNITY in
 filter-list 20 in
 inherit peer-policy PRIMARY-IN 20
 inherit peer-policy GLOBAL 10
 exit-peer-policy
```

The following example configures the 10.0.0.1 neighbor in address family mode to inherit the peer policy template name CUSTOMER-A. The 10.0.0.1 neighbor will also indirectly inherit the peer policy templates named PRIMARY-IN and GLOBAL.

```
router bgp 101
 neighbor 10.0.0.1 remote-as 202
 address-family ipv4 unicast
 neighbor 10.0.0.1 inherit peer-policy CUSTOMER-A
 exit
```

## Monitoring and Maintaining BGP Dynamic Update Peer-Groups: Examples

No configuration is required to enable the BGP dynamic update of peer groups and the algorithm runs automatically. The following examples show how BGP update group information can be cleared or displayed.

### clear ip bgp update-group Example

The following example clears the membership of neighbor 10.0.0.1 from an update group:

```
Router# clear ip bgp update-group 10.0.0.1
```

### debug ip bgp groups Example

The following example output from the **debug ip bgp groups** command shows the recalculation of update groups after the **clear ip bgp groups** command was issued:

```
Router# debug ip bgp groups
```

```
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.5 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.5 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.8 flags 0x0 cap 0x0 and updgrp 2 fl0
5w4d: BGP-DYN(0): Update-group 2 flags 0x0 cap 0x0 policies same as 10.4.9.8 fl0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Down User reset
5w4d: BGP-DYN(0): Comparing neighbor 10.4.9.21 flags 0x0 cap 0x0 and updgrp 1 f0
5w4d: BGP-DYN(0): Update-group 1 flags 0x0 cap 0x0 policies same as 10.4.9.21 f0
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.5 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.21 Up
5w4d: %BGP-5-ADJCHANGE: neighbor 10.4.9.8 Up
```

### show ip bgp replication Example

The following sample output from the **show ip bgp replication** command shows update group replication information for all for neighbors:

```
Router# show ip bgp replication
```

```
BGP Total Messages Formatted/Enqueued : 0/0
```

Index	Type	Members	Leader	MsgFmt	MsgRepl	Csize	Qsize
1	internal	1	10.4.9.21	0	0	0	0
2	internal	2	10.4.9.5	0	0	0	0

### show ip bgp update-group Example

The following sample output from the **show ip bgp update-group** command shows update group information for all neighbors:

```
Router# show ip bgp update-group
```

```
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
BGP Update version : 0, messages 0/0
Route map for outgoing advertisements is COST1
Update messages formatted 0, replicated 0
Number of NLRI in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 1 member:
10.4.9.21
```

```
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
BGP Update version : 0, messages 0/0
Update messages formatted 0, replicated 0
```

```

Number of NLRI's in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 2 members:
10.4.9.5 10.4.9.8

```

## Where to Go Next

- If you want to connect to an external service provider, see the “[Connecting to a Service Provider Using External BGP](#)” module.
- If you want to configure some iBGP features, see the “[Configuring Internal BGP Features](#)” chapter of the BGP section of the *Cisco IOS IP Routing Configuration Guide*, 12.4.

## Additional References

The following sections provide references related to configuring basic BGP tasks.

### Related Documents

Related Topic	Document Title
BGP commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4
IPv6 commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<a href="#">Cisco IOS IPv6 Command Reference</a> , Release 12.4
IPv6 configuration modules	<a href="#">Cisco IOS IPv6 Configuration Library</a> , Release 12.4
Overview of Cisco BGP conceptual information with links to all the individual BGP modules	“Cisco BGP Overview” module
Multiprotocol Label Switching (MPLS) and BGP configuration example using the IPv4 VRF address family	<a href="#">Inter-AS MPLS VPN Configuration with VPNv4 eBGP Sessions Between ASBRs</a>
Basic MPLS and BGP configuration example	<a href="#">Configuring a Basic MPLS VPN</a>
MPLS VPN over ATM with BGP configuration example	<a href="#">MPLS VPN over ATM: with BGP or RIP on the Customer Site</a>

## Standards

Standard	Title
MDT SAFI	<a href="#">MDT SAFI</a>

## MIBs

MIB	MIBs Link
CISCO-BGP4-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 1771	<i>A Border Gateway Protocol 4 (BGP-4)</i>
RFC 1772	<i>Application of the Border Gateway Protocol in the Internet</i>
RFC 1773	<i>Experience with the BGP Protocol</i>
RFC 1774	<i>BGP-4 Protocol Analysis</i>
RFC 1930	<i>Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)</i>
RFC 2519	<i>A Framework for Inter-Domain Route Aggregation</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>
RFC 2918	<i>Route Refresh Capability for BGP-4</i>
RFC 3392	<i>Capabilities Advertisement with BGP-4</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuring a Basic BGP Network

[Table 7](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for a specific command was introduced, see the command reference documentation.

For information on a feature in this technology that is not documented here, see the “Cisco BGP Implementation Roadmap”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

**Note**

[Table 7](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 7**      *Feature Information for Configuring Basic BGP*

Feature Name	Releases	Feature Configuration Information
BGP Conditional Route Injection	12.2(4)T 12.2(14)S 12.0(22)S	<p>The BGP Conditional Route Injection feature allows you to inject more specific prefixes into a BGP routing table over less specific prefixes that were selected through normal route aggregation. These more specific prefixes can be used to provide a finer granularity of traffic engineering or administrative control than is possible with aggregated routes.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Route Aggregation, page 28</a></li> <li>• <a href="#">Conditionally Injecting BGP Routes, page 62</a></li> </ul>
BGP Configuration Using Peer Templates	12.0(24)S 12.2(18)S 12.3(4)T	<p>The BGP Configuration Using Peer Templates feature introduces a new mechanism that groups distinct neighbor configurations for BGP neighbors that share policies. This type of policy configuration has been traditionally configured with BGP peer groups. However, peer groups have certain limitations because peer group configuration is bound to update grouping and specific session characteristics. Configuration templates provide an alternative to peer group configuration and overcome some of the limitations of peer groups.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Peer Templates, page 29</a></li> <li>• <a href="#">Configuring Peer Session Templates, page 70</a></li> <li>• <a href="#">Configuring Peer Policy Templates, page 78</a></li> </ul>
BGP Dynamic Update Peer Groups	12.0(24)S 12.2(18)S 12.3(4)T	<p>The BGP Dynamic Update Peer Groups feature introduces a new algorithm that dynamically calculates and optimizes update groups of neighbors that share the same outbound policies and can share the same update messages. In previous versions of Cisco IOS software, BGP update messages were grouped based on peer-group configurations. This method of grouping updates limited outbound policies and specific-session configurations. The BGP Dynamic Update Peer Group feature separates update group replication from peer group configuration, which improves convergence time and flexibility of neighbor configuration.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Peer Groups and BGP Update Messages, page 28</a></li> <li>• <a href="#">BGP Update Group, page 29</a></li> <li>• <a href="#">Monitoring and Maintaining BGP Dynamic Update Peer-Groups: Examples, page 93</a></li> </ul>

**Table 7** *Feature Information for Configuring Basic BGP (continued)*

Feature Name	Releases	Feature Configuration Information
BGP Hybrid CLI	12.0(22)S 12.2(15)T	<p>The BGP Hybrid CLI feature simplifies the migration of BGP networks and existing configurations from the NLRI format to the AFI format. This new functionality allows the network operator to configure commands in the AFI format and save these command configurations to existing NLRI formatted configurations. The feature provides the network operator with the capability to take advantage of new features and provides support for migration from the NLRI format to the AFI format.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Cisco Implementation of BGP Global and Address Family Configuration Commands, page 26</a></li> <li>• <a href="#">NLRI to AFI Configuration: Example, page 88</a></li> </ul>
Suppress BGP Advertisement for Inactive Routes	12.2(25)S	<p>The Suppress BGP Advertisements for Inactive Routes features allows you to configure the suppression of advertisements for routes that are not installed in the Routing Information Base (RIB). Configuring this feature allows Border Gateway Protocol (BGP) updates to be more consistent with data used for traffic forwarding.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Route Aggregation, page 28</a></li> <li>• <a href="#">Aggregating Route Prefixes Using BGP, page 52</a></li> <li>• <a href="#">Aggregating Prefixes Using BGP: Examples, page 90</a></li> </ul>





# Connecting to a Service Provider Using External BGP

---

This module describes configuration tasks that will enable your Border Gateway Protocol (BGP) network to access peer devices in external networks such as those from Internet service providers (ISPs). BGP is an interdomain routing protocol designed to provide loop-free routing between organizations. External BGP (eBGP) peering sessions are configured to allow peers from different autonomous systems to exchange routing updates. Tasks to help manage the traffic flowing inbound and outbound are described, as are tasks to configure BGP policies to filter the traffic. Multihoming techniques that provide redundancy for connections to a service provider are also described.

## Module History

This module was first published on May 2, 2005, and last updated on August 29, 2006.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all features. To find information about feature support and configuration, use the [“Feature Information for Connecting to a Service Provider Using External BGP”](#) section on page 162.

## Contents

- [Prerequisites for Connecting to a Service Provider Using External BGP, page 100](#)
- [Restrictions for Connecting to a Service Provider Using External BGP, page 100](#)
- [Information About Connecting to a Service Provider Using External BGP, page 100](#)
- [How to Connect to a Service Provider Using External BGP, page 108](#)
- [Configuration Examples for Connecting to a Service Provider Using External BGP, page 154](#)
- [Where to Go Next, page 160](#)
- [Additional References, page 161](#)
- [Feature Information for Connecting to a Service Provider Using External BGP, page 162](#)

## Prerequisites for Connecting to a Service Provider Using External BGP

- Before connecting to a service provider you need to understand how to configure the basic BGP process and peers. See the [“Cisco BGP Overview”](#) and [“Configuring a Basic BGP Network”](#) modules for more details.
- The tasks and concepts in this chapter will help you configure advanced BGP features that would be useful if you are connecting your network to a service provider. For each connection to the Internet you must have an assigned autonomous system number from the Internet Assigned Numbers Authority (IANA).

## Restrictions for Connecting to a Service Provider Using External BGP

- A router that runs Cisco IOS software can be configured to run only one BGP routing process and to be a member of only one BGP autonomous system. However, a BGP routing process and autonomous system can support multiple address family configurations.
- Policy lists are not supported in versions of Cisco IOS software prior to Cisco IOS Release 12.0(22)S and 12.2(15)T. Reloading a router that is running an older version of Cisco IOS software may cause some routing policy configurations to be lost.

## Information About Connecting to a Service Provider Using External BGP

To configure tasks to connect to an ISP using external BGP you should understand the following concepts:

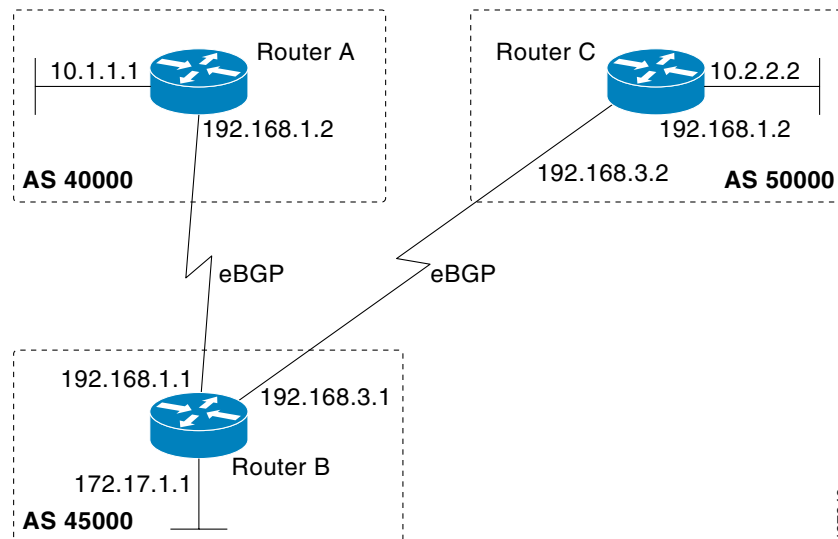
- [External BGP Peering, page 101](#)
- [BGP Attributes, page 102](#)
- [BGP Multipath Support, page 103](#)
- [Multihoming, page 104](#)
- [Transit Versus Nontransit Traffic, page 104](#)
- [BGP Policy Configuration, page 105](#)
- [BGP Communities, page 105](#)
- [Extended Communities, page 106](#)
- [Administrative Distance, page 107](#)
- [BGP Route Map Policy Lists, page 107](#)

## External BGP Peering

BGP is an interdomain routing protocol designed to provide loop-free routing links between organizations. BGP is designed to run over a reliable transport protocol and it uses TCP (Port 179) as the transport protocol. The destination TCP port is assigned 179, and the local port is assigned a random port number. Cisco IOS software supports BGP version 4, which has been used by ISPs to help build the Internet. RFC 1771 introduced and discussed a number of new BGP features to allow the protocol to scale for Internet use.

External BGP peering sessions are configured to allow BGP peers from different autonomous systems to exchange routing updates. By design, a BGP routing process expects eBGP peers to be directly connected, for example, over a WAN connection. However, there are many real-world scenarios where this rule would prevent routing from occurring. Peering sessions for multihop neighbors are configured with the **neighbor ebgp-multihop** command. Figure 9 shows simple eBGP peering between three routers. Router B peers with Router A and Router C. In Figure 9, the **neighbor ebgp-multihop** command could be used to establish peering between Router A and Router C although this is a very simple network design. BGP forwards information about the next hop in the network using the NEXT\_HOP attribute, which is set to the IP address of the interface that advertises a route in an eBGP peering session by default. The source interface can be a physical interface or a loopback interface.

**Figure 9** BGP Peers in Different Autonomous Systems



Loopback interfaces are preferred for establishing eBGP peering sessions because loopback interfaces are less susceptible to interface flapping. Interfaces on networking devices can fail, and they can also be taken out of service for maintenance. When an interface is administratively brought up or down, due to failure or maintenance, it is referred to as a flap. Loopback interfaces provide a stable source interface to ensure that the IP address assigned to the interface is always reachable as long as the IP routing protocols continue to advertise the subnet assigned to the loopback interface. Loopback interfaces allow you to conserve address space by configuring a single address with /32 bit mask. Before a loopback interface is configured for an eBGP peering session, you must configure the **neighbor update-source** command and specify the loopback interface. With this configuration, the loopback interface becomes the source interface and its IP address is advertised as the next hop for routes that are advertised through this loopback. If loopback interfaces are used to connect single-hop eBGP peers, you must configure the **neighbor disable-connected-check** command before you can establish the eBGP peering session.

Connecting to external networks enables traffic from your network to be forwarded to other networks and across the Internet. Traffic will also be flowing into, and possibly through, your network. BGP contains various techniques to influence how the traffic flows into and out of your network, and to create BGP policies that filter the traffic, inbound and outbound. To influence the traffic flow, BGP uses certain BGP attributes that can be included in update messages or used by the BGP routing algorithm. BGP policies to filter traffic also use some of the BGP attributes with route maps, access lists including AS-path access lists, filter lists, policy lists, and distribute lists. Managing your external connections may involve multihoming techniques where there is more than one connection to an ISP or connections to more than one ISP for backup or performance purposes. Tagging BGP routes with different community attributes across autonomous system or physical boundaries can prevent the need to configure long lists of individual permit or deny statements.

## BGP Attributes

BGP selects a single path, by default, as the best path to a destination host or network. The best path selection algorithm analyzes path attributes to determine which route is installed as the best path in the BGP routing table. Each path carries various attributes that are used in BGP best path analysis. Cisco IOS software provides the ability to influence BGP path selection by altering these attributes in the command-line interface (CLI). BGP path selection can also be influenced through standard BGP policy configuration.

BGP can include path attribute information in update messages. BGP attributes describe the characteristic of the route, and the software uses these attributes to help make decisions about which routes to advertise. Some of this attribute information can be configured at a BGP-speaking networking device. There are some mandatory attributes that are always included in the update message and some discretionary attributes. The following BGP attributes can be configured:

- AS-path
- Community
- Local\_Pref
- Multi\_Exit\_Discriminator (MED)
- Origin

### AS-path

This attribute contains a list or set of the autonomous system numbers through which routing information has passed. The BGP speaker adds its own autonomous system number to the list when it forwards the update message to external peers.

### Community

BGP communities are used to group networking devices that share common properties, regardless of network, autonomous system, or any physical boundaries. In large networks applying a common routing policy through prefix lists or access lists requires individual peer statements on each networking device. Using the BGP community attribute BGP speakers, with common routing policies, can implement inbound or outbound route filters based on the community tag rather than consult large lists of individual permit or deny statements.

### Local\_Pref

Within an autonomous system the Local\_Pref attribute is included in all update messages between BGP peers. If there are several paths to the same destination the local preference attribute with the highest value indicates the preferred outbound path from the local autonomous system. The highest ranking route is advertised to internal peers. The Local\_Pref value is not forwarded to external peers.

### Multi\_Exit\_Discriminator

The MED attribute indicates (to an external peer) a preferred path into an autonomous system. If there are multiple entry points into an autonomous system, the MED can be used to influence another autonomous system to choose one particular entry point. A metric is assigned where a lower MED metric is preferred by the software over a higher MED metric. The MED metric is exchanged between autonomous systems, but after a MED is forwarded into an autonomous system the MED metric is reset to the default value of 0. When an update is sent to an internal BGP (iBGP) peer, the MED is passed along without any change, allowing all the peers in the same autonomous system to make a consistent path selection.

By default a router will compare the MED attribute for paths only from BGP peers that reside in the same autonomous system. The **bgp always-compare-med** command can be configured to allow the router to compare metrics from peers in different autonomous systems.



#### Note

The Internet Engineering Task Force (IETF) decision regarding BGP MED assigns a value of infinity to the missing MED, making the route lacking the MED variable the least preferred. The default behavior of BGP routers running Cisco IOS software is to treat routes without the MED attribute as having a MED of 0, making the route lacking the MED variable the most preferred. To configure the router to conform to the IETF standard, use the **bgp bestpath med missing-as-worst** router configuration command.

### Origin

This attribute indicates how the route was included in a BGP routing table. Using Cisco IOS software a route defined using the BGP **network** command is given an origin code of Interior Gateway Protocol (IGP). Routes distributed from an Exterior Gateway Protocol (EGP) are coded with an origin of EGP, and routes redistributed from other protocols are defined as Incomplete. BGP decision policy for origin prefers IGP over EGP, then EGP over Incomplete.

## BGP Multipath Support

When a BGP speaker learns two identical eBGP paths for a prefix from a neighboring autonomous system, it will choose the path with the lowest route ID as the best path. This best path is installed in the IP routing table. If BGP multipath support is enabled and the eBGP paths are learned from the same neighboring autonomous system, instead of one best path being picked, multiple paths are installed in the IP routing table.

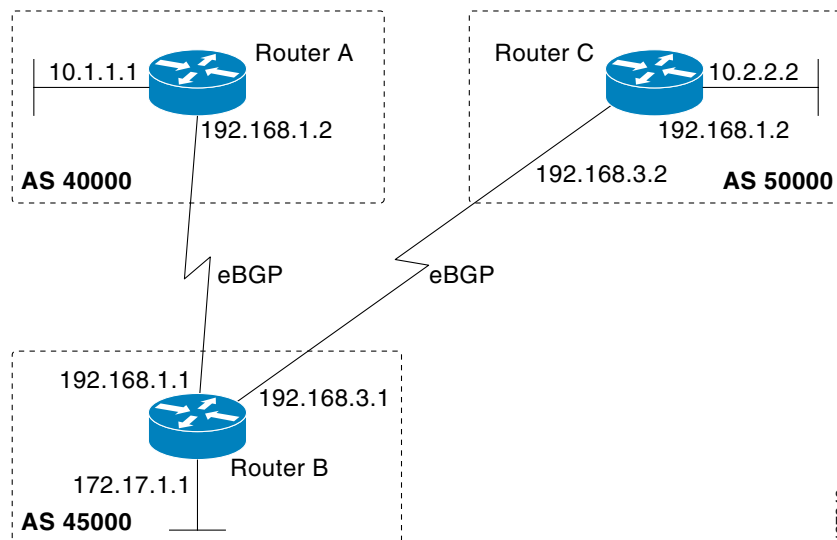
During packet switching, depending on the switching mode, either per-packet or per-destination load balancing is performed among the multiple paths. A maximum of six paths is supported. The **maximum-paths** command controls the number of paths allowed. By default, BGP will install only one path to the IP routing table.

## Multihoming

Multihoming is defined as connecting an autonomous system with more than one service provider. If you have any reliability issues with one service provider, then you have a backup connection. Performance issues can also be addressed by multihoming because better paths to the destination network can be utilized.

Unless you are a service provider, you must plan your routing configuration carefully to avoid Internet traffic traveling through your autonomous system and consuming all your bandwidth. Figure 10 shows that autonomous system 45000 is multihomed to autonomous system 40000 and autonomous system 50000. Assuming autonomous system 45000 is not a service provider, then several techniques such as load balancing or some form of routing policy must be configured to allow traffic from autonomous system 45000 to reach either autonomous system 40000 or autonomous system 50000 but not allow much, if any, transit traffic.

**Figure 10**      **Multihoming Topology**



## Transit Versus Nontransit Traffic

Most of the traffic within an autonomous system contains a source or destination IP address residing within the autonomous system, and this traffic is referred to as nontransit (or local) traffic. Other traffic is defined as transit traffic. As traffic across the Internet increases, controlling transit traffic becomes more important.

A service provider is considered to be a transit autonomous system and must provide connectivity to all other transit providers. In reality, few service providers actually have enough bandwidth to allow all transit traffic, and most service providers have to purchase such connectivity from Tier 1 service providers.

An autonomous system that does not usually allow transit traffic is called a stub autonomous system and will link to the Internet through one service provider.

## BGP Policy Configuration

BGP policy configuration is used to control prefix processing by the BGP routing process and to filter routes from inbound and outbound advertisements. Prefix processing can be controlled by adjusting BGP timers, altering how BGP handles path attributes, limiting the number of prefixes that the routing process will accept, and configuring BGP prefix dampening. Prefixes in inbound and outbound advertisements are filtered using route maps, filter lists, IP prefix lists, autonomous-system-path access lists, IP policy lists, and distribute lists. [Table 8](#) shows the processing order of BGP policy filters.

**Table 8** *BGP Policy Processing Order*

Inbound	Outbound
Route map	Distribute list
Filter list, AS-path access list, or IP policy	IP prefix list
IP prefix list	Filter list, AS-path access list, or IP policy
Distribute list	Route map



**Note**

In Cisco IOS Releases 12.0(22)S, 12.2(15)T, and 12.2(18)S and later releases the maximum number of autonomous system access lists that can be configured with the **ip as-path access-list** command is increased from 199 to 500.

Whenever there is a change in the routing policy due to a configuration change, BGP peering sessions must be reset using the **clear ip bgp** command. Cisco IOS software supports the following three mechanisms to reset BGP peering sessions:

- Hard reset—A hard reset tears down the specified peering sessions, including the TCP connection, and deletes routes coming from the specified peer.
- Soft reset—A soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reset uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply a new BGP policy without disrupting the network. Soft reset can be configured for inbound or outbound sessions.
- Dynamic inbound soft reset—The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for nondisruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh must first be advertised through BGP capability negotiation between peers. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

## BGP Communities

BGP communities are used to group routes (also referred to as color routes) that share common properties, regardless of network, autonomous system, or any physical boundaries. In large networks applying a common routing policy through prefix-lists or access-lists requires individual peer statements

on each networking device. Using the BGP community attribute BGP speakers, with common routing policies, can implement inbound or outbound route filters based on the community tag rather than consult large lists of individual permit or deny statements.

Standard community lists are used to configure well-known communities and specific community numbers. Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes.

The community attribute is optional, which means that it will not be passed on by networking devices that do not understand communities. Networking devices that understand communities must be configured to handle the communities or they will be discarded.

There are four predefined communities:

- no-export—Do not advertise to external BGP peers.
- no-advertise—Do not advertise this route to any peer.
- internet—Advertise this route to the Internet community; all BGP-speaking networking devices belong to it.
- local-as—Do not send outside the local autonomous system.

In Cisco IOS Release 12.2(8)T BGP named community lists were introduced. BGP named community lists allow meaningful names to be assigned to community lists with no limit on the number of community lists that can be configured. A named community list can be configured with regular expressions and with numbered community lists. All the rules of numbered communities apply to named community lists except that there is no limitation on the number of named community lists that can be configured.



#### Note

Both standard and expanded community lists have a limitation of 100 community groups that can be configured within each type of list. A named community list does not have this limitation.

## Extended Communities

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding (VRF) instances and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). All of the standard rules of access lists apply to the configuration of extended community lists. Regular expressions are supported by the expanded range of extended community list numbers. All regular expression configuration options are supported. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists.

### Route Target Extended Community Attribute

The RT extended community attribute is configured with the **rt** keyword of the **ip extcommunity-list** command. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended community attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

### Site of Origin Extended Community Attribute

The SOO extended community attribute is configured with the **soo** keyword of the **ip extcommunity-list** command. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended



community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO extended community attribute can be applied to routes that are learned from VRFs. The SOO extended community attribute should not be configured for stub sites or sites that are not multihomed.

### IP Extended Community-List Configuration Mode

Named and numbered extended community lists can be configured in IP extended community-list configuration mode. The IP extended community-list configuration mode supports all of the functions that are available in global configuration mode. In addition, the following operations can be performed:

- Configure sequence numbers for extended community list entries
- Resequence existing sequence numbers for extended community list entries
- Configure an extended community list to use default values

### Default Sequence Numbering

Extended community list entries start with the number 10 and increment by 10 for each subsequent entry when no sequence number is specified, when default behavior is configured, and when an extended community list is resequenced without specifying the first entry number or the increment range for subsequent entries.

### Resequencing Extended Community Lists

Extended community-list entries are sequenced and resequenced on a per-extended community list basis. The **resequence** command can be used without any arguments to set all entries in a list to default sequence numbering. The **resequence** command also allows the sequence number of the first entry and increment range to be set for each subsequent entry. The range of configurable sequence numbers is from 1 to 2147483647.

## Administrative Distance

Administrative distance is a measure of the preference of different routing protocols. BGP has a **distance bgp** command that allows you to set different administrative distances for three route types: external, internal, and local. BGP, like other protocols, prefers the route with the lowest administrative distance.

## BGP Route Map Policy Lists

BGP route map policy lists allow a network operator to group route map match clauses into named lists called policy lists. A policy list functions like a macro. When a policy list is referenced in a route map, all of the match clauses are evaluated and processed as if they had been configured directly in the route map. This enhancement simplifies the configuration of BGP routing policy in medium-size and large networks because a network operator can preconfigure policy lists with groups of match clauses and then reference these policy lists within different route maps. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.

A policy lists functions like a macro when it is configured in a route map and has the following capabilities and characteristics:

- When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed.
- Two or more policy lists can be configured with a route map. Policy lists can be configured within a route map to be evaluated with AND or OR semantics.

- Policy lists can coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy lists.
- When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

Policy lists support only match clauses and do not support set clauses. Policy lists can be configured for all applications of route maps, including redistribution, and can also coexist, within the same route map entry, with match and set clauses that are configured separately from the policy lists.

**Note**

Policy lists are supported only by BGP and are not supported by other IP routing protocols.

## How to Connect to a Service Provider Using External BGP

This section contains the following tasks:

- [Influencing Inbound Path Selection, page 108](#)
- [Influencing Outbound Path Selection, page 116](#)
- [Configuring BGP Peering with ISPs, page 122](#)
- [Configuring BGP Policies, page 134](#)

### Influencing Inbound Path Selection

BGP can be used to influence the choice of paths in another autonomous system. There may be several reasons for wanting BGP to choose a path that is not the obvious best route, for example, to avoid some types of transit traffic passing through an autonomous system or perhaps to avoid a very slow or congested link. BGP can influence inbound path selection using one of the following BGP attributes:

- AS-path
- MED

Perform one of the following tasks to influence inbound path selection:

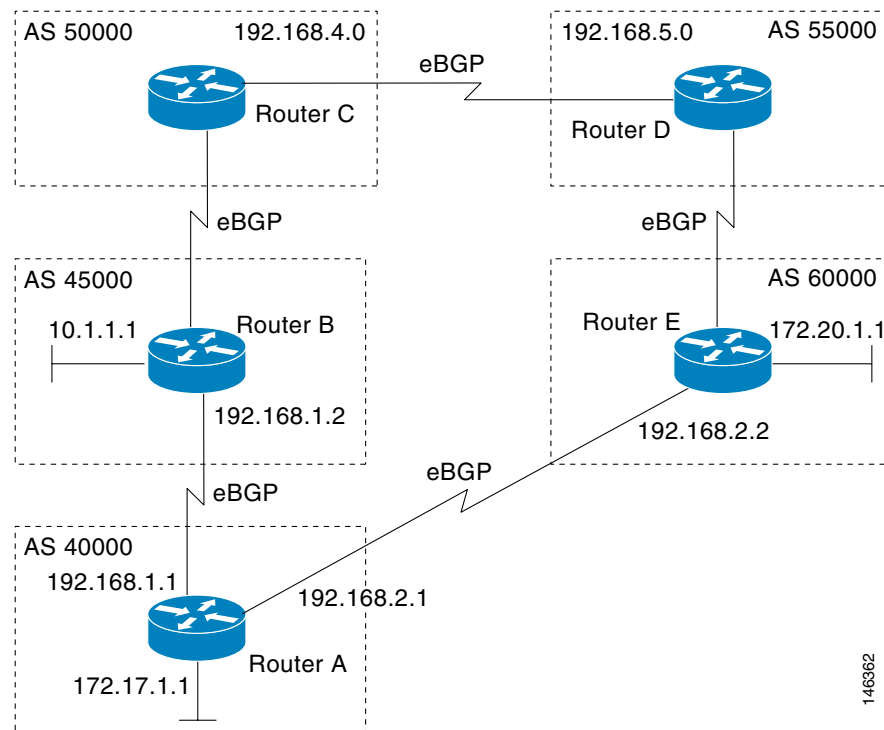
- [Influencing Inbound Path Selection by Modifying the AS-path Attribute, page 108](#)
- [Influencing Inbound Path Selection by Setting the MED Attribute, page 112](#)

### Influencing Inbound Path Selection by Modifying the AS-path Attribute

One of the methods that BGP can use to influence the choice of paths in another autonomous system is to modify the AS-path attribute. For example, in [Figure 11](#), Router A advertises its own network, 172.17.1.0, to its BGP peers in autonomous system 45000 and autonomous system 60000. When the routing information is propagated to autonomous system 50000, the routers in autonomous system 50000 have network reachability information about network 172.17.1.0 from two different routes. The first route is from autonomous system 45000 with an AS-path consisting of 45000, 40000, the second route is through autonomous system 55000 with an AS-path of 55000, 60000, 40000. If all other BGP attribute values are the same, Router C in autonomous system 50000 would choose the route through autonomous system 45000 for traffic destined for network 172.17.1.0 because it is the shortest route in terms of autonomous systems traversed.

Autonomous system 40000 now receives all traffic from autonomous system 50000 for the 172.17.1.0 network through autonomous system 45000. If, however, the link between autonomous system 45000 and autonomous system 40000 is a really slow and congested link, the **set as-path prepend** command can be used at Router A to influence inbound path selection for the 172.17.1.0 network by making the route through autonomous system 45000 appear to be longer than the path through autonomous system 60000. The configuration is done at Router A in [Figure 11](#) by applying a route map to the outbound BGP updates to Router B. Using the **set as-path prepend** command, all the outbound BGP updates from Router A to Router B will have their AS-path attribute modified to add the local autonomous system number 40000 twice. After the configuration, autonomous system 50000 receives updates about 172.17.1 network through autonomous system 45000. The new AS-path is 45000, 40000, 40000, and 40000, which is now longer than the AS-path from autonomous system 55000 (unchanged at a value of 55000, 60000, 40000). Networking devices in autonomous system 50000 will now prefer the route through autonomous system 55000 to forward packets with a destination address in the 172.17.1.0 network.

**Figure 11** Network Topology for Modifying the AS-path Attribute



Perform this task to influence the inbound path selection by modifying the AS-path attribute. The configuration is performed at Router A in [Figure 11](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [*unicast* | *multicast* | *vrf vrf-name*]
5. **network** *network-number* [*mask network-mask*] [**route-map** *route-map-name*]

6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
9. **exit**
10. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
11. **set as-path** {*tag* | **prepend** *as-path-string*}
12. **end**
13. **show running-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode for the specified routing process.
Step 4	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 5	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>

	Command or Action	Purpose
Step 6	<b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 remote-as 45000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>In this example, the BGP peer on Router B at 192.168.1.2 is added to the IPv4 multiprotocol BGP neighbor table and will receive BGP updates.</li> </ul>
Step 7	<b>neighbor</b> {ip-address   peer-group-name} <b>route-map</b> map-name {in   out}  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 route-map PREPEND out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named PREPEND is applied to outbound routes to Router B.</li> </ul>
Step 8	<b>neighbor</b> {ip-address   peer-group-name} <b>activate</b>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 activate	Enables address exchange for address family IPv4 unicast for the BGP neighbor at 192.168.1.2 on Router B.
Step 9	<b>exit</b>  <b>Example:</b> Router(config-router-af)# exit	Exits address family configuration mode and enters global configuration mode.
Step 10	<b>route-map</b> map-name [permit   deny] [sequence-number]  <b>Example:</b> Router(config)# route-map PREPEND permit 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named PREPEND is created and if there is a subsequent matching of criteria.</li> </ul>
Step 11	<b>set as-path</b> {tag   prepend as-path-string}  <b>Example:</b> Router(config-route-map)# set as-path prepend 40000 40000	Modifies an autonomous system path for BGP routes. <ul style="list-style-type: none"> <li>Use the <b>prepend</b> keyword to "prepend" an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.</li> <li>In this example, two additional autonomous system entries are added to the autonomous system path for outbound routes to Router B.</li> </ul>
Step 12	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 13	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration file.

## Examples

The following partial output of the **show running-config** command shows the configuration from this task.

### Router A:

```
Router# show running-config

!
router bgp 40000
 neighbor 192.168.1.2 remote-as 60000
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 route-map PREPEND out
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 !
 route-map PREPEND permit 10
  set as-path prepend 40000 40000
 .
 .
 .
```

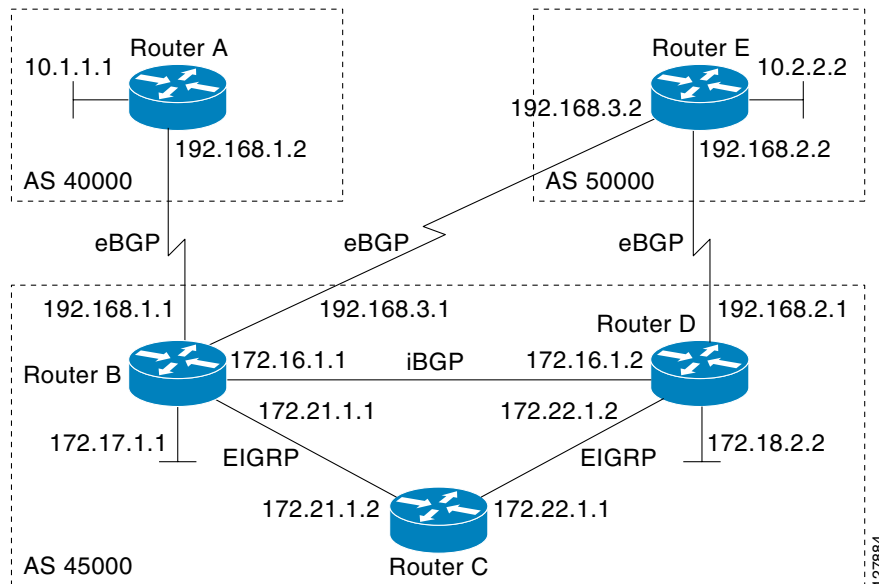
## What To Do Next

In this task the configuration advertises only one network, 172.17.1.0, and it will prepend the extra autonomous system paths to all BGP updates. In your network you may need to advertise multiple networks but only prepend the autonomous system paths to BGP updates about one specific network. For a configuration example that uses an access list to specify that extra autonomous system paths are prepended to one specific network, see the first configuration example in the [“Influencing Inbound Path Selection: Examples”](#) section on page 154.

## Influencing Inbound Path Selection by Setting the MED Attribute

One of the methods that BGP can use to influence the choice of paths into another autonomous system is to set the MED attribute. The MED attribute indicates (to an external peer) a preferred path to an autonomous system. If there are multiple entry points to an autonomous system, the MED can be used to influence another autonomous system to choose one particular entry point. A metric is assigned using route maps where a lower MED metric is preferred by the software over a higher MED metric.

Perform this task to influence inbound path selection by setting the MED metric attribute. The configuration is performed at Router B and Router D in [Figure 12](#). Router B advertises the network 172.16.1.0. to its BGP peer, Router E in autonomous system 50000. Using a simple route map Router B sets the MED metric to 50 for outbound updates. The task is repeated at Router D but the MED metric is set to 120. When Router E receives the updates from both Router B and Router D the MED metric is stored in the BGP routing table. Before forwarding packets to network 172.16.1.0, Router E compares the attributes from peers in the same autonomous system (both Router B and Router D are in autonomous system 45000). The MED metric for Router B is less than the MED for Router D, so Router E will forward the packets through Router B.

**Figure 12** Network Topology for Setting the MED Attribute

Use the **bgp always-compare-med** command to compare MED attributes from peers in other autonomous systems.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [*unicast* | *multicast* | *vrf vrf-name*]
6. **network** *network-number* [*mask network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {*in* | *out*}
8. **exit**
9. **route-map** *map-name* [*permit* | *deny*] [*sequence-number*]
10. **set metric** *value*
11. **end**
12. Repeat Step 1 through Step 11 at Router D.
13. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 5	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router-af)# network 172.16.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 route-map MED out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named MED is applied to outbound routes to the BGP peer at Router E.</li> </ul>



	Command or Action	Purpose
Step 8	<b>exit</b>  <b>Example:</b> Router(config-router-af)# exit	Exits address family configuration mode and enters router configuration mode. <ul style="list-style-type: none"><li>Repeat this step to exit to global configuration mode.</li></ul>
Step 9	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map MED permit 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"><li>In this example, a route map named MED is created.</li></ul>
Step 10	<b>set metric</b> <i>value</i>  <b>Example:</b> Router(config-route-map)# set metric 50	Sets the MED metric value.
Step 11	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 12	Repeat <a href="#">Step 1</a> through <a href="#">Step 11</a> at Router D.	—
Step 13	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp 172.17.1.0 255.255.255.0	(Optional) Displays the entries in the BGP routing table. <ul style="list-style-type: none"><li>Use this command at Router E in <a href="#">Figure 12</a> when both Router B and Router D have configured the MED attribute.</li><li>Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</li></ul>

## Examples

The following output is from Router E in [Figure 12](#) after this task has been performed at both Router B and Router D. Note the metric (MED) values for the two routes to network 172.16.1.0. The peer 192.168.2.1 at Router D has a metric of 120 for the path to network 172.16.1.0 whereas the peer 192.168.3.1 at Router B has a metric of 50. The entry for the peer 192.168.3.1 at Router B has the word **best** at the end of the entry to show that Router E will choose to send packets destined for network 172.16.1.0 via Router B because the MED metric is lower.

```
Router# show ip bgp 172.16.1.0
```

```
BGP routing table entry for 172.16.1.0/24, version 10
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  45000
    192.168.2.1 from 192.168.2.1 (192.168.2.1)
      Origin IGP, metric 120, localpref 100, valid, external
  45000
    192.168.3.1 from 192.168.3.1 (172.17.1.99)
      Origin IGP, metric 50, localpref 100, valid, external, best
```

## Influencing Outbound Path Selection

BGP can be used to influence the choice of paths for outbound traffic from the local autonomous system. This section contains two methods that BGP can use to influence inbound path selection:

- Using the Local\_Pref attribute
- Using the BGP outbound route filter (ORF) capability

Perform one of the following tasks to influence outbound path selection:

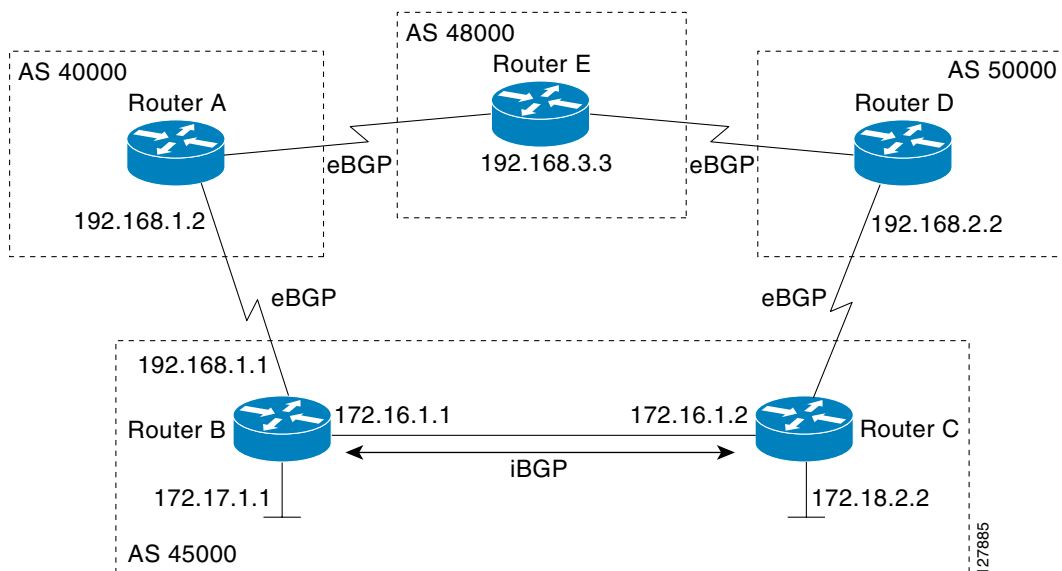
- [Influencing Outbound Path Selection Using the Local\\_Pref Attribute, page 116](#)
- [Filtering Outbound BGP Route Prefixes, page 119](#)

### Influencing Outbound Path Selection Using the Local\_Pref Attribute

One of the methods to influence outbound path selection is to use the BGP Local-Pref attribute. Perform this task using the local preference attribute to influence outbound path selection. If there are several paths to the same destination the local preference attribute with the highest value indicates the preferred path.

Refer to [Figure 13](#) for the network topology used in this task. Both Router B and Router C are configured. autonomous system 45000 receives updates for network 192.168.3.0 via autonomous system 40000 and autonomous system 50000. Router B is configured to set the local preference value to 150 for all updates to autonomous system 40000. Router C is configured to set the local preference value for all updates to autonomous system 50000 to 200. After the configuration, local preference information is exchanged within autonomous system 45000. Router B and Router C now see that updates for network 192.168.3.0 have a higher preference value from autonomous system 50000 so all traffic in autonomous system 45000 with a destination network of 192.168.3.0 is sent out via Router C.

**Figure 13** Network Topology for Outbound Path Selection



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **bgp default local-preference** *value*
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
9. **end**
10. Repeat [Step 1](#) through [Step 9](#) at Router C.
11. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>

	Command or Action	Purpose
Step 5	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 7	<b>bgp default local-preference</b> <i>value</i>  <b>Example:</b> Router(config-router-af)# bgp default local-preference 150	Changes the default local preference value. <ul style="list-style-type: none"> <li>In this example, the local preference is changed to 150 for all updates from autonomous system 40000 to autonomous system 45000.</li> <li>By default, the local preference value is 100.</li> </ul>
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 activate	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 9	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 10	Repeat Step 1 through Step 9 at Router C but change the IP address of the peer, the autonomous system number, and set the local preference value to 200.	—
Step 11	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp 192.168.3.0 255.255.255.0	Displays the entries in the BGP routing table. <ul style="list-style-type: none"> <li>Enter this command at both Router B and Router C and note the Local_Pref value. The route with the highest preference value will be the preferred route to network 192.168.3.0.</li> </ul> <p><b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</p>

## Filtering Outbound BGP Route Prefixes

Perform this task to use BGP prefix-based outbound route filtering to influence outbound path selection.

### BGP Prefix-Based Outbound Route Filtering

BGP prefix-based outbound route filtering uses the BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring BGP ORF can help reduce the amount of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, BGP ORF can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.

The BGP prefix-based outbound route filtering is enabled through the advertisement of ORF capabilities to peer routers. The advertisement of the ORF capability indicates that a BGP peer will accept a prefix list from a neighbor and apply the prefix list to locally configured ORFs (if any exist). When this capability is enabled, the BGP speaker can install the inbound prefix list filter to the remote peer as an outbound filter, which reduces unwanted routing updates.

The BGP prefix-based outbound route filtering can be configured with send or receive ORF capabilities. The local peer advertises the ORF capability in send mode. The remote peer receives the ORF capability in receive mode and applies the filter as an outbound policy. The local and remote peers exchange updates to maintain the ORF on each router. Updates are exchanged between peer routers by address family depending on the ORF prefix list capability that is advertised. The remote peer starts sending updates to the local peer after a route refresh has been requested with the **clear ip bgp in prefix-filter** command or after an ORF prefix list with immediate status is processed. The BGP peer will continue to apply the inbound prefix list to received updates after the local peer pushes the inbound prefix list to the remote peer.

### Prerequisites

BGP peering sessions must be established, and BGP ORF capabilities must be enabled on each participating router before prefix-based ORF announcements can be received.

### Restrictions

- BGP prefix-based outbound route filtering does not support multicast.
- IP addresses that are used for outbound route filtering must be defined in an IP prefix list. BGP distribute lists and IP access lists are not supported.
- Outbound route filtering is configured on only a per-address family basis and cannot be configured under the general session or BGP routing process.
- Outbound route filtering is configured for external peering sessions only.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] [**deny** *network/length* | **permit** *network/length*] [**ge** *ge-value*] [**le** *le-value*]
4. **router bgp** *autonomous-system-number*
5. **address-family** **ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]

6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **ebgp-multihop** [*hop-count*]
8. **neighbor** *ip-address* **capability orf prefix-list** [*send* | *receive* | *both*]
9. **end**
10. **clear ip bgp** {*ip-address* | \*} **in prefix-filter**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip prefix-list</b> <i>list-name</i> [ <b>seq</b> <i>seq-value</i> ] { <b>deny</b> <i>network/length</i>   <b>permit</b> <i>network/length</i> } [ <b>ge</b> <i>ge-value</i> ] [ <b>le</b> <i>le-value</i> ]  <b>Example:</b> Router(config)# ip prefix-list FILTER seq 10 permit 192.168.1.0/24	Creates a prefix list for prefix-based outbound route filtering. <ul style="list-style-type: none"> <li>Outbound route filtering supports prefix length matching, wildcard-based prefix matching, and exact address prefix matching on a per address-family basis.</li> <li>The prefix list is created to define the outbound route filter. The filter must be created when the outbound route filtering capability is configured to be advertised in send mode or both mode. It is not required when a peer is configured to advertise receive mode only.</li> <li>The example creates a prefix list named FILTER that defines the 192.168.1.0/24 subnet for outbound route filtering.</li> </ul>
Step 4	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 100	Enters router configuration mode, and creates a BGP routing process.

	Command or Action	Purpose
Step 5	<p><b>address-family ipv4</b> [<b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b> Router(config-router)# address-family ipv4 unicast</p>	<p>Specifies the IPv4 address family and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> <p><b>Note</b> Outbound route filtering is configured on a per-address family basis.</p>
Step 6	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>} <b>remote-as</b> <i>autonomous-system-number</i></p> <p><b>Example:</b> Router(config-router-af)# neighbor 10.1.1.1 remote-as 200</p>	<p>Establishes peering with the specified neighbor or peer group. BGP peering must be established before ORF capabilities can be exchanged.</p> <ul style="list-style-type: none"> <li>The example establishes peering with the 10.1.1.1 neighbor.</li> </ul>
Step 7	<p><b>neighbor ip-address ebgp-multihop</b> [<i>hop-count</i>]</p> <p><b>Example:</b> Router(config-router-af)# neighbor 10.1.1.1 ebgp-multihop</p>	<p>Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.</p>
Step 8	<p><b>neighbor ip-address capability orf prefix-list</b> [<b>send</b>   <b>receive</b>   <b>both</b>]</p> <p><b>Example:</b> Router(config-router-af)# neighbor 10.1.1.1 capability orf prefix-list both</p>	<p>Enables the ORF capability on the local router, and enables ORF capability advertisement to the BGP peer specified with the <i>ip-address</i> argument.</p> <ul style="list-style-type: none"> <li>The <b>send</b> keyword configures a router to advertise ORF send capabilities.</li> <li>The <b>receive</b> keyword configures a router to advertise ORF receive capabilities.</li> <li>The <b>both</b> keyword configures a router to advertise send and receive capabilities.</li> <li>The remote peer must be configured to either send or receive ORF capabilities before outbound route filtering is enabled.</li> <li>The example configures the router to advertise send and receive capabilities to the 10.1.1.1 neighbor.</li> </ul>

	Command or Action	Purpose
Step 9	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode, and enters privileged EXEC mode.
Step 10	<b>clear ip bgp {ip-address   *} in prefix-filter</b>  <b>Example:</b> Router# clear ip bgp 192.168.1.2 in prefix-filter	(Optional) Clears BGP outbound route filters and initiates an inbound soft reset. A single neighbor or all neighbors can be specified.

## Configuring BGP Peering with ISPs

BGP was developed as an interdomain routing protocol and connecting to ISPs is one of the main functions of BGP. Depending on the size of your network and the purpose of your business, there are many different ways to connect to your ISP. Multihoming to one or more ISPs provides redundancy in case an external link to an ISP fails. This section introduces some optional tasks that can be used to connect to a service provider using multihoming techniques. Smaller companies may use just one ISP but require a backup route to the ISP. Larger companies may have access to two ISPs, using one of the connections as a backup, or may need to configure a transit autonomous system.

Perform one of the following optional tasks to connect to one or more ISPs:

- [Configuring Multihoming with Two ISPs, page 122](#)
- [Multihoming with a Single ISP, page 126](#)
- [Configuring Multihoming to Receive the Full Internet Routing Table, page 131](#)

## Configuring Multihoming with Two ISPs

Perform this task to configure your network to access two ISPs, where one ISP is the preferred route and the second ISP is a backup route. In [Figure 14](#) Router B in autonomous system 45000 has BGP peers in two ISPs, autonomous system 40000 and autonomous system 50000. Using this task, Router B will be configured to prefer the route to the BGP peer at Router A in autonomous system 40000.

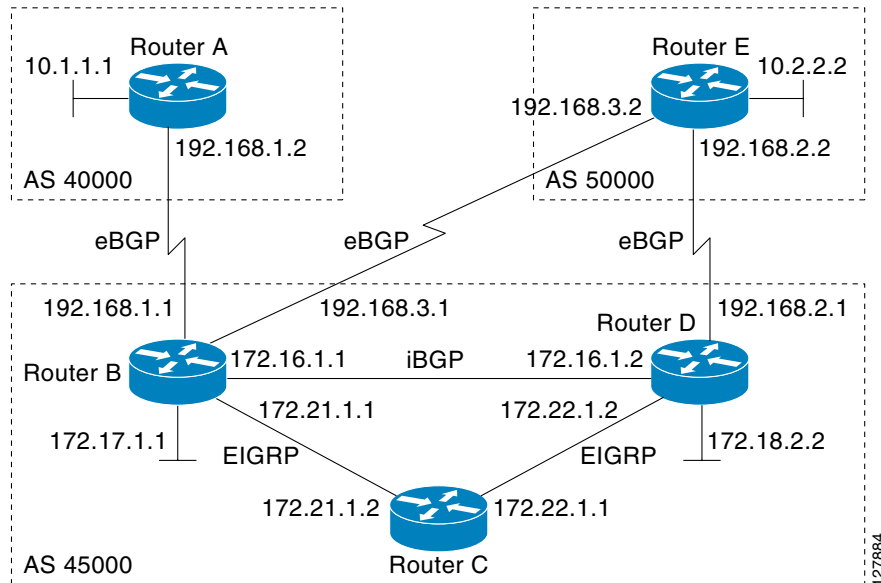
All routes learned from this neighbor will have an assigned weight. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.



### Note

The weights assigned with the **set weight** route-map configuration command override the weights assigned using the **neighbor weight** command.



**Figure 14**      **Multihoming with Two ISPs****SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [*unicast* | *multicast* | *vrf vrf-name*]
5. **network** *network-number* [**mask** *network-mask*]
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **weight** *number*
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
9. **neighbor** {*ip-address* | *peer-group-name*} **weight** *number*
10. **end**
11. **clear ip bgp** [*\** | *ip-address* | *peer-group-name*] [**soft** [*in* | *out*]]
12. **show ip bgp** [*network-address*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode, and creates a BGP routing process.
Step 4	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 5	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]  <b>Example:</b> Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>weight</b> <i>number</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 weight 150	Assigns a weight to a BGP peer connection. <ul style="list-style-type: none"> <li>In this example, the weight attribute for routes received from the BGP peer 192.168.1.2 is set to 150.</li> </ul>

	Command or Action	Purpose
Step 8	<b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 9	<b>neighbor</b> {ip-address   peer-group-name} <b>weight</b> number  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 weight 100	Assigns a weight to a BGP peer connection. <ul style="list-style-type: none"> <li>In this example, the weight attribute for routes received from the BGP peer 192.168.3.2 is set to 100.</li> </ul>
Step 10	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode and enters privileged EXEC mode.
Step 11	<b>clear ip bgp</b> { *   ip-address   peer-group-name } [soft [in   out]]  <b>Example:</b> Router# clear ip bgp *	(Optional) Clears BGP outbound route filters and initiates an outbound soft reset. A single neighbor or all neighbors can be specified.
Step 12	<b>show ip bgp</b> [network] [network-mask]  <b>Example:</b> Router# show ip bgp	Displays the entries in the BGP routing table. <ul style="list-style-type: none"> <li>Enter this command at Router B to see the weight attribute for each route to a BGP peer. The route with the highest weight attribute will be the preferred route to network 172.17.1.0.</li> </ul> <p><b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</p>

## Examples

The following example shows the BGP routing table at Router B with the weight attributes assigned to routes. The route through 192.168.3.2 (Router E in [Figure 14](#)) has the highest weight attribute and will be the preferred route to network 172.17.1.0.

```
BGP table version is 8, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.1.1.0/24	192.168.1.2	0		100	40000 i
*> 10.2.2.0/24	192.168.3.2	0		150	50000 i
*> 172.17.1.0/24	0.0.0.0	0		32768	i

## Multihoming with a Single ISP

Perform this task to configure your network to access one of two connections to a single ISP, where one of the connections is the preferred route and the second connection is a backup route. In [Figure 14](#) Router E in autonomous system 50000 has two BGP peers in a single autonomous system, autonomous system 45000. Using this task, autonomous system 50000 does not learn any routes from autonomous system 45000 and is sending its own routes using BGP. This task is configured at Router E in [Figure 14](#) and covers three features about multihoming to a single ISP:

- Outbound traffic—Router E will forward default routes and traffic to autonomous system 45000 with Router B as the primary link and Router D as the backup link. Static routes are configured to both Router B and Router D with a lower distance configured for the link to Router B.
- Inbound traffic—Inbound traffic from autonomous system 45000 is configured to be sent from Router B unless the link fails when the backup route is to send traffic from Router D. To achieve this, outbound filters are set using the MED metric.
- Prevention of transit traffic—A route map is configured at Router E in autonomous system 50000 to block all incoming BGP routing updates to prevent autonomous system 50000 from receiving transit traffic from the ISP in autonomous system 45000.

### MED Attribute

Configuring the MED attribute is another method that BGP can use to influence the choice of paths into another autonomous system. The MED attribute indicates (to an external peer) a preferred path into an autonomous system. If there are multiple entry points into an autonomous system, the MED can be used to influence another autonomous system to choose one particular entry point. A metric is assigned using route maps where a lower MED metric is preferred by the software over a higher MED metric.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. Repeat Step 7 to apply another route map to the neighbor specified in Step 7.
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
10. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
11. Repeat Step 10 to apply another route map to the neighbor specified in Step 10.
12. **exit**
13. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track** *number*] [**tag** *tag*]
14. Repeat Step 13 to configure another route map.
15. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
16. **set metric** *value*

17. **exit**
18. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
19. **set metric** *value*
20. **exit**
21. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
22. **end**
23. **show ip route** [*ip-address*] [*mask*] [**longer-prefixes**]
24. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] [ <b>route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Router(config-router)# network 10.2.2.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 5	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>

	Command or Action	Purpose
Step 6	<b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router-af)# neighbor 192.168.2.1 remote-as 45000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>In this example, the BGP peer at Router D is added to the BGP routing table.</li> </ul>
Step 7	<b>neighbor</b> {ip-address   peer-group-name} <b>route-map</b> map-name {in   out}  <b>Example:</b> Router(config-router-af)# neighbor 192.168.2.1 route-map BLOCK in and  <b>Example:</b> Router(config-router-af)# neighbor 192.168.2.1 route-map SETMETRIC1 out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In the first example, the route map named BLOCK is applied to inbound routes at Router E.</li> <li>In the second example, the route map named SETMETRIC1 is applied to outbound routes to Router D.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p>
Step 8	Repeat Step 7 to apply another route map to the neighbor specified in Step 7.	—
Step 9	<b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.1 remote-as 45000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>In this example, the BGP peer at Router D is added to the BGP routing table.</li> </ul>
Step 10	<b>neighbor</b> {ip-address   peer-group-name} <b>route-map</b> map-name {in   out}  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.1 route-map BLOCK in and  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.1 route-map SETMETRIC2 out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In the first example, the route map named BLOCK is applied to inbound routes at Router E.</li> <li>In the second example, the route map named SETMETRIC2 is applied to outbound routes to Router D.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p>
Step 11	Repeat Step 10 to apply another route map to the neighbor specified in Step 10.	—
Step 12	<b>exit</b>  <b>Example:</b> Router(config-router-af)# exit	Exits address family configuration mode and enters router configuration mode. <ul style="list-style-type: none"> <li>Repeat this command to exit router configuration mode and enter global configuration mode.</li> </ul>

	Command or Action	Purpose
Step 13	<p><b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]}</i> [<i>distance</i>] [<i>name</i>] [<b>permanent</b>   <b>track number</b>] [<b>tag tag</b>]</p> <p><b>Example:</b> Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 50</p> <p><b>Example:</b> Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1 50 and</p> <p><b>Example:</b> Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.3.1 40</p>	<p>Establishes a static route.</p> <ul style="list-style-type: none"> <li>In the first example, a static route to BGP peer 192.168.2.1 is established and given an administrative distance of 50.</li> <li>In the second example, a static route to BGP peer 192.168.3.1 is established and given an administrative distance of 40. The lower administrative distance makes this route via Router B the preferred route.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p>
Step 14	Repeat Step 13 to establish another static route.	—
Step 15	<p><b>route-map</b> <i>map-name</i> [<b>permit</b>   <b>deny</b>] [<i>sequence-number</i>]</p> <p><b>Example:</b> Router(config)# route-map SETMETRIC1 permit 10</p>	<p>Configures a route map and enters route map configuration mode.</p> <ul style="list-style-type: none"> <li>In this example, a route map named SETMETRIC1 is created.</li> </ul>
Step 16	<p><b>set metric</b> <i>value</i></p> <p><b>Example:</b> Router(config-route-map)# set metric 100</p>	Sets the MED metric value.
Step 17	<p><b>exit</b></p> <p><b>Example:</b> Router(config-route-map)# exit</p>	Exits route map configuration mode and enters global configuration mode.
Step 18	<p><b>route-map</b> <i>map-name</i> [<b>permit</b>   <b>deny</b>] [<i>sequence-number</i>]</p> <p><b>Example:</b> Router(config)# route-map SETMETRIC2 permit 10</p>	<p>Configures a route map and enters route map configuration mode.</p> <ul style="list-style-type: none"> <li>In this example, a route map named SETMETRIC2 is created.</li> </ul>
Step 19	<p><b>set metric</b> <i>value</i></p> <p><b>Example:</b> Router(config-route-map)# set metric 50</p>	Sets the MED metric value.
Step 20	<p><b>exit</b></p> <p><b>Example:</b> Router(config-route-map)# exit</p>	Exits route map configuration mode and enters global configuration mode.

	Command or Action	Purpose
<b>Step 21</b>	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] <i>[sequence-number]</i>  <b>Example:</b> Router(config)# route-map BLOCK deny 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named BLOCK is created to block all incoming routes from autonomous system 45000.</li> </ul>
<b>Step 22</b>	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
<b>Step 23</b>	<b>show ip route</b> [ <i>ip-address</i> ] [ <i>mask</i> ] <i>[longer-prefixes]</i>  <b>Example:</b> Router# show ip route	(Optional) Displays route information from the routing tables. <ul style="list-style-type: none"> <li>Use this command at Router E in <a href="#">Figure 14</a> after Router B and Router D have received update information containing the MED metric from Router E.</li> <li>Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</li> </ul>
<b>Step 24</b>	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp 172.17.1.0 255.255.255.0	(Optional) Displays the entries in the BGP routing table. <ul style="list-style-type: none"> <li>Use this command at Router E in <a href="#">Figure 14</a> after Router B and Router D have received update information containing the MED metric from Router E.</li> <li>Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</li> </ul>

## Examples

The following example shows output from the **show ip route** command entered at Router E after this task has been configured and Router B and Router D have received update information containing the MED metric. Note that the gateway of last resort is set as 192.168.3.1, which is the route to Router B.

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is 192.168.3.1 to network 0.0.0.0
```

```
    10.0.0.0/24 is subnetted, 1 subnets
C       10.2.2.0 is directly connected, Ethernet0/0
C       192.168.2.0/24 is directly connected, Serial3/0
C       192.168.3.0/24 is directly connected, Serial2/0
S*      0.0.0.0/0 [40/0] via 192.168.3.1
```



The following example shows output from the **show ip bgp** command entered at Router E after this task has been configured and Router B and Router D have received routing updates. The route map BLOCK has denied all routes coming in from autonomous system 45000 so the only network shown is the local network.

```
Router# show ip bgp
```

```
BGP table version is 2, local router ID is 10.2.2.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.2.2.0/24	0.0.0.0	0		32768	i

The following example shows output from the **show ip bgp** command entered at Router B after this task has been configured at Router E and Router B has received routing updates. Note the metric of 50 for network 10.2.2.0.

```
Router# show ip bgp
```

```
BGP table version is 7, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.1.1.0/24	192.168.1.2	0		0	40000 i
*> 10.2.2.0/24	192.168.3.2	50		0	50000 i
*> 172.16.1.0/24	0.0.0.0	0		32768	i
*> 172.17.1.0/24	0.0.0.0	0		32768	i

The following example shows output from the **show ip bgp** command entered at Router D after this task has been configured at Router E and Router D has received routing updates. Note the metric of 100 for network 10.2.2.0.

```
Router# show ip bgp
```

```
BGP table version is 3, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.2.2.0/24	192.168.2.2	100		0	50000 i
*> 172.16.1.0/24	0.0.0.0	0		32768	i

## Configuring Multihoming to Receive the Full Internet Routing Table

Perform this task to configure your network to build neighbor relationships with other routers in other autonomous systems while filtering outbound routes. In this task the full Internet routing table will be received from the service providers in the neighboring autonomous systems but only locally originated routes will be advertised to the service providers. This task is configured at Router B in [Figure 14](#) and uses an access list to permit only locally originated routes and a route map to ensure that only the locally originated routes are advertised outbound to other autonomous systems.

**Note**

Be aware that receiving the full Internet routing table from two ISPs may use all the memory in smaller routers.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
5. **network** *network-number* [**mask** *network-mask*]
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
9. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
10. **exit**
11. **ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression*
12. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
13. **match as-path** *path-list-number*
14. **end**
15. **show ip bgp** [*network*] [*network-mask*]

**DETAILED STEPS**

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.

	Command or Action	Purpose
Step 4	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 5	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]  <b>Example:</b> Router(config-router-af)# network 172.17.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>
Step 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router-af)# neighbor 192.168.1.2 route-map localonly out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named localonly is applied to outbound routes to Router A.</li> </ul>
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 9	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router-af)# neighbor 192.168.3.2 route-map localonly out	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named localonly is applied to outbound routes to Router E.</li> </ul>
Step 10	<b>exit</b>  <b>Example:</b> Router(config-router-af)# exit	Exits address family configuration mode and enters router configuration mode. <ul style="list-style-type: none"> <li>Repeat the <b>exit</b> command to enter global configuration mode.</li> </ul>

	Command or Action	Purpose
Step 11	<b>ip as-path access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>as-regular-expression</i>  <b>Example:</b> Router(config)# ip as-path access-list 10 permit ^\$	Defines a BGP-related access list. <ul style="list-style-type: none"> <li>In this example, the access list number 10 is defined to permit only locally originated BGP routes.</li> </ul>
Step 12	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map localonly permit 10	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named localonly is created.</li> </ul>
Step 13	<b>match as-path</b> <i>path-list-number</i>  <b>Example:</b> Router(config-route-map)# match as-path 10	Matches a BGP autonomous system path access list. <ul style="list-style-type: none"> <li>In this example, the BGP autonomous system path access list created in Step 11 is used for the match clause.</li> </ul>
Step 14	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 15	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> Router# show ip bgp	Displays the entries in the BGP routing table.  <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.

## Examples

The following example shows the BGP routing table for Router B in [Figure 14](#) after this task has been configured. Note that the routing table contains the information about the networks in the autonomous systems 40000 and 50000.

```
BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.1.1.0/24	192.168.1.2	0		0	40000 i
*> 10.2.2.0/24	192.168.3.2	0		0	50000 i
*> 172.17.1.0/24	0.0.0.0	0		32768	i

## Configuring BGP Policies

The tasks in this section help you configure BGP policies that filter the traffic in your BGP network. The following optional tasks demonstrate some of the various methods by which traffic can be filtered in your BGP network:

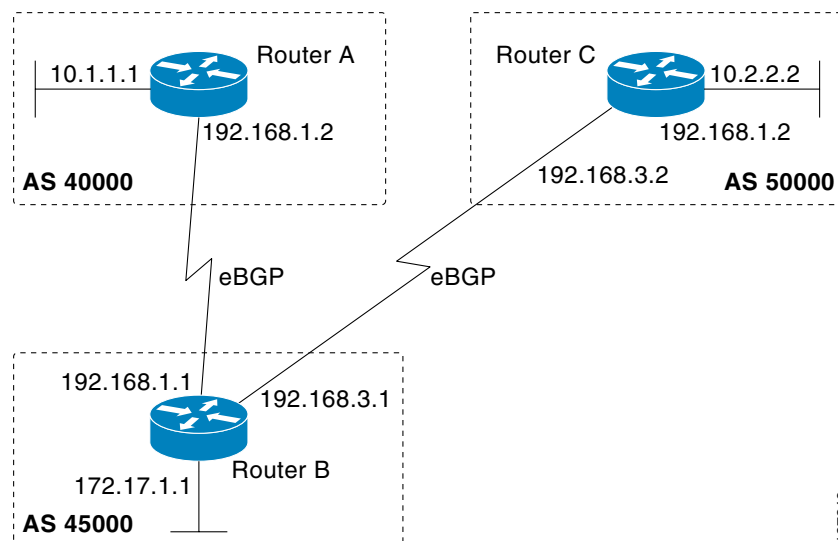
- [Restrictions, page 135](#)
- [Filtering BGP Prefixes with AS-path Filters, page 138](#)

- [Filtering Traffic Using Community Lists, page 140](#)
- [Filtering Traffic Using Extended Community Lists, page 144](#)
- [Filtering Traffic Using a BGP Route Map Policy List, page 147](#)
- [Filtering Traffic Using BGP Route Map Continue Clauses, page 150](#)

## Filtering BGP Prefixes with Prefix Lists

Perform this task to use prefix lists to filter BGP route information. The task is configured at Router B in [Figure 15](#) where both Router A and Router C are set up as BGP peers. A prefix list is configured to permit only routes from the network 10.2.2.0/24 to be outbound. In effect, this will restrict the information that is received from Router C to be forwarded to Router A. Optional steps are included to display the prefix list information and to reset the hit count.

**Figure 15** *BGP Topology for Configuring BGP Policies Tasks*



### Restrictions

The **neighbor prefix-list** and the **neighbor distribute-list** commands are mutually exclusive for a BGP peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*]
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. Repeat Step 5 for all BGP peers.
7. **aggregate-address** *address mask* [**as-set**]

8. **neighbor** *ip-address* **prefix-list** *list-name* {**in** | **out**}
9. **exit**
10. **ip prefix-list** *list-name* [**seq** *seq-number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-value*] [**le** *le-value*] [**eq** *eq-value*]
11. **end**
12. **show ip prefix-list** [**detail** | **summary**] [*prefix-list-name*] [*network/length*] [**seq** *seq-number*] [**longer**] [**first-match**]
13. **clear ip prefix-list** {**\*** | *ip-address* | *peer-group-name*} **out**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]  <b>Example:</b> Router(config-router)# network 172.17.1.0 mask 255.255.255.0	(Optional) Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"><li>• For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li></ul>
Step 5	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address of the neighbor in the specified autonomous system BGP neighbor table of the local router.
Step 6	Repeat Step 5 for all BGP peers.	—

	Command or Action	Purpose
Step 7	<b>aggregate-address</b> <i>address mask [as-set]</i>  <b>Example:</b> Router(config-router)# aggregate-address 172.0.0.0 255.0.0.0	Creates an aggregate entry in a BGP routing table. <ul style="list-style-type: none"> <li>A specified route must exist in the BGP table.</li> <li>Use the <b>aggregate-address</b> command with no keywords to create an aggregate entry if any more-specific BGP routes are available that fall in the specified range.</li> </ul> <b>Note</b> Only partial syntax is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 8	<b>neighbor</b> <i>ip-address prefix-list list-name {in   out}</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 prefix-list super172 out	Distributes BGP neighbor information as specified in a prefix list. <ul style="list-style-type: none"> <li>In this example, a prefix list called super172 is set for outgoing routes to Router A.</li> </ul>
Step 9	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 10	<b>ip prefix-list</b> <i>list-name [seq seq-number] {deny network/length   permit network/length} [ge ge-value] [le le-value] [eq eq-value]</i>  <b>Example:</b> Router(config)# ip prefix-list super172 permit 172.0.0.0/8	Defines a BGP-related prefix list and enters access list configuration mode. <ul style="list-style-type: none"> <li>In this example, the prefix list called super172 is defined to permit only route 172.0.0.0/8 to be forwarded.</li> <li>All other routes will be denied because there is an implicit deny at the end of all prefix lists.</li> </ul>
Step 11	<b>end</b>  <b>Example:</b> Router(config-access-list)# end	Exits access list configuration mode and enters privileged EXEC mode.
Step 12	<b>show ip prefix-list</b> [ <i>detail   summary</i> ] [ <i>prefix-list-name</i> ] [ <i>network/length</i> ] [ <i>seq seq-number</i> ] [ <i>longer</i> ] [ <i>first-match</i> ]  <b>Example:</b> Router# show ip prefix-list detail super172	Displays information about prefix lists. <ul style="list-style-type: none"> <li>In this example, details of the prefix list named super172 will be displayed, including the hit count. Hit count is the number of times the entry has matched a route.</li> </ul>
Step 13	<b>clear ip prefix-list</b> <i>{*   ip-address   peer-group-name} out</i>  <b>Example:</b> Router# clear ip prefix-list super172 out	Resets the hit count of the prefix list entries. <ul style="list-style-type: none"> <li>In this example, the hit count for the prefix list called super172 will be reset.</li> </ul>

## Examples

The following output from the **show ip prefix-list** command shows details of the prefix list named **super172**, including the hit count. The **clear ip prefix-list** command is entered to reset the hit count and the **show ip prefix-list** command is entered again to show the hit count reset to 0.

```
Router# show ip prefix-list detail super172

ip prefix-list super172:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 4
  seq 5 permit 172.0.0.0/8 (hit count: 1, refcount: 1)

Router# clear ip prefix-list super172

Router# show ip prefix-list detail super172

ip prefix-list super172:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 4
  seq 5 permit 172.0.0.0/8 (hit count: 0, refcount: 1)
```

## Filtering BGP Prefixes with AS-path Filters

Perform this task to filter BGP prefixes using AS-path filters with an access list based on the value of the AS-path attribute to filter route information. An AS-path access list is configured at Router B in [Figure 15](#). The first line of the access list denies all matches to the AS-path 50000 and the second line allows all other paths. The router uses the **neighbor filter-list** command to specify the AS-path access list as an outbound filter. After the filtering is enabled, traffic can be received from both Router A and Router C but updates originating from autonomous system 50000 (Router C) are not forwarded by Router B to Router A. If any updates from Router C originated from another autonomous system, they would be forwarded because they would contain both autonomous system 50000 plus another autonomous system number, and that would not match the AS-path access list.



### Note

In Cisco IOS Releases 12.0(22)S, 12.2(15)T, and 12.2(18)S and later releases the maximum number of autonomous system access lists that can be configured with the **ip as-path access-list** command is increased from 199 to 500.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *network-number* [**mask** *network-mask*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. Repeat Step 5 for all BGP peers.
7. **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *access-list-number* {**in** | **out**}
8. **exit**
9. **ip as-path access-list** *access-list-number* {**deny** | **permit**} *as-regular-expression*
10. Repeat Step 9 for all entries required in the AS-path access list.
11. **end**
12. **show ip bgp regexp** *as-regular-expression*



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 4	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]  <b>Example:</b> Router(config-router)# network 172.17.1.0 mask 255.255.255.0	(Optional) Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"><li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li></ul> <b>Note</b> Only partial syntax is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 5	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 remote-as 40000	Adds the IP address or peer group name of the neighbor in the specified autonomous system BGP neighbor table of the local router.
Step 6	Repeat Step 5 for all BGP peers.	—
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>filter-list</b> { <i>access-list-number</i> } { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router)# neighbor 192.168.1.2 filter-list 100 out	Distributes BGP neighbor information as specified in a prefix list. <ul style="list-style-type: none"><li>In this example, an access list number 100 is set for outgoing routes to Router A.</li></ul>
Step 8	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 9	<p><b>ip as-path access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <i>as-regular-expression</i></p> <p><b>Example:</b> Router(config)# ip as-path access-list 100 deny ^50000\$ and</p> <p><b>Example:</b> Router(config)# ip as-path access-list 100 permit .*</p>	<p>Defines a BGP-related access list and enters access list configuration mode.</p> <ul style="list-style-type: none"> <li>In the first example, access list number 100 is defined to deny any AS-path that starts and ends with 50000.</li> <li>In the second example, all routes that do not match the criteria in the first example of the AS-path access list will be permitted. The period and asterisk symbols imply that all characters in the AS-path will match so Router B will forward those updates to Router A.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p>
Step 10	Repeat Step 9 for all entries required in the AS-path access list.	—
Step 11	<p><b>end</b></p> <p><b>Example:</b> Router(config-access-list)# end</p>	Exits access list configuration mode and enters privileged EXEC mode.
Step 12	<p><b>show ip bgp regexp</b> <i>as-regular-expression</i></p> <p><b>Example:</b> Router# show ip bgp regexp ^50000\$</p>	<p>Displays routes matching the regular expression.</p> <ul style="list-style-type: none"> <li>To verify the regular expression you can use this command.</li> <li>In this example, all paths that match the expression “starts and ends with 50000” will be displayed.</li> </ul>

## Examples

The following output from the **show ip bgp regexp** command shows the autonomous system paths that match the regular expression—start and end with AS-path 50000:

```
Router# show ip bgp regexp ^50000$
```

```
BGP table version is 9, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```

Network          Next Hop           Metric LocPrf Weight Path
*> 10.2.2.0/24    192.168.3.2        0             150 50000 i
```

## Filtering Traffic Using Community Lists

Perform this task to filter traffic by creating BGP community lists and then reference them within a route map to control incoming routes. BGP communities provide a method of filtering inbound or outbound routes for large, complex networks. Instead of compiling long access or prefix lists of individual peers, BGP allows grouping of peers with identical routing policies even though they reside in different autonomous systems or networks.

In this task, Router B in [Figure 15](#) is configured with several route maps and community lists to control incoming routes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *route-map-name* {**in** | **out**}
6. **exit**
7. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
8. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
9. **set weight** *weight*
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
13. **set community** *community-number*
14. **exit**
15. **ip community-list** {*standard-list-number* | **standard** *list-name* {**deny** | **permit**} [*community-number*] [*AA:NN*] [**internet**] [**local-AS**] [**no-advertise**] [**no-export**] } | {*expanded-list-number* | **expanded** *list-name* {**deny** | **permit**} *regular-expression*}
16. Repeat Step 15 to create all the required community lists.
17. **end**
18. **show ip community-list** [*standard-list-number* | *expanded-list-number* | *community-list-name*] [**exact-match**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>	Enters router configuration mode for the specified routing process.
	<b>Example:</b> Router(config)# router bgp 45000	

	Command or Action	Purpose
Step 4	<b>neighbor</b> {ip-address   peer-group-name} <b>remote-as</b> autonomous-system-number  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system BGP neighbor table of the local router.
Step 5	<b>neighbor</b> {ip-address   peer-group-name} <b>route-map</b> route-map-name {in   out}  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 route-map 2000 in	Applies a route map to inbound or outbound routes. <ul style="list-style-type: none"> <li>In this example, the route map called 2000 is applied to inbound routes from the BGP peer at 192.168.3.2.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 7	<b>route-map</b> map-name [permit   deny] [sequence-number]  <b>Example:</b> Router(config)# route-map 2000 permit 10	Creates a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, the route map called 2000 is defined.</li> </ul>
Step 8	<b>match community</b> {standard-list-number   expanded-list-number   community-list-name [exact]}  <b>Example:</b> Router(config-route-map)# match community 1	Matches a BGP community list. <ul style="list-style-type: none"> <li>In this example, the community attribute is matched to community list 1.</li> </ul>
Step 9	<b>set weight</b> weight  <b>Example:</b> Router(config-route-map)# set weight 30	Specifies the BGP weight for the routing table. <ul style="list-style-type: none"> <li>In this example, any route that matches community list 1 will have the BGP weight set to 30.</li> </ul>
Step 10	<b>exit</b>  <b>Example:</b> Router(config-route-map)# exit	Exits route map configuration mode and enters global configuration mode.
Step 11	<b>route-map</b> map-name [permit   deny] [sequence-number]  <b>Example:</b> Router(config)# route-map 3000 permit 10	Creates a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, the route map called 3000 is defined.</li> </ul>
Step 12	<b>match community</b> {standard-list-number   expanded-list-number   community-list-name [exact]}  <b>Example:</b> Router(config-route-map)# match community 2	Matches a BGP community list. <ul style="list-style-type: none"> <li>In this example, the community attribute is matched to community list 2.</li> </ul>

	Command or Action	Purpose
Step 13	<pre>set community community-number</pre> <p><b>Example:</b> Router(config-route-map)# set community 99</p>	<p>Sets the BGP communities attribute.</p> <ul style="list-style-type: none"> <li>In this example, any route that matches community list 2 will have the BGP community attribute set to 99.</li> </ul>
Step 14	<pre>exit</pre> <p><b>Example:</b> Router(config-route-map)# exit</p>	Exits route map configuration mode and enters global configuration mode.
Step 15	<pre>ip community-list {standard-list-number   standard list-name {deny   permit} [community-number] [AA:NN] [internet] [local-AS] [no-advertise] [no-export]}   {expanded-list-number   expanded list-name {deny   permit} regular-expression}</pre> <p><b>Example:</b> Router(config)# ip community-list 1 permit 100 and</p> <p><b>Example:</b> Router(config)# ip community-list 2 permit internet</p>	<p>Creates a community list for BGP and controls access to it.</p> <ul style="list-style-type: none"> <li>In the first example, community list 1 permits routes with a community attribute of 100. Router C routes all have community attribute of 100 so their weight will be set to 30.</li> <li>In the second example, community list 2 effectively permits all routes by using the <b>internet</b> keyword. Any routes that did not match community list 1 are checked against community list 2. All routes are permitted but no changes are made to the route attributes.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p>
Step 16	Repeat Step 15 to create all the required community lists.	—
Step 17	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode and enters privileged EXEC mode.
Step 18	<pre>show ip community-list [standard-list-number   expanded-list-number   community-list-name] [exact-match]</pre> <p><b>Example:</b> Router# show ip community-list 1</p>	Displays configured BGP community list entries.

## Examples

The following sample output verifies that community list 1 has been created, with the output showing that community list 1 permits routes with a community attribute of 100:

```
Router# show ip community-list 1
Community standard list 1
    permit 100
```

The following sample output verifies that community list 2 has been created, with the output showing that community list 2 effectively permits all routes by using the **internet** keyword:

```
Router# show ip community-list 2
Community standard list 2
    permit internet
```

## Filtering Traffic Using Extended Community Lists

Perform this task to filter traffic by creating an extended BGP community list to control outbound routes. BGP communities provide a method of filtering inbound or outbound routes for large, complex networks. Instead of compiling long access or prefix lists of individual peers, BGP allows grouping of peers with identical routing policies even though they reside in different autonomous systems or networks.

In this task, Router B in [Figure 15](#) is configured with an extended named community list to specify that the BGP peer at 192.1681.2 is not sent advertisements about any path through or from autonomous system 50000. The IP extended community-list configuration mode is used and the ability to resequence entries is shown.

### Extended Community Lists

Extended community attributes are used to configure, filter, and identify routes for VRF instances and MPLS VPNs. The **ip extcommunity-list** command is used to configure named or numbered extended community lists. All of the standard rules of access lists apply to the configuration of extended community lists. Regular expressions are supported by the expanded range of extended community list numbers.

### Restrictions

A sequence number is applied to all extended community list entries by default regardless of the configuration mode. Explicit sequencing and resequencing of extended community list entries can be configured only in IP extended community-list configuration mode and not in global configuration mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** { *expanded-list-number* | **expanded** *list-name* | *standard-list-number* | **standard** *list-name* }
4. [*sequence-number*] { **deny** [*regular-expression*] | **exit** | **permit** [*regular-expression*] }
5. Repeat Step 4 for all the required permit or deny entries in the extended community list.
6. **resequence** [*starting-sequence*] [*sequence-increment*]
7. **exit**
8. **router bgp** *autonomous-system-number*
9. **network** *network-number* [**mask** *network-mask*]
10. **neighbor** { *ip-address* | *peer-group-name* } **remote-as** *autonomous-system-number*
11. Repeat Step 10 for all the required BGP peers.
12. **end**
13. **show ip extcommunity-list** [*list-number* | *list-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip extcommunity-list</b> {expanded-list-number   expanded list-name   standard-list-number   standard list-name}  <b>Example:</b> Router(config)# ip extcommunity-list expanded DENY50000	Enters IP extended community-list configuration mode to create or configure an extended community list. <ul style="list-style-type: none"> <li>In this example, the expanded community list DENY50000 is created.</li> </ul>
Step 4	[sequence-number] {deny [regular-expression]   exit   permit [regular-expression]}  <b>Example:</b> Router(config-extcomm-list)# 10 deny _50000_ and  <b>Example:</b> Router(config-extcomm-list)# 20 deny ^50000 .*	Configures an expanded community list entry. <ul style="list-style-type: none"> <li>In the first example, an expanded community list entry with the sequence number 10 is configured to deny advertisements about paths from autonomous system 50000.</li> <li>In the second example, an expanded community list entry with the sequence number 20 is configured to deny advertisements about paths through autonomous system 50000.</li> </ul> <p><b>Note</b> Two examples are shown here because the task example requires both these statements to be configured.</p> <p><b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</p>
Step 5	Repeat Step 4 for all the required permit or deny entries in the extended community list.	—
Step 6	<b>resequence</b> [starting-sequence] [sequence-increment]  <b>Example:</b> Router(config-extcomm-list)# resequence 50 100	Resequences expanded community list entries. <ul style="list-style-type: none"> <li>In this example, the sequence number of the first expanded community list entry is set to 50 and subsequent entries are set to increment by 100. The second expanded community list entry is therefore set to 150.</li> </ul> <p><b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>, Release 12.4.</p>

	Command or Action	Purpose
Step 7	<b>exit</b>  <b>Example:</b> Router(config-extcomm-list)# exit	Exits expanded community-list configuration mode and enters global configuration mode.
Step 8	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 45000	Enters router configuration mode for the specified routing process.
Step 9	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]  <b>Example:</b> Router(config-router)# network 172.17.1.0 mask 255.255.255.0	(Optional) Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"><li>For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li></ul> <b>Note</b> Only the syntax applicable to this task is used in this example. For more details, see the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 10	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 192.168.3.2 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system BGP neighbor table of the local router.
Step 11	Repeat Step 10 for all the required BGP peers.	—
Step 12	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and enters privileged EXEC mode.
Step 13	<b>show ip extcommunity-list</b> [ <i>list-number</i>   <i>list-name</i> ]  <b>Example:</b> Router# show ip extcommunity-list DENY50000	Displays configured BGP expanded community list entries.

## Examples

The following sample output verifies that the BGP expanded community list DENY50000 has been created, with the output showing that the entries to deny advertisements about autonomous system 50000 have been resequenced from 10 and 20 to 50 and 150:

```
Router# show ip extcommunity-list 1
Expanded extended community-list DENY50000
  50 deny _50000_
 150 deny ^50000 .*
```



## Filtering Traffic Using a BGP Route Map Policy List

Perform this task to create a BGP policy list and then reference it within a route map.

A policy list is like a route map that contains only match clauses. With policy lists there are no changes to match clause semantics and route map functions. The match clauses are configured in policy lists with permit and deny statements and the route map evaluates and processes each match clause to permit or deny routes based on the configuration. AND and OR semantics in the route map function the same way for policy lists as they do for match clauses.

Policy lists simplify the configuration of BGP routing policy in medium-size and large networks. The network operator can reference preconfigured policy lists with groups of match clauses in route maps and easily apply general changes to BGP routing policy. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.

Perform this task to create a BGP policy list to filter traffic that matches the autonomous system path and MED of a router and then create a route map to reference the policy list.

### Prerequisites

BGP routing must be configured in your network and BGP neighbors must be established.

### Restrictions

- BGP route map policy lists do not support the configuration of IP version 6 (IPv6) match clauses in policy lists.
- Policy lists are not supported in versions of Cisco IOS software prior to Cisco IOS Releases 12.0(22)S and 12.2(15)T. Reloading a router that is running an older version of Cisco IOS software may cause some routing policy configurations to be lost.
- Policy lists support only match clauses and do not support set clauses. However, policy lists can coexist, within the same route map entry, with match and set clauses that are configured separately from the policy lists.
- Policy lists are supported only by BGP. They are not supported by other IP routing protocols. This limitation does not interfere with normal operations of a route map, including redistribution, because policy list functions operate transparently within BGP and are not visible to other IP routing protocols.
- Policy lists support only match clauses and do not support set clauses. However, policy lists can coexist, within the same route map entry, with match and set clauses that are configured separately from the policy lists. The first route map example configures AND semantics, and the second route map configuration example configures semantics. Both examples in this section show sample route map configurations that reference policy lists and separate match and set clauses in the same configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip policy-list** *policy-list-name* {**permit** | **deny**}
4. **match as-path** *as-number*
5. **match metric** *metric*
6. **exit**

7. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
8. **match ip-address** {*access-list-number* | *access-list-name*} [... *access-list-number* | ...  
*access-list-name*]
9. **match policy-list** *policy-list-name*
10. **set community** {*community-number* [**additive**] [*well-known-community*] | **none**}
11. **set local-preference** *preference-value*
12. **end**
13. **show ip policy-list** *policy-list-name*
14. **show route-map** [*route-map-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip policy-list</b> <i>policy-list-name</i> { <b>permit</b>   <b>deny</b> }  <b>Example:</b> Router(config)# ip policy-list POLICY_LIST_NAME-1 permit	Enters policy list configuration mode and creates a BGP policy list that will permit routes that are allowed by the match clauses that follow.
Step 4	<b>match as-path</b> <i>as-number</i>  <b>Example:</b> Router(config-policy-list)# match as-path 40000	Creates a match clause to permit routes from the specified autonomous system path.
Step 5	<b>match metric</b> <i>metric</i>  <b>Example:</b> Router(config-policy-list)# match metric 10	Creates a match clause to permit routes with the specified metric.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-policy-list)# exit	Exits policy list configuration mode and enters global configuration mode.
Step 7	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map MAP-NAME-1 permit 10	Creates a route map and enters route map configuration mode.

	Command or Action	Purpose
Step 8	<b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i> } [... <i>access-list-number</i>   ... <i>access-list-name</i> ]  <b>Example:</b> Router(config-route-map)# match ip address 1	Creates a match clause to permit routes that match the specified <i>access-list-number</i> or <i>access-list-name</i> argument.
Step 9	<b>match policy-list</b> <i>policy-list-name</i>  <b>Example:</b> Router(config-route-map)# match policy-list POLICY-LIST-NAME-1	Creates a clause that will match the specified policy list. <ul style="list-style-type: none"> <li>All match clauses within the policy list will be evaluated and processed. Multiple policy lists can be referenced with this command.</li> <li>This command also supports AND or OR semantics like a standard match clause.</li> </ul>
Step 10	<b>set community</b> <i>community-number</i> [ <b>additive</b> ] [ <i>well-known-community</i> ]   <b>none</b>  <b>Example:</b> Router(config-route-map)# set community 10:1	Creates a clause to set or remove the specified community.
Step 11	<b>set local-preference</b> <i>preference-value</i>  <b>Example:</b> Router(config-route-map)# set local-preference 140	Creates a clause to set the specified local preference value.
Step 12	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route map configuration mode and enters privileged EXEC mode.
Step 13	<b>show ip policy-list</b> [ <i>policy-list-name</i> ]  <b>Example:</b> Router# show ip policy-list POLICY-LIST-NAME-1	Display information about configured policy lists and policy list entries.
Step 14	<b>show route-map</b> [ <i>route-map-name</i> ]  <b>Example:</b> Router# show route-map	Displays locally configured route maps and route map entries.

## Examples

The following sample output verifies that a policy list has been created, with the output displaying the policy list name and configured match clauses:

```
Router# show ip policy-list POLICY-LIST-NAME-1
policy-list POLICY-LIST-NAME-1 permit
Match clauses:
  metric 20
  as-path (as-path filter): 1
```

**Note**

A policy list name can be specified when the **show ip policy-list** command is entered. This option can be useful for filtering the output of this command and verifying a single policy list.

The following sample output from the **show route-map** command verifies that a route map has been created and a policy list is referenced. The output of this command displays the route map name and policy lists that are referenced by the configured route maps.

```
Router# show route-map
route-map ROUTE-MAP-NAME-1, deny, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME-1, permit, sequence 10
  Match clauses:
    IP Policy lists:
      POLICY-LIST-NAME-1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

## Filtering Traffic Using BGP Route Map Continue Clauses

In Cisco IOS Release 12.3(2)T, 12.0(24)S, and later releases, the continue clause was introduced into BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduced the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map. Before the continue clause was introduced, route map configuration was linear and did not allow any control over the flow of a route map. Perform this task to filter traffic using BGP route map continue clauses.

### Route Map Operation Without Continue Clauses

A route map evaluates match clauses until a successful match occurs. After the match occurs, the route map stops evaluating match clauses and starts executing set clauses, in the order in which they were configured. If a successful match does not occur, the route map “falls through” and evaluates the next sequence number of the route map until all configured route map entries have been evaluated or a successful match occurs. Each route map sequence is tagged with a sequence number to identify the entry. Route map entries are evaluated in order starting with the lowest sequence number and ending with the highest sequence number. If the route map contains only set clauses, the set clauses will be executed automatically, and the route map will not evaluate any other route map entries.

### Route Map Operation with Continue Clauses

When a continue clause is configured, the route map will continue to evaluate and execute match clauses in the specified route map entry after a successful match occurs. The continue clause can be configured to go to (or jump to) a specific route map entry by specifying the sequence number, or if a sequence number is not specified, the continue clause will go to the next sequence number. This behavior is called an “implied continue.” If a match clause exists, the continue clause is executed only if a match occurs. If no successful matches occur, the continue clause is ignored.

## Match Operations with Continue Clauses

If a match clause does not exist in the route map entry but a continue clause does, the continue clause will be automatically executed and go to the specified route map entry. If a match clause exists in a route map entry, the continue clause is executed only when a successful match occurs. When a successful match occurs and a continue clause exists, the route map executes the set clauses and then goes to the specified route map entry. If the next route map entry contains a continue clause, the route map will execute the continue clause if a successful match occurs. If a continue clause does not exist in the next route map entry, the route map will be evaluated normally. If a continue clause exists in the next route map entry but a match does not occur, the route map will not continue and will “fall through” to the next sequence number if one exists.

## Set Operations with Continue Clauses

Set clauses are saved during the match clause evaluation process and executed after the route-map evaluation is completed. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are executed only after a successful match occurs, unless the route map does not contain a match clause. The continue statement proceeds to the specified route map entry only after configured set actions are performed. If a set action occurs in the first route map and then the same set action occurs again, with a different value, in a subsequent route map entry, the last set action will override any previous set actions that were configured with the same **set** command.



### Note

A continue clause can be executed, without a successful match, if a route map entry does not contain a match clause.

## Restrictions

- Continue clauses for outbound route maps are supported only in Cisco IOS Release 12.0(31)S and later releases.
- Continue clauses can go only to a higher route-map entry (a route map entry with a higher sequence number) and cannot go to a lower route map entry.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
6. **exit**
7. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
8. **match ip-address** {*access-list-number* | *access-list-name*} [... *access-list-number* | ... *access-list-name*]
9. **set community** {*community-number* [**additive**] [*well-known-community*] | **none**}
10. **continue** [*sequence-number*]
11. **end**
12. **show route-map** [*map-name*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config)# router bgp 50000	Enters router configuration mode, and creates a BGP routing process.
Step 4	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Router(config-router)# neighbor 10.0.0.1 remote-as 50000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.
Step 5	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> Router(config-router)# neighbor 10.0.0.1 route-map ROUTE-MAP-NAME in	Applies the inbound route map to routes received from the specified neighbor, or applies an outbound route map to routes advertised to the specified neighbor.  <b>Note</b> Outbound route maps are supported in Cisco IOS Release 12.0(31)S and later releases.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and enters global configuration mode.
Step 7	<b>route-map</b> <i>map-name</i> { <b>permit</b>   <b>deny</b> } [ <i>sequence-number</i> ]  <b>Example:</b> Router(config)# route-map ROUTE-MAP-NAME permit 10	Enters route-map configuration mode to create or configure a route map.

	Command or Action	Purpose
Step 8	<b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i> } [... <i>access-list-number</i>   ... <i>access-list-name</i> ]  <b>Example:</b> Router(config-route-map)# match ip address 1	Configures a <b>match</b> command that specifies the conditions under which policy routing and route filtering occur. <ul style="list-style-type: none"> <li>Multiple <b>match</b> commands can be configured. If a <b>match</b> command is configured, a match must occur in order for the continue statement to be executed. If a <b>match</b> command is not configured, set and continue clauses will be executed.</li> </ul> <b>Note</b> The <b>match</b> and <b>set</b> commands used in this task are examples that are used to help describe the operation of the <b>continue</b> command. For a list of specific <b>match</b> and <b>set</b> commands, see the <b>continue</b> command in the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4.
Step 9	<b>set community</b> <i>community-number</i> [ <b>additive</b> ] [ <i>well-known-community</i> ]   <b>none</b>  <b>Example:</b> Router(config-route-map)# set community 10:1	Configures a <b>set</b> command that specifies the routing action to perform if the criteria enforced by the <b>match</b> commands are met. <ul style="list-style-type: none"> <li>Multiple <b>set</b> commands can be configured.</li> <li>In this example, a clause is created to set the specified community.</li> </ul>
Step 10	<b>continue</b> [ <i>sequence-number</i> ]  <b>Example:</b> Router(config-route-map)# continue	Configures a route map to continue to evaluate and execute match statements after a successful match occurs. <ul style="list-style-type: none"> <li>If a sequence number is configured, the continue clause will go to the route map with the specified sequence number.</li> <li>If no sequence number is specified, the continue clause will go to the route map with the next sequence number. This behavior is called an “implied continue.”</li> </ul>
Step 11	<b>end</b>  <b>Example:</b> Router(config-route-map)# end	Exits route-map configuration mode and enters privileged EXEC mode.
Step 12	<b>show route-map</b> [ <i>map-name</i> ]  <b>Example:</b> Router# show route-map	(Optional) Displays locally configured route maps. The name of the route map can be specified in the syntax of this command to filter the output.

## Examples

The following sample output shows how to verify the configuration of continue clauses using the **show route-map** command. The output displays configured route maps including the match, set, and continue clauses.

```
Router# show route-map
route-map ROUTE-MAP-NAME, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
    metric 10
  Continue: sequence 40
```

```

Set clauses:
  as-path prepend 10
Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 20
Match clauses:
  ip address (access-lists): 2
  metric 20
Set clauses:
  as-path prepend 10 10
Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 30
Match clauses:
  Continue: to next entry 40
Set clauses:
  as-path prepend 10 10 10
Policy routing matches: 0 packets, 0 bytes
route-map ROUTE-MAP-NAME, permit, sequence 40
Match clauses:
  community (community-list filter): 10:1
Set clauses:
  local-preference 104
Policy routing matches: 0 packets, 0 bytes
route-map LOCAL-POLICY-MAP, permit, sequence 10
Match clauses:
Set clauses:
  community 655370
Policy routing matches: 0 packets, 0 bytes

```

## Configuration Examples for Connecting to a Service Provider Using External BGP

This section contains the following examples:

- [Influencing Inbound Path Selection: Examples, page 154](#)
- [Influencing Outbound Path Selection: Examples, page 156](#)
- [Filtering BGP Prefixes with Prefix Lists: Examples, page 157](#)
- [Filtering Traffic Using Community Lists: Examples, page 158](#)
- [Filtering Traffic Using AS-path Filters: Example, page 159](#)
- [Filtering Traffic Using a BGP Route Map: Example, page 159](#)
- [Filtering Traffic Using a BGP Route Map Continue Clause: Example, page 160](#)

### Influencing Inbound Path Selection: Examples

The following example shows how to influence the inbound path selection by modifying the AS-path attribute. Using the network shown in [Figure 11](#), this task is similar to the “[Influencing Inbound Path Selection by Modifying the AS-path Attribute](#)” section on [page 108](#), but this example introduces the use of an access list to control which BGP updates will have the extra autonomous system paths prepended. A second network, 172.16.1.0 (not shown in the network diagram) is configured to be advertised. Using access list 1, only updates for the 172.17.1.0 network will be modified. This configuration is done at Router A in [Figure 11](#).

```

router bgp 40000
address-family ipv4

```



```

network 172.17.1.0 mask 255.255.255.0
network 172.16.1.0 mask 255.255.255.0
neighbor 192.168.1.2 remote-as 60000
neighbor 192.168.1.2 route-map PREPEND out
neighbor 192.168.1.2 activate
exit-address-family
access-list 1 permit 172.17.1.0 0.0.0.255
route-map PREPEND permit 10
  match ip address 1
  set as-path prepend 40000 40000
exit
route-map PREPEND permit 20

```

The following example shows how you can use route maps to modify incoming data from a neighbor. Any route received from 10.222.1.1 that matches the filter parameters set in autonomous system access list 200 will have its weight set to 200 and its local preference set to 250, and it will be accepted.

```

router bgp 100
!
neighbor 10.222.1.1 route-map FIX-WEIGHT in
neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map FIX-WEIGHT permit 10
  match as-path 200
  set local-preference 250
  set weight 200

```

In the following example, the route map named finance marks all paths originating from autonomous system 690 with an MED metric attribute of 127. The second permit clause is required so that routes not matching autonomous system path list 1 will still be sent to neighbor 10.1.1.1.

```

router bgp 100
neighbor 10.1.1.1 route-map finance out
!
ip as-path access-list 1 permit ^690_
ip as-path access-list 2 permit .*
!
route-map finance permit 10
  match as-path 1
  set metric 127
!
route-map finance permit 20
  match as-path 2

```

Inbound route maps could perform prefix-based matching and set various parameters of the update. Inbound prefix matching is available in addition to autonomous system path and community list matching. The following example shows how the **set local-preference** route-map configuration command sets the local preference of the inbound prefix 172.20.0.0/16 to 120:

```

!
router bgp 100
network 10.108.0.0
neighbor 10.108.1.1 remote-as 200
neighbor 10.108.1.1 route-map set-local-pref in
!
route-map set-local-pref permit 10
  match ip address 2
  set local preference 120
!
route-map set-local-pref permit 20

```

```
!
access-list 2 permit 172.20.0.0 0.0.255.255
access-list 2 deny any
```

## Influencing Outbound Path Selection: Examples

The following example creates an outbound route filter and configures Router-A (10.1.1.1) to advertise the filter to Router-B (172.16.1.2). An IP prefix list named FILTER is created to specify the 192.168.1.0/24 subnet for outbound route filtering. The ORF send capability is configured on Router-A so that Router-A can advertise the outbound route filter to Router-B.

### Router-A Configuration (Sender)

```
ip prefix-list FILTER seq 10 permit 192.168.1.0/24
!
router bgp 100
 address-family ipv4 unicast
  neighbor 172.16.1.2 remote-as 200
  neighbor 172.16.1.2 ebgp-multihop
  neighbor 172.16.1.2 capability orf prefix-list send
end
```

### Router-B Configuration (Receiver)

The following example configures Router-B to advertise the ORF receive capability to Router-A. Router-B will install the outbound route filter, defined in the FILTER prefix list, after ORF capabilities have been exchanged. An inbound soft reset is initiated on Router-B at the end of this configuration to activate the outbound route filter.

```
router bgp 200
 address-family ipv4 unicast
  neighbor 10.1.1.1 remote-as 100
  neighbor 10.1.1.1 ebgp-multihop 255
  neighbor 10.1.1.1 capability orf prefix-list receive
end
clear ip bgp 192.168.1.2 in prefix-filter
```

The following example shows how the route map named set-as-path is applied to outbound updates to the neighbor 10.69.232.70. The route map will prepend the autonomous system path “100 100” to routes that pass access list 1. The second part of the route map is to permit the advertisement of other routes.

```
router bgp 100
 network 172.16.0.0
 network 172.17.0.0
 neighbor 10.69.232.70 remote-as 200
 neighbor 10.69.232.70 route-map set-as-path out
!
route-map set-as-path 10 permit
 match address 1
 set as-path prepend 100 100
!
route-map set-as-path 20 permit
 match address 2
!
access-list 1 permit 172.16.0.0 0.0.255.255
access-list 1 permit 172.17.0.0 0.0.255.255
!
access-list 2 permit 0.0.0.0 255.255.255.255
```

## Filtering BGP Prefixes with Prefix Lists: Examples

This section contains the following examples:

- [Filtering BGP Prefixes Using a Single Prefix List](#)
- [Filtering BGP Prefixes Using a Group of Prefixes](#)
- [Adding or Deleting Prefix List Entries](#)

### Filtering BGP Prefixes Using a Single Prefix List

The following example shows how a prefix list denies the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example shows how a prefix list permits a route that matches the prefix 10.0.0.0/8:

```
ip prefix-list abc permit 10.0.0.0/8
```

The following example shows how to configure the BGP process so that it accepts only prefixes with a prefix length of /8 to /24:

```
router bgp 40000
network 10.20.20.0
distribute-list prefix max24 in
!
ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

The following example configuration shows how to conditionally originate a default route (0.0.0.0/0) in Routing Information Protocol (RIP) when a prefix 10.1.1.0/24 exists in the routing table:

```
ip prefix-list cond permit 10.1.1.0/24
!
route-map default-condition permit 10
match ip address prefix-list cond
!
router rip
default-information originate route-map default-condition
```

The following example shows how to configure BGP to accept routing updates from 192.168.1.1 only, besides filtering on the prefix length:

```
router bgp 40000
distribute-list prefix max24 gateway allowlist in
!
ip prefix-list allowlist seq 5 permit 192.168.1.1/32
!
```

The following example shows how to direct the BGP process to filter incoming updates to the prefix using name1, and match the gateway (next hop) of the prefix being updated to the prefix list name2, on Ethernet interface 0:

```
router bgp 103
distribute-list prefix name1 gateway name2 in ethernet 0.
```

### Filtering BGP Prefixes Using a Group of Prefixes

The following example shows how to configure BGP to permit routes with a prefix length up to 24 in network 192/8:

```
ip prefix-list abc permit 192.0.0.0/8 le 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than 25 in 192/8:

```
ip prefix-list abc deny 192.0.0.0/8 ge 25
```

The following example shows how to configure BGP to permit routes with a prefix length greater than 8 and less than 24 in all address space:

```
ip prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to configure BGP to deny routes with a prefix length greater than 25 in all address space:

```
ip prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to configure BGP to deny all routes in network 10/8, because any route in the Class A network 10.0.0.0/8 is denied if its mask is less than or equal to 32 bits:

```
ip prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to configure BGP to deny routes with a mask greater than 25 in 192.168.1.0/24:

```
ip prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to configure BGP to permit all routes:

```
ip prefix-list abc permit 0.0.0.0/0 le 32
```

## Adding or Deleting Prefix List Entries

You can add or delete individual entries in a prefix list if a prefix list has the following initial configuration:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 192.168.0.0/15
```

The following example shows how to delete an entry from the prefix list so that 192.168.0.0 is not permitted, and add a new entry that permits 10.0.0.0/8:

```
no ip prefix-list abc permit 192.168.0.0/15
ip prefix-list abc permit 10.0.0.0/8
```

The new configuration is as follows:

```
ip prefix-list abc deny 0.0.0.0/0 le 7
ip prefix-list abc deny 0.0.0.0/0 ge 25
ip prefix-list abc permit 10.0.0.0/8
```

## Filtering Traffic Using Community Lists: Examples

This section contains two examples of the use of BGP communities with route maps.

The first example shows how the route map named set-community is applied to the outbound updates to the neighbor 172.16.232.50. The routes that pass access list 1 have the special community attribute value no-export. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers in autonomous system 200.

```
router bgp 100
 neighbor 172.16.232.50 remote-as 200
```

```

neighbor 172.16.232.50 send-community
neighbor 172.16.232.50 route-map set-community out
!
route-map set-community permit 10
match address 1
set community no-export
!
route-map set-community permit 20
match address 2

```

The second example shows how the route map named set-community is applied to the outbound updates to neighbor 172.16.232.90. All the routes that originate from autonomous system 70 have the community values 200 200 added to their already existing values. All other routes are advertised as normal.

```

route-map bgp 200
neighbor 172.16.232.90 remote-as 100
neighbor 172.16.232.90 send-community
neighbor 172.16.232.90 route-map set-community out
!
route-map set-community permit 10
match as-path 1
set community 200 200 additive
!
route-map set-community permit 20
!
ip as-path access-list 1 permit 70$
ip as-path access-list 2 permit .*

```

## Filtering Traffic Using AS-path Filters: Example

The following example shows BGP path filtering by neighbor. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.12.10. Similarly, only routes passing access list 3 will be accepted from 192.168.12.10.

```

router bgp 200
neighbor 192.168.12.10 remote-as 100
neighbor 192.168.12.10 filter-list 1 out
neighbor 192.168.12.10 filter-list 2 in
ip as-path access-list 1 permit _109_
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*

```

## Filtering Traffic Using a BGP Route Map: Example

The following example shows how to use an address family to configure BGP so that any unicast and multicast routes from neighbor 10.1.1.1 are accepted if they match access list 1:

```

router bgp 109
neighbor 10.1.1.1 remote-as 1
address-family ipv4 unicast
neighbor 10.1.1.1 route-map in filter-some-multicast

router bgp 109
neighbor 10.1.1.1 remote-as 1
address-family ipv4 multicast
neighbor 10.1.1.1 route-map in filter-some-multicast
neighbor 10.1.1.1 activate

```

```
route-map filter-some-multicast
match ip address 1
```

## Filtering Traffic Using a BGP Route Map Continue Clause: Example

The following example shows continue clause configuration in a route map sequence.

The first continue clause in route map entry 10 indicates that the route map will go to route map entry 30 if a successful matches occurs. If a match does not occur, the route map will “fall through” to route map entry 20. If a successful match occurs in route map entry 20, the set action will be executed and the route map will not evaluate any additional route map entries. Only the first successful match ip address clause is supported.

If a successful match does not occur in route map entry 20, the route map will “fall through” to route map entry 30. This sequence does not contain a match clause, so the set clause will be automatically executed and the continue clause will go to the next route map entry because a sequence number is not specified.

If there are no successful matches, the route-map will “fall through” to route map entry 30 and execute the set clause. A sequence number is not specified for the continue clause so route map entry 40 will be evaluated.

```
route-map ROUTE-MAP-NAME permit 10
match ip address 1
match metric 10
set as-path prepend 10
continue 30
!
route-map ROUTE-MAP-NAME permit 20
match ip address 2
match metric 20
set as-path prepend 10 10
!
route-map ROUTE-MAP-NAME permit 30
set as-path prepend 10 10 10
continue
!
route-map ROUTE-MAP-NAME permit 40
match community 10:1
set local-preference 104
```

## Where to Go Next

To configure more advanced BGP tasks, proceed to the [“Configuring Advanced BGP Features”](#) chapter of the *Cisco IOS IP Routing Configuration Guide*, Release 12.4.

# Additional References

The following sections provide references related to connecting to a service provider using external BGP.

## Related Documents

Related Topic	Document Title
BGP commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	<a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4
Roadmap of BGP features	<a href="#">“BGP Features Roadmap”</a>
BGP overview	<a href="#">“Cisco BGP Overview”</a> module
Configuring basic BGP tasks	<a href="#">“Configuring a Basic BGP Network”</a> module
Configuring internal BGP features	<a href="#">“Configuring Internal BGP Features”</a> chapter of the <i>Cisco IOS IP Routing Protocols Configuration Guide</i> , Release 12.4
BGP fundamentals and description	<i>Large-Scale IP Network Solutions</i> , Khalid Raza and Mark Turner, Cisco Press, 2000
Implementing and controlling BGP in scalable networks	<i>Building Scalable Cisco Networks</i> , Catherine Paquet and Diane Teare, Cisco Press, 2001
Interdomain routing basics	<i>Internet Routing Architectures</i> , Bassam Halabi, Cisco Press, 1997

## Standards

Standard	Title
MDT SAFI	<a href="#">MDT SAFI</a>

## MIBs

MIB	MIBs Link
CISCO-BGP4-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 1771	<i>A Border Gateway Protocol 4 (BGP-4)</i>
RFC 1772	<i>Application of the Border Gateway Protocol in the Internet</i>
RFC 1773	<i>Experience with the BGP Protocol</i>

RFC	Title
RFC 1774	<i>BGP-4 Protocol Analysis</i>
RFC 1930	<i>Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)</i>
RFC 2519	<i>A Framework for Inter-Domain Route Aggregation</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>
RFC 2918	<i>Route Refresh Capability for BGP-4</i>
RFC 3392	<i>Capabilities Advertisement with BGP-4</i>

## Technical Assistance.

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Feature Information for Connecting to a Service Provider Using External BGP

Table 9 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or later releases appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

For information on a feature in this technology that is not documented here, see the “Cisco BGP Implementation Roadmap.”

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



### Note

Table 9 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.



**Table 9**      *Feature Information for Connecting to a Service Provider Using External BGP*

Feature Name	Releases	Feature Configuration Information
BGP Increased Support of Numbered AS-Path Access Lists to 500	12.0(22)S 12.2(15)T 12.2(18)S	<p>The BGP Increased Support of Numbered AS-Path Access Lists to 500 feature increases the maximum number of autonomous systems access lists that can be configured using the <b>ip as-path access-list</b> command from 199 to 500.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Policy Configuration, page 105</a></li> <li>• <a href="#">Filtering BGP Prefixes with AS-path Filters, page 138</a></li> </ul>
BGP Named Community Lists	12.2(8)T	<p>The BGP Named Community Lists feature introduces a new type of community list called the named community list. The BGP Named Community Lists feature allows the network operator to assign meaningful names to community lists and increases the number of community lists that can be configured. A named community list can be configured with regular expressions and with numbered community lists. All rules of numbered communities apply to named community lists except that there is no limitation on the number of community attributes that can be configured for a named community list.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Communities, page 105</a></li> <li>• <a href="#">Filtering Traffic Using Community Lists, page 140</a></li> </ul>
BGP Prefix-Based Outbound Route Filtering	12.0(22)S 12.2(4)T 12.2(14)S	<p>The BGP Prefix-Based Outbound Route Filtering feature uses BGP ORF send and receive capabilities to minimize the number of BGP updates that are sent between BGP peers. Configuring this feature can help reduce the amount of system resources required for generating and processing routing updates by filtering out unwanted routing updates at the source. For example, this feature can be used to reduce the amount of processing required on a router that is not accepting full routes from a service provider network.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Filtering Outbound BGP Route Prefixes, page 119</a></li> <li>• <a href="#">Influencing Outbound Path Selection: Examples, page 156</a></li> </ul>

**Table 9**      **Feature Information for Connecting to a Service Provider Using External BGP (continued)**

Feature Name	Releases	Feature Configuration Information
BGP Route-Map Continue	12.0(24)S 12.0(31)S 12.2(18)S 12.3(2)T	<p>The BGP Route-Map Continue feature introduces the continue clause to BGP route map configuration. The continue clause allows for more programmable policy configuration and route filtering and introduces the capability to execute additional entries in a route map after an entry is executed with successful match and set clauses. Continue clauses allow the network operator to configure and organize more modular policy definitions so that specific policy configurations need not be repeated within the same route map.</p> <p>Continue clauses for outbound route maps are supported only in Cisco IOS Release 12.0(31)S and later releases.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Filtering Traffic Using BGP Route Map Continue Clauses, page 150</a></li> <li>• <a href="#">Filtering Traffic Using a BGP Route Map Continue Clause: Example, page 160</a></li> </ul>
BGP Route-Map Policy List Support	12.0(22)S 12.2(15)T 12.2(18)S	<p>The BGP Route-Map Policy List Support feature introduces new functionality to BGP route maps. This feature adds the capability for a network operator to group route map match clauses into named lists called policy lists. A policy list functions like a macro. When a policy list is referenced in a route map, all of the match clauses are evaluated and processed as if they had been configured directly in the route map. This enhancement simplifies the configuration of BGP routing policy in medium-size and large networks because a network operator can preconfigure policy lists with groups of match clauses and then reference these policy lists within different route maps. The network operator no longer needs to manually reconfigure each recurring group of match clauses that occur in multiple route map entries.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Route Map Policy Lists, page 107</a></li> <li>• <a href="#">Filtering Traffic Using a BGP Route Map Policy List, page 147</a></li> </ul>

**Table 9**      **Feature Information for Connecting to a Service Provider Using External BGP (continued)**

Feature Name	Releases	Feature Configuration Information
BGP Support for Named Extended Community Lists	12.2(25)S 12.3(11)T	<p>The BGP Support for Named Extended Community Lists feature introduces the ability to configure extended community lists using names in addition to the existing numbered format.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Communities, page 105</a></li> <li>• <a href="#">Filtering Traffic Using Extended Community Lists, page 144</a></li> </ul>
BGP Support for Sequenced Entries in Extended Community Lists	12.2(25)S 12.3(11)T	<p>The BGP Support for Sequenced Entries in Extended Community Lists feature introduces automatic sequencing of individual entries in BGP extended community lists. This feature also introduces the ability to remove or resequence extended community list entries without deleting the entire existing extended community list.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Communities, page 105</a></li> <li>• <a href="#">Filtering Traffic Using Extended Community Lists, page 144</a></li> </ul>





## Configuring Internal BGP Features

---

This chapter describes how to configure internal Border Gateway Protocol (BGP) features. BGP is an interdomain routing protocol designed to provide loop-free routing between organizations. For a complete description of the BGP commands in this chapter, refer to the “BGP Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

For an overview of BGP, see the “[Cisco BGP Overview](#)” module.

For details about basic BGP tasks, see the “[Configuring a Basic BGP Network](#)” module.

For details about connecting to a service provider, see the “[Connecting to a Service Provider Using External BGP](#)” module.

For protocol-independent features, see the chapter “Configuring IP Routing Protocol-Independent Features” in this book.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

## Configuring Internal BGP Features

The following sections contain optional internal BGP (iBGP) configuration tasks:

- [Configuring a Routing Domain Confederation](#) (Optional)
- [Configuring a Route Reflector](#) (Optional)
- [Adjusting BGP Timers](#) (Optional)
- [Configuring the Router to Consider a Missing MED as Worst Path](#) (Optional)
- [Configuring the Router to Consider the MED to Choose a Path from Subautonomous System Paths](#) (Optional)
- [Configuring the Router to Use the MED to Choose a Path in a Confederation](#) (Optional)
- [Configuring Route Dampening](#) (Optional)

For information on configuring features that apply to multiple IP routing protocols (such as redistributing routing information), see the chapter “Configuring IP Routing Protocol-Independent Features.”

## Configuring a Routing Domain Confederation

One way to reduce the internal BGP (iBGP) mesh is to divide an autonomous system into multiple subautonomous systems and group them into a single confederation. To the outside world, the confederation looks like a single autonomous system. Each autonomous system is fully meshed within itself, and has a few connections to other autonomous systems in the same confederation. Even though the peers in different autonomous systems have external BGP (eBGP) sessions, they exchange routing information as if they were iBGP peers. Specifically, the next hop, Multi\_Exit\_Discriminator (MED) attribute, and local preference information is preserved. This feature allows the you to retain a single Interior Gateway Protocol (IGP) for all of the autonomous systems.

To configure a BGP confederation, you must specify a confederation identifier. To the outside world, the group of autonomous systems will look like a single autonomous system with the confederation identifier as the autonomous system number. To configure a BGP confederation identifier, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp confederation identifier</b> <i>as-number</i>	Configures a BGP confederation.

In order to treat the neighbors from other autonomous systems within the confederation as special eBGP peers, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp confederation peers</b> <i>as-number</i> [ <i>as-number</i> ]	Specifies the autonomous systems that belong to the confederation.

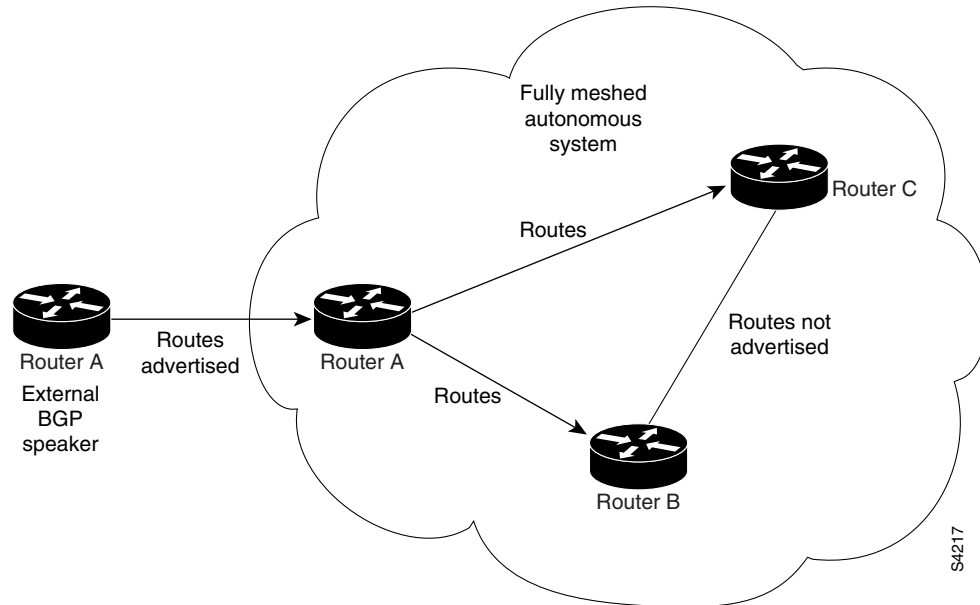
For an alternative way to reduce the iBGP mesh, see the next section, “[Configuring a Route Reflector](#).”

## Configuring a Route Reflector

BGP requires that all iBGP speakers be fully meshed. However, this requirement does not scale well when there are many iBGP speakers. Instead of configuring a confederation, another way to reduce the iBGP mesh is to configure a *route reflector*.

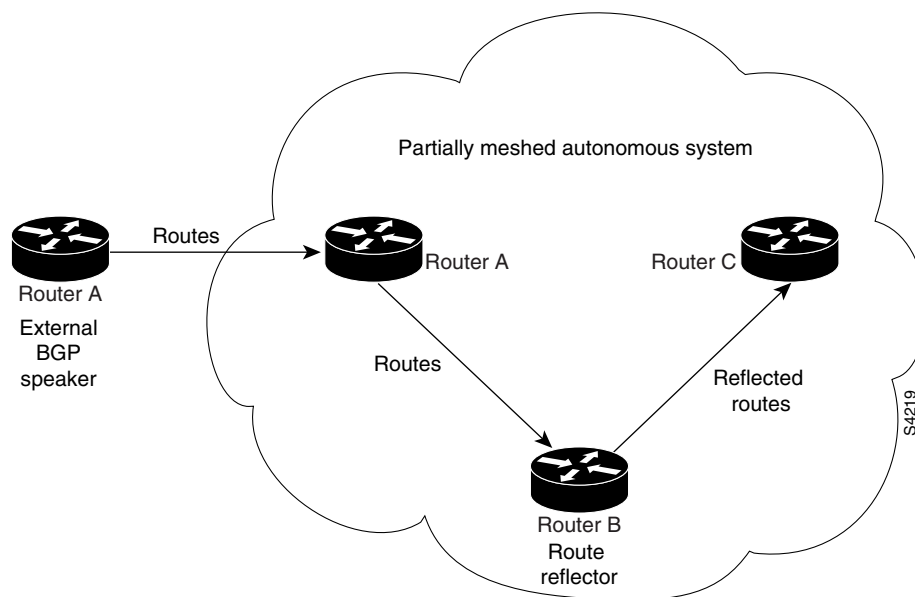
[Figure 16](#) illustrates a simple iBGP configuration with three iBGP speakers (Routers A, B, and C). Without route reflectors, when Router A receives a route from an external neighbor, it must advertise it to both routers B and C. Routers B and C do not readvertise the iBGP learned route to other iBGP speakers because the routers do not pass on routes learned from internal neighbors to other internal neighbors, thus preventing a routing information loop.

**Figure 16** *Three Fully Meshed iBGP Speakers*



With route reflectors, all iBGP speakers need not be fully meshed because there is a method to pass learned routes to neighbors. In this model, an iBGP peer is configured to be a route reflector responsible for passing iBGP learned routes to a set of iBGP neighbors. In [Figure 17](#), Router B is configured as a route reflector. When the route reflector receives routes advertised from Router A, it advertises them to Router C, and vice versa. This scheme eliminates the need for the iBGP session between Routers A and C.

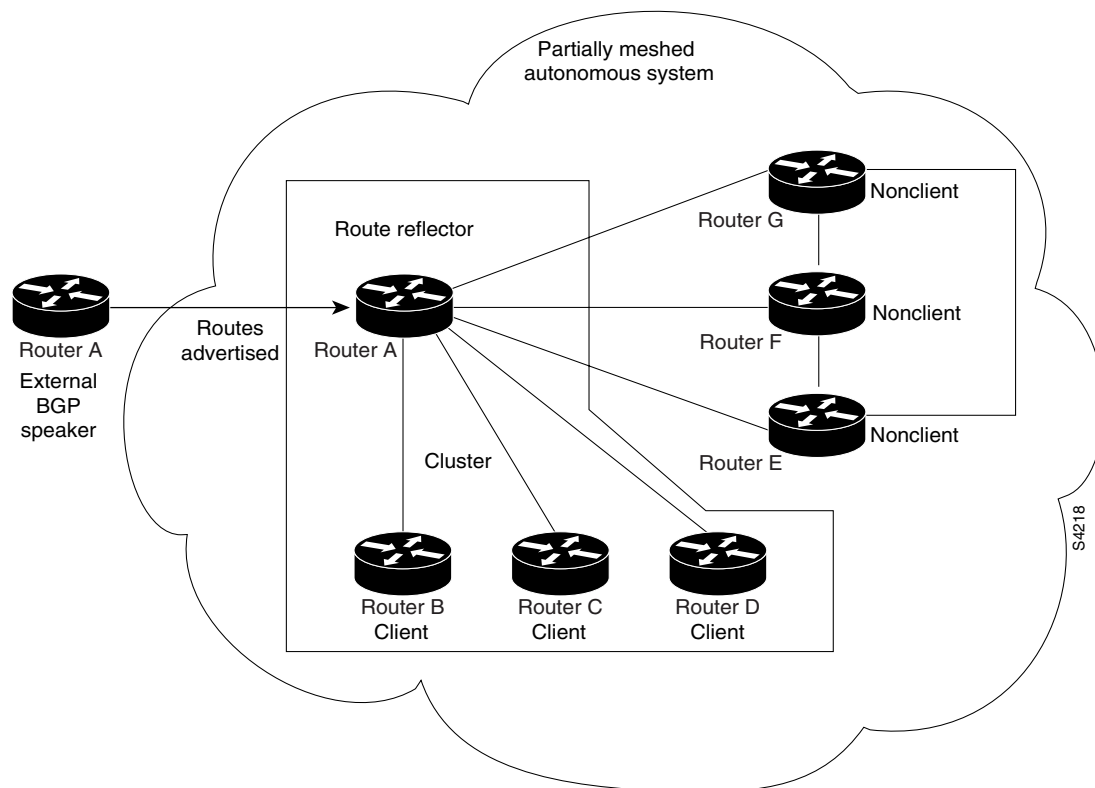
**Figure 17** *Simple BGP Model with a Route Reflector*



The internal peers of the route reflector are divided into two groups: client peers and all the other routers in the autonomous system (nonclient peers). A route reflector reflects routes between these two groups. The route reflector and its client peers form a *cluster*. The nonclient peers must be fully meshed with each other, but the client peers need not be fully meshed. The clients in the cluster do not communicate with iBGP speakers outside their cluster.

Figure 18 illustrates a more complex route reflector scheme. Router A is the route reflector in a cluster with routers B, C, and D. Routers E, F, and G are fully meshed, nonclient routers.

**Figure 18** More Complex BGP Route Reflector Model



When the route reflector receives an advertised route, depending on the neighbor, it takes the following actions:

- A route from an external BGP speaker is advertised to all clients and nonclient peers.
- A route from a nonclient peer is advertised to all clients.
- A route from a client is advertised to all clients and nonclient peers. Hence, the clients need not be fully meshed.

To configure a route reflector and its clients, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>neighbor</b> {ip-address   peer-group-name} <b>route-reflector-client</b>	Configures the local router as a BGP route reflector and the specified neighbor as a client.



Along with route reflector-aware BGP speakers, it is possible to have BGP speakers that do not understand the concept of route reflectors. They can be members of either client or nonclient groups allowing an easy and gradual migration from the old BGP model to the route reflector model. Initially, you could create a single cluster with a route reflector and a few clients. All the other iBGP speakers could be nonclient peers to the route reflector and then more clusters could be created gradually.

An autonomous system can have multiple route reflectors. A route reflector treats other route reflectors just like other iBGP speakers. A route reflector can be configured to have other route reflectors in a client group or nonclient group. In a simple configuration, the backbone could be divided into many clusters. Each route reflector would be configured with other route reflectors as nonclient peers (thus, all the route reflectors will be fully meshed). The clients are configured to maintain iBGP sessions with only the route reflector in their cluster.

Usually a cluster of clients will have a single route reflector. In that case, the cluster is identified by the router ID of the route reflector. To increase redundancy and avoid a single point of failure, a cluster might have more than one route reflector. In this case, all route reflectors in the cluster must be configured with the 4-byte cluster ID so that a route reflector can recognize updates from route reflectors in the same cluster. All the route reflectors serving a cluster should be fully meshed and all of them should have identical sets of client and nonclient peers.

If the cluster has more than one route reflector, configure the cluster ID by using the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp cluster-id</b> <i>cluster-id</i>	Configures the cluster ID.

Use the **show ip bgp EXEC** command to display the originator ID and the cluster-list attributes.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, the route reflector need not reflect routes to clients.

To disable client-to-client route reflection, use the **no bgp client-to-client reflection** command in router configuration mode:

Command	Purpose
Router(config-router)# <b>no bgp client-to-client reflection</b>	Disables client-to-client route reflection.

As the iBGP learned routes are reflected, routing information may loop. The route reflector model has the following mechanisms to avoid routing loops:

- Originator ID is an optional, nontransitive BGP attribute. It is a 4-byte attribute created by a route reflector. The attribute carries the router ID of the originator of the route in the local autonomous system. Therefore, if a misconfiguration causes routing information to come back to the originator, the information is ignored.
- Cluster-list is an optional, nontransitive BGP attribute. It is a sequence of cluster IDs that the route has passed. When a route reflector reflects a route from its clients to nonclient peers, and vice versa, it appends the local cluster ID to the cluster list. If the cluster list is empty, a new cluster list is created. Using this attribute, a route reflector can identify if routing information is looped back to the same cluster due to misconfiguration. If the local cluster ID is found in the cluster list, the advertisement is ignored.

- The use of **set** clauses in outbound route maps can modify attributes and possibly create routing loops. To avoid this behavior, **set** clauses of outbound route maps are ignored for routes reflected to iBGP peers.

## Adjusting BGP Timers

BGP uses certain timers to control periodic activities such as the sending of keepalive messages and the interval after not receiving a keepalive message after which the Cisco IOS software declares a peer dead. By default, the keepalive timer is 60 seconds, and the hold-time timer is 180 seconds. You can adjust these timers. When a connection is started, BGP will negotiate the hold time with the neighbor. The smaller of the two hold times will be chosen. The keepalive timer is then set based on the negotiated hold time and the configured keepalive time.

To adjust BGP timers for all neighbors, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>timers bgp</b> <i>keepalive holdtime</i>	Adjusts BGP timers for all neighbors.

To adjust BGP keepalive and hold-time timers for a specific neighbor, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>neighbor</b> [ <i>ip-address</i>   <i>peer-group-name</i> ] <b>timers</b> <i>keepalive holdtime</i>	Sets the keepalive and hold-time timers (in seconds) for the specified peer or peer group.



### Note

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** router configuration command.

To clear the timers for a BGP neighbor or peer group, use the **no** form of the **neighbor timers** command.

## Configuring the Router to Consider a Missing MED as Worst Path

To configure the router to consider a path with a missing MED attribute as the worst path, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp bestpath med missing-as-worst</b>	Configures the router to consider a missing MED as having a value of infinity, making the path without a MED value the least desirable path.

## Configuring the Router to Consider the MED to Choose a Path from Subautonomous System Paths

To configure the router to consider the MED value in choosing a path, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp bestpath med confed</b>	Configures the router to consider the MED in choosing a path from among those advertised by different subautonomous systems within a confederation.

The comparison between MEDs is made only if there are no external autonomous systems in the path (an external autonomous system is an autonomous system that is not within the confederation). If there is an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison is not made.

The following example compares route A with these paths:

```
path= 65000 65004, med=2
path= 65001 65004, med=3
path= 65002 65004, med=4
path= 65003 1, med=1
```

In this case, path 1 would be chosen if the **bgp bestpath med confed** router configuration command is enabled. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system in this path.

## Configuring the Router to Use the MED to Choose a Path in a Confederation

To configure the router to use the MED to choose the best path from among paths advertised by a single subautonomous system within a confederation, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp deterministic med</b>	Configures the router to compare the MED variable when choosing among routes advertised by different peers in the same autonomous system.



### Note

If the **bgp always-compare-med** router configuration command is enabled, all paths are fully comparable, including those from other autonomous systems in the confederation, even if the **bgp deterministic med** command is also enabled.

## Configuring Route Dampening

Route dampening is a BGP feature designed to minimize the propagation of flapping routes across an internetwork. A route is considered to be flapping when its availability alternates repeatedly.

For example, consider a network with three BGP autonomous systems: autonomous system 1, autonomous system 2, and autonomous system 3. Suppose the route to network A in autonomous system 1 flaps (it becomes unavailable). Under circumstances without route dampening, the eBGP neighbor of autonomous system 1 to autonomous system 2 sends a withdraw message to autonomous system 2. The border router in autonomous system 2, in turn, propagates the withdraw message to autonomous system 3. When the route to network A reappears, autonomous system 1 sends an advertisement message to

autonomous system 2, which sends it to autonomous system 3. If the route to network A repeatedly becomes unavailable, then available, many withdrawal and advertisement messages are sent. This is a problem in an internetwork connected to the Internet because a route flap in the Internet backbone usually involves many routes.

**Note**

No penalty is applied to a BGP peer reset when route dampening is enabled. Although the reset withdraws the route, no penalty is applied in this instance, even if route flap dampening is enabled.

## Minimizing Flapping

The route dampening feature minimizes the flapping problem as follows. Suppose again that the route to network A flaps. The router in autonomous system 2 (where route dampening is enabled) assigns network A a penalty of 1000 and moves it to history state. The router in autonomous system 2 continues to advertise the status of the route to neighbors. The penalties are cumulative. When the route flaps so often that the penalty exceeds a configurable suppress limit, the router stops advertising the route to network A, regardless of how many times it flaps. Thus, the route is dampened.

The penalty placed on network A is decayed until the reuse limit is reached, upon which the route is once again advertised. At half of the reuse limit, the dampening information for the route to network A is removed.

## Understanding Route Dampening Terms

The following terms are used when describing route dampening:

- **Flap**—A route whose availability alternates repeatedly.
- **History state**—After a route flaps once, it is assigned a penalty and put into history state, meaning the router does not have the best path, based on historical information.
- **Penalty**—Each time a route flaps, the router configured for route dampening in another autonomous system assigns the route a penalty of 1000. Penalties are cumulative. The penalty for the route is stored in the BGP routing table until the penalty exceeds the suppress limit. At that point, the route state changes from history to damp.
- **Damp state**—In this state, the route has flapped so often that the router will not advertise this route to BGP neighbors.
- **Suppress limit**—A route is suppressed when its penalty exceeds this limit. The default value is 2000.
- **Half-life**—Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds.
- **Reuse limit**—As the penalty for a flapping route decreases and falls below this reuse limit, the route is unsuppressed. That is, the route is added back to the BGP table and once again used for forwarding. The default reuse limit is 750. The process of unsuppressing routes occurs at 10-second increments. Every 10 seconds, the router finds out which routes are now unsuppressed and advertises them to the world.
- **Maximum suppress limit**—This value is the maximum amount of time a route can be suppressed. The default value is four times the half-life.

The routes external to an autonomous system learned via iBGP are not dampened. This policy prevents the iBGP peers from having a higher penalty for routes external to the autonomous system.

## Enabling Route Dampening

To enable BGP route dampening, use the following command in address family or router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp dampening</b>	Enables BGP route dampening.

To change the default values of various dampening factors, use the following command in address family or router configuration mode:

Command	Purpose
Router(config-router)# <b>bgp dampening</b> <i>half-life reuse suppress max-suppress [route-map map-name]</i>	Changes the default values of route dampening factors.

## Monitoring and Maintaining BGP Route Dampening

You can monitor the flaps of all the paths that are flapping. The statistics will be deleted once the route is not suppressed and is stable for at least one half-life. To display flap statistics, use the following commands in EXEC mode as needed:

Command	Purpose
Router# <b>show ip bgp flap-statistics</b>	Displays BGP flap statistics for all paths.
Router# <b>show ip bgp flap-statistics regexp</b> <i>regexp</i>	Displays BGP flap statistics for all paths that match the regular expression.
Router# <b>show ip bgp flap-statistics filter-list</b> <i>access-list</i>	Displays BGP flap statistics for all paths that pass the filter.
Router# <b>show ip bgp flap-statistics ip-address mask</b>	Displays BGP flap statistics for a single entry.
Router# <b>show ip bgp flap-statistics ip-address mask longer-prefix</b>	Displays BGP flap statistics for more specific entries.

To clear BGP flap statistics (thus making it less likely that the route will be dampened), use the following commands in EXEC mode as needed:

Command	Purpose
Router# <b>clear ip bgp flap-statistics</b>	Clears BGP flap statistics for all routes.
Router# <b>clear ip bgp flap-statistics regexp</b> <i>regexp</i>	Clears BGP flap statistics for all paths that match the regular expression.
Router# <b>clear ip bgp flap-statistics filter-list</b> <i>list</i>	Clears BGP flap statistics for all paths that pass the filter.
Router# <b>clear ip bgp flap-statistics ip-address mask</b>	Clears BGP flap statistics for a single entry.
Router# <b>clear ip bgp ip-address flap-statistics</b>	Clears BGP flap statistics for all paths from a neighbor.

**Note**

The flap statistics for a route are also cleared when a BGP peer is reset. Although the reset withdraws the route, there is no penalty applied in this instance, even if route flap dampening is enabled.

Once a route is dampened, you can display BGP route dampening information, including the time remaining before the dampened routes will be unsuppressed. To display the information, use the following command in EXEC mode:

Command	Purpose
Router# <b>show ip bgp dampened-paths</b>	Displays the dampened routes, including the time remaining before they will be unsuppressed.

You can clear BGP route dampening information and unsuppress any suppressed routes by using the following command in EXEC mode:

Command	Purpose
Router# <b>clear ip bgp dampening</b> [ <i>ip-address network-mask</i> ]	Clears route dampening information and unsuppresses the suppressed routes.

## Internal BGP Feature Configuration Examples

The following sections provide internal BGP feature configuration examples:

- [BGP Confederation Configurations with Route Maps Example](#)
- [BGP Confederation Examples](#)

### BGP Confederation Configurations with Route Maps Example

This section contains an example of the use of a BGP confederation configuration that includes BGP communities and route maps. For more examples of how to configure a BGP confederation, see the section “[BGP Confederation Examples](#)” in this chapter.

This example shows how BGP community attributes are used with a BGP confederation configuration to filter routes.

In this example, the route map named set-community is applied to the outbound updates to neighbor 172.16.232.50 and the local-as community attribute is used to filter the routes. The routes that pass access list 1 have the special community attribute value local-as. The remaining routes are advertised normally. This special community value automatically prevents the advertisement of those routes by the BGP speakers outside autonomous system 200.

```
router bgp 65000
 network 10.0.1.0 route-map set-community
 bgp confederation identifier 200
 bgp confederation peers 65001
 neighbor 172.16.232.50 remote-as 100
 neighbor 172.16.233.2 remote-as 65001
!
route-map set-community permit 10
 match ip address 1
```

```
set community local-as
!
```

## BGP Confederation Examples

The following is a sample configuration that shows several peers in a confederation. The confederation consists of three internal autonomous systems with autonomous system numbers 6001, 6002, and 6003. To the BGP speakers outside the confederation, the confederation looks like a normal autonomous system with autonomous system number 666 (specified via the **bgp confederation identifier** router configuration command).

In a BGP speaker in autonomous system 6001, the **bgp confederation peers** router configuration command marks the peers from autonomous systems 6002 and 6003 as special eBGP peers. Hence peers 172.16.232.55 and 172.16.232.56 will get the local preference, next hop, and MED unmodified in the updates. The router at 10.16.69.1 is a normal eBGP speaker and the updates received by it from this peer will be just like a normal eBGP update from a peer in autonomous system 600.

```
router bgp 6001
  bgp confederation identifier 600
  bgp confederation peers 6002 6003
  neighbor 172.16.232.55 remote-as 6002
  neighbor 172.16.232.56 remote-as 6003
  neighbor 10.16.69.1 remote-as 777
```

In a BGP speaker in autonomous system 6002, the peers from autonomous systems 6001 and 6003 are configured as special eBGP peers. 10.70.70.1 is a normal iBGP peer and 10.99.99.2 is a normal eBGP peer from autonomous system 700.

```
router bgp 6002
  bgp confederation identifier 666
  bgp confederation peers 6001 6003
  neighbor 10.70.70.1 remote-as 6002
  neighbor 172.16.232.57 remote-as 6001
  neighbor 172.16.232.56 remote-as 6003
  neighbor 10.99.99.2 remote-as 700
```

In a BGP speaker in autonomous system 6003, the peers from autonomous systems 6001 and 6002 are configured as special eBGP peers. 10.200.200.200 is a normal eBGP peer from autonomous system 701.

```
router bgp 6003
  bgp confederation identifier 666
  bgp confederation peers 6001 6002
  neighbor 172.16.232.57 remote-as 6001
  neighbor 172.16.232.55 remote-as 6002
  neighbor 10.200.200.200 remote-as 701
```

The following is a part of the configuration from the BGP speaker 10.200.200.205 from autonomous system 701 in the same example. Neighbor 172.16.232.56 is configured as a normal eBGP speaker from autonomous system 666. The internal division of the autonomous system into multiple autonomous systems is not known to the peers external to the confederation.

```
router bgp 701
  neighbor 172.16.232.56 remote-as 666
  neighbor 10.200.200.205 remote-as 701
```







## BGP Link Bandwidth

The Border Gateway Protocol (BGP) Link Bandwidth feature is used to advertise the bandwidth of an autonomous system exit link as an extended community. This feature is configured for links between directly connected external BGP (eBGP) neighbors. The link bandwidth extended community attribute is propagated to iBGP peers when extended community exchange is enabled. This feature is used with BGP multipath features to configure load balancing over links with unequal bandwidth.

### History for the BGP Link Bandwidth Feature

Release	Modification
12.2(2)T	This feature was introduced.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.0(14)S.
12.2(11)T	This feature was integrated in Cisco IOS Release 12.2(11)T.
12.0(24)S	This feature was integrated into Cisco IOS Release 12.0(24)S.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Link Bandwidth, page 180](#)
- [Restrictions for BGP Link Bandwidth, page 180](#)
- [Information About BGP Link Bandwidth, page 180](#)
- [How to Configure BGP Link Bandwidth, page 181](#)
- [Configuration Examples for BGP Link Bandwidth, page 183](#)
- [Additional References, page 187](#)
- [Command Reference, page 189](#)

## Prerequisites for BGP Link Bandwidth

- BGP load balancing or multipath load balancing must be configured before this feature is enabled.
- BGP extended community exchange must be enabled between iBGP neighbors to which the link bandwidth attribute is to be advertised.
- Cisco Express Forwarding (CEF) or distributed CEF (dCEF) must be enabled on all participating routers.

## Restrictions for BGP Link Bandwidth

- This feature can be configured only under IPv4 and VPNv4 address family sessions.
- BGP can originate the link bandwidth community only for directly connected links to eBGP neighbors.
- Both iBGP and eBGP load balancing are supported in IPv4 and VPNv4 address families. However, eiBGP load balancing is supported only in VPNv4 address-family.

## Information About BGP Link Bandwidth

To configure the BGP Link Bandwidth feature, you must understand the following concept:

- [BGP Link Bandwidth Overview, page 180](#)
- [Link Bandwidth Extended Community Attribute, page 181](#)
- [Benefits of the BGP Link Bandwidth Feature, page 181](#)

## BGP Link Bandwidth Overview

The BGP Link Bandwidth feature used to enable multipath load balancing for external links with unequal bandwidth capacity. This feature is enabled under an IPv4 or VPNv4 address family sessions by entering the **bgp dmzlink-bw** command. This feature supports both iBGP, eBGP multipath load balancing, and eiBGP multipath load balancing in Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). When this feature is enabled, routes learned from directly connected external neighbor are propagated through the internal BGP (iBGP) network with the bandwidth of the source external link.

The link bandwidth extended community indicates the preference of an autonomous system exit link in terms of bandwidth. This extended community is applied to external links between directly connected eBGP peers by entering the **neighbor dmzlink-bw** command. The link bandwidth extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command.

## Link Bandwidth Extended Community Attribute

The link bandwidth extended community attribute is a 4-byte value that is configured for a link that on the demilitarized zone (DMZ) interface that connects two single hop eBGP peers. The link bandwidth extended community attribute is used as a traffic sharing value relative to other paths while forwarding traffic. Two paths are designated as equal for load balancing if the weight, local-pref, as-path length, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) costs are the same.

## Benefits of the BGP Link Bandwidth Feature

The BGP Link Bandwidth feature allows BGP to be configured to send traffic over multiple iBGP or eBGP learned paths where the traffic that is sent is proportional to the bandwidth of the links that are used to exit the autonomous system. The configuration of this feature can be used with eBGP and iBGP multipath features to enable unequal cost load balancing over multiple links. Unequal cost load balancing over links with unequal bandwidth was not possible in BGP before the BGP Link Bandwidth feature was introduced.

## How to Configure BGP Link Bandwidth

This section contains the following procedures:

- [Configuring BGP Link Bandwidth, page 181](#)
- [Verifying BGP Link Bandwidth Configuration, page 183](#)

## Configuring BGP Link Bandwidth

To configure the BGP Link Bandwidth feature, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure {terminal | memory | network}**
3. **router bgp *as-number***
4. **address-family ipv4 [mdt | multicast | tunnel | unicast [*vrf vrf-name*] | vrf *vrf-name*] | ipv6 [multicast | unicast] | vpnv4 [unicast]**
5. **bgp dmzlink-bw**
6. **neighbor *ip-address* dmzlink-bw**
7. **neighbor *ip-address* send-community [both | extended | standard]**
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure {terminal   memory   network}</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp as-number</b>  <b>Example:</b> Router(config)# router bgp 50000	Enters router configuration mode to create or configure a BGP routing process.
Step 4	<b>address-family ipv4 [mdt   multicast   tunnel   unicast [vrf vrf-name]   vrf vrf-name]   ipv6 [multicast   unicast]   vpnv4 [unicast]</b>  <b>Example:</b> Router(config-router)# address-family ipv4	Places the router in address family configuration mode. <ul style="list-style-type: none"> <li>The BGP Link Bandwidth feature is supported only under the IPv4 and VPNv4 address families.</li> </ul>
Step 5	<b>bgp dmzlink-bw</b>  <b>Example:</b> Router(config-router-af)# bgp dmzlink-bw	Configures BGP to distribute traffic proportionally to the bandwidth of the link. <ul style="list-style-type: none"> <li>This command must be entered on each router that contains an external interface that is to be used for multipath load balancing.</li> </ul>
Step 6	<b>neighbor ip-address dmzlink-bw</b>  <b>Example:</b> Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw	Configures BGP to include the link bandwidth attribute for routes learned from the external interface specified IP address. <ul style="list-style-type: none"> <li>This command must be configured for each eBGP link that is to be configured as a multipath. Enabling this command allows the bandwidth of the external link to be propagated through the link bandwidth extended community.</li> </ul>
Step 7	<b>neighbor ip-address send-community [both   extended   standard]</b>  <b>Example:</b> Router(config-router-af)# neighbor 10.10.10.1 send-community extended	(Optional) Enables community and/or extended community exchange with the specified neighbor. <ul style="list-style-type: none"> <li>This command must be configured for iBGP peers to which the link bandwidth extended community attribute is to be propagated.</li> </ul>
Step 8	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode, and enters Privileged EXEC mode.

## Verifying BGP Link Bandwidth Configuration

To verify the BGP Link Bandwidth feature, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp** *ip-address* [**longer-prefixes** [*injected*] | **shorter-prefixes** [*mask-length*]]
3. **show ip route** [[*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*] | [**static download**]]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show ip bgp</b> <i>ip-address</i> [ <b>longer-prefixes</b> [ <i>injected</i> ]   <b>shorter-prefixes</b> [ <i>mask-length</i> ]]  <b>Example:</b> Router# show ip bgp 10.0.0.0	Displays information about the TCP and BGP connections to neighbors. <ul style="list-style-type: none"> <li>• The output displays the status of the link bandwidth configuration. The bandwidth of the link is shown in kilobytes.</li> </ul>
Step 3	<b>show ip route</b> [[ <i>ip-address</i> [ <i>mask</i> ] [ <b>longer-prefixes</b> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]   [ <b>list</b> <i>access-list-number</i>   <i>access-list-name</i> ]   [ <b>static download</b> ]]  <b>Example:</b> Router# show ip route 10.0.0.0	Displays the current state of the routing table. <ul style="list-style-type: none"> <li>• The output displays traffic share values, including the weights of the links that are used to direct traffic proportionally to the bandwidth of each link.</li> </ul>

## Configuration Examples for BGP Link Bandwidth

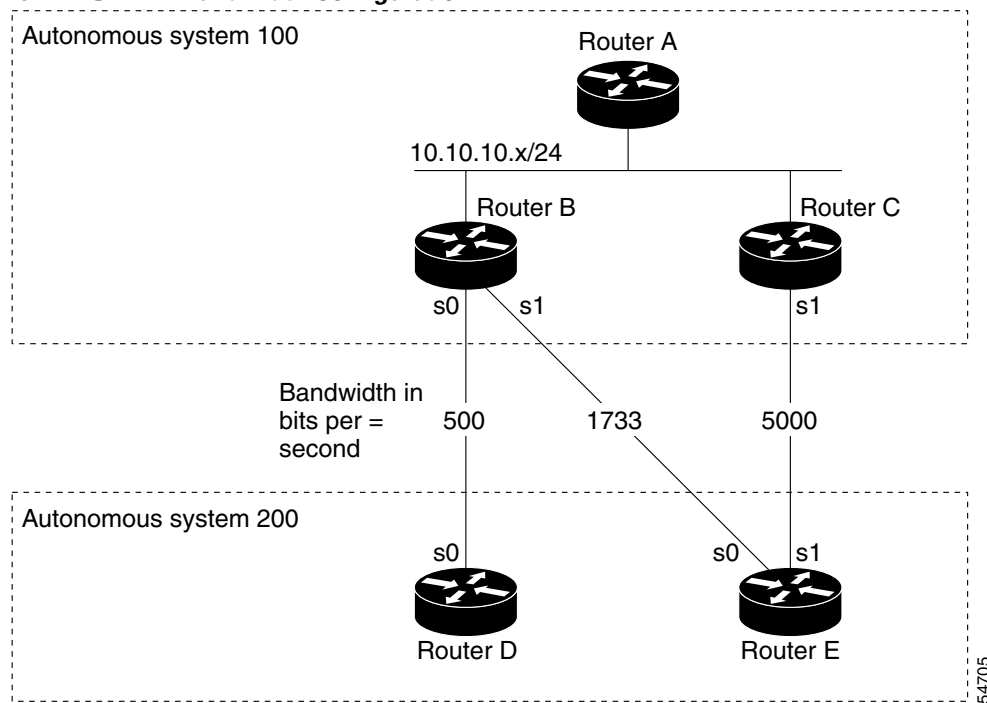
The following examples show how to configure and verify this feature:

- [BGP Link Bandwidth Configuration Example, page 184](#)
- [Verifying BGP Link Bandwidth, page 186](#)

## BGP Link Bandwidth Configuration Example

In the following examples, the BGP Link Bandwidth feature is configured so BGP will distribute traffic proportionally to the bandwidth of each external link. Figure 19 shows two external autonomous systems connected by three links that each carry a different amount of bandwidth (unequal cost links). Multipath load balancing is enabled and traffic is balanced proportionally.

**Figure 19 BGP Link Bandwidth Configuration**



### Router A Configuration

In the following example, Router A is configured to support iBGP multipath load balancing and to exchange the BGP extended community attribute with iBGP neighbors:

```
Router A(config)# router bgp 100
Router A(config-router)# neighbor 10.10.10.2 remote-as 100
Router A(config-router)# neighbor 10.10.10.2 update-source Loopback 0
Router A(config-router)# neighbor 10.10.10.3 remote-as 100
Router A(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router A(config-router)# address-family ipv4
Router A(config-router)# bgp dmzlink-bw
Router A(config-router-af)# neighbor 10.10.10.2 activate
Router A(config-router-af)# neighbor 10.10.10.2 send-community both
Router A(config-router-af)# neighbor 10.10.10.3 activate
Router A(config-router-af)# neighbor 10.10.10.3 send-community both
Router A(config-router-af)# maximum-paths ibgp 6
```

### Router B Configuration

In the following example, Router B is configured to support multipath load balancing, to distribute Router D and Router E link traffic proportionally to the bandwidth of each link, and to advertise the bandwidth of these links to iBGP neighbors as an extended community:

```
Router B(config)# router bgp 100
Router B(config-router)# neighbor 10.10.10.1 remote-as 100
Router B(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router B(config-router)# neighbor 10.10.10.3 remote-as 100
Router B(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router B(config-router)# neighbor 172.16.1.1 remote-as 200
Router B(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router B(config-router)# neighbor 172.16.2.2 remote-as 200
Router B(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router B(config-router)# address-family ipv4
Router B(config-router-af)# bgp dmzlink-bw
Router B(config-router-af)# neighbor 10.10.10.1 activate
Router B(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router B(config-router-af)# neighbor 10.10.10.1 send-community both
Router B(config-router-af)# neighbor 10.10.10.3 activate
Router B(config-router-af)# neighbor 10.10.10.3 next-hop-self
Router B(config-router-af)# neighbor 10.10.10.3 send-community both
Router B(config-router-af)# neighbor 172.16.1.1 activate
Router B(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
Router B(config-router-af)# neighbor 172.16.2.2 activate
Router B(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router B(config-router-af)# maximum-paths ibgp 6
Router B(config-router-af)# maximum-paths 6
```

### Router C Configuration

In the following example, Router C is configured to support multipath load balancing and to advertise the bandwidth of the link with Router E to iBGP neighbors as an extended community:

```
Router C(config)# router bgp 100
Router C(config-router)# neighbor 10.10.10.1 remote-as 100
Router C(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router C(config-router)# neighbor 10.10.10.2 remote-as 100
Router C(config-router)# neighbor 10.10.10.2 update-source Loopback 0
Router C(config-router)# neighbor 172.16.3.30 remote-as 200
Router C(config-router)# neighbor 172.16.3.30 ebgp-multihop 1
Router C(config-router)# address-family ipv4
Router C(config-router-af)# bgp dmzlink-bw
Router C(config-router-af)# neighbor 10.10.10.1 activate
Router C(config-router-af)# neighbor 10.10.10.1 send-community both
Router C(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router C(config-router-af)# neighbor 10.10.10.2 activate
Router C(config-router-af)# neighbor 10.10.10.2 send-community both
Router C(config-router-af)# neighbor 10.10.10.2 next-hop-self
Router C(config-router-af)# neighbor 172.16.3.3 activate
Router C(config-router-af)# neighbor 172.16.3.3 dmzlink-bw
Router C(config-router-af)# maximum-paths ibgp 6
Router C(config-router-af)# maximum-paths 6
```

## Verifying BGP Link Bandwidth

The examples in this section show the verification of this feature on Router A and Router B.

### Router B

In the following example, the **show ip bgp** command is entered on Router B to verify that two unequal cost best paths have been installed into the BGP routing table. The bandwidth for each link is displayed with each route.

```
Router B# show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 48
Paths: (2 available, best #2)
Multipath: eBGP
  Advertised to update-groups:
    1          2
200
  172.16.1.1 from 172.16.1.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 278 kbytes
200
  172.16.2.2 from 172.16.2.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 625 kbytes
```

### Router A

In the following example, the **show ip bgp** command is entered on Router A to verify that the link bandwidth extended community has been propagated through the iBGP network to Router A. The output shows that a route for each exit link (on Router B and Router C) to autonomous system 200 has been installed as a best path in the BGP routing table.

```
Router A# show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 48
Paths: (3 available, best #3)
Multipath: eBGP
  Advertised to update-groups:
    1          2
200
  172.16.1.1 from 172.16.1.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath
    Extended Community: 0x0:0:0
    DMZ-Link Bw 278 kbytes
200
  172.16.2.2 from 172.16.2.2 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 625 kbytes
200
  172.16.3.3 from 172.16.3.3 (192.168.1.1)
    Origin incomplete, metric 0, localpref 100, valid, external, multipath, best
    Extended Community: 0x0:0:0
    DMZ-Link Bw 2500 kbytes
```



**Router A**

In the following example, the **show ip route** command is entered on Router A to verify the multipath routes that are advertised and the associated traffic share values:

```
Router A# show ip route 192.168.1.0
Routing entry for 192.168.1.0/24
  Known via "bgp 100", distance 200, metric 0
  Tag 200, type internal
  Last update from 172.168.1.1 00:01:43 ago
  Routing Descriptor Blocks:
    * 172.168.1.1, from 172.168.1.1, 00:01:43 ago
      Route metric is 0, traffic share count is 13
      AS Hops 1, BGP network version 0
      Route tag 200
    172.168.2.2, from 172.168.2.2, 00:01:43 ago
      Route metric is 0, traffic share count is 30
      AS Hops 1, BGP network version 0
      Route tag 200
    172.168.3.3, from 172.168.3.3, 00:01:43 ago
      Route metric is 0, traffic share count is 120
      AS Hops 1, BGP network version 0
      Route tag 200
```

## Where to Go Next

For information about the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature, refer to the following document:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s\\_eibmpl.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s_eibmpl.htm)

For more information about the iBGP Multipath Load Sharing feature, refer to the following document:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftbgpls.htm>

## Additional References

The following sections provide references related to BGP Link Bandwidth feature.

## Related Documents

Related Topic	Document Title
BGP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul>
BGP configuration tasks	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>
CEF configuration tasks	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS Switching Services Configuration Guide, 12.3</a></li> </ul>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFCs

RFC	Title
draft-ramachandra-bgp-ext-communities-09.txt	<i>BGP Extended Communities Attribute</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	TAC Home Page: <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> BGP Support Page: <a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a>

# Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **bgp dmzlink-bw**
- **neighbor dmzlink-bw**





# iBGP Multipath Load Sharing

## Feature History

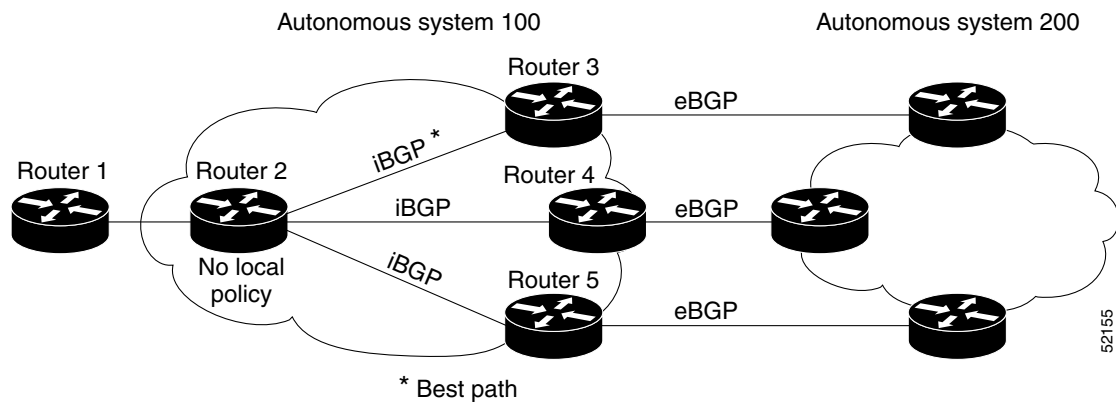
Release	Modification
12.2(2)T	This feature was introduced.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This feature module describes the iBGP Multipath Load Sharing feature. It includes the following sections:

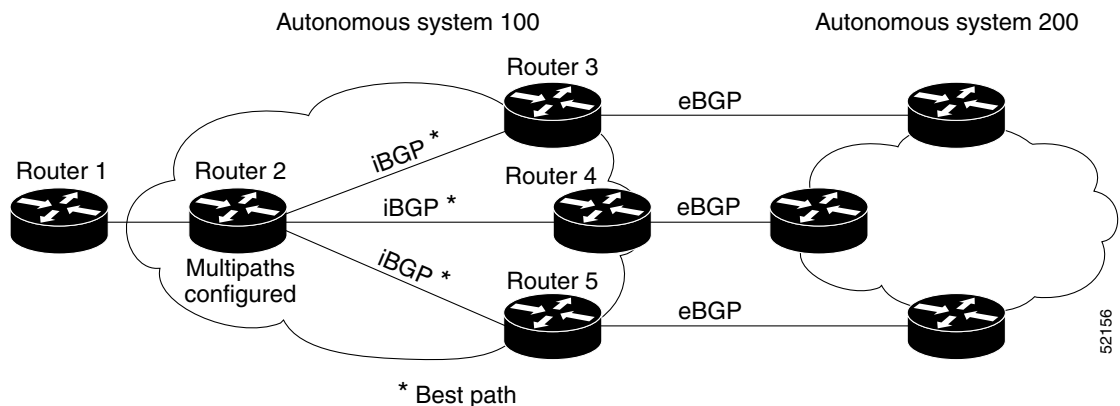
- [Feature Overview, page 191](#)
- [Supported Platforms, page 194](#)
- [Supported Standards, MIBs, and RFCs, page 195](#)
- [Configuration Tasks, page 195](#)
- [Monitoring and Maintaining iBGP Multipath Load Sharing, page 198](#)
- [Configuration Examples, page 198](#)
- [Command Reference, page 200](#)

## Feature Overview

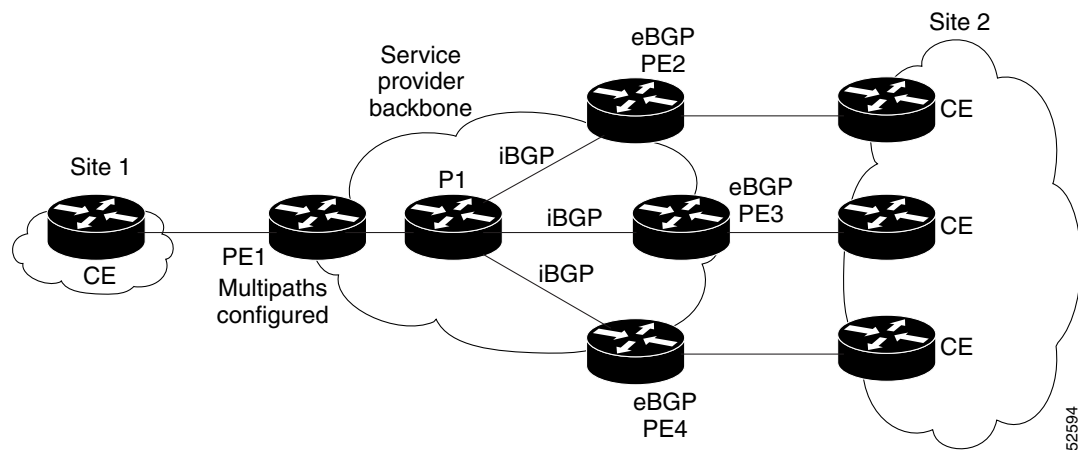
When a Border Gateway Protocol (BGP) speaking router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP (iBGP) for the same destination, the router will choose one iBGP path as the best path. The best path is then installed in the IP routing table of the router. For example, in [Figure 20](#), although there are three paths to autonomous system 200, Router 2 determines that one of the paths to autonomous system 200 is the best path and uses this path only to reach autonomous system 200.

**Figure 20** *Non-MPLS Topology with One Best Path*

The iBGP Multipath Load Sharing feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination. The best paths or multipaths are then installed in the IP routing table of the router. For example, on router 2 in [Figure 21](#), the paths to routers 3, 4, and 5 are configured as multipaths and can be used to reach autonomous system 200, thereby equally sharing the load to autonomous system 200.

**Figure 21** *Non-MPLS Topology with Three Multipaths*

The iBGP Multipath Load Sharing feature functions similarly in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) with a service provider backbone. For example, on router PE1 in [Figure 22](#), the paths to routers PE2, PE3, and PE4 can be selected as multipaths and can be used to equally share the load to site 2.

**Figure 22** *MPLS VPN with Three Multipaths*

For multiple paths to the same destination to be considered as multipaths, the following criteria must be met:

- All attributes must be the same. The attributes include weight, local preference, autonomous system path (entire attribute and not just length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.
- The next hop router for each multipath must be different.

Even if the criteria are met and multiple paths are considered multipaths, the BGP speaking router will still designate one of the multipaths as the best path and advertise this best path to its neighbors.

## Benefits

Configuring multiple iBGP best paths enables a router to evenly share the traffic destined for a particular site.

## Restrictions

### Route Reflector Limitation

With multiple iBGP paths installed in a routing table, a route reflector will advertise only one of the paths (one next hop).

### Memory Consumption Restriction

Each IP routing table entry for a BGP prefix that has multiple iBGP paths uses approximately 350 bytes of additional memory. We recommend not using this feature on a router with a low amount of available memory and especially when the router is carrying a full Internet routing table.

## Related Features and Technologies

The iBGP Multipath Load Sharing feature is similar to BGP multipath support for external BGP (eBGP) paths; however, the iBGP Multipath Load Sharing feature is applied to internal rather than eBGP paths. BGP multipath support for eBGP paths is documented in the “Configuring BGP” chapter of the *Cisco IOS IP Routing Configuration Guide* and in the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

The iBGP Multipath Load Sharing feature is related to the BGP Link Bandwidth feature, which is documented in the “New Features in Release 12.2(14)S” area of Cisco.com.

## Related Documents

For related information on this feature, refer to the following documents:

- *Cisco IOS IP Routing Configuration Guide*, Release 12.2.
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*
- *BGP Link Bandwidth*

For more information on MPLS VPNs, refer to the following documents:

- *Cisco IOS Switching Services Configuration Guide*, Release 12.2.
- *Cisco IOS Switching Services Command Reference*, Release 12.2.

## Supported Platforms

The iBGP Multipath Load Sharing feature is supported for the following platforms in Cisco IOS Release 12.2(14)S:

- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.



Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

#### Standards

No new or modified standards are supported by this feature.

#### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

#### RFCs

No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the iBGP Multipath Load Sharing feature. Each task in the list is identified as either required or optional.

- [Configuring iBGP Multipath Load Sharing](#) (required)
- [Verifying iBGP Multipath Load Sharing](#) (optional)

## Configuring iBGP Multipath Load Sharing

To configure the iBGP Multipath Load Sharing feature, use the following command in router configuration mode:

Command	Purpose
Router(config-router)# <b>maximum-paths ibgp</b> <i>maximum-number</i>	Controls the maximum number of parallel iBGP routes that can be installed in a routing table.

## Verifying iBGP Multipath Load Sharing

To verify that the iBGP Multipath Load Sharing feature is configured correctly, perform the following steps:

- Step 1** Enter the **show ip bgp network-number** EXEC command to display attributes for a network in a non-MPLS topology, or the **show ip bgp vpnv4 all ip-prefix** EXEC command to display attributes for a network in an MPLS VPN:

```
Router# show ip bgp 10.22.22.0
```

```
BGP routing table entry for 10.22.22.0/24, version 119
Paths:(6 available, best #1)
Multipath:iBGP
Flag:0x820
  Advertised to non peer-group peers:
    10.1.12.12
    22
    10.2.3.8 (metric 11) from 10.1.3.4 (100.0.0.5)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Originator:100.0.0.5, Cluster list:100.0.0.4
    22
    10.2.1.9 (metric 11) from 10.1.1.2 (100.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.9, Cluster list:100.0.0.2
    22
    10.2.5.10 (metric 11) from 10.1.5.6 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.6
    22
    10.2.4.10 (metric 11) from 10.1.4.5 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.5
    22
    10.2.6.10 (metric 11) from 10.1.6.7 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Originator:100.0.0.10, Cluster list:100.0.0.7
```

```
Router# show ip bgp vpnv4 all 10.22.22.0
```

```
BGP routing table entry for 100:1:10.22.22.0/24, version 50
Paths:(6 available, best #1)
Multipath:iBGP
  Advertised to non peer-group peers:
    200.1.12.12
    22
    10.22.7.8 (metric 11) from 10.11.3.4 (100.0.0.8)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
      Extended Community:RT:100:1
      Originator:100.0.0.8, Cluster list:100.1.1.44
    22
    10.22.1.9 (metric 11) from 10.11.1.2 (100.0.0.9)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.9, Cluster list:100.1.1.22
    22
    10.22.6.10 (metric 11) from 10.11.6.7 (100.0.0.10)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1
      Originator:100.0.0.10, Cluster list:100.0.0.7
    22
```

```

10.22.4.10 (metric 11) from 10.11.4.5 (100.0.0.10)
  Origin IGP, metric 0, localpref 100, valid, internal, multipath
  Extended Community:RT:100:1
  Originator:100.0.0.10, Cluster list:100.0.0.5
22
10.22.5.10 (metric 11) from 10.11.5.6 (100.0.0.10)
  Origin IGP, metric 0, localpref 100, valid, internal, multipath
  Extended Community:RT:100:1
  Originator:100.0.0.10, Cluster list:100.0.0.6

```

**Step 2** In the display resulting from the **show ip bgp network-number EXEC** command or the **show ip bgp vpnv4 all ip-prefix EXEC** command, verify that the intended multipaths are marked as “multipaths.” Notice that one of the multipaths is marked as “best.”

**Step 3** Enter the **show ip route ip-address EXEC** command to display routing information for a network in a non-MPLS topology or the **show ip route vrf vrf-name ip-prefix EXEC** command to display routing information for a network in an MPLS VPN:

```
Router# show ip route 10.22.22.0
```

```

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.2.6.10 00:00:03 ago
  Routing Descriptor Blocks:
  * 10.2.3.8, from 10.1.3.4, 00:00:03 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.2.1.9, from 10.1.1.2, 00:00:03 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.2.5.10, from 10.1.5.6, 00:00:03 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.2.4.10, from 10.1.4.5, 00:00:03 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.2.6.10, from 10.1.6.7, 00:00:03 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1

```

```
Router# show ip route vrf PATH 10.22.22.0
```

```

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1

```

- Step 4** Verify that the paths marked as “multipath” in the display resulting from the **show ip bgp *ip-prefix*** EXEC command or the **show ip bgp vpnv4 all *ip-prefix*** EXEC command are included in the routing information. (The routing information is displayed after performing [Step 3](#).)

## Monitoring and Maintaining iBGP Multipath Load Sharing

To display iBGP Multipath Load Sharing information, use the following commands in EXEC mode, as needed:

Command	Purpose
Router# <b>show ip bgp <i>ip-prefix</i></b>	Displays attributes and multipaths for a network in a non-MPLS topology.
Router# <b>show ip bgp vpnv4 all <i>ip-prefix</i></b>	Displays attributes and multipaths for a network in an MPLS VPN.
Router# <b>show ip route <i>ip-prefix</i></b>	Displays routing information for a network in a non-MPLS topology.
Router# <b>show ip route vrf <i>vrf-name ip-prefix</i></b>	Displays routing information for a network in an MPLS VPN.

## Configuration Examples

This section provides the following configuration examples:

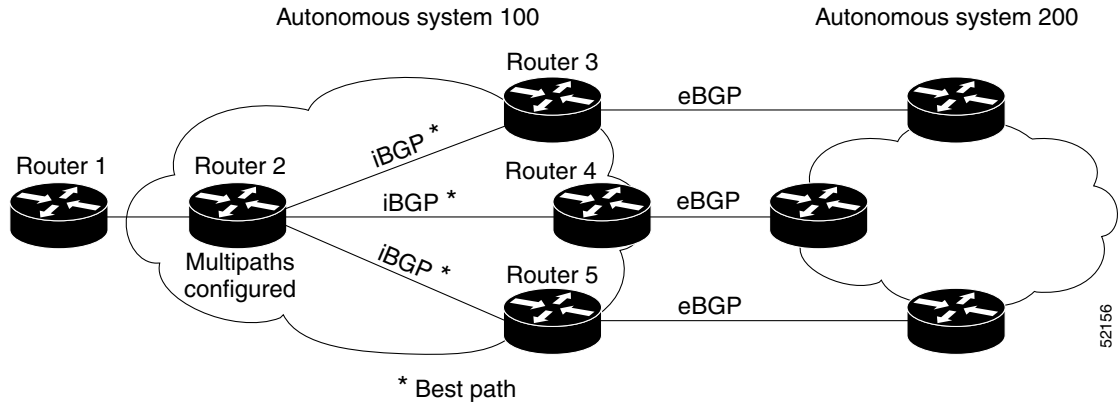
- [Non-MPLS Topology Example](#)
- [MPLS VPN Topology Example](#)

Both examples assume that the appropriate attributes for each path are equal and that the next hop router for each multipath is different.

## Non-MPLS Topology Example

The following example shows how to set up the iBGP Multipath Load Sharing feature in a non-MPLS topology (see [Figure 23](#)).

**Figure 23** Non-MPLS Topology Example



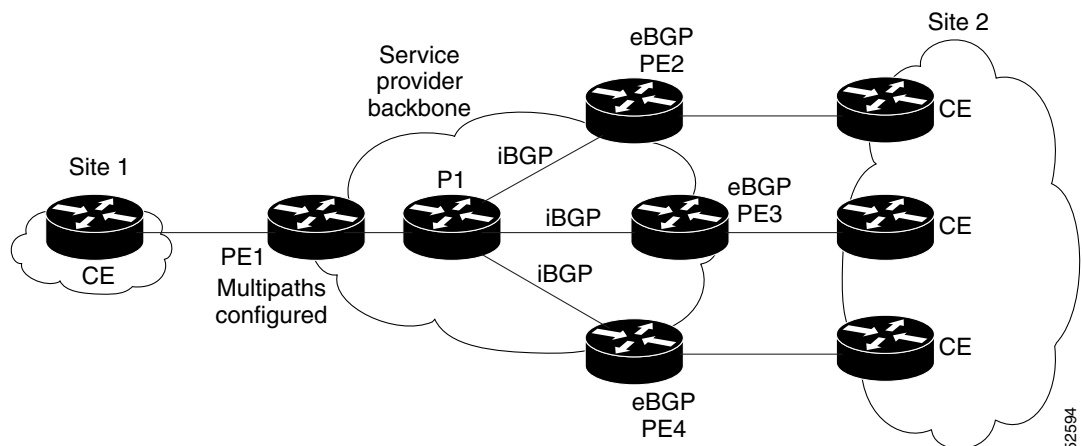
### Router 2 Configuration

```
router bgp 100
maximum-paths ibgp 3
```

## MPLS VPN Topology Example

The following example shows how to set up the iBGP Multipath Load Sharing feature in an MPLS VPN topology (see [Figure 24](#)).

**Figure 24** MPLS VPN Topology Example



**Router PE1 Configuration**

```
router bgp 100
address-family ipv4 unicast vrf site2
maximum-paths ibgp 3
```

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

**New Commands**

- **maximum-paths ibgp**

**Modified Commands**

- **show ip bgp**
- **show ip bgp vpnv4**
- **show ip route**
- **show ip route vrf**



## BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

The BGP Multipath Load Sharing for eBGP and iBGP feature allows you to configure multipath load balancing with both external BGP (eBGP) and internal BGP (iBGP) paths in Border Gateway Protocol (BGP) networks that are configured to use Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). This feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.

### Feature History for the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN Feature

Release	Modification
12.2(4)T	This feature was introduced.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.0(24)S	This feature was integrated into Cisco IOS Release 12.0(24)S.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

# Contents

- [Prerequisites for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN, page 202](#)
- [Restrictions for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN, page 202](#)
- [Information About BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN, page 203](#)
- [How to Configure BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN, page 205](#)
- [Configuration Examples for the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN Feature, page 208](#)
- [Additional References, page 210](#)
- [Command Reference, page 211](#)

## Prerequisites for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

### Load Balancing is Configured Under CEF

Cisco Express Forwarding (CEF) or distributed CEF (dCEF) must be enabled on all participating routers.

## Restrictions for BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

### Address Family Support

This feature is configured on a per VPN routing and forwarding instance (VRF) basis. This feature can be configured under only the IPv4 VRF address family.

### Memory Consumption Restriction

Each BGP multipath routing table entry will use additional memory. We recommend that you do not use this feature on a router with a low amount of available memory and especially if router is carries full Internet routing tables.

### Route Reflector Limitation

When multiple iBGP paths installed in a routing table, a route reflector will advertise only one paths (next hop). If a router is behind a route reflector, all routers that are connected to multihomed sites will not be advertised unless a different route distinguisher is configured for each VRF.



# Information About BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

To configure the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN feature, you must understand the following concepts:

- [Multipath Load Sharing Between eBGP and iBGP, page 203](#)
- [eBGP and iBGP Multipath Load Sharing in a BGP MPLS Network, page 204](#)
- [eBGP and iBGP Multipath Load Sharing With Route Reflectors, page 205](#)
- [Benefits of Multipath Load Sharing for Both eBGP and iBGP, page 205](#)

## Multipath Load Sharing Between eBGP and iBGP

A BGP routing process will install a single path as the best path in the routing information base (RIB) by default. The **maximum-paths** command allows you to configure BGP to install multiple paths in the RIB for multipath load sharing. BGP uses the best path algorithm to still select a single multipath as the best path and advertise the best path to BGP peers.

**Note**

The number of paths of multipaths that can be configured is documented on the **maximum-paths** command reference page.

Load balancing over the multipaths is performed by CEF. CEF load balancing is configured on a per-packet round robin or on a per session (source and destination pair) basis. For information about CEF, refer to *Cisco IOS Switching Services Configuration Guide* documentation:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/swit\\_vcg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/swit_vcg.htm)

The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature is enabled only under the IPv4 VRF address family configuration mode. When enabled, this feature can perform load balancing on eBGP and/or iBGP paths that are imported into the VRF. The number of multipaths is configured on a per VRF basis. Separate VRF multipath configurations are isolated by unique route distinguisher.

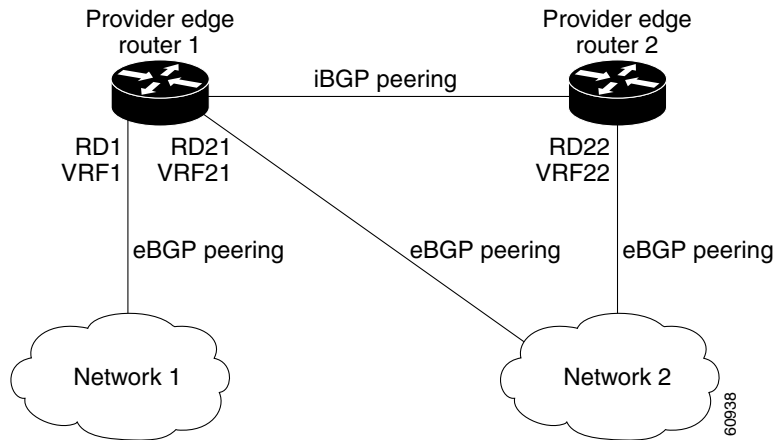
**Note**

The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature operates within the parameters of configured outbound routing policy.

## eBGP and iBGP Multipath Load Sharing in a BGP MPLS Network

Figure 25 shows a service provider BGP MPLS network that connects two remote networks to PE router 1 and PE router 2. PE router 1 and PE router 2 are both configured for VPNv4 unicast iBGP peering. Network 2 is a multihomed network that is connected to PE router 1 and PE router 2. Network 2 also has extranet VPN services configured with Network 1. Both Network 1 and Network 2 are configured for eBGP peering with the PE routers.

**Figure 25** A Service Provider BGP MPLS Network

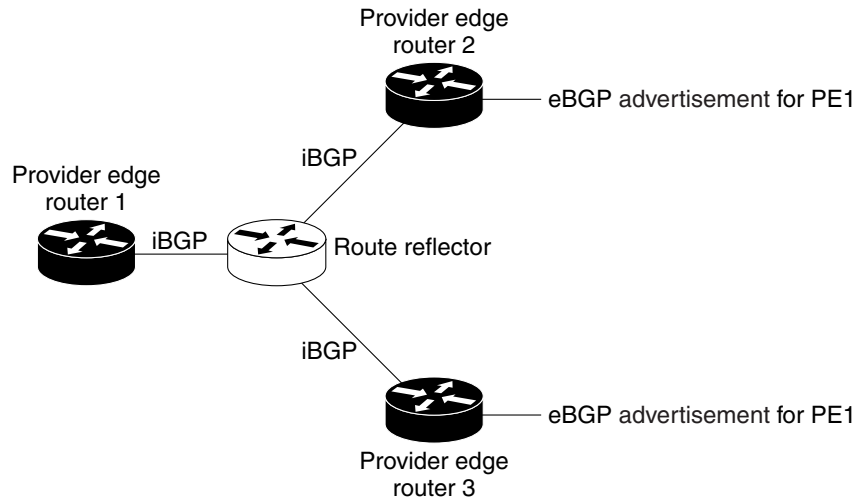


PE router 1 can be configured with the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature so that both iBGP and eBGP paths can be selected as multipaths and imported into the VRF of Network 1. The multipaths will be used by CEF to perform load balancing. IP traffic that is sent from Network 2 to PE router 1 and PE router 2 will be sent across the eBGP paths as IP traffic. IP traffic that is sent across the iBGP path will be sent as MPLS traffic, and MPLS traffic that is sent across an eBGP path will be sent as IP traffic. Any prefix that is advertised from Network 2 will be received by PE router 1 through route distinguisher (RD) 21 and RD 22. The advertisement through RD 21 will be carried in IP packets, and the advertisement through RD 22 will be carried in MPLS packets. Both paths can be selected as multipaths for VRF1 and installed into the VRF1 RIB.

## eBGP and iBGP Multipath Load Sharing With Route Reflectors

Figure 26 shows a topology that contains three PE routers and a route reflector, all configured for iBGP peering. PE router 2 and PE router 3 each advertise an equal preference eBGP path to PE router 1. By default, the route reflector will choose only one path and advertise PE router 1.

**Figure 26** A Topology With a Route Reflector



For all equal preference paths to PE router 1 to be advertised through the route reflector, you must configure each VRF with a different RD. The prefixes received by the route reflector will be recognized differently and advertised to PE router 1.

## Benefits of Multipath Load Sharing for Both eBGP and iBGP

The BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN feature allows multihomed autonomous systems and PE routers to be configured to distribute traffic across both eBGP and iBGP paths.

## How to Configure BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN

This section contains the following procedures:

- [Configuring Multipath Load Sharing for Both eBGP and iBGP, page 206](#)
- [Verifying Multipath Load Sharing for Both eBGP and iBGP, page 207](#)

## Configuring Multipath Load Sharing for Both eBGP and iBGP

To configure this feature, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf vrf-name**] | **vrf vrf-name**] | **ipv6** [**multicast** | **unicast**] | **vpn4** [**unicast**]
5. **maximum-paths eibgp** *number* [**import** *number*]
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router bgp 40000	Enters router configuration mode to create or configure a BGP routing process.
Step 4	<b>address-family ipv4 vrf vrf-name</b>  <b>Example:</b> Router(config-router)# address-family ipv4 vrf RED	Places the router in address family configuration mode. <ul style="list-style-type: none"><li>• Separate VRF multipath configurations are isolated by unique route distinguisher.</li></ul>
Step 5	<b>maximum-paths eibgp</b> <i>number</i> [ <b>import</b> <i>number</i> ]  <b>Example:</b> Router(config-router-af)# maximum-paths eibgp 6	Configures the number of parallel iBGP and eBGP routes that can be installed into a routing table.  <b>Note</b> The maximum-paths eibgp command can be configured only under the IPv4 VRF address family configuration mode and cannot be configured in any other address family configuration mode.
Step 6	<b>end</b>  <b>Example:</b> Router(config-router-af)# end	Exits address family configuration mode, and enters Privileged EXEC mode.

## Verifying Multipath Load Sharing for Both eBGP and iBGP

To verify this feature, perform the steps in this section

### SUMMARY STEPS

1. **enable**
2. **show ip bgp neighbors** [*neighbor-address*] [**advertised-routes**] [**dampened-routes**] [**flap-statistics**] [**paths** [*regex*]] [**received prefix-filter**] [**received-routes**] [**routes**]]
3. **show ip bgp vpnv4** {**all** | **rd** [*route-distinguisher*] | **vrf** [*vrf-name*]} [*ip-prefix/length*] [**longer-prefixes**] [*output-modifiers*] | [*network-address*] [*mask*] [**longer-prefixes**] [*output-modifiers*] [**cidr-only**] | [**community** [*number*] | **exact-match**] | **local-as** | **no-advertise** | **no-export**]] | [**community-list** [*name*] | *number*] [**exact-match**]] | [**dampening** [**dampened-paths**] | [**flap-statistics**] | [**parameters**]] | [**filter-list** [*regex-acl*]] | [**inconsistent-as**] | [**injected-paths**] | [**labels**] | [**neighbors**] | [**paths** [*regex*]]] | [**peer-group** [*name*] [**summary**]]] | [**quote-regex** [*regex*]] | [**regex** [*string*]] | [**replication** [*update-group*] [*ip-address*]] | [*ip-address*]] | [**rib-failure**] | [**route-map** [*name*]] | [**summary**] | [**templates** [**peer-policy** [*name*]] | [**peer-session** [*name*]] | [**update-group** [*update-group*] [*ip-address*]] | [*ip-address*]]
4. **show ip route vrf** [*vrf-name*] [**connected**] [**protocol** [*process-number*]] [**tag**] [*output-modifiers*]] [*ip-prefix*] [**list** [*number*] [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary**] [*output-modifiers*]] [**supernets-only**] [*output-modifiers*]] [**traffic-engineering**] [*output-modifiers*]]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show ip bgp neighbors</b> [ <i>neighbor-address</i> ] [ <b>advertised-routes</b> ] [ <b>dampened-routes</b> ] [ <b>flap-statistics</b> ] [ <b>paths</b> [ <i>regex</i> ]] [ <b>received prefix-filter</b> ] [ <b>received-routes</b> ] [ <b>routes</b> ]]  <b>Example:</b> Router# show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

	Command or Action	Purpose
Step 3	<pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} ip-prefix/length [longer-prefixes] [output-modifiers]   network-address [mask] [longer-prefixes] [output-modifiers] [cidr-only]   [community number   exact-match   local-as   no-advertise   no-export]]   [community-list name   number [exact-match]]   [dampening dampened-paths   flap-statistics   parameters]   [filter-list regex-acl]   [inconsistent-as]   [injected-paths]   [labels]   [neighbors]   [paths [regex]]   [peer-group [name summary]]   [quote-regex [regex]]   [regex string]   [replication [update-group [ip-address]]   [ip-address]]   [rib-failure]   [route-map name]   [summary]   [templates peer-policy [name]   peer-session[name]]   update-group [update-group [ip-address]]   [ip-address]]</pre> <p><b>Example:</b> Router# show ip bgp vpnv4 vrf RED</p>	Displays VPN address information from the BGP table. This command is used to verify that the VRF has been received by BGP.
Step 4	<pre>show ip route vrf vrf-name [connected] [protocol [process-number] [tag] [output-modifiers]] [ip-prefix] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]</pre> <p><b>Example:</b> Router# show ip route vrf RED</p>	Displays the IP routing table associated with a VRF instance. The show ip route vrf command is used to verify that the VRF is in the routing table.

## Configuration Examples for the BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN Feature

The following examples show how to configure and verify this feature:

- [eBGP and iBGP Multipath Load Sharing Configuration Example, page 208](#)
- [eBGP and iBGP Multipath Load Sharing Verification Examples, page 209](#)

### eBGP and iBGP Multipath Load Sharing Configuration Example

This following configuration example configures a router in address-family mode to select six BGP routes (eBGP or iBGP) as multipaths:

```
Router(config)# router bgp 40000
Router(config-router)# address-family ipv4 vrf RED
```

```
Router(config-router-af)# maximum-paths eibgp 6
Router(config-router-af)# end
```

## eBGP and iBGP Multipath Load Sharing Verification Examples

To verify that iBGP and eBGP routes have been configured for load sharing, use the **show ip bgp vpnv4 EXEC** command or the **show ip route vrf EXEC** command.

In the following example, the **show ip bgp vpnv4** command is entered to display multipaths installed in the VPNv4 RIB:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10.1:22.22.22.0/24, version 19
Paths:(5 available, best #5)
Multipath:eiBGP
  Advertised to non peer-group peers:
    10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
  22
    10.0.0.2 (metric 20) from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.4
    22
    10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.5
    22
    10.0.0.2 (metric 20) from 10.0.0.2 (10.0.0.2)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:RT:100:1 0x0:0:0
    22
    10.0.0.2 (metric 20) from 10.0.0.3 (10.0.0.3)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
      Extended Community:0x0:0:0 RT:100:1 0x0:0:0
      Originator:10.0.0.2, Cluster list:10.0.0.3
    22
    10.1.1.12 from 10.1.1.12 (10.22.22.12)
      Origin IGP, metric 0, localpref 100, valid, external, multipath, best
      Extended Community:RT:100:1
```

In the following example, the **show ip route vrf** command is entered to display multipath routes in the VRF table:

```
Router# show ip route vrf PATH 10.22.22.0

Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 20, metric 0
  Tag 22, type external
  Last update from 10.1.1.12 01:59:31 ago
  Routing Descriptor Blocks:
  * 10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.4, 01:59:31 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.5, 01:59:31 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.2, 01:59:31 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.0.0.2 (Default-IP-Routing-Table), from 10.0.0.3, 01:59:31 ago
    Route metric is 0, traffic share count is 1
```

```

AS Hops 1
10.1.1.12, from 10.1.1.12, 01:59:31 ago
Route metric is 0, traffic share count is 1
AS Hops 1

```

## Where to Go Next

For information about advertising the bandwidth of an autonomous system exit link as an extended community, refer to the BGP Link Bandwidth document:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s\\_bgplb.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/s_bgplb.htm)

## Additional References

For additional information related to BGP Dynamic Update Peer-Groups, refer to the following references:

## Related Documents

Related Topic	Document Title
BGP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul>
BGP configuration tasks	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>
Comprehensive BGP link bandwidth configuration examples and tasks	<ul style="list-style-type: none"> <li><a href="#">BGP Link Bandwidth, Release 12.0(24)S</a></li> </ul>
CEF configuration tasks	<ul style="list-style-type: none"> <li><a href="#">Cisco IOS Switching Services Configuration Guide</a></li> </ul>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—



## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFCs

RFCs	Title
RFC 1771	<i>A Border Gateway Protocol 4 (BGP4)</i>
RFC 2547	<i>BGP/MPLS VPNs</i>
RFC 2858	<i>Multiprotocol Extensions for BGP-4</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **maximum-paths eibgp**





## BGP Hide Local-Autonomous System

The BGP Hide Local-Autonomous System feature simplifies the task of changing the autonomous system number in a Border Gateway Protocol (BGP) network. Without this feature, this task can be difficult because, during the transition, internal BGP (iBGP) peers will reject external routes from peers with a local autonomous system number in the autonomous system number path to prevent routing loops. This feature allows you to transparently change the autonomous system number for the entire BGP network and ensure that routes can be propagated throughout the autonomous system, while the autonomous system number transition is incomplete.

### Feature History for BGP Hide Local-Autonomous System

Release	Modification
12.0(18)S	This feature was introduced in Cisco IOS Release 12.0(18)S.
12.2(8)T	This feature was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Hide Local-Autonomous System, page 214](#)
- [Restrictions for BGP Hide Local-Autonomous System, page 214](#)
- [Information About BGP Hide Local-Autonomous System, page 214](#)
- [How to Configure BGP Hide Local-Autonomous System, page 215](#)
- [Additional References, page 218](#)
- [Command Reference, page 219](#)

# Prerequisites for BGP Hide Local-Autonomous System

This document assumes that BGP is enabled and peering has been established in all participating networks.

## Restrictions for BGP Hide Local-Autonomous System

- This feature can be configured for only external BGP (eBGP) peers.
- This feature should be deconfigured after the transition to the new autonomous system number is completed to minimize the possible creation of routing loops.

## Information About BGP Hide Local-Autonomous System

To configure the BGP Hide Local-Autonomous System feature, you must understand the following concepts:

- [Changing the Autonomous System Number in a BGP Network, page 214](#)
- [Configuring the BGP Hide Local-Autonomous System Feature, page 214](#)
- [Benefits of the BGP Hide Local-Autonomous System Feature, page 215](#)

## Changing the Autonomous System Number in a BGP Network

Changing the autonomous system number may be necessary when 2 separate BGP networks are combined under a single autonomous system. This typically occurs when one ISP purchases another ISP. The **neighbor local-as** command is used initially to configure BGP peers to support 2 local autonomous system numbers to maintain peering between 2 separate BGP networks. This configuration allows the ISP to immediately make the transition without any impact on existing customer configurations.

When the customer configurations have been updated, The next step is to complete the transition from the old autonomous system number to the new autonomous system number. However, when the **neighbor local-as** command is configured on a BGP peer, the local autonomous system number is automatically prepended to all routes that are learned from eBGP peers by default. This behavior, however, makes changing the autonomous system number for a service provider or large BGP network difficult because routes, with the prepended autonomous system number, will be rejected by internal BGP (iBGP) peers that are configured with the same autonomous system number. For example, if you configure an iBGP peer with the **neighbor 10.0.0.2 local-as 20** statement, all routes that are learned from the 10.0.0.2 external peer will automatically have the autonomous system number 20 prepended. Internal routers that are configured with the autonomous number 20 will detect these routes as routing loops and reject them. This behavior requires you to change the autonomous system number for all iBGP peers at the same time.

## Configuring the BGP Hide Local-Autonomous System Feature

The BGP Hide Local-Autonomous System feature introduces the **no-prepend** keyword to the **neighbor local-as** command. The use of the **no-prepend** keyword will allow you to configure a BGP speaker to not prepend the local autonomous system number to any routes that are received from eBGP peers. This

feature can be used to help transparently change the autonomous system number of a BGP network and ensure that routes are propagated throughout the autonomous system, while the autonomous system number transition is incomplete. Because the local autonomous system number is not prepended to these routes, external routes will not be rejected by internal peers during the transition from one autonomous system number to another.

**Caution**

BGP prepends the autonomous system number from each BGP network that a route traverses. This behavior is designed to maintain network reachability information and to prevent routing loops from occurring. Configuring this feature incorrectly could create routing loops. So, the configuration of this feature should only be attempted by an experienced network operator.

## Benefits of the BGP Hide Local-Autonomous System Feature

You can use the BGP Hide Local-Autonomous System feature to transparently change the autonomous system number of a BGP network and ensure that routes can be propagated throughout the autonomous system while the autonomous system number transition is incomplete.

## How to Configure BGP Hide Local-Autonomous System

This section contains the following procedures:

- [Configuring BGP to Not Prepend the Local Autonomous System Number to Routes Learned From External Peers, page 215](#)
- [Verifying the Configuration of the BGP Hide Local-Autonomous Feature, page 217](#)

## Configuring BGP to Not Prepend the Local Autonomous System Number to Routes Learned From External Peers

To configure a router that is running BGP with the BGP Hide Local-Autonomous System feature to not prepend the local autonomous system number to routes that are received from external peers, use the following steps.

### Configuring the no-prepend Keyword

The **no-prepend** keyword should be used only to change the autonomous system number in a BGP network and should be deconfigured after the transition is complete because routing loops can be created if this feature is used incorrectly.

**Caution**

BGP prepends the autonomous system number from each BGP network that a route traverses. This behavior is designed to maintain network reachability information and to prevent routing loops from occurring. Configuring this feature incorrectly could create routing loops. So, the configuration of this feature should only be attempted by an experienced network operator.

## Restrictions

- This feature can only be configured for eBGP peers.
- This feature should be deconfigured after the transition to the new autonomous system number is completed to minimize the possible creation of routing loops.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family** {**ipv4** | **ipv6** | **vpnvp4**} [**multicast** | **unicast** | **vrf** {*vrf-name*}]
5. **network** *ip-address* [*network-mask*] [**route-map** *map-name*] [**backdoor**]
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **neighbor** *ip-address* **local-as** *as-number* **no-prepend**
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router(config)# router bgp 100	Enters router configuration mode, and creates a BGP routing process.
Step 4	<b>address-family</b> <b>ipv4</b>   <b>ipv6</b>   <b>vpnvp4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> { <i>vrf-name</i> }]  <b>Example:</b> Router(config-router-af)# address-family ipv4 unicast	Enter address family configuration mode to configure BGP peers to accept address family specific configurations. <ul style="list-style-type: none"> <li>• The example command creates an IPv4 unicast address family session.</li> </ul>
Step 5	<b>network</b> <i>ip-address</i> [ <i>network-mask</i> ] [ <b>route-map</b> <i>map-name</i> ] [ <b>backdoor</b> ]  <b>Example:</b> Router(config-router-af)# network 10.1.1.1 remote-as 100	Specifies the networks to be advertised by the BGP and multiprotocol BGP routing processes.

	Command or Action	Purpose
Step 6	<b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i>  <b>Example:</b> Router(config-router-af)# neighbor 10.1.1.1 remote-as 100	Establishes peering with the specified neighbor and configures the neighbor as internal to the local autonomous system.
Step 7	<b>neighbor</b> <i>ip-address</i> <b>local-as</b> <i>as-number</i> [ <b>no-prepend</b> ]  <b>Example:</b> Router(config-router-af)# neighbor 10.1.1.1 local-as 300 no-prepend	Allows the customization of the autonomous system number for eBGP peer groupings. <ul style="list-style-type: none"> <li>Using the <b>no-prepend</b> keyword configures the router to not prepend the local autonomous system number to routes that are received from external peers.</li> </ul>
Step 8	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits address-family configuration mode, and enters Privileged EXEC mode.

## Examples

The following example configures the router to not prepend autonomous system number 300 to routes that are received from external peers:

```
router bgp 100
 network 10.1.1.0
 neighbor 10.1.1.1 remote-as 100
 neighbor 10.1.1.1 local-as 300 no-prepend
end
```

## What to Do Next

You can verify that this feature is configured correctly with the **show ip bgp neighbors** command. Go to the [Verifying the Configuration of the BGP Hide Local-Autonomous Feature](#) section for instructions and example output.

## Verifying the Configuration of the BGP Hide Local-Autonomous Feature

To verify that the local autonomous system number is not prepended to received external routes, use the **show ip bgp neighbors** command. The output of this command will display the local autonomous system number and then “no-prepend” for received external routes when this feature is configured.

The following example shows that autonomous system number 300 will not be prepended to the 10.1.1.1 peer:

```
Router# show ip bgp neighbors
BGP neighbor is 10.1.1.1, remote AS 100, local AS 300 no-prepend, external link
  BGP version 4, remote router ID 10.1.1.1
  BGP state = Established, up for 00:00:49
  Last read 00:00:49, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
    IPv4 MPLS Label capability:
  Received 10 messages, 1 notifications, 0 in queue
```

```
Sent 10 messages, 0 notifications, 0 in queue
Default minimum time between advertisement runs is 30 seconds
```

## Additional References

The following sections provide references related to BGP Prefix-Based Outbound Route Filtering feature.

## Related Documents

Related Topic	Document Title
The BGP Hide Local-Autonomous System feature is an extension of the BGP routing protocol. For more information about configuring BGP, autonomous systems, and route filtering, refer to the “Configuring BGP” chapter of the Release 12.2 <i>Cisco IOS IP Configuration Guide</i> and <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> .	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> <li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3</a></li> <li>• <a href="#">Configuring the BGP Local-AS Feature</a> (</li> </ul>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p>

## RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—



## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	TAC Home Page: <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>  BGP Support Page: <a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a>

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **neighbor local-as**
- **show ip bgp neighbors**





# BGP 4 MIB Support for per-Peer Received Routes

## Feature History

Release	Modification
12.0(21)S	The Cisco BGP Version 4 MIB was modified.
12.2(13)T	BGP 4 MIB Support for per-Peer Received Routes was integrated into 12.2(13)T.

This document describes BGP 4 MIB Support for per-Peer Received Routes and includes the following sections:

- [Feature Overview, page 221](#)
- [Benefits, page 225](#)
- [Related Features and Technologies, page 225](#)
- [Supported Platforms, page 225](#)
- [Supported Standards, MIBs, and RFCs, page 226](#)
- [Command Reference, page 227](#)
- [Glossary, page 228](#)

## Feature Overview

BGP 4 MIB Support for per-Peer Received Routes introduces a new table in the CISCO-BGP4-MIB that provides the capability to query (by using Simple Network Management Protocol [SNMP] commands) for routes that are learned from individual Border Gateway Protocol (BGP) peers.

Before this new MIB table was introduced, a network operator could obtain the routes learned by a local BGP-speaking router by querying the local BGP speaker with an SNMP command (for example, the **snmpwalk** command). The network operator used the SNMP command to query the **bgp4PathAttrTable** of the CISCO-BGP4-MIB. The routes that were returned from a **bgp4PathAttrTable** query were indexed in the following order:

- Prefix
- Prefix length
- Peer address

Because the `bgp4PathAttrTable` indexes the prefixes first, obtaining routes learned from individual BGP peers will require the network operator to walk through the complete `bgp4PathAttrTable` and filter out routes from the interested peer. A BGP RIB could potentially contain 10,000 or more routes, which makes a manual walk operation impossible and automated walk operations very inefficient.

BGP 4 MIB Support for per-Peer Received Routes introduces a Cisco-specific enterprise extension to the CISCO-BGP4-MIB that defines a new table called the `cbgpRouterTable`. The `cbgpRouterTable` provides the same information as the `bgp4PathAttrTable` with the following two differences:

- Routes are indexed in the following order:
  - Peer address
  - Prefix
  - Prefix length

The search criteria for SNMP queries of local routes is improved because peer addresses are indexed before prefixes. A search for routes that are learned from individual peers is improved with this enhancement because peer addresses are indexed before prefixes. A network operator will no longer need to search through potentially thousands of routes to obtain the learned routes of a local BGP RIB table.

- Support is added for Multiprotocol (mBGP), Address Family Identifier (AFI), and Subsequent Address Family Identifier (SAFI) information. This information is added in the form of indexes to the `cbgpRouterTable`. The CISCO-BGP4-MIB can be queried for any combination of AFIs and SAFIs that are supported by the local BGP speaker.


**Note**

The MIB will be populated only if the router is configured to run a BGP process. The present implementation of BGP 4 MIB Support for per-Peer Received Routes will show only routes contained in IPv4 AFI and unicast SAFI BGP local RIB tables. Support for showing routes contained in other local RIB tables will be added in the future.

## BGP 4 per-Peer Received Routes Table Elements and Objects

The following section describe new table elements, AFI and SAFI tables and objects, and network address prefixes in the Network Layer Reachability Information (NLRI) fields that have been introduced by the BGP 4 MIB Support for per-Peer Received Routes enhancement.

### MIB Tables and Objects

[Table 10](#) describes the MIB indexes of the `cbgpRouterTable`.

For a complete description of the MIB, see the CISCO-BGP4-MIB file CISCO-BGP4-MIB.my, available through Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

**Table 10** *MIB Indexes of the cbgpRouterTable*

MIB Indexes	Description
cbgpRouteAfi	Represents the AFI of the network layer protocol that is associated with the route.
cbgpRouteSafi	Represents the SAFI of the route. It gives additional information about the type of the route. The AFI and SAFI are used together to determine which local RIB (Loc-RIB) contains a particular route.
cbgpRoutePeerType	Represents the type of network layer address that is stored in the cbgpRoutePeer object.
cbgpRoutePeer	Represents the network layer address of the peer from which the route information has been learned.
cbgpRouteAddrPrefix	Represents the network address prefix that is carried in a BGP update message.  See <a href="#">Table 11</a> for information about the types of network layer addresses that can be stored in specific types of AFI and SAFI objects.
cbgpRouteAddrPrefixLen	Represents the length in bits of the network address prefix in the NLRI field.  See <a href="#">Table 12</a> for a description of the 13 possible entries.

## AFIs and SAFIs

[Table 11](#) lists the AFI and SAFI values that can be assigned to or held by the cbgpRouteAfi and cbgpRouteSafi indexes, respectively. [Table 11](#) also displays the network address prefix type that can be held by specific combinations of AFIs and SAFIs. The type of network address prefix that can be carried in a BGP update message depends on the combination of AFIs and SAFIs.

**Table 11** *AFIs and SAFIs*

AFI	SAFI	Type
ipv4(1)	unicast(1)	IPv4 address
ipv4(1)	multicast(2)	IPv4 address
ipv4(1)	vpn(128)	VPN-IPv4 address
ipv6(2)	unicast(1)	IPv6 address



### Note

A VPN-IPv4 address is a 12-byte quantity that begins with an 8-byte Route Distinguisher (RD) and ends with a 4-byte IPv4 address. Any bits beyond the length specified by cbgpRouteAddrPrefixLen are represented as zeros.

## Network Address Prefix Descriptions for the NLRI Field

Table 12 describes the length in bits of the network address prefix in the NLRI field of the cbgpRouteTable. Each entry in the table provides the following information about the route that is selected by any of the six indexes in Table 10.

**Table 12**      *Network Address Prefix Descriptions for the NLRI Field*

Table or Object (or index)	Description
cbgpRouteOrigin	The ultimate origin of the route information.
cbgpRouteASPathSegment	The sequence of autonomous system path segments.
cbgpRouteNextHop	The network layer address of the autonomous system border router that traffic should pass through to get to the destination network.
cbgpRouteMedPresent	Indicates that the MULTI_EXIT_DISC attribute for the route is either present or absent.
cbgpRouteMultiExitDisc	Metric that is used to discriminate between multiple exit points to an adjacent autonomous system. The value of this object is irrelevant if the value of the cbgpRouteMedPresent object is "false(2)."
cbgpRouteLocalPrefPresent	Indicates that the LOCAL_PREF attribute for the route is either present or absent.
cbgpRouteLocalPref	Determines the degree of preference for an advertised route by an originating BGP speaker. The value of this object is irrelevant if the value of the cbgpRouteLocalPrefPresent object is "false(2)."
cbgpRouteAtomicAggregate	Determines if the system has selected a less specific route without selecting a more specific route.
cbgpRouteAggregatorAS	The autonomous system number of the last BGP speaker that performed route aggregation. A value of 0 indicates the absence of this attribute.
cbgpRouteAggregatorAddrType	Represents the type of Network Layer address that is stored in the cbgpRouteAggregatorAddr object.
cbgpRouteAggregatorAddr	The network layer address of the last BGP 4 speaker that performed route aggregation. A value of all zeros indicates the absence of this attribute.
cbgpRouteBest	An indication of whether this route was chosen as the best BGP 4 route.
cbgpRouteUnknownAttr	One or more path attributes not understood by the local BGP speaker. A size of 0 indicates that this attribute is absent.

## Benefits

### Improved SNMP Query Capabilities

The search criteria for SNMP queries for routes that are advertised by individual peers is improved because the peer address is indexed before the prefix. A network operator will no longer need to search through potentially thousands of routes to obtain the learned routes of a local BGP RIB table.

### Improved AFI and SAFI Support

Support is added for mBGP. AFI and SAFI are added as indexes to the table. The CISCO-BGP4-MIB can be queried for any combination of AFIs and SAFIs that are supported by the local BGP speaker.

## Restrictions

BGP 4 MIB Support for per-Peer Received Routes supports only routes that are contained in IPv4 AFIs and unicast SAFIs in the local BGP RIB. The BGP 4 MIB Support for per-Peer Received Routes enhancement is supported only by BGP Version 4.

## Related Features and Technologies

BGP 4 MIB Support for per-Peer Received Routes is an extension of the BGP routing protocol. For more information about configuring BGP, refer to the “Configuring BGP” chapter of the Release 12.0 *Cisco IOS Network Protocols Configuration Guide* and the *Network Protocols, Part 1*.

## Related Documents

For information about configuring SNMP, refer to the following documents:

- The “Configuring SNMP Support” chapter of *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- The “SNMP Commands” chapter of *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2

## Supported Platforms

For information about platforms supported in Cisco IOS Release 12.0(21)S and 12.2(13)T, refer to Feature Navigator.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>


**Note**

Cisco Feature Navigator does not support Cisco IOS Release 12.2(8)B.

**Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

**Standards**

No new or modified standards are supported by this MIB.

**MIBs**

- CISCO-BGP4-MIB.my

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

**RFCs**

- RFC-1657, *BGP-4 MIB*
- RFC-1771, *A Border Gateway Protocol 4 (BGP-4)*
- RFC-2547, *BGP/MPLS VPNs*
- RFC-2858, *Multiprotocol Extensions for BGP-4*

## Configuration Tasks

None



## Configuration Examples

None

## Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

# Glossary

**AFI**—Address Family Identifier. Carries the identity of the network layer protocol that is associated with the network address.

**BGP**—Border Gateway Protocol. An interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined by RFC 1163, *A Border Gateway Protocol (BGP)*. The current implementation of BGP is BGP Version 4 (BGP4). BGP4 is the predominant interdomain routing protocol that is used on the Internet. It supports CIDR and uses route aggregation mechanisms to reduce the size of routing tables.

**MBGP**—multiprotocol BGP. An enhanced version of BGP that carries routing information for multiple network layer protocols and IP multicast routes. It is defined in RFC 2858, *Multiprotocol Extensions for BGP-4*.

**MIB**—Management Information Base. A group of managed objects that are contained within a virtual information store or database. MIB objects are stored so that values can be assigned to object identifiers and to assist managed agents by defining which MIB objects should be implemented. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**NLRI**—Network Layer Reachability Information. Carries route attributes that describe a route and how to connect to a destination. This information is carried in BGP update messages. A BGP update message can carry one or more NLRI prefixes.

**RIB**—A Routing Information Base (RIB). A central repository of routes that contains Layer 3 reachability information and destination IP addresses or prefixes. The RIB is also known as the routing table.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices and to manage configurations, statistics collection, performance, and security.

**snmpwalk**—The **snmpwalk** command is a Simple Network Management Protocol (SNMP) application that is used to communicate with a network entity MIB using SNMP.

**SAFI**—Subsequent Address Family Identifier. Provides additional information about the type of the Network Layer Reachability Information that is carried in the attribute.

**VPN**—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses a tunnel to encrypt all information at the IP level.



# BGP Policy Accounting

## Feature History

Release	Modification
12.0(9)S	This feature was introduced.
12.0(17)ST	This feature was integrated into Cisco IOS Release 12.0(17)ST.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T.

This document describes the BGP Policy Accounting feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

- [Feature Overview, page 229](#)
- [Supported Platforms, page 231](#)
- [Supported Standards, MIBs, and RFCs, page 232](#)
- [Prerequisites, page 232](#)
- [Configuration Tasks, page 233](#)
- [Monitoring and Maintaining BGP Policy Accounting, page 235](#)
- [Configuration Examples, page 236](#)
- [Command Reference, page 237](#)
- [Glossary, page 237](#)

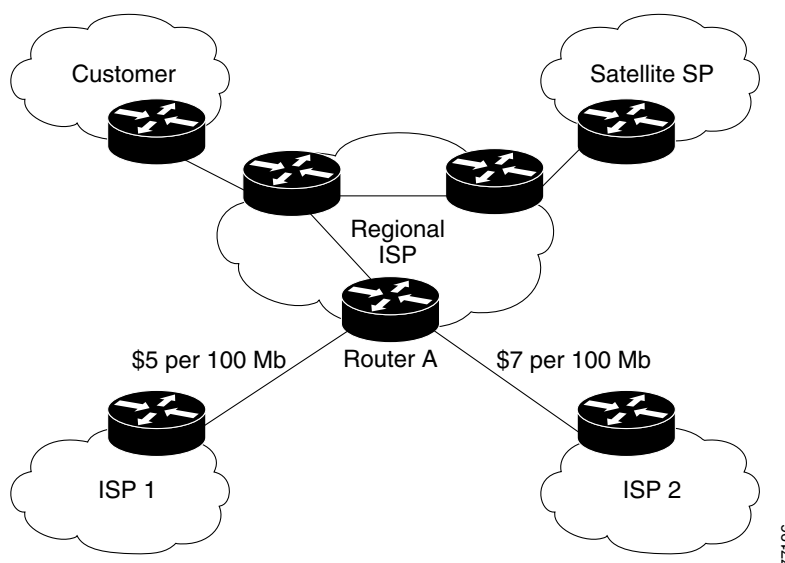
## Feature Overview

Border Gateway Protocol (BGP) policy accounting measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting is enabled on an input interface, and counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

Using the BGP **table-map** command, prefixes added to the routing table are classified by BGP attribute, autonomous system number, or autonomous system path. Packet and byte counters are incremented per input interface. A Cisco IOS policy-based classifier maps the traffic into one of eight possible buckets, representing different traffic classes.

Using BGP policy accounting, you can account for traffic according to the route it traverses. Service providers (SPs) can identify and account for all traffic by customer and bill accordingly. In Figure 27, BGP policy accounting can be implemented in Router A to measure packet and byte volumes in autonomous system buckets. Customers are billed appropriately for traffic that is routed from a domestic, international, or satellite source.

**Figure 27** Sample Topology for BGP Policy Accounting



BGP policy accounting using autonomous system numbers can be used to improve the design of network circuit peering and transit agreements between Internet service providers (ISPs).

## Benefits

### Account for IP Traffic Differentially

BGP policy accounting classifies IP traffic by autonomous system number, autonomous system path, or community list string, and increments packet and byte counters. Service providers can account for traffic and apply billing, according to the route specific traffic traverses.

### Efficient Network Circuit Peering and Transit Agreement Design

Implementing BGP policy accounting on an edge router can highlight potential design improvements for peering and transit agreements.

## Related Features and Technologies

Additional BGP command and configuration information is documented in the “Configuring BGP” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2 and *Cisco IOS IP Command Reference*, Volume 2 of 3: *Routing Protocols*, Release 12.2.

Additional Cisco Express Forwarding (CEF) and distributed CEF (dCEF) command and configuration information is documented in the “Cisco Express Forwarding Overview” and in the “Configuring Cisco Express Forwarding” chapters of the *Cisco IOS Switching Services Configuration Guide*, Release 12.2 and *Cisco IOS Switching Services Command Reference*, Release 12.2.

## Related Documents

- *Cisco IOS IP Configuration Guide*, Release 12.2
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2
- *Cisco IOS Switching Services Configuration Guide*, Release 12.2
- *Cisco IOS Switching Services Command Reference*, Release 12.2

## Supported Platforms

The BGP Policy Accounting feature is supported by the following platforms that support Cisco IOS Release 12.2(13)T:

- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2600 series
- Cisco 3600 series
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400
- Cisco AS5800
- Cisco AS5850
- Cisco ICS7750
- Cisco IGX 8400 URM
- Cisco MC3810
- Cisco MGX 8850
- Cisco uBR7200 series

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### **Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Supported Standards, MIBs, and RFCs

### **Standards**

No new or modified standards are supported by this feature.

### **MIBs**

- CISCO-BGP-POLICY-ACCOUNTING-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

### **RFCs**

No new or modified RFCs are supported by this feature.

## Prerequisites

Before using the BGP Policy Accounting feature you must enable BGP and CEF or dCEF on the router.

# Configuration Tasks

See the following sections for configuration tasks for the BGP Policy Accounting feature. Each task in the list is identified as either required or optional.

- [Specifying the Match Criteria for BGP Policy Accounting, page 233](#) (required)
- [Classifying the IP Traffic and Enabling BGP Policy Accounting, page 234](#) (required)
- [Verifying BGP Policy Accounting, page 234](#) (optional)

## Specifying the Match Criteria for BGP Policy Accounting

The first task in configuring BGP policy accounting is to specify the criteria that must be matched. Community lists, autonomous system paths, or autonomous system numbers are examples of BGP attributes that can be specified and subsequently matched using a route map.

To specify the BGP attribute to use for BGP policy accounting and create the match criteria in a route map, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>ip community-list</b> <i>community-list-number</i> { <b>permit</b>   <b>deny</b> } <i>community-number</i>	Creates a community list for BGP and controls access to it. This step must be repeated for each community to be specified.
Step 2	Router(config)# <b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]	Enters route-map configuration mode and defines the conditions for policy routing.  The <i>map-name</i> argument identifies a route map.  The optional <b>permit</b> and <b>deny</b> keywords work with the match and set criteria to control how the packets are accounted for.  The optional <i>sequence-number</i> argument indicates the position a new route map is to have in the list of route maps already configured with the same name.
Step 3	Router(config-route-map)# <b>match community-list</b> <i>community-list-number</i> [ <b>exact</b> ]	Matches a BGP community.
Step 4	Router(config-route-map)# <b>set traffic-index</b> <i>bucket-number</i>	Indicates where to output packets that pass a match clause of a route map for BGP policy accounting.

## Classifying the IP Traffic and Enabling BGP Policy Accounting

After a route map has been defined to specify match criteria, you must configure a way to classify the IP traffic before enabling BGP policy accounting.

Using the **table-map** command, BGP classifies each prefix it adds to the routing table based on the match criteria. When the **bgp-policy accounting** command is configured on an interface, BGP policy accounting is enabled.

To classify the IP traffic and enable BGP policy accounting, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>router bgp</b> <i>as-number</i>	Configures a BGP routing process and enters router configuration mode for the specified routing process.
Step 2	Router(config-router)# <b>table-map</b> <i>route-map-name</i>	Classifies BGP prefixes entered in the routing table.
Step 3	Router(config-router)# <b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]	Specifies a network to be advertised by the BGP routing process.
Step 4	Router(config-router)# <b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i>	Specifies a BGP peer by adding an entry to the BGP routing table.
Step 5	Router(config-router)# <b>exit</b>	Exits to global configuration mode.
Step 6	Router(config)# <b>interface</b> <i>interface-type</i> <i>interface-number</i>	Specifies the interface type and number and enters interface configuration mode.
Step 7	Router(config-if)# <b>no ip</b> <b>directed-broadcast</b>	Configures the interface to drop directed broadcasts destined for the subnet to which that interface is attached, rather than being broadcast. This is a security issue.
Step 8	Router(config-if)# <b>ip address</b> <i>ip-address</i> <i>mask</i>	Configures the interface with an IP address.
Step 9	Router(config-if)# <b>bgp-policy accounting</b>	Enables BGP policy accounting for the interface.

## Verifying BGP Policy Accounting

To verify that BGP policy accounting is operating, perform the following steps:

- 
- Step 1** Enter the **show ip cef EXEC** command with the **detail** keyword to learn which accounting bucket is assigned to a specified prefix.
- In this example, the output is displayed for the prefix 192.168.5.0. It shows that the accounting bucket number 4 (traffic\_index 4) is assigned to this prefix.
- ```
Router# show ip cef 192.168.5.0 detail

192.168.5.0/24, version 21, cached adjacency to POS7/2
0 packets, 0 bytes, traffic_index 4
  via 10.14.1.1, 0 dependencies, recursive
  next hop 10.14.1.1, POS7/2 via 10.14.1.0/30
  valid cached adjacency
```
- Step 2** Enter the **show ip bgp EXEC** command for the same prefix used in Step 1—192.168.5.0—to learn which community is assigned to this prefix.



In this example, the output is displayed for the prefix 192.168.5.0. It shows that the community of 100:197 is assigned to this prefix.

```
Router# show ip bgp 192.168.5.0
```

```
BGP routing table entry for 192.168.5.0/24, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
    100
      10.14.1.1 from 10.14.1.1 (32.32.32.32)
        Origin IGP, metric 0, localpref 100, valid, external, best
        Community: 100:197
```

**Step 3** Enter the **show cef interface policy-statistics EXEC** command to display the per-interface traffic statistics.

In this example, the output shows the number of packets and bytes that have been assigned to each accounting bucket:

```
LC-Slot7# show cef interface policy-statistics
```

```
POS7/0 is up (if_number 8)
Bucket      Packets      Bytes
1           0           0
2           0           0
3           50          5000
4          100         10000
5          100         10000
6           10          1000
7           0           0
8           0           0
```

## Monitoring and Maintaining BGP Policy Accounting

To monitor and maintain the BGP Policy Accounting feature, use the following commands in EXEC mode, as needed:

| Command                                                                                           | Purpose                                                                               |
|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Router# <b>show cef interface</b> [ <i>type number</i> ]<br><b>policy-statistics</b>              | Displays detailed CEF policy statistical information for all interfaces.              |
| Router# <b>show ip bgp</b> [ <i>network</i> ] [ <i>network mask</i> ]<br><b>[longer-prefixes]</b> | Displays entries in the BGP routing table.                                            |
| Router# <b>show ip cef</b> [ <i>network [mask]</i> ] [ <b>detail</b> ]                            | Displays entries in the Forwarding Information Base (FIB) or FIB summary information. |

# Configuration Examples

This section provides the following configuration examples:

- [Specifying the Match Criteria for BGP Policy Accounting Example](#)
- [Classifying the IP Traffic and Enabling BGP Policy Accounting Example](#)

## Specifying the Match Criteria for BGP Policy Accounting Example

In the following example, BGP communities are specified in community lists, and a route map named `set_bucket` is configured to match each of the community lists to a specific accounting bucket using the `set traffic-index` command:

```
ip community-list 30 permit 100:190
ip community-list 40 permit 100:198
ip community-list 50 permit 100:197
ip community-list 60 permit 100:296
!
route-map set_bucket permit 10
match community 30
set traffic-index 2
!
route-map set_bucket permit 20
match community 40
set traffic-index 3
!
route-map set_bucket permit 30
match community 50
set traffic-index 4
!
route-map set_bucket permit 40
match community 60
set traffic-index 5
```

## Classifying the IP Traffic and Enabling BGP Policy Accounting Example

In the following example, BGP policy accounting is enabled on POS interface 7/0 and the `table-map` command is used to modify the bucket number when the IP routing table is updated with routes learned from BGP:

```
router bgp 65000
 table-map set_bucket
 network 10.15.1.0 mask 255.255.255.0
 neighbor 10.14.1.1 remote-as 65100
!
ip classless
ip bgp-community new-format
!
interface POS7/0
 ip address 10.15.1.2 255.255.255.0
 no ip directed-broadcast
 bgp-policy accounting
 no keepalive
 crc 32
 clock source internal
```

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **bgp-policy**
- **set traffic-index**
- **show cef interface policy-statistics**
- **show ip bgp**
- **show ip cef**

## Glossary

**AS**—autonomous system. An IP term to describe a routing domain that has its own independent routing policy, and is administered by a single authority.

**BGP**—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems.

**CEF**—Cisco Express Forwarding.

**dCEF**—distributed Cisco Express Forwarding.

**Note**

---

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---





# BGP Nonstop Forwarding (NSF) Awareness

Nonstop Forwarding (NSF) awareness allows a router to assist NSF-capable neighbors to continue forwarding packets during a Stateful Switchover (SSO) operation. The BGP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running BGP to forward packets along routes that are already known for a router that is performing an SSO operation. This capability allows the BGP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

NSF works with the SSO feature in Cisco IOS software. SSO is a prerequisite of NSF. NSF works with SSO to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of NSF is to continue forwarding IP packets following a Route Processor (RP) switchover. NSF/SSO is configured in the core of your network, and NSF awareness is configured on iBGP peers in the core and on the edge of the network.

## Feature Specifications for the BGP Nonstop Forwarding (NSF) Awareness feature

### Feature History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.2(15)T | This feature was introduced. |

### Supported Platforms

For platforms supported in Cisco IOS Release 12.2(15)T, use Cisco Feature Navigator as described below.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Nonstop Forwarding Awareness, page 240](#)
- [Restrictions for BGP Nonstop Forwarding Awareness, page 240](#)
- [Information About BGP Nonstop Forwarding Awareness, page 240](#)
- [How to Configure BGP Nonstop Forwarding Awareness, page 243](#)

- [Configuration Examples for Nonstop Forwarding, page 247](#)
- [Additional References, page 249](#)
- [Command Reference, page 251](#)

## Prerequisites for BGP Nonstop Forwarding Awareness

This document assumes that your network is configured to run BGP. You will also need to complete the following tasks before you can configure this feature:

- On platforms supporting the Route Switch Processor (RSP), and where the CEF switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command. This command is enabled by default on the Cisco 12000 Series Internet Router.

## Restrictions for BGP Nonstop Forwarding Awareness

The following restrictions apply to the BGP Nonstop Forwarding Awareness feature:

- All neighboring devices participating in BGP NSF must be NSF-capable or NSF-aware, having been configured for BGP graceful restart.
- BGP graceful restart does not support two neighbors performing an NSF restart operation at the same time because these peers cannot hold routes for each other during an SSO operation. However, both neighbors will still reestablish peering sessions after the NSF restart operation is complete. Each router will reestablish peering with the other as if it were a new router joining the network.
- Existing sessions must be reset by issuing the **clear ip bgp \*** command or by reloading the router before graceful restart capabilities will be exchanged.
- BGP graceful restart does not yet support Virtual Routing and Forwarding (VRF) instances and VPNv4 sessions and configurations.

## Information About BGP Nonstop Forwarding Awareness

To configure this feature, you must understand the following concepts:

- [Cisco NSF Routing and Forwarding Operation, page 240](#)
- [Cisco Express Forwarding, page 241](#)
- [BGP Graceful Restart, page 241](#)
- [BGP NSF Awareness, page 242](#)

## Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, EIGRP, OSPF, and IS-IS have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices.

In this document, a networking device is said to be NSF-aware if it is running NSF-compatible software. A device is said to be NSF-capable if it has been configured to support NSF; therefore, it would rebuild routing information from NSF-aware or NSF-capable neighbors.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF then updates the line cards with the new FIB information.



**Note** Currently, EIGRP supports only NSF awareness. SSO support for EIGRP will be integrated into a future release.

## Cisco Express Forwarding

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates for CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables.



**Note** For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

## BGP Graceful Restart

When an NSF-capable router begins a BGP session with a BGP peer, it sends an OPEN message to the peer. Included in the message is a declaration that the NSF-capable or NSF-aware router has “graceful restart capability.” Graceful restart is the mechanism by which BGP routing peers avoid a routing flap following a switchover. If the BGP peer has received this capability, it is aware that the device sending the message is NSF-capable. Both the NSF-capable router and its BGP peer(s) (NSF-aware peers) need

to exchange the graceful restart capability in their OPEN messages, at the time of session establishment. If both the peers do not exchange the graceful restart capability, the session will not be graceful restart capable.

If the BGP session is lost during the RP switchover, the NSF-aware BGP peer marks all the routes associated with the NSF-capable router as stale; however, it continues to use these routes to make forwarding decisions for a set period of time. This functionality means that no packets are lost while the newly active RP is waiting for convergence of the routing information with the BGP peers.

After an RP switchover occurs, the NSF-capable router reestablishes the session with the BGP peer. In establishing the new session, it sends a new graceful restart message that identifies the NSF-capable router as having restarted.

At this point, the routing information is exchanged between the two BGP peers. Once this exchange is complete, the NSF-capable device uses the routing information to update the RIB and the FIB with the new forwarding information. The NSF-aware device uses the network information to remove stale routes from its BGP table. Following that, the BGP protocol is fully converged.

If a BGP peer does not support the graceful restart capability, it will ignore the graceful restart capability in an OPEN message but will establish a BGP session with the NSF-capable device. This functionality will allow interoperability with non-NSF-aware BGP peers (and without NSF functionality), but the BGP session with non-NSF-aware BGP peers will not be graceful restart capable.

## BGP NSF Awareness

BGP support for NSF requires that neighbor routers are NSF-aware or NSF-capable. NSF awareness in BGP is also enabled by the graceful restart mechanism. A router that is NSF-aware functions like a router that is NSF-capable with one exception: an NSF-aware router is incapable of performing an SSO operation. However, a router that is NSF-aware is capable of maintaining a peering relationship with a NSF-capable neighbor during a NSF SSO operation, as well as holding routes for this neighbor during the SSO operation.

The BGP Nonstop Forwarding Awareness feature provides an NSF-aware router with the capability to detect a neighbor that is undergoing an SSO operation, maintain the peering session with this neighbor, retain known routes, and continue to forward packets for these routes. The deployment of BGP NSF awareness can minimize the affects of route-processor (RP) failure conditions and improve the overall network stability by reducing the amount of resources that are normally required for reestablishing peering with a failed router.

NSF awareness for BGP is not enabled by default. The **bgp graceful-restart** command is used to enable NSF awareness on a router that is running BGP. NSF-aware operations are also transparent to the network operator and BGP peers that do not support NSF capabilities.



### Note

NSF awareness is enabled automatically in supported software images for Interior Gateway Protocols, such as EIGRP, IS-IS, and OSPF. In BGP, NSF awareness is not enabled automatically and must be started by issuing the **bgp graceful-restart** command in router configuration mode.



# How to Configure BGP Nonstop Forwarding Awareness

This section contains the following procedures:

- [Configuring BGP Nonstop Forwarding Awareness, page 243](#)
- [Configuring BGP NSF Awareness Timers, page 245](#)
- [Verifying the Configuration of BGP Nonstop Forwarding Awareness, page 247](#)

## Configuring BGP Nonstop Forwarding Awareness

### BGP Graceful Restart

The BGP Nonstop Forwarding (NSF) Awareness feature is part of the graceful restart mechanism. BGP NSF awareness is enabled by issuing the **bgp graceful-restart** command in router configuration mode. BGP NSF awareness allows NSF-aware routers to support NSF-capable routers during an SSO operation. NSF-awareness is not enabled by default and should be configured on all neighbors that participate in BGP NSF.

#### Restrictions

The configuration of the restart and stalepath timers is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

#### SUMMARY STEPS

1. **enable**
2. **configure {terminal | memory | network}**
3. **router bgp *as-number***
4. **bgp graceful-restart**
5. **exit**

#### DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure {terminal   memory   network}</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                                                   |

|        | Command or Action                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>router bgp</b> <i>as-number</i>                                                                             | Enters router configuration mode and creates a BGP routing process.                                                                                                                                                                                                                                                                       |
|        | <b>Example:</b><br>Router(config)# router bgp 101                                                              |                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>bgp graceful-restart</b> [ <b>restart-time</b> <i>seconds</i> ]<br>[ <b>stalepath-time</b> <i>seconds</i> ] | Enables the BGP graceful restart capability and BGP NSF awareness.<br><br>If you enter this command after the BGP session has been established, you must restart the session for the capability to be exchanged with the BGP neighbor.<br><br>Use this command on the restarting router and all of its peers (NSF-capable and NSF-aware). |
|        | <b>Example:</b><br>Router(config-router)# bgp graceful-restart                                                 |                                                                                                                                                                                                                                                                                                                                           |
| Step 5 | Router(config-router)# <b>exit</b>                                                                             | Exits router configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                     |
|        | <b>Example:</b><br>Router(config-router)# exit                                                                 |                                                                                                                                                                                                                                                                                                                                           |

## Troubleshooting Tips

To troubleshoot the NSF feature, use the following commands in privileged EXEC mode, as needed:

| Command                             | Purpose                                                                                                                                                                     |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>debug ip bgp</b>         | Displays open messages that advertise the graceful restart capability.                                                                                                      |
| Router# <b>debug ip bgp updates</b> | Displays sent and received EOR messages. The EOR message is used by the NSF-aware router to start the stalepath timer, if configured.                                       |
| Router# <b>debug ip bgp event</b>   | Displays graceful restart timer events, such as the restart timer and the stalepath timer.                                                                                  |
| Router> <b>show ip bgp</b>          | Displays entries in the BGP routing table. The output from this command will display routes that are marked as stale by displaying the letter “S” next to each stale route. |
| Router# <b>show ip bgp neighbor</b> | Displays information about the TCP and BGP connections to neighbor devices. When enabled, the graceful restart capability is displayed in the output of this command.       |

## What to do next

If the **bgp graceful-restart** command has been issued after the BGP session has been established, you must reset by issuing the **clear ip bgp \*** command or by reloading the router before graceful restart capabilities will be exchanged. For more information about resetting BGP sessions and using the **clear ip bgp** command, refer to the following documents:

### BGP Command Reference Documentation

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip2r/bgp\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip2r/bgp_r/index.htm)

### BGP Configuration Documentation

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcprt2/1cfbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfbgp.htm)

## Configuring BGP NSF Awareness Timers

### BGP NSF Awareness Timers

This section documents the configuration of the BGP graceful restart timers.

- (Optional) The **restart-time** argument determines how long peer routers will wait to delete stale routes before a BGP open message is received. The default value is 120 seconds.
- (Optional) The **stalepath-time** argument determines how long a router will wait before deleting stale routes after an end of record (EOR) message is received from the restarting router. The default value is 360 seconds.

### Restrictions

The configuration of the restart and stalepath timers is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

### SUMMARY STEPS

1. **enable**
2. **configure {terminal | memory | network}**
3. **router bgp** *as-number*
4. **bgp graceful-restart restart-time** *seconds*
5. **bgp graceful-restart stalepath-time** *seconds*
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                     | Enables higher privilege levels, such as privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                       |
| Step 2 | <b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }<br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 101                                                                                                                | Enters router configuration mode and creates a BGP routing process.                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>bgp graceful-restart</b> [ <b>restart-time</b> <i>seconds</i> ]<br>[ <b>stalepath-time</b> <i>seconds</i> ]<br><br><b>Example:</b><br>Router(config-router)# bgp graceful-restart<br>restart-time 130   | Enables the BGP graceful restart capability and BGP NSF awareness.<br><br>The <b>restart-time</b> argument determines how long peer routers will wait to delete stale routes before a BGP open message is received.<br><br>The default value is 120 seconds. The configurable range is from 1 to 3600 seconds.                                           |
| Step 5 | <b>bgp graceful-restart</b> [ <b>restart-time</b> <i>seconds</i> ]<br>[ <b>stalepath-time</b> <i>seconds</i> ]<br><br><b>Example:</b><br>Router(config-router)# bgp graceful-restart<br>stalepath-time 350 | Enables the BGP graceful restart capability and BGP NSF awareness.<br><br>The <b>stalepath-time</b> argument determines how long a router will wait before deleting stale routes after an end of record (EOR) message is received from the restarting router.<br><br>The default value is 360 seconds. The configurable range is from 1 to 3600 seconds. |
| Step 6 | Router(config-router)# <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                                   | Exits router configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                    |

## What to do next

If the **bgp graceful-restart** command has been issued after the BGP session has been established, you must reset by issuing the **clear ip bgp \*** command or by reloading the router before graceful restart capabilities will be exchanged. For more information about resetting BGP sessions and using the **clear ip bgp** command, refer to the following documents:

**BGP Command Reference Documentation**

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip2r/bgp\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122tcr/122tip2r/bgp_r/index.htm)

**BGP Configuration Documentation**

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcprt2/1cfbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfbgp.htm)

## Verifying the Configuration of BGP Nonstop Forwarding Awareness

Use the following steps to verify the local configuration of BGP NSF awareness on a router and to verify the configuration NSF awareness on peer routers in a BGP network.

### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show ip bgp neighbors ip-address**

### DETAILED STEPS

|        | Command or Action                                                                                                | Purpose                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                           | Enables higher privilege levels, such as privileged EXEC mode.<br><br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                    |
| Step 2 | <b>show running-config</b><br><br><b>Example:</b><br>Router# show running-config                                 | Displays the running configuration on the local router. The output will display the configuration of the <b>bgp graceful-restart</b> command in the BGP section.                                                              |
| Step 3 | <b>show ip bgp neighbors ip-address</b><br><br><b>Example:</b><br>Router(config)# show ip bgp neighbors 10.0.0.1 | Displays information about TCP and BGP connections to neighbors. "Graceful Restart Capability:advertised and received" will be displayed for each neighbor that has exchanged graceful restart capabilities with this router. |

## Configuration Examples for Nonstop Forwarding

- [Configuring BGP NSF Awareness Example, page 248](#)
- [Configuring the Restart Time for BGP NSF Awareness, page 248](#)
- [Configuring the Stalepath Time for BGP NSF Awareness, page 248](#)
- [Verifying BGP NSF Awareness, page 248](#)

## Configuring BGP NSF Awareness Example

The following example configures BGP NSF awareness on a router that is running BGP:

```
router# configure terminal
router(config)# router bgp 101
router(config-router)# bgp graceful-restart
```

## Configuring the Restart Time for BGP NSF Awareness

The following example configures BGP NSF awareness on a router that is running BGP and sets the restart time to 130 seconds. The configuration of this timer is optional and the preconfigured default value is optimal for most network deployments.

```
router# configure terminal
router(config)# router bgp 101
router(config-router)# bgp graceful-restart restart-time 130
```

## Configuring the Stalepath Time for BGP NSF Awareness

The following example configures BGP NSF awareness on a router that is running BGP and sets the stale path time to 350 seconds. The configuration of this timer is optional and the preconfigured default value is optimal for most network deployments.

```
router# configure terminal
router(config)# router bgp 101
router(config-router)# bgp graceful-restart stalepath-time 350
```

## Verifying BGP NSF Awareness

To verify NSF for BGP, you must check that the graceful restart function is configured on the SSO-enabled networking device and on the neighbor devices. Perform the following steps:

- 
- Step 1** Verify that “bgp graceful-restart” appears in the BGP configuration of the SSO-enabled router by entering the **show running-config** command:

```
Router# show running-config

.
.
.
router bgp 120
.
.
.
bgp graceful-restart
neighbor 10.2.2.2 remote-as 300
.
.
.
```

- Step 2** Repeat step 1 on each of the BGP neighbors.

- Step 3** On peer devices (NSF-capable and NSF-aware), verify that the graceful restart function is shown as both advertised and received, and confirm the address families that have the graceful restart capability. If no address families are listed, then BGP NSF awareness is not enabled:

```
router#show ip bgp neighbors x.x.x.x

BGP neighbor is 192.168.2.2, remote AS YY, external link
  BGP version 4, remote router ID 192.168.2.2
  BGP state = Established, up for 00:01:18
  Last read 00:00:17, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh:advertised and received(new)
    Address family IPv4 Unicast:advertised and received
    Address family IPv4 Multicast:advertised and received
    Graceful Restart Capability:advertised and received
      Remote Restart timer is 120 seconds
      Address families preserved by peer:
        IPv4 Unicast, IPv4 Multicast
  Received 1539 messages, 0 notifications, 0 in queue
  Sent 1544 messages, 0 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
```

## Where to Go Next

For more information about NSF and SSO configuration, refer to the following documents:

- *Cisco Nonstop Forwarding*, Release 12.0(24)S  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/nsf24s.htm>
- *Stateful Switchover*, Release 12.0(24)S  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/sso24s.htm>

## Additional References

For additional information related to BGP NSF Awareness, refer to the following documents:

## Related Documents

| Related Topic           | Document Title                                                                                                       |
|-------------------------|----------------------------------------------------------------------------------------------------------------------|
| BGP commands            | “BGP Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2 |
| BGP configuration tasks | “Configuring BGP” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                              |

## Standards

| Standards <sup>1</sup>                                                                                                                | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

1. Not all supported standards are listed.

## MIBs

| MIBs <sup>1</sup>                                                                                                           | MIBs Link                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs <sup>1</sup>             | Title                                     |
|-------------------------------|-------------------------------------------|
| draft-ietf-idr-restart-06.txt | <i>Graceful Restart Mechanism for BGP</i> |

1. Not all supported RFCs are listed.



## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <p><a href="#">TAC Home Page:</a></p> <p><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></p> <p><a href="#">BGP Support Page:</a></p> <p><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a></p> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Commands

- **bgp graceful-restart**

### Modified Commands

- **show ip bgp**
- **show ip bgp neighbors**





## BGP Restart Session After Max-Prefix Limit

The BGP Restart Session After Max-Prefix Limit feature enhances the capabilities of the **neighbor maximum-prefix** command with the introduction of the **restart** keyword. This enhancement allows the network operator to configure the time interval at which a peering session is reestablished by a router when the number of prefixes that have been received from a peer has exceeded the maximum prefix limit. The **restart** keyword has a configurable timer argument that is specified in minutes. The time range of the timer argument is from 1 to 65535.

### Feature History for the BGP Restart Session After Max-Prefix Limit feature

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(22)S | This feature was introduced. |
| 12.2(15)T | This feature was integrated. |
| 12.2(18)S | This feature was integrated. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Restart Session After Max-Prefix Limit, page 254](#)
- [Restrictions for Restart Session After Max-Prefix Limit, page 254](#)
- [Information About Restart Session After Max-Prefix Limit, page 254](#)
- [How to Configure the Restart Session After Max-Prefix Limit feature, page 255](#)
- [Configuration Examples for the Restart Session After Max-Prefix Limit feature, page 258](#)
- [Additional References, page 260](#)
- [Command Reference, page 261](#)

# Prerequisites for Restart Session After Max-Prefix Limit

This document assumes that BGP is configured in your network and that peering has been established.

## Restrictions for Restart Session After Max-Prefix Limit

This feature attempts to reestablish a disabled peering session at the configured time interval that is specified by the network operator. However, the configuration of the restart timer alone cannot change or correct a peer that is sending an excessive number of prefixes. The network operator will need to reconfigure the maximum-prefix limit or reduce the number of prefixes that are sent from the peer. A peer that is configured to send too many prefixes can cause instability in the network, where an excessive number of prefixes are rapidly advertised and withdrawn. In this case, the **warning-only** keyword can be configured to disable the restart capability, while the network operator corrects the underlying problem.



### Note

The **bgp dampening** command can be used to configure the dampening of a flapping route or interface when a peer is sending too many prefixes and causing network instability. The use of this command should be necessary only when troubleshooting or tuning a router that is sending an excessive number of prefixes.

## Information About Restart Session After Max-Prefix Limit

This section contains the following procedures:

- [Prefix Limits and Peering Sessions, page 254](#)
- [Reestablishing Sessions After the Maximum Prefix Limit, page 254](#)

## Prefix Limits and Peering Sessions

There is a configurable limit on the maximum number of prefixes that a router that is running BGP can receive from a peer router. This limit is configured with the **neighbor maximum-prefix** command. When the router receives too many prefixes from a peer router and the maximum-prefix limit is exceeded, the peering session is disabled or brought down. The session stays down until the network operator manually brings the session back up by entering the **clear ip bgp** command. Entering the **clear ip bgp** command clears stored prefixes.

## Reestablishing Sessions After the Maximum Prefix Limit

The BGP Restart Session After Maximum-Prefix Limit feature enhances the capabilities of the **neighbor maximum-prefix** command with the introduction of the **restart** keyword. This enhancement allows the network operator to configure a router to automatically reestablish a peering session when one has been disabled or brought down. There is configurable time interval at which peering can be reestablished automatically. The configurable timer argument for the **restart** keyword is specified in minutes. The time range is from 1 to 65,535 minutes.

# How to Configure the Restart Session After Max-Prefix Limit feature

This section contains the following procedures:

- [Configuring a Router to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded, page 255](#)
- [Verifying that a Router is Configured to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded, page 257](#)

## Configuring a Router to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded

### Reestablishing Peering Sessions

The network operator can configure a router that is running BGP to automatically reestablish a peering session that has been brought down because the configured maximum-prefix limit has been exceeded. No intervention from the network operator is required when this feature is enabled.

### Restrictions

This feature attempts to reestablish a disabled peering session at the configured time interval that is specified by the network operator. However, the configuration of the restart timer alone cannot change or correct a peer that is sending an excessive number of prefixes. The network operator will need to reconfigure the maximum-prefix limit or reduce the number of prefixes that are sent from the peer. A peer that is configured to send too many prefixes can cause instability in the network, where an excessive number of prefixes are rapidly advertised and withdrawn. In this case, the **warning-only** keyword can be configured to disable the restart capability, while the network operator corrects the underlying problem.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **command** [**keyword** *argument*]
5. **neighbor** {*ip-address* | *peer-group-name*} {**maximum-prefix** *maximum* [*threshold*]}
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 101                                                                                                                                                                                                                               | Enters router configuration mode and creates a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } { <b>maximum-prefix</b> <i>maximum</i> [ <i>threshold</i> ]} [ <b>restart</b> <i>restart-interval</i> ] [ <b>warning-only</b> ]<br><br><b>Example:</b><br>Router(config-router)#neighbor 10.4.9.5 maximum-prefix 1000 90 restart 60 | Configures the maximum-prefix limit on a router that is running BGP, and optionally configures the router to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The configurable range of the <i>restart-interval</i> is from 1 to 65535 minutes.<br><br><b>Note</b> If the <i>restart-interval</i> is not configured, the disabled session will stay down after the maximum-prefix limit is exceeded. This is the default behavior. |
| Step 5 | Router(config-router)# <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                                                                                                                                                  | Exits router configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Troubleshooting Tips

### Useful Commands

The commands in the following table can be useful for trouble shooting issues related to configuring this feature:

| Command                              | Purpose                                                                                                                                                                                                                    |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>clear ip bgp</b>          | Resets a BGP connection using BGP soft reconfiguration. This command can be used to clear stored prefixes to prevent a router that is running BGP from exceeding the maximum-prefix limit.                                 |
| Router# <b>show ip bgp neighbors</b> | Displays information about the TCP and BGP connections to neighbors. The output of this command will display the status and configured restart timer value for the BGP Restart Session After Maximum-Prefix Limit feature. |

### Error Messages

Display of the following error messages can indicate an underlying problem that is causing the peering session to become disabled. The network operator should check the values that are configured for the maximum-prefix limit and the configuration of any peers that are sending an excessive number of prefixes. The following sample error messages below are similar to the error messages that may be displayed:

```
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Up
00:01:14:%BGP-4-MAXPFX:No. of unicast prefix received from 10.10.10.2 reaches 5, max 6
00:01:14:%BGP-3-MAXPFXEXCEED:No.of unicast prefix received from 10.10.10.2:7 exceed limit6
00:01:14:%BGP-5-ADJCHANGE:neighbor 10.10.10.2 Down - BGP Notification sent
00:01:14:%BGP-3-NOTIFICATION:sent to neighbor 10.10.10.2 3/1 (update malformed) 0 byte
```

### What to Do Next

The **bgp dampening** command can be used to configure the dampening of a flapping route or interface when a peer is sending too many prefixes and causing network instability. The use of this command should be necessary only when troubleshooting or tuning a router that is sending an excessive number of prefixes.

## Verifying that a Router is Configured to Reestablish a Peering Session After the Maximum Prefix Limit has Been Exceeded

### SUMMARY STEPS

1. **show ip bgp neighbors ip-address**

## DETAILED STEPS

|        | Command or Action                                                                                        | Purpose                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>show ip bgp neighbors ip-address</b><br><br><b>Example:</b><br>Router> show ip bgp neighbors 10.4.9.5 | Displays information about the TCP and BGP connections to neighbors. The output from this command will display the status and configured restart timer value for the BGP Restart Session After Maximum-Prefix Limit feature. |

## Configuration Examples for the Restart Session After Max-Prefix Limit feature

- [Restart Session After Max-Prefix Limit Configuration Example, page 258](#)
- [Restart Session After Max-Prefix Limit Verification Example, page 258](#)

### Restart Session After Max-Prefix Limit Configuration Example

The following example sets the maximum number of prefixes allowed from the neighbor at 192.168.6.6 to 2000 and configures the router to reestablish a peering session after 30 minutes if one has been disabled:

```
router bgp 101
 network 172.16.0.0
 neighbor 192.168.6.6 maximum-prefix 2000 restart 30
```

### Restart Session After Max-Prefix Limit Verification Example

To verify that a router has been configured to automatically reestablish disabled peering sessions, use the **show ip bgp neighbors** command. The output of this command will display the status and configured restart timer value for the BGP Restart Session After Maximum-Prefix Limit feature. The following output shows that the maximum prefix limit for neighbor 10.4.9.5 is set to 1000 prefixes. The restart threshold is set to 90%

```
Router# show ip bgp neighbors 10.4.9.5
BGP neighbor is 10.4.9.5, remote AS 101, internal link
BGP version 4, remote router ID 10.4.9.5
BGP state = Established, up for 2w2d
Last read 00:00:14, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

              Sent          Rcvd
Opens:          1            1
Notifications:  0            0
```



```

Updates:                0          0
Keepalives:            23095      23095
Route Refresh:          0          0
Total:                  23096      23096
Default minimum time between advertisement runs is 5 seconds

```

For address family: IPv4 Unicast

```

BGP table version 1, neighbor versions 1/0 1/0
Output queue sizes : 0 self, 0 replicated
Index 2, Offset 0, Mask 0x4
Member of update-group 2

```

|                    | Sent | Rcvd |
|--------------------|------|------|
| Prefix activity:   | ---- | ---- |
| Prefixes Current:  | 0    | 0    |
| Prefixes Total:    | 0    | 0    |
| Implicit Withdraw: | 0    | 0    |
| Explicit Withdraw: | 0    | 0    |
| Used as bestpath:  | n/a  | 0    |
| Used as multipath: | n/a  | 0    |

|                               | Outbound | Inbound |
|-------------------------------|----------|---------|
| Local Policy Denied Prefixes: | -----    | -----   |
| Total:                        | 0        | 0       |

```

Maximum prefixes allowed 1000
Threshold for warning message 90%, restart interval 60 min
Number of NLRI's in the update sent: max 0, min 0

```

Connections established 1; dropped 0

Last reset never

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Local host: 10.4.9.21, Local port: 179

Foreign host: 10.4.9.5, Foreign port: 11871

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x5296BD2C):

| Timer     | Starts | Wakeups | Next |
|-----------|--------|---------|------|
| Retrans   | 23098  | 0       | 0x0  |
| TimeWait  | 0      | 0       | 0x0  |
| AckHold   | 23096  | 22692   | 0x0  |
| SendWnd   | 0      | 0       | 0x0  |
| KeepAlive | 0      | 0       | 0x0  |
| GiveUp    | 0      | 0       | 0x0  |
| PmtuAger  | 0      | 0       | 0x0  |
| DeadWait  | 0      | 0       | 0x0  |

```

iss: 1900546793 snduna: 1900985663 sndnxt: 1900985663 sndwnd: 14959
irs: 2894590641 rcvnxt: 2895029492 rcvwnd: 14978 delrcvwnd: 1406

```

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms

minRTT: 0 ms, maxRTT: 316 ms, ACK hold: 200 ms

Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):

Rcvd: 46021 (out of order: 0), with data: 23096, total data bytes: 438850

Sent: 46095 (retransmit: 0, fastretransmit: 0), with data: 23097, total data by9

## Additional References

For additional information related to BGP Restart Session After Max-Prefix Limit feature, refer to the following references:

## Related Documents

| Related Topic           | Document Title                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands            | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.0 Network Protocols Command Reference, Part 1</a></li> <li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2</a></li> <li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3</a></li> </ul> |
| BGP configuration tasks | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1</a></li> <li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.2</a></li> <li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                                               |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">TAC Home Page:</a><br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter%20networking:BGP">BGP Support Page:</a><br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter%20networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **neighbor maximum-prefix**
- **show ip bgp neighbors**





## BGP Cost Community

The BGP Cost Community feature introduces the cost extended community attribute. The cost community is a non-transitive extended community attribute that is passed to internal BGP (iBGP) and confederation peers but not to external BGP (eBGP) peers. The cost community feature allows you to customize the local route preference and influence the best path selection process by assigning cost values to specific routes.

### History for the BGP Cost Community Feature

| Release   | Modification                                                                                                                                                                                                                                                                               |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(24)S | This feature was introduced.                                                                                                                                                                                                                                                               |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.                                                                                                                                                                                                                               |
| 12.2(18)S | This feature was integrated Cisco IOS Release 12.2(18)S.                                                                                                                                                                                                                                   |
| 12.0(27)S | <ul style="list-style-type: none"><li>The <i>BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links</i> feature was introduced. It provides support for mixed EIGRP MPLS VPN network topologies that contain back door routes.</li></ul>                                  |
| 12.3(8)T  | <ul style="list-style-type: none"><li>The <i>BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links</i> feature was integrated into Cisco IOS Release 12.3(8)T. It provides support for mixed EIGRP MPLS VPN network topologies that contain back door routes.</li></ul>  |
| 12.2(25)S | <ul style="list-style-type: none"><li>The <i>BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links</i> feature was integrated into Cisco IOS Release 12.2(25)S. It provides support for mixed EIGRP MPLS VPN network topologies that contain back door routes.</li></ul> |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for the BGP Cost Community Feature, page 264](#)
- [Restrictions for the BGP Cost Community Feature, page 264](#)
- [Information About the BGP Cost Community Feature, page 264](#)

- [How to Configure the BGP Cost Community Feature, page 267](#)
- [Configuration Examples for the BGP Cost Community Feature, page 270](#)
- [Additional References, page 272](#)
- [Command Reference, page 273](#)

## Prerequisites for the BGP Cost Community Feature

This document assumes that BGP is configured in your network and that peering has been established.

## Restrictions for the BGP Cost Community Feature

The following restrictions apply to the BGP Cost Community feature:

- The BGP Cost Community feature can be configured only within an autonomous system or confederation. The cost community is a non-transitive extended community that is passed to iBGP and confederation peers only and is not passed to eBGP peers.
- The BGP Cost Community feature must be supported on all routers in the autonomous system or confederation before cost community filtering is configured. The cost community should be applied consistently throughout the local autonomous system or confederation to avoid potential routing loops.
- Multiple cost community set clauses may be configured with the **set extcommunity cost** command in a single route map block or sequence. However, each set clause must be configured with a different ID value (0-255) for each point of insertion (POI). The ID value determines preference when all other attributes are equal. The lowest ID value is preferred.

## Information About the BGP Cost Community Feature

To configure the BGP Cost Community feature, you must understand the following concepts:

- [BGP Cost Community Overview, page 264](#)
- [How the BGP Cost Community Influences the Best Path Selection Process, page 265](#)
- [Cost Community Support for Aggregate Routes and Multipaths, page 266](#)
- [Influencing Route Preference in a Multi-Exit IGP Network, page 266](#)
- [BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links, page 267](#)

## BGP Cost Community Overview

The cost community is a non-transitive extended community attribute that is passed to iBGP and confederation peers but not to eBGP peers. The configuration of the BGP Cost Community feature allows you to customize the BGP best path selection process for a local autonomous system or confederation.

The cost community attribute is applied to internal routes by configuring the **set extcommunity cost** command in a route map. The cost community set clause is configured with a cost community ID number (0-255) and cost number (0-4294967295). The cost number value determines the preference for the path.

The path with the lowest cost community number is preferred. Paths that are not specifically configured with the cost community attribute are assigned a default cost number value of 2147483647 (The midpoint between 0 and 4294967295) and evaluated by the best path selection process accordingly. In the case where two paths have been configured with the same cost number value, the path selection process will then prefer the path with the lowest cost community ID. The cost extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command.

The following commands can be used to apply the route map that is configured with the cost community set clause:

- **aggregate-address**
- **neighbor default-originate route-map {in | out}**
- **neighbor route-map**
- **network route-map**
- **redistribute route-map**

## How the BGP Cost Community Influences the Best Path Selection Process

The cost community attribute influences the BGP best path selection process at the point of insertion (POI). By default, the POI follows the IGP metric comparison. When BGP receives multiple paths to the same destination, it uses the best path selection process to determine which path is the best path. BGP automatically makes the decision and installs the best path into the routing table. The POI allows you to assign a preference to a specific path when multiple equal cost paths are available. If the POI is not valid for local best path selection, the cost community attribute is silently ignored.

Multiple paths can be configured with the cost community attribute for the same POI. The path with the lowest cost community ID is considered first. In other words, all of the cost community paths for a specific POI are considered, starting with the one with the lowest cost community. Paths that do not contain the cost community (for the POI and community ID being evaluated) are assigned the default community cost value (2147483647). If the cost community values are equal, then cost community comparison proceeds to the next lowest community ID for this POI.



### Note

Paths that are not configured with the cost community attribute are considered by the best path selection process to have the default *cost-value* (half of the maximum value [4294967295] or 2147483647).

Applying the cost community attribute at the POI allows you to assign a value to a path originated or learned by a peer in any part of the local autonomous system or confederation. The cost community can be used as a “tie breaker” during the best path selection process. Multiple instances of the cost community can be configured for separate equal cost paths within the same autonomous system or confederation. For example, a lower cost community value can be applied to a specific exit path in a network with multiple equal cost exits points, and the specific exit path will be preferred by the BGP best path selection process. See the scenario described in the [Influencing Route Preference in a Multi-Exit IGP Network](#) section.

## Cost Community Support for Aggregate Routes and Multipaths

Aggregate routes and multipaths are supported by the BGP Cost Community feature. The cost community attribute can be applied to either type of route. The cost community attribute is passed to the aggregate or multipath route from component routes that carry the cost community attribute. Only unique IDs are passed, and only the highest cost of any individual component route will be applied to the aggregate on a per-ID basis. If multiple component routes contain the same ID, the highest configured cost is applied to the route. For example, the following two component routes are configured with the cost community attribute via an inbound route map:

- 10.0.0.1 (POI=IGP, ID=1, Cost=100)
- 192.168.0.1 (POI=IGP, ID=1, Cost=200)

If these component routes are aggregated or configured as a multipath, the cost value 200 (POI=IGP, ID=1, Cost=200) will be advertised because it is the highest cost.

If one or more component routes does not carry the cost community attribute or if the component routes are configured with different IDs, then the default value (2147483647) will be advertised for the aggregate or multipath route. For example, the following three component routes are configured with the cost community attribute via an inbound route map. However, the component routes are configured with two different IDs.

- 10.0.0.1 (POI=IGP, ID=1, Cost=100)
- 172.16.0.1 (POI=IGP, ID=2, Cost=100)
- 192.168.0.1 (POI=IGP, ID=1, Cost=200)

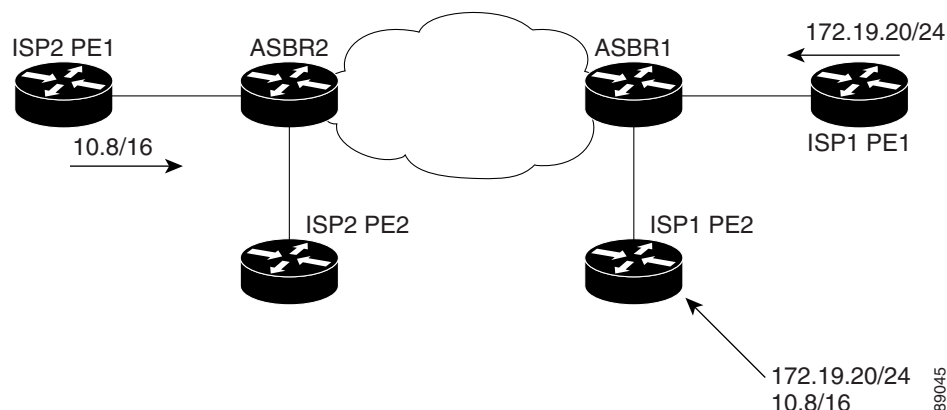
The single advertised path will include the aggregated cost communities as follows:

- {POI=IGP, ID=1, Cost=2147483647} {POI=IGP, ID=2, Cost=2147483647}

## Influencing Route Preference in a Multi-Exit IGP Network

Figure 28 shows an Interior Gateway Protocol (IGP) network with two autonomous system boundary routers (ASBRs) on the edge. Each ASBR has an equal cost path to network 10.8/16.

**Figure 28** Multi-Exit Point IGP Network





Both paths are considered to be equal by BGP. If multipath loadsharing is configured, both paths will be installed to the routing table and will be used to load balance traffic. If multipath load balancing is not configured, then BGP will select the path that was learned first as the best path and install this path to the routing table. This behavior may not be desirable under some conditions. For example, the path is learned from ISP1 PE2 first, but the link between ISP1 PE2 and ASBR1 is a low-speed link.

The configuration of the cost community attribute can be used to influence the BGP best path selection process by applying a lower cost community value to the path learned by ASBR2. For example, the following configuration is applied to ASBR2.

```
route-map ISP2_PE1 permit 10
  set extcommunity cost 1 1
  match ip address 13
!
ip access-list 13 permit 10.8.0.0 0.0.255.255
```

The above route map applies a cost community number value of 1 to the 10.8.0.0 route. By default, the path learned from ASBR1 will be assigned a cost community value of 2147483647. Because the path learned from ASBR2 has lower cost community value, this path will be preferred.

## BGP Cost Community Support for EIGRP MPLS VPN PE-CE with Backdoor Links

Before EIGRP Site of Origin (SoO) BGP Cost Community support was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Back door links in an EIGRP MPLS VPN topology will be preferred by BGP if the back door link is learned first. (A back door link, or a route, is a connection that is configured outside of the VPN between a remote and main site. For example, a WAN leased line that connects a remote site to the corporate network).

The “pre-bestpath” point of insertion (POI) was introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-best path” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when Cisco IOS Release 12.0(27)S is installed to a PE, CE, or back door router.

For information about configuring EIGRP MPLS VPNs, refer to the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge document in Cisco IOS Release 12.0(27)S.

For more information about the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature, refer to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature documentation in Cisco IOS Release 12.0(27)S.

## How to Configure the BGP Cost Community Feature

This section contains the following procedures:

- [Configuring the BGP Cost Community, page 268](#)
- [Verifying the Configuration of the BGP Cost Community, page 269](#)

## Configuring the BGP Cost Community

To configure the cost community, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **router bgp** *as-number*
4. **neighbor** *ip-address* **remote-as** *as-number*
5. **address-family** **ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **ipv6** [**multicast** | **unicast**] | **vpn4** [**unicast**]
6. **neighbor** *ip-address* **route-map** *map-name* {**in** | **out**}
7. **exit**
8. **route-map** *map-name* {**permit** | **deny**}[*sequence-number*]
9. **set** **extcommunity cost** [**igp** | **pre-bestpath**] *community-id* *cost-value*
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                     | Enables higher privilege levels, such as privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }<br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                 | Enters global configuration mode.                                                                                                                    |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 50000                                                                                                                                                                                                                              | Enters router configuration mode to create or configure a BGP routing process.                                                                       |
| Step 4 | <b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remote-as 101                                                                                                                                                                    | Establishes peering with the specified neighbor or peer-group.                                                                                       |
| Step 5 | <b>address-family</b> <b>ipv4</b> [ <b>mdt</b>   <b>multicast</b>   <b>tunnel</b>   <b>unicast</b> [ <b>vrf</b> <i>vrf-name</i> ]   <b>vrf</b> <i>vrf-name</i> ]   <b>ipv6</b> [ <b>multicast</b>   <b>unicast</b> ]   <b>vpn4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 | Places the router in address family configuration mode.                                                                                              |

|         | Command or Action                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>neighbor</b> <i>ip-address</i> <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }<br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 route-map MAP-NAME in | Applies an incoming or outgoing route map for the specified neighbor or peer-group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                                      | Exits router configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 8  | <b>route-map</b> <i>map-name</i> { <b>permit</b>   <b>deny</b> } [ <i>sequence-number</i> ]<br><br><b>Example:</b><br>Router(config)# route-map MAP-NAME permit 10                     | Enters route map configuration mode to create or configure a route map.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 9  | <b>set extcommunity cost</b> [ <b>igp</b> ] <i>community-id</i> <i>cost-value</i><br><br><b>Example:</b><br>Router(config-route-map)# set extcommunity cost 1 100                      | Creates a set clause to apply the cost community attribute. <ul style="list-style-type: none"> <li>Multiple cost community set clauses can be configured in each route map block or sequence. Each cost community set clause must have a different ID (0-255). The cost community set clause with the lowest <i>cost-value</i> is preferred by the best path selection process when all other attributes are equal.</li> <li>Paths that are not configured with the cost community attribute will be assigned the default <i>cost-value</i>, which is half of the maximum value (4294967295) or 2147483647.</li> </ul> |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-route-map)# end                                                                                                                     | Exits route map configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Verifying the Configuration of the BGP Cost Community

BGP cost community configuration can be verified locally or for a specific neighbor. To verify the local configuration cost community, use the **show route-map** or **show running-config** command. To verify that a specific neighbor carries the cost community, use the **show ip bgp ip-address** command. The output from these commands displays the POI (IGP is the default POI), the configured ID, and configured cost. For large cost community values, the output from these commands will also show, with + and - values, the difference between the configured cost and the default cost. See the [BGP Cost Community Verification Examples](#) section for specific example output.

## Troubleshooting Tips

- The **bgp bestpath cost-community ignore** command can be used to disable the evaluation of the cost community attribute to help isolate problems and troubleshoot issues that relate to BGP best path selection.

- The **debug ip bgp updates** command can be used to print BGP update messages. The cost community extended community attribute will be displayed in the output of this command when received from a neighbor. A message will also be displayed if a non-transitive extended community is received from an external peer.

## Configuration Examples for the BGP Cost Community Feature

The following examples show the configuration and verification of this feature:

- [BGP Cost Community Configuration Example, page 270](#)
- [BGP Cost Community Verification Examples, page 270](#)

### BGP Cost Community Configuration Example

The following example configuration shows the configuration of the **set extcommunity cost** command. The following example applies the cost community ID of 1 and cost community value of 100 to routes that are permitted by the route map. This configuration will cause the best path selection process to prefer this route over other equal cost paths that were not permitted by this route map sequence.

```
Router(config)# router bgp 50000
Router(config-router)# neighbor 10.0.0.1 remote-as 50000
Router(config-router)# neighbor 10.0.0.1 update-source Loopback 0
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.1 activate
Router(config-router-af)# neighbor 10.0.0.1 route-map COST1 in
Router(config-router-af)# neighbor 10.0.0.1 send-community both
Router(config-router-af)# exit
Router(config)# route-map COST1 permit 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# set extcommunity cost 1 100
```

### BGP Cost Community Verification Examples

BGP cost community configuration can be verified locally or for a specific neighbor. To verify the local configuration cost community, use the **show route-map** or **show running-config** command. To verify that a specific neighbor carries the cost community, use the **show ip bgp ip-address** command.

The output of the **show route-map** command will display locally configured route-maps, match, set, continue clauses, and the status and configuration of the cost community attribute. The following sample output is similar to the output that will be displayed:

```
Router# show route-map
route-map COST1, permit, sequence 10
  Match clauses:
    as-path (as-path filter): 1
  Set clauses:
    extended community Cost:igp:1:100
  Policy routing matches: 0 packets, 0 bytes
route-map COST1, permit, sequence 20
  Match clauses:
    ip next-hop (access-lists): 2
  Set clauses:
    extended community Cost:igp:2:200
  Policy routing matches: 0 packets, 0 bytes
```

```

route-map COST1, permit, sequence 30
  Match clauses:
    interface FastEthernet0/0
    extcommunity (extcommunity-list filter):300
  Set clauses:
    extended community Cost:igp:3:300
  Policy routing matches: 0 packets, 0 bytes

```

The following sample output shows locally configured routes with large cost community values:

```

Router# show route-map
route-map set-cost, permit, sequence 10
  Match clauses:
  Set clauses:
    extended community RT:1:1 RT:2:2 RT:3:3 RT:4:4 RT:5:5 RT:6:6 RT:7:7
      RT:100:100 RT:200:200 RT:300:300 RT:400:400 RT:500:500 RT:600:600
      RT:700:700 additive
    extended community Cost:igp:1:4294967295 (default+2147483648)
      Cost:igp:2:200 Cost:igp:3:300 Cost:igp:4:400
      Cost:igp:5:2147483648 (default+1) Cost:igp:6:2147484648 (default+1001)
      Cost:igp:7:2147284648 (default-198999)
  Policy routing matches: 0 packets, 0 bytes

```

The output of the **show running-config** command will display match, set, and continue clauses that are configured within a route-map. The following sample output is filtered to show only the relevant part of the running configuration:

```

Router# show running-config | begin route-map
route-map COST1 permit 20
  match ip next-hop 2
  set extcommunity cost igp 2 200
!
route-map COST1 permit 30
  match interface FastEthernet0/0
  match extcommunity 300
  set extcommunity cost igp 3 300
.
.
.

```

The output of the **show ip bgp ip-address** command can be used to verify if a specific neighbor carries a path that is configured with the cost community attribute. The cost community attribute information is displayed in the “Extended Community” field. The POI, the cost community ID, and the cost community number value are displayed. The following sample output shows that neighbor 172.16.1.2 carries a cost community with an ID of 1 and a cost of 100:

```

Router# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
  2 2 2
    172.16.1.2 from 172.16.1.2 (172.16.1.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: Cost:igp:1:100

```

If the specified neighbor is configured with the default cost community number value or if the default value is assigned automatically for cost community evaluation, “default” with + and - values will be displayed after the cost community number value in the output.

## Where to Go Next

For information about configuring EIGRP MPLS VPNs, refer to the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature documentation introduced in Cisco IOS Release 12.0(27)S.

For more information about the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature, refer to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature documentation introduced in Cisco IOS Release 12.0(27)S.

## Additional References

For additional information related to the BGP Cost Community feature, refer to the following references:

## Related Documents

| Related Topic           | Document Title                                                                                                                                    |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP Best Path Selection | <ul style="list-style-type: none"> <li><a href="#">BGP Best Path Selection Algorithm</a></li> </ul>                                               |
| BGP commands            | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| BGP configuration tasks | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                  |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

## RFCs

| RFCs                                    | Title                                       |
|-----------------------------------------|---------------------------------------------|
| draft-retana-bgp-custom-decision-00.txt | <a href="#">BGP Custom Decision Process</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Commands

- **bgp bestpath cost-community ignore**
- **debug ip bgp updates**
- **set extcommunity cost**







# Loadsharing IP Packets Over More Than Six Parallel Paths

The Loadsharing IP Packets Over More Than Six Parallel Paths feature increases the maximum number of parallel routes that can be installed to the routing table for multipath loadsharing.

## Feature History for the Loadsharing IP Packets Over More Than Six Parallel Paths Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.3(2)T  | This feature was introduced.                                  |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Restrictions for Loadsharing IP Packets Over More Than Six Parallel Paths, page 275](#)
- [Loadsharing IP Packets Over More Than Six Parallel Paths Overview, page 276](#)
- [Additional References, page 276](#)
- [Command Reference, page 277](#)

## Restrictions for Loadsharing IP Packets Over More Than Six Parallel Paths

The Loadsharing IP Packets Over More Than Six Parallel Paths feature is only available in software images for supported platforms in Cisco IOS Release 12.3(2)T and later 12.3T releases.

# Loadsharing IP Packets Over More Than Six Parallel Paths Overview

The Loadsharing IP Packets Over More Than Six Parallel Paths feature increases the maximum number of parallel routes that can be installed to the routing table. The maximum number has been increased from six to sixteen for the following commands:

- **maximum-paths**
- **maximum-paths eibgp**
- **maximum-paths ibgp**

The output of the **show ip route summary** command has been updated to show the number of parallel routes supported by the routing table.

The benefits of this feature include the following:

- More flexible configuration of parallel routes in the routing table.
- Ability to configure multipath loadsharing over more links to allow for the configuration of higher-bandwidth aggregation using lower-speed links.

## Additional References

For additional information related to multipath load sharing and the configuration of parallel routes, refer to the following references:

## Related Documents

| Related Topic                      | Document Title                                                                                                                                                                                             |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multipath Load Sharing and Routing | <ul style="list-style-type: none"> <li>• <i>Cisco IOS IP Configuration Guide</i>, Release 12.3</li> <li>• <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i>, Release 12.3</li> </ul> |
| eiBGP Multipath Load Sharing       | <ul style="list-style-type: none"> <li>• <i>BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN</i></li> </ul>                                                                                |
| iBGP Multipath Load Sharing        | <ul style="list-style-type: none"> <li>• <i>iBGP Multipath Load Sharing</i></li> </ul>                                                                                                                     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |

## RFCs

| RFCs <sup>1</sup>                                                                                                           | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **maximum-paths**
- **maximum-paths eibgp**
- **maximum-paths ibgp**
- **show ip route summary**





# BGP Policy Accounting Output Interface Accounting

Border Gateway Protocol (BGP) policy accounting (PA) measures and classifies IP traffic that is sent to, or received from, different peers. Policy accounting was previously available on an input interface only. The BGP Policy Accounting Output Interface Accounting feature introduces several extensions to enable BGP PA on an output interface and to include accounting based on a source address for both input and output traffic on an interface. Counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

## Feature History for BGP PA Output Interface Accounting

| Release    | Modification                                                              |
|------------|---------------------------------------------------------------------------|
| 12.0(9)S   | This feature was introduced.                                              |
| 12.0(17)ST | This feature was integrated into Cisco IOS Release 12.0(17)ST.            |
| 12.0(22)S  | Output interface accounting was added, and the bucket size was increased. |
| 12.3(4)T   | This feature was integrated into Cisco IOS Release 12.3(4)T.              |
| 12.2(22)S  | This feature was integrated into Cisco IOS Release 12.2(22)S.             |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP PA Output Interface Accounting, page 280](#)
- [Information About BGP PA Output Interface Accounting, page 280](#)
- [How to Configure BGP PA Output Interface Accounting, page 281](#)
- [Configuration Examples for BGP PA Output Interface Accounting, page 288](#)

- [Where to Go Next, page 289](#)
- [Additional References, page 289](#)
- [Command Reference, page 290](#)
- [Glossary, page 291](#)

## Prerequisites for BGP PA Output Interface Accounting

Before using the BGP Policy Accounting Output Interface Accounting feature, you must enable BGP and Cisco Express Forwarding (CEF) or distributed CEF (dCEF) on the router.

## Information About BGP PA Output Interface Accounting

To configure BGP PA output interface accounting, you should understand the following concepts:

- [BGP PA Output Interface Accounting, page 280](#)
- [Benefits of BGP PA Output Interface Accounting, page 281](#)

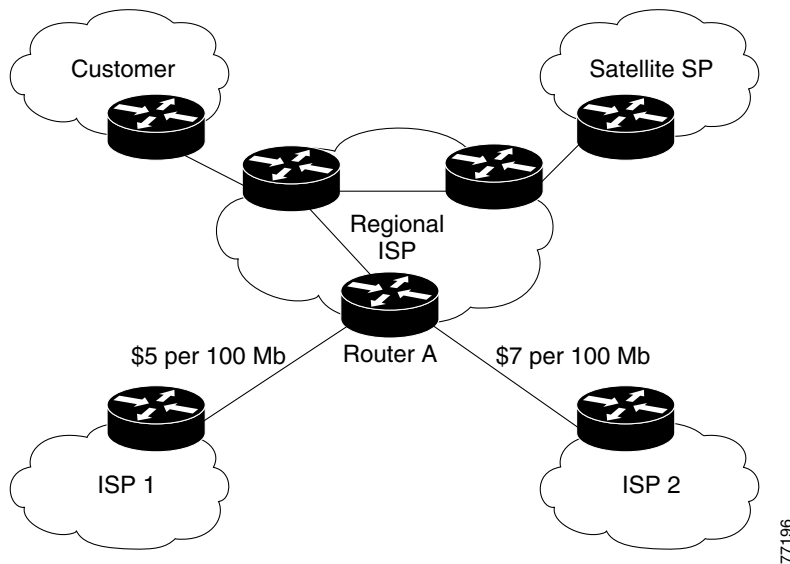
## BGP PA Output Interface Accounting

Policy accounting using BGP measures and classifies IP traffic that is sent to, or received from, different peers. Originally, BGP PA was available on an input interface only. BGP PA output interface accounting introduces several extensions to enable BGP PA on an output interface and to include accounting based on a source address for both input and output traffic on an interface. Counters based on parameters such as community list, autonomous system number, or autonomous system path are assigned to identify the IP traffic.

Using the BGP **table-map** command, prefixes added to the routing table are classified by BGP attribute, autonomous system number, or autonomous system path. Packet and byte counters are incremented per input or output interface. A Cisco IOS policy-based classifier maps the traffic into one of eight possible buckets that represent different traffic classes.

Using BGP PA, you can account for traffic according to its origin or the route it traverses. Service providers (SPs) can identify and account for all traffic by customer and can bill accordingly. In [Figure 29](#), BGP PA can be implemented in Router A to measure packet and byte volumes in autonomous system buckets. Customers are billed appropriately for traffic that is routed from a domestic, international, or satellite source.

**Figure 29**      **Sample Topology for BGP Policy Accounting**



BGP policy accounting using autonomous system numbers can be used to improve the design of network circuit peering and transit agreements between Internet service providers (ISPs).

## Benefits of BGP PA Output Interface Accounting

### Accounting for IP Traffic Differentially

BGP policy accounting classifies IP traffic by autonomous system number, autonomous system path, or community list string, and increments packet and byte counters. Policy accounting can also be based on the source address. Service providers can account for traffic and apply billing according to the origin of the traffic or the route that specific traffic traverses.

### Efficient Network Circuit Peering and Transit Agreement Design

Implementing BGP policy accounting on an edge router can highlight potential design improvements for peering and transit agreements.

## How to Configure BGP PA Output Interface Accounting

This section contains the following tasks:

- [Specifying the Match Criteria for BGP PA, page 282](#) (required)
- [Classifying the IP Traffic and Enabling BGP PA, page 283](#) (required)
- [Verifying BGP Policy Accounting, page 285](#) (optional)

## Specifying the Match Criteria for BGP PA

The first task in configuring BGP PA is to specify the criteria that must be matched. Community lists, autonomous system paths, or autonomous system numbers are examples of BGP attributes that can be specified and subsequently matched using a route map. Perform this task to specify the BGP attribute to use for BGP PA and to create the match criteria in a route map.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip community-list** {*standard-list-number* | *expanded-list-number* [*regular-expression*] | {**standard** | **expanded**} *community-list-name*} {**permit** | **deny**} {*community-number* | *regular-expression*}
4. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
5. **match community-list** *community-list-number* [**exact**]
6. **set traffic-index** *bucket-number*
7. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                              |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                                | Enters global configuration mode.                                                                                                                                    |
| Step 3 | <b>ip community-list</b> { <i>standard-list-number</i>   <i>expanded-list-number</i> [ <i>regular-expression</i> ]   { <b>standard</b>   <b>expanded</b> } <i>community-list-name</i> } { <b>permit</b>   <b>deny</b> } { <i>community-number</i>   <i>regular-expression</i> }<br><br><b>Example:</b><br>Router(config)# ip community-list 30 permit 100:190 | Creates a community list for BGP and controls access to it. <ul style="list-style-type: none"> <li>• Repeat this step for each community to be specified.</li> </ul> |



|        | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ]<br><i>[sequence-number]</i><br><br><b>Example:</b><br>Router(config)# route-map set_bucket permit 10 | Enters route-map configuration mode and defines the conditions for policy routing. <ul style="list-style-type: none"> <li>The <i>map-name</i> argument identifies a route map.</li> <li>The optional <b>permit</b> and <b>deny</b> keywords work with the match and set criteria to control how the packets are accounted for.</li> <li>The optional <i>sequence-number</i> argument indicates the position that a new route map is to have in the list of route maps already configured with the same name.</li> </ul> |
| Step 5 | <b>match community-list</b> <i>community-list-number</i><br><i>[exact]</i><br><br><b>Example:</b><br>Router(config-route-map)# match community-list 30                | Matches a BGP community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 6 | <b>set traffic-index</b> <i>bucket-number</i><br><br><b>Example:</b><br>Router(config-route-map)# set traffic-index 2                                                 | Indicates where to output packets that pass a match clause of a route map for BGP policy accounting.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-route-map)# exit                                                                                                  | Exits route-map configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Classifying the IP Traffic and Enabling BGP PA

After a route map has been defined to specify match criteria, you must configure a way to classify the IP traffic before enabling BGP policy accounting.

Using the **table-map** command, BGP classifies each prefix that it adds to the routing table according to the match criteria. When the **bgp-policy accounting** command is configured on an interface, BGP policy accounting is enabled.

Perform this task to classify the IP traffic and enable BGP policy accounting.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **table-map** *route-map-name*
5. **network** *network-number* [**mask** *network-mask*]
6. **neighbor** *ip-address* **remote-as** *as-number*
7. **exit**
8. **interface** *type number*

9. **ip address** *ip-address mask*
10. **bgp-policy accounting** [**input** | **output**] [**source**]
11. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 65000                                                                  | Configures a BGP routing process and enters router configuration mode for the specified routing process. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument identifies a BGP autonomous system number.</li> </ul>                                                                                                                   |
| Step 4 | <b>table-map</b> <i>route-map-name</i><br><br><b>Example:</b><br>Router(config-router)# table-map set_bucket                                                   | Classifies BGP prefixes entered in the routing table.                                                                                                                                                                                                                                                                                                 |
| Step 5 | <b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ]<br><br><b>Example:</b><br>Router(config-router)# network 10.15.1.0 mask 255.255.255.0 | Specifies a network to be advertised by the BGP routing process.                                                                                                                                                                                                                                                                                      |
| Step 6 | <b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.14.1.1 remote-as 65100        | Specifies a BGP peer by adding an entry to the BGP routing table.                                                                                                                                                                                                                                                                                     |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                              | Exits router configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                             |
| Step 8 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface POS 7/0                                                                | Specifies the interface type and number and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument identifies the type of interface.</li> <li>The <i>number</i> argument identifies the slot and port numbers of the interface. The space between the interface type and number is optional.</li> </ul> |

|         | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>ip address</b> <i>ip-address mask</i><br><br><b>Example:</b><br>Router(config-if)# ip-address 10.15.1.2<br>255.255.255.0                                        | Configures the interface with an IP address.                                                                                                                                                                                                                                                                                                                                                       |
| Step 10 | <b>bgp-policy accounting</b> [ <b>input</b>   <b>output</b> ] [ <b>source</b> ]<br><br><b>Example:</b><br>Router(config-if)# bgp-policy accounting input<br>source | Enables BGP policy accounting for the interface. <ul style="list-style-type: none"> <li>Use the optional <b>input</b> or <b>output</b> keyword to account for traffic either entering or leaving the router. By default, BGP policy accounting is based on traffic entering the router.</li> <li>Use the optional <b>source</b> keyword to account for traffic based on source address.</li> </ul> |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                      | Exits interface configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                       |

## Verifying BGP Policy Accounting

Perform this task to verify that BGP policy accounting is operating.

### SUMMARY STEPS

1. **show ip cef** [*network [mask]*] [**detail**]
2. **show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
3. **show cef interface** [*type number*] **policy-statistics** [**input** | **output**]
4. **show cef interface** [*type number*] [**statistics**] [**detail**]

### DETAILED STEPS

- |               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>show ip cef</b> [ <i>network [mask]</i> ] [ <b>detail</b> ]<br><br>Enter the <b>show ip cef</b> command with the <b>detail</b> keyword to learn which accounting bucket is assigned to a specified prefix.<br><br>In this example, the output is displayed for the prefix 192.168.5.0. It shows that accounting bucket number 4 (traffic_index 4) is assigned to this prefix.<br><br>Router# <b>show ip cef 192.168.5.0 detail</b><br><br><pre> 192.168.5.0/24, version 21, cached adjacency to POS7/2 0 packets, 0 bytes, traffic_index 4   via 10.14.1.1, 0 dependencies, recursive     next hop 10.14.1.1, POS7/2 via 10.14.1.0/30     valid cached adjacency </pre> |
| <b>Step 2</b> | <b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ] [ <b>longer-prefixes</b> ]<br><br>Enter the <b>show ip bgp</b> command for the same prefix used in Step 1—192.168.5.0—to learn which community is assigned to this prefix.                                                                                                                                                                                                                                                                                                                                                                                                                                   |

In this example, the output is displayed for the prefix 192.168.5.0. It shows that the community of 100:197 is assigned to this prefix.

```
Router# show ip bgp 192.168.5.0
```

```
BGP routing table entry for 192.168.5.0/24, version 2
```

```
Paths: (1 available, best #1)
```

```
Not advertised to any peer
```

```
100
```

```
10.14.1.1 from 10.14.1.1 (32.32.32.32)
```

```
Origin IGP, metric 0, localpref 100, valid, external, best
```

```
Community: 100:197
```

### Step 3 show cef interface [type number] policy-statistics [input | output]

Enter the **show cef interface policy-statistics** command to display the per-interface traffic statistics.

In this example, the output shows the number of packets and bytes that have been assigned to each accounting bucket:

```
Router# show cef interface policy-statistics input
```

```
FastEthernet1/0/0 is up (if_number 6)
```

```
Corresponding hwidb fast_if_number 6
```

```
Corresponding hwidb firstsw->if_number 6
```

```
BGP based Policy accounting on input is enabled
```

| Index | Packets | Bytes  |
|-------|---------|--------|
| 1     | 9999    | 999900 |
| 2     | 0       | 0      |
| 3     | 0       | 0      |
| 4     | 0       | 0      |
| 5     | 0       | 0      |
| 6     | 0       | 0      |
| 7     | 0       | 0      |
| 8     | 0       | 0      |
| 9     | 0       | 0      |
| 10    | 0       | 0      |
| 11    | 0       | 0      |
| 12    | 0       | 0      |
| 13    | 0       | 0      |
| 14    | 0       | 0      |
| 15    | 0       | 0      |
| 16    | 0       | 0      |
| 17    | 0       | 0      |
| 18    | 0       | 0      |
| 19    | 0       | 0      |
| 20    | 0       | 0      |
| 21    | 0       | 0      |
| 22    | 0       | 0      |
| 23    | 0       | 0      |
| 24    | 0       | 0      |
| 25    | 0       | 0      |
| 26    | 0       | 0      |
| 27    | 0       | 0      |
| 28    | 0       | 0      |
| 29    | 0       | 0      |
| 30    | 0       | 0      |
| 31    | 0       | 0      |
| 32    | 0       | 0      |
| 33    | 0       | 0      |
| 34    | 1234    | 123400 |
| 35    | 0       | 0      |
| 36    | 0       | 0      |
| 37    | 0       | 0      |

|    |      |         |
|----|------|---------|
| 38 | 0    | 0       |
| 39 | 0    | 0       |
| 40 | 0    | 0       |
| 41 | 0    | 0       |
| 42 | 0    | 0       |
| 43 | 0    | 0       |
| 44 | 0    | 0       |
| 45 | 1000 | 100000  |
| 46 | 0    | 0       |
| 47 | 0    | 0       |
| 48 | 0    | 0       |
| 49 | 0    | 0       |
| 50 | 0    | 0       |
| 51 | 0    | 0       |
| 52 | 0    | 0       |
| 53 | 0    | 0       |
| 54 | 5123 | 1198782 |
| 55 | 0    | 0       |
| 56 | 0    | 0       |
| 57 | 0    | 0       |
| 58 | 0    | 0       |
| 59 | 0    | 0       |
| 60 | 0    | 0       |
| 61 | 0    | 0       |
| 62 | 0    | 0       |
| 63 | 0    | 0       |
| 64 | 0    | 0       |

**Step 4** **show cef interface** [*type number*] [**statistics**] [**detail**]

Enter the **show cef interface EXEC** command to display the state of BGP policy accounting on a specified interface.

In this example, the output shows that BGP policy accounting has been configured to be based on input traffic at Fast Ethernet interface 1/0/0:

```
Router# show cef interface Fast Ethernet 1/0/0

FastEthernet1/0/0 is up (if_number 6)
Corresponding hwidb fast_if_number 6
Corresponding hwidb firstsw->if_number 6
Internet address is 10.1.1.1/24
ICMP redirects are always sent
Per packet load-sharing is disabled
IP unicast RPF check is disabled
Inbound access list is not set
Outbound access list is not set
IP policy routing is disabled
BGP based policy accounting on input is enabled
BGP based policy accounting on output is disabled
Hardware idb is FastEthernet1/0/0 (6)
Software idb is FastEthernet1/0/0 (6)
Fast switching type 1, interface type 18
IP Distributed CEF switching enabled
IP Feature Fast switching turbo vector
IP Feature CEF switching turbo vector
Input fast flags 0x100, Output fast flags 0x0, Flags 0x0
ifindex 7(7)
Slot 1 Slot unit 0 VC -1
Transmit limit accumulator 0xE8001A82 (0xE8001A82)
IP MTU 1500
```

# Configuration Examples for BGP PA Output Interface Accounting

This section contains the following configuration examples:

- [Specifying the Match Criteria for BGP Policy Accounting: Example, page 288](#)
- [Classifying the IP Traffic and Enabling BGP Policy Accounting: Example, page 288](#)

## Specifying the Match Criteria for BGP Policy Accounting: Example

In the following example, BGP communities are specified in community lists, and a route map named `set_bucket` is configured to match each of the community lists to a specific accounting bucket using the `set traffic-index` command:

```
ip community-list 30 permit 100:190
ip community-list 40 permit 100:198
ip community-list 50 permit 100:197
ip community-list 60 permit 100:296
!
route-map set_bucket permit 10
  match community-list 30
  set traffic-index 2
!
route-map set_bucket permit 20
  match community-list 40
  set traffic-index 3
!
route-map set_bucket permit 30
  match community-list 50
  set traffic-index 4
!
route-map set_bucket permit 40
  match community-list 60
  set traffic-index 5
```

## Classifying the IP Traffic and Enabling BGP Policy Accounting: Example

In the following example, BGP policy accounting is enabled on POS interface 7/0. The policy accounting criteria is based on the source address of the input traffic, and the `table-map` command is used to modify the bucket number when the IP routing table is updated with routes learned from BGP.

```
router bgp 65000
  table-map set_bucket
  network 10.15.1.0 mask 255.255.255.0
  neighbor 10.14.1.1 remote-as 65100
!
ip classless
ip bgp-community new-format
!
interface POS7/0
  ip address 10.15.1.2 255.255.255.0
  bgp-policy accounting input source
  no keepalive
  crc 32
  clock source internal
```

## Where to Go Next

Additional BGP, CEF, and dCEF command and configuration information is available from the appropriate Cisco IOS command reference or configuration guide documents. For more details, see the [“Related Documents”](#) section.

## Additional References

The following sections provide references related to BGP policy accounting.

### Related Documents

| Related Topic                                                                                       | Document Title                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands: complete command syntax, command mode, defaults, usage guidelines, and examples       | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</a>, Release 12.2</li><li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a>, Release 12.3 T</li></ul> |
| BGP configuration                                                                                   | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Configuration Guide</a>, Release 12.2</li><li>• <a href="#">Cisco IOS IP Configuration Guide</a>, Release 12.3</li></ul>                                                                   |
| Switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS Switching Services Command Reference</a>, Release 12.2</li><li>• <a href="#">Cisco IOS Switching Services Command Reference</a>, Release 12.3 T</li></ul>                                     |
| Switching configuration                                                                             | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS Switching Services Configuration Guide</a>, Release 12.2</li><li>• <a href="#">Cisco IOS Switching Services Configuration Guide</a>, Release 12.3</li></ul>                                   |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                            | MIBs Link                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-BGP-POLICY-ACCOUNTING-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **bgp-policy**
- **set traffic-index**
- **show cef interface**
- **show cef interface policy-statistics**



# Glossary

**AS**—autonomous system. An IP term to describe a routing domain that has its own independent routing policy and is administered by a single authority.

**BGP**—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems.

**CEF**—Cisco Express Forwarding.

**dCEF**—distributed Cisco Express Forwarding.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---





# Regex Engine Performance Enhancement

The Regex Engine Performance Enhancement feature introduces a new regular expression engine that is designed to process complex regular expressions. This new regular expression engine does not replace the existing engine. The existing engine is preferred for simple regular expressions and is the default engine and in Cisco IOS software. Either engine can be selected from the command-line interface (CLI).

## Feature History for the Regex Engine Performance Enhancement Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(26)S | This feature was introduced.                                  |
| 12.3(4)T  | This feature was integrated into Cisco IOS Release 12.3(4)T.  |
| 12.2(22)S | This feature was integrated into Cisco IOS Release 12.2(22)S. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Regex Engine Performance Enhancement, page 294](#)
- [Information About Regex Engine Performance Enhancement, page 294](#)
- [How to Change the Regular Expression Engine, page 295](#)
- [Additional References, page 296](#)
- [Command Reference, page 297](#)

# Prerequisites for Regex Engine Performance Enhancement

The regular expression engine can be selected only under a Border Gateway Protocol (BGP) routing process in router configuration mode. So, the engine can be changed only after BGP has been enabled.

## Information About Regex Engine Performance Enhancement

To select a regular expression engine in Cisco IOS software, you must understand the following concepts:

- [Regular Expression Overview, page 294](#)
- [Default Regular Expression Engine, page 294](#)
- [New Regular Expression Engine Selection, page 294](#)

## Regular Expression Overview

A regular expression is a pattern to match against an input string. You specify the pattern that a string must match when you compose a regular expression. Matching a string to the specified pattern is called “pattern matching.” Pattern matching either succeeds or fails.

A regular expression can be a single-character pattern or a multiple-character pattern. That is, a regular expression can be a single character that matches the same single character in the input string or multiple characters that match the same multiple characters in the input string.

## Default Regular Expression Engine

The default Cisco IOS regular expression engine uses a recursive algorithm. This engine is effective but uses more system resources as the complexity of regular expressions increase. The recursive algorithm works well for simple regular expressions, but is less efficient when processing very complex regular expressions because of the backtracking that is required by the default engine to process partial matches. In some cases, CPU watchdog timeouts and stack overflow traces have occurred because of the length of time that the default engine requires to process very complex regular expressions.

## New Regular Expression Engine Selection

The Regex Engine Performance Enhancement feature introduces a deterministic processing time regular expression engine in Cisco IOS software. This new engine does not replace the default regular expression engine. The new engine employs an improved algorithm that eliminates excessive backtracking and greatly improves performance when processing complex regular expressions. When the new engine is enabled, complex regular expressions are evaluated more quickly, and CPU watchdog timeouts and stack overflow traces will not occur. However, the new regular expression engine takes longer to process simple regular expressions than the default engine.

We recommend that you use the new regular expression engine if you need to evaluate complex regular expressions or if you have observed problems related to evaluating regular expressions. We recommend that you use the default regular expression engine if you use only simple regular expressions. The new engine can be enabled by entering the **bgp regexp deterministic** command under a BGP routing process. The default regular expression engine can be reenabled by entering the **no** form of this command.

# How to Change the Regular Expression Engine

## Selecting the New Regular Expression Engine

We recommend that you use the new regular expression engine if you need to evaluate complex regular expressions or if you have observed problems related to evaluating regular expressions. We recommend that you use the default regular expression engine if you only use simple regular expressions.

## Prerequisites

The regular expression engine can be selected only under a BGP routing process in router configuration mode. So, the engine can be changed only after BGP has been enabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp regexp deterministic**
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                         | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal            | Enters global configuration mode.                                                                                |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 1 | Enters router configuration mode, and creates a BGP routing process.                                             |

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>bgp regexp deterministic</b><br><br><b>Example:</b><br>Router(config-router)# no bgp regexp deterministic | Configures Cisco IOS to use a deterministic regular expression engine. <ul style="list-style-type: none"> <li>The default regular expression engine in Cisco IOS software is nondeterministic.</li> <li>The default engine can be restored by entering the <b>no</b> form of this command.</li> </ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                            | Exits router configuration mode, and enters global configuration mode.                                                                                                                                                                                                                                |

## Examples

The following example configures Cisco IOS software to use the default regular expression engine:

```
router bgp 1
 no bgp regexp deterministic
```

The following example configures Cisco IOS software to use the deterministic processing time regular expression engine:

```
router bgp 1
 bgp regexp deterministic
```

## Additional References

The following sections provide references related to the Regex Engine Performance Enhancement feature.

## Related Documents

| Related Topic       | Document Title                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------|
| Regular Expressions | <a href="#">“Regular Expressions” appendix of the <i>Cisco IOS Terminal Services Configuration Guide</i></a> |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **bgp regexp deterministic**







## BGP MIB Support Enhancements

The BGP MIB Support Enhancements feature enhances or introduces the following capabilities for Simple Network Management (SNMP) monitoring of Border Gateway Protocol (BGP) using the CISCO-BGP4-MIB:

- *BGP FSM Transition Change Support*—Enhances support for notification of BGP Finite State Machine (FSM) transition changes.
- *BGP Route Received Route Support*—Introduces the capability to query for the total number of routes received by a BGP neighbor.
- *BGP Prefix Threshold Notification Support*—Introduces the capability to send notifications when the prefix limit for a BGP peer has been reached.
- *VPNv4 Unicast Address Family Route Support*—Enhances the cbgpRouteTable object to provide support for SNMP GET operations on VPNv4 unicast routes.

### Feature History for the BGP MIB Support Enhancements Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(26)S | This feature was introduced.                                  |
| 12.3(7)T  | This feature was integrated into Cisco IOS Release 12.3(7)T.  |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP MIB Support Enhancements, page 300](#)
- [Restrictions for BGP MIB Support Enhancements, page 300](#)
- [BGP MIB Support Enhancements Overview, page 300](#)

- [How to Enable BGP MIB Support on a Router, page 302](#)
- [Configuration Examples for BGP MIB Support Enhancements, page 303](#)
- [Additional References, page 303](#)
- [Command Reference, page 304](#)

## Prerequisites for BGP MIB Support Enhancements

- SNMP must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.

## Restrictions for BGP MIB Support Enhancements

- All enhancements that are introduced by this feature are supported by only the CISCO-BGP4-MIB.

## BGP MIB Support Enhancements Overview

The BGP MIB Support Enhancements feature introduces support in the CISCO-BGP4-MIB for new SNMP notifications. To enable BGP support for the enhancement described in this document, use the **snmp-server enable traps bgp** command in global configuration mode. The following sections describe the objects and notifications (traps) that have been enhanced by this feature:

- [BGP FSM Transition Change Support, page 300](#)
- [BGP Route Received Route Support, page 301](#)
- [BGP Prefix Threshold Notification Support, page 301](#)
- [VPNv4 Unicast Address Family Route Support, page 301](#)

### BGP FSM Transition Change Support

The *cbgpFsmStateChange* object was introduced to allow the network operator to configure SNMP notifications (traps) for all BGP Finite State Machine (FSM) transition state changes. This notification contains the following MIB objects:

- *bgpPeerLastError*
- *bgpPeerState*
- *cbgpPeerLastErrorTxt*
- *cbgpPeerPrevState*

The *cbgpBackwardTransition* object has also been enhanced to support all BGP FSM transition state changes. This object is sent each time the BGP FSM moves to either a higher or lower numbered state. This notification contains the following MIB objects:

- *bgpPeerLastError*
- *bgpPeerState*
- *cbgpPeerLastErrorTxt*

- *cbgpPeerPrevState*

The enhancement to the **snmp-server enable bgp traps** privileged EXEC command allows you to enable the newly introduced traps individually or together with the existing FSM backward transition and established state traps as defined in [RFC 1657](#).

## BGP Route Received Route Support

The *cbgpRouteTable* object has been enhanced to accommodate the total number of routes received by a BGP neighbor for all supported address families. Routes are indexed by the address-family identifier (AFI) or subaddress-family identifier (SAFI).

## BGP Prefix Threshold Notification Support

The *cbgpPrefixMaxThresholdExceed* and *cbgpPrfexMaxThresholdClear* objects were introduced to allow you to poll for the total number of routes received by a BGP peer.

The *cbgpPrefixMaxThresholdExceed* object was introduced to allow you to configure SNMP notifications to be sent when the prefix count for a BGP session has exceeded the configured value. This notification is configured on a per address family basis. The prefix threshold is configured with the **neighbor maximum-prefix** command. This notification contains the following MIB objects:

- *cbgpPeerPrefixAdminLimit*
- *cbgpPeerPrefixThreshold*

The *cbgpPrfexMaxThresholdClear* object was introduced to allow you to configure SNMP notifications to be sent when the prefix count drops below the clear trap limit. This notification is configured on a per address family basis. This notification contains the following objects:

- *cbgpPeerPrefixAdminLimit*
- *cbgpPeerPrefixClearThreshold*

Notifications are sent when the prefix count drops below the clear trap limit for an address family under a BGP session after the *cbgpPrefixMaxThresholdExceed* notification is generated. The clear trap limit is calculated by subtracting 5 percent from the maximum prefix limit value configured with the **neighbor maximum-prefix** command. This notification will not be generated if the session goes down for any other reason after the *cbgpPrefixMaxThresholdExceed* is generated.

## VPNv4 Unicast Address Family Route Support

The *cbgpRouteTable* object was enhanced to allow you to configure SNMP GET operations for VPNv4 unicast address-family routes. Each route is indexed by peer address, prefix, and prefix length. This object indexes BGP routes by the AFI and then by the SAFI. The AFI table is the primary index, and the SAFI table is the secondary index. Each BGP speaker maintains a local Routing Information Base (RIB) for each supported AFI and SAFI combination. The *cbgpRouteTable* object has been enhanced to allow you to configure SNMP GET operations for VPNv4 unicast routes.

# How to Enable BGP MIB Support on a Router

SNMP notifications can be configured on the router and GET operations can be performed from an external management station only after BGP SNMP support is enabled.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps bgp [state-changes {[all] [backward-trans] [limited]}] | [threshold prefix]**
4. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                     | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>snmp-server enable traps bgp [state-changes {[all] [backward-trans] [limited]}]   [threshold prefix]</b><br><br><b>Example:</b><br>Router# snmp-server enable traps bgp | Enables BGP support for SNMP operations. Entering this command with no keywords or arguments enables support for all BGP events.<br><br>The <b>state-changes</b> keyword is used to enable support for FSM transition events.<br><ul style="list-style-type: none"><li>• The <b>all</b> keyword enables support for FSM transitions events.</li><li>• The <b>backward-trans</b> keyword enables support only for backward transition state change events.</li><li>• The <b>limited</b> keyword enables support for backward transition state changes and established state events.</li></ul> The <b>threshold prefix</b> keywords are used to enable notifications when the configured maximum prefix limit is reached on the specified peer. |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                 | Exits global configuration mode, and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

# Configuration Examples for BGP MIB Support Enhancements

The following examples show how to configure and verify the BGP MIB Support Enhancements feature:

- [Configuring BGP MIB Support Enhancements: Example](#)
- [Verifying BGP MIB Support Enhancements: Example](#)

## Configuring BGP MIB Support Enhancements: Example

The following example enables SNMP support for all supported BGP events:

```
Router(config)# snmp-server enable traps bgp
```

## Verifying BGP MIB Support Enhancements: Example

The following verification example shows that SNMP support for BGP is enabled and shown the running-config file:

```
Router# show run | include snmp-server
snmp-server enable traps bgp
```

## Where to Go Next

For more information about SNMP and SNMP operations, refer to the “[Configuring SNMP Support](#)” section of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide*, Release 12.3.

## Additional References

The following sections provide references related to BGP MIB Support Enhancements.

## Related Documents

| Related Topic           | Document Title                                                                                    |
|-------------------------|---------------------------------------------------------------------------------------------------|
| BGP commands            | • <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a> |
| BGP configuration tasks | • <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a>                                  |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                             | MIBs Link                                                                                                                                                                                                                         |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>CISCO-BGP4-MIB</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs     | Title                                                                                                            |
|----------|------------------------------------------------------------------------------------------------------------------|
| RFC 1657 | <i>Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIPv2</i> |
| RFC 1771 | <i>A Border Gateway Protocol 4 (BGP-4)</i>                                                                       |
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                                                                             |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                                                                     |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                                                                        |
| RFC 2918 | <i>Route Refresh Capability for BGP-4</i>                                                                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- snmp-server enable traps bgp**



## BGP Support for TTL Security Check

The BGP Support for TTL Security Check feature introduces a lightweight security mechanism to protect external Border Gateway Protocol (eBGP) peering sessions from CPU utilization-based attacks using forged IP packets. Enabling this feature prevents attempts to hijack the eBGP peering session by a host on a network segment that is not part of either BGP network or by a host on a network segment that is not between the eBGP peers.

You enable this feature by configuring a minimum Time To Live (TTL) value for incoming IP packets received from a specific eBGP peer. When this feature is enabled, BGP will establish and maintain the session only if the TTL value in the IP packet header is equal to or greater than the TTL value configured for the peering session. If the value is less than the configured value, the packet is silently discarded and no Internet Control Message Protocol (ICMP) message is generated. This feature is both effective and easy to deploy.

### Feature History for the BGP Support for TTL Security Check Feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(27)S   | This feature was introduced.                                    |
| 12.3(7)T    | This feature was integrated into Cisco IOS Release 12.3(7)T.    |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Support for TTL Security Check, page 306](#)
- [Restrictions for BGP Support for TTL Security Check, page 306](#)
- [Information About BGP Support for TTL Security Check, page 306](#)

- [How to Secure BGP Sessions with the BGP Support for TTL Security Check Feature, page 308](#)
- [Configuration Examples for the BGP Support for TTL Security Check Feature, page 311](#)
- [Additional References, page 313](#)
- [Command Reference, page 314](#)

## Prerequisites for BGP Support for TTL Security Check

- BGP must be configured in your network and eBGP peering sessions must be established.
- This feature needs to be configured on each participating router. It protects the eBGP peering session in the incoming direction only and has no effect on outgoing IP packets or the remote router.

## Restrictions for BGP Support for TTL Security Check

- This feature is designed to protect only eBGP peering sessions and is not supported for internal BGP (iBGP) peers and iBGP peer groups.
- When configuring the BGP Support for TTL Security Check feature to support an existing multihop peering session, you must first disable the **neighbor ebgp-multihop** router configuration command by entering the **no neighbor ebgp-multihop** command before configuring this feature with the **neighbor ttl-security** router configuration command. These commands are mutually exclusive, and only one command is required to establish a multihop peering session. If you attempt to configure both commands for the same peering session, an error message will be displayed in the console.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside your network. This restriction also includes BGP peers that are not part of the local or external BGP network but are connected to the network segment between the BGP peers (for example, a switch or hub that is used to connect the local and external BGP networks).
- This feature does not protect the integrity of data sent between eBGP peers and does not validate eBGP peers through any authentication method. This feature validates only the locally configured TTL count against the TTL field in the IP packet header.

## Information About BGP Support for TTL Security Check

To configure the BGP Support for TTL Security Check feature, you must understand the following concepts:

- [BGP Support for TTL Security Check Feature Overview, page 307](#)
- [Configuring the TTL Security Check for BGP Peering Sessions, page 307](#)
- [Configuring the TTL Security Check for Multihop BGP Peering Sessions, page 307](#)
- [Benefits of the BGP Support for TTL Security Check Feature, page 308](#)



## BGP Support for TTL Security Check Feature Overview

The BGP Support for TTL Security Check feature introduces a lightweight security mechanism to protect eBGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses.

This feature protects the eBGP peering session by comparing the value in the TTL field of received IP packets against a hop count that is configured locally for each eBGP peering session. If the value in the TTL field of the incoming IP packet is greater than or equal to the locally configured value, the IP packet is accepted and processed normally. If the TTL value in the IP packet is less than the locally configured value, the packet is silently discarded and no ICMP message is generated. This is designed behavior; a response to a forged packet is unnecessary.

Accurately forging the TTL count in an IP packet is generally considered to be impossible. It is possible to forge the TTL field in an IP packet header. However, accurately forging a packet to match the TTL count from a trusted peer is not possible unless the network to which the trusted peer belongs has been compromised.

This feature supports both directly connected peering sessions and multihop eBGP peering sessions. The BGP peering session is not affected by incoming packets that contain invalid TTL values. The BGP peering session will remain open, and the router will silently discard the invalid packet. The BGP session, however, can still expire if keepalive packets are not received before the session timer expires.

## Configuring the TTL Security Check for BGP Peering Sessions

The BGP Support for TTL Security Check feature is configured with the **neighbor ttl-security** command in router configuration mode or address family configuration mode. When this feature is enabled, BGP will establish or maintain a session only if the TTL value in the IP packet header is equal to or greater than the TTL value configured for the peering session. Enabling this feature secures the eBGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router. The *hop-count* argument is used to configure the maximum number of hops that separate the two peers. The TTL value is determined by the router from the configured hop count. The value for this argument is a number from 1 to 254.

## Configuring the TTL Security Check for Multihop BGP Peering Sessions

The BGP Support for TTL Security Check feature supports both directly connected peering sessions and multihop peering sessions. When this feature is configured for a multihop peering session, the **neighbor ebgp-multihop** router configuration command cannot be configured and is not needed to establish the peering session. These commands are mutually exclusive, and only one command is required to establish a multihop peering session. If you attempt to configure both commands for the same peering session, an error message will be displayed in the console.

To configure this feature for an existing multihop session, you must first disable the existing peering session with the **no neighbor ebgp-multihop** command. The multihop peering session will be restored when you enable this feature with the **neighbor ttl-security** command.

This feature should be configured on each participating router. To maximize the effectiveness of this feature, the *hop-count* argument should be strictly configured to match the number of hops between the local and external network. However, you should also consider path variation when configuring this feature for a multihop peering session.

## Benefits of the BGP Support for TTL Security Check Feature

The BGP Support for TTL Security Check feature provides an effective and easy-to-deploy solution to protect eBGP peering sessions from CPU utilization-based attacks. When this feature is enabled, a host cannot attack a BGP session if the host is not a member of the local or remote BGP network or if the host is not directly connected to a network segment between the local and remote BGP networks. This solution greatly reduces the effectiveness of DoS attacks against a BGP autonomous system.

## How to Secure BGP Sessions with the BGP Support for TTL Security Check Feature

This section contains the following procedures:

- [Configuring the TTL-Security Check, page 308](#) (required)
- [Verifying the TTL-Security Check Configuration, page 310](#) (optional)

## Configuring the TTL-Security Check

To configure the BGP Support for TTL Security Check Feature, perform the steps in this section.

### Prerequisites

- To maximize the effectiveness of this feature, we recommend that you configure it on each participating router. Enabling this feature secures the eBGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router.

### Restrictions

- The **neighbor ebgp-multihop** command is not needed when this feature is configured for a multihop peering session and should be disabled before configuring this feature.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside of the local and remote network. This restriction also includes peers that are on the network segment between the local and remote network.

### SUMMARY STEPS

1. **enable**
2. **trace [protocol] destination**
3. **configure terminal**
4. **router bgp autonomous-system-number**
5. **neighbor ip-address ttl-security hops hop-count**
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>trace</b> [ <b>protocol</b> ] <i>destination</i><br><br><b>Example:</b><br>Router# trace ip 10.1.1.1                                                               | Discovers the routes of the specified protocol that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>Enter the <b>trace</b> command to determine the number of hops to the specified peer.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 65000                                                          | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 5 | <b>neighbor</b> <i>ip-address</i> <b>ttl-security hops</b> <i>hop-count</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.1.1.1<br>ttl-security hops 2 | Configures the maximum number of hops that separate two peers. <ul style="list-style-type: none"> <li>The <i>hop-count</i> argument is set to number of hops that separate the local and remote peer. If the expected TTL value in the IP packet header is 254, then the number 1 should be configured for the <i>hop-count</i> argument. The range of values is a number from 1 to 254.</li> <li>When this feature is enabled, BGP will accept incoming IP packets with a TTL value that is equal to or greater than the expected TTL value. Packets that are not accepted are silently discarded.</li> <li>The example configuration sets the expected incoming TTL value to 2. The local router will accept the peering session from the 10.1.1.1 neighbor only if it is 1 or 2 hops away.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                      | Exits router configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Examples

The following example sets the expected incoming TTL value for a directly connected eBGP peer. The *hop-count* argument is set to 2 configuring BGP to only accept IP packets with a TTL count in the header that is equal to or greater than 253. If the 10.1.1.1 neighbor is more than 2 hops away, the peering session will not be accepted.

```
neighbor 10.1.1.1 ttl-security hops 2
```

## What to Do Next

The next task is to verify the TTL-security check configuration. Use the steps in the Verifying TTL-Security Check Configuration section.

## Verifying the TTL-Security Check Configuration

You can verify the local configuration of this feature with the **show running-config** and **show ip bgp neighbors** commands.

### SUMMARY STEPS

1. **enable**
2. **show running-config** [*interface type number*] [*linenum*] [*map-class*]
3. **show ip bgp neighbors** *neighbor-address* [**advertised-routes** | **dampened-routes** | **paths** *regular-expression*] | **policy** | **received-routes** | **routes** | **received prefix-filter**]

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                    |
| Step 2 | <b>show running-config</b> [ <b>interface type number</b> ] [ <b>linenum</b> ] [ <b>map-class</b> ]<br><br><b>Example:</b><br>Router# show running-config   begin bgp                                                                                                                                              | Displays the contents of the currently running configuration file.<br><ul style="list-style-type: none"> <li>• The output of this command displays the configuration of the <b>neighbor ttl-security</b> command for each peer under the BGP configuration section. This section includes the neighbor address and the configured hop count.</li> </ul>  |
| Step 3 | <b>show ip bgp neighbors</b> <i>neighbor-address</i> [ <b>advertised-routes</b>   <b>dampened-routes</b>   <b>paths</b> { <i>regular-expression</i> }   <b>policy</b>   <b>received-routes</b>   <b>routes</b>   <b>received prefix-filter</b> ]<br><br><b>Example:</b><br>Router# show ip bgp neighbors 10.1.1.14 | Displays information about the TCP and BGP connections to neighbors.<br><ul style="list-style-type: none"> <li>• The <b>show ip bgp neighbors</b> command displays “External BGP neighbor may be up to <i>number</i> hops away” when this feature is enabled. The <i>number</i> value represents the hop count. It is a number from 1 to 254.</li> </ul> |

# Configuration Examples for the BGP Support for TTL Security Check Feature

The following examples show how to configure and verify this feature:

- [Configuring the TTL-Security Check: Example, page 311](#)
- [Verifying the TTL-Security Check Configuration: Example, page 311](#)

## Configuring the TTL-Security Check: Example

The example configurations in this section show how to configure the BGP Support for TTL Security Check feature.

The following example uses the **trace** command to determine the hop count to an eBGP peer. The hop count number is displayed in the output for each networking device that IP packets traverse to reach the specified neighbor. In the example below, the hop count for the 10.1.1.1 neighbor is 1.

```
Router# trace ip 10.1.1.1
```

```
Type escape sequence to abort.  
Tracing the route to 10.1.1.1
```

```
  1 10.1.1.1 0 msec *  0 msec
```

The following example sets the hop count to 2 for the 10.1.1.1 neighbor. Because the *hop-count* argument is set to 2, BGP will only accept IP packets with a TTL count in the header that is equal to or greater than 253.

```
Router(config-router)# neighbor 10.1.1.1 ttl-security hops 2
```

## Verifying the TTL-Security Check Configuration: Example

The configuration of the BGP Support for TTL Security Check feature can be verified with the **show running-config** and **show ip bgp neighbors** commands. This feature is configured locally on each peer, so there is no remote configuration to verify.

The following is sample output from the **show running-config** command. The output shows that neighbor 10.1.1.1 is configured to establish or maintain the peering session only if the expected TTL count in the incoming IP packet is 253 or 254.

```
Router# show running-config | begin bgp  
router bgp 65000  
  no synchronization  
  bgp log-neighbor-changes  
  neighbor 10.1.1.1 remote-as 55000  
  neighbor 10.1.1.1 ttl-security hops 2  
  no auto-summary  
.  
.  
.
```

The following is sample output from the **show ip bgp neighbors** command. The output shows that the local router will accept packets from the 10.1.1.1 neighbor if it is no more than 2 hops away. The configuration of this feature is displayed in the address family section of the output. The relevant line is bolded in the output.

```
Router# show ip bgp neighbors 10.1.1.1

BGP neighbor is 10.1.1.1, remote AS 55000, external link
  BGP version 4, remote router ID 10.2.2.22
  BGP state = Established, up for 00:59:21
  Last read 00:00:21, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

      Sent      Rcvd
Opens:           2         2
Notifications:   0         0
Updates:         0         0
Keepalives:     226       227
Route Refresh:   0         0
Total:          228       229
Default minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1/0
  Output queue sizes : 0 self, 0 replicated
  Index 1, Offset 0, Mask 0x2
  Member of update-group 1

      Sent      Rcvd
Prefix activity: ----
Prefixes Current:    0         0
Prefixes Total:      0         0
Implicit Withdraw:   0         0
Explicit Withdraw:   0         0
Used as bestpath:    n/a        0
Used as multipath:    n/a        0

      Outbound   Inbound
Local Policy Denied Prefixes: -----
Total:                0         0
Number of NLRI in the update sent: max 0, min 0

Connections established 2; dropped 1
Last reset 00:59:50, due to User reset
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.2.2.22, Local port: 179
Foreign host: 10.1.1.1, Foreign port: 11001

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xCC28EC):
Timer      Starts    Wakeups      Next
Retrans      63         0          0x0
TimeWait      0         0          0x0
AckHold      62        50          0x0
SendWnd       0         0          0x0
KeepAlive     0         0          0x0
GiveUp        0         0          0x0
PmtuAger      0         0          0x0
DeadWait      0         0          0x0
```

```

iss: 712702676  snduna: 712703881  sndnxt: 712703881      sndwnd: 15180
irs: 2255946817  rcvnxt: 2255948041  rcvwnd: 15161  delrcvwnd: 1223

```

```

SRTT: 300 ms, RTTO: 607 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

```

```

Datagrams (max data segment is 1460 bytes):
Rcvd: 76 (out of order: 0), with data: 63, total data bytes: 1223
Sent: 113 (retransmit: 0, fastretransmit: 0), with data: 62, total data bytes: 4

```

## Additional References

The following sections provide references related to the BGP Support For TTL Security Check feature.

## Related Documents

| Related Topic           | Document Title                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands            | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS Release 12.0 Network Protocols Command Reference, Part 1</a></li> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2</a></li> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| BGP configuration tasks | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1</a></li> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.2</a></li> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                                                |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs     | Title                                                |
|----------|------------------------------------------------------|
| RFC 3682 | <i>The Generalized TTL Security Mechanism (GTSM)</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Command

- **neighbor ttl-security**

### Modified Command

- **show ip bgp neighbors**





# BGP Support for Dual AS Configuration for Network AS Migrations

The BGP Support for Dual AS Configuration for Network AS Migrations feature extends the functionality of the BGP Local-AS feature by providing additional autonomous-system path customization configuration options. The configuration of this feature is transparent to customer peering sessions, allowing the provider to merge two autonomous-systems without interrupting customer peering arrangements. Customer peering sessions can later be updated during a maintenance window or during other scheduled downtime.

## Feature History for BGP Support for Dual AS Configuration for Network AS Migrations

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(27)S | This feature was introduced.                                  |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S. |
| 12.3(11)T | This feature was integrated into Cisco IOS Release 12.3(11)T. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Support for Dual AS Configuration for Network AS Migrations, page 316](#)
- [Restrictions for BGP Support for Dual AS Configuration for Network AS Migrations, page 316](#)
- [Information About BGP Support for Dual AS Configuration for Network AS Migrations, page 316](#)
- [How to Configure Autonomous System Migration, page 317](#)
- [Configuration Examples for Autonomous-System Migration, page 321](#)
- [Additional References, page 322](#)
- [Command Reference, page 323](#)

## Prerequisites for BGP Support for Dual AS Configuration for Network AS Migrations

- This document assumes that BGP is configured and eBGP peering sessions have been established.

## Restrictions for BGP Support for Dual AS Configuration for Network AS Migrations

- BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This feature should be configured only for autonomous-system migration, and should be deconfigured after the transition has been completed. This procedure should be attempted only by an experienced network operator, as routing loops can be created with improper configuration.
- This feature can be configured for only true eBGP peering sessions. This feature cannot be configured for two peers in different subautonomous systems of a confederation.
- This feature can be configured for individual peering sessions and configurations applied through peer-groups and peer templates. If this command is applied to a group of peers, the peers cannot be individually customized.

## Information About BGP Support for Dual AS Configuration for Network AS Migrations

Autonomous-system migration can be necessary when a telecommunications or Internet service provider purchases another network. It is desirable for the provider to be able integrate the second autonomous system without disrupting existing customer peering arrangements. The amount of configuration required in the customer networks can make this a cumbersome task that is difficult to complete without disrupting service.

The BGP Support for Dual AS Configuration for Network AS Migrations feature allows you to merge a secondary autonomous system under a primary autonomous system, without disrupting customer peering sessions. The configuration of this feature is transparent to customer networks. This feature allows a router to appear, to external peers, as a member of secondary autonomous system during the autonomous-system migration. This feature allows the network operator to merge the autonomous systems and then later migrate customers to new configurations during normal service windows without disrupting existing peering arrangements.

# How to Configure Autonomous System Migration

This section contains the following procedures:

- [Configuring Dual-AS Peering for Network Migration, page 317](#)
- [Verifying Autonomous System Number Configuration, page 320](#)

## Configuring Dual-AS Peering for Network Migration

The **neighbor local-as** command is used to customize the AS\_PATH attribute by adding and removing autonomous system numbers for routes received from eBGP neighbors. This feature allows a router to appear to external peers as a member of another autonomous system for the purpose of autonomous system number migration. This feature simplifies this process of changing the autonomous-system number in a BGP network by allowing the network operator to merge a secondary autonomous system into a primary autonomous system and then later update the customer configurations during normal service windows without disrupting existing peering arrangements.

## Confederations, Individual Peering Sessions and Peer Groupings are Supported

This feature supports confederations, individual peering sessions and configurations applied through peer-groups and peer templates. If this feature is applied to a group peers, the individual peers cannot be customized.

## Ingress Filtering can be Applied to Minimize the Possibility of Routing Loop Creation

Autonomous-system path customization increases the possibility that routing loops can be created if misconfigured. The larger the number of customer peerings, the greater the risk. You can minimize this possibility by applying policies on the ingress interfaces to block the autonomous-system number that is in transition or routes that have no **local-as** configuration.



### Caution

BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This feature should be configured only for autonomous-system migration, and should be deconfigured after the transition has been completed. This procedure should be attempted only by an experienced network operator, as routing loops can be created with improper configuration.

## Restrictions

- This feature can be configured for only true eBGP peering sessions. This feature cannot be configured for two peers in different subautonomous systems of a confederation.
- This feature can be configured for individual peering sessions and configurations applied through peer-groups and peer templates. If this command is applied to a group of peers, the peers cannot be individually customized.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **router bgp** *as-number*
4. **neighbor** *ip-address* **remote-as** *as-number*
5. **neighbor** *ip-address* **local-as** [*as-number* [**no-prepend** [**replace-as** [**dual-as**]]]
6. **neighbor** *ip-address* **remove-private-as**
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                                                                              | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remote-as 200                                                                                  | Establishes a peering session with a BGP neighbor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 5 | <b>neighbor</b> <i>ip-address</i> <b>local-as</b> [ <i>as-number</i> [ <b>no-prepend</b> [ <b>replace-as</b> [ <b>dual-as</b> ]]]]<br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>local-as 300 replace-as dual-as | Customizes the AS_PATH attribute for routes received from an eBGP neighbor. <ul style="list-style-type: none"> <li>The <b>replace-as</b> keyword is used to prepend only the local autonomous-system number (as configured with the <i>ip-address</i> argument) to the AS_PATH attribute. The autonomous-system number from the local BGP routing process is not prepended.</li> <li>The <b>dual-as</b> keyword is used to configure the eBGP neighbor to establish a peering session using the real autonomous-system number (from the local BGP routing process) or by using the autonomous-system number configured with the <i>ip-address</i> argument (local-as).</li> <li>The example configures the peering session with the 10.0.0.1 neighbor to accept the real autonomous system number and the local-as number.</li> </ul> |

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>neighbor <i>ip-address</i> remove-private-as</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remove-private-as | (Optional) Removes private autonomous-system numbers from outbound routing updates. <ul style="list-style-type: none"> <li>This command can be used with the <b>replace-as</b> functionality to remove the private autonomous-system number and replace it with an external autonomous system number.</li> <li>Private autonomous-system numbers (64512 to 65535) are automatically removed from the AS_PATH attribute when this command is configured.</li> </ul> |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                             | Exits router configuration mode, and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                  |

## Verifying Autonomous System Number Configuration

The **show ip bgp** and **show ip bgp neighbors EXEC** commands can be used to verify autonomous system number for entries in the routing table and the status of this feature.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp** [**network**] [*network-mask*] [*longer-prefixes*] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]
3. **show ip bgp neighbors** [*neighbor-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regex* | **dampened-routes** | **received** *prefix-filter*]

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                        |
| Step 2 | <b>show ip bgp</b> [ <b>network</b> ] [ <i>network-mask</i> ] [ <i>longer-prefixes</i> ] [ <b>prefix-list</b> <i>prefix-list-name</i>   <b>route-map</b> <i>route-map-name</i> ] [ <b>shorter prefixes</b> <i>mask-length</i> ]<br><br><b>Example:</b><br>Router# show ip bgp              | Displays entries in the BGP routing table. <ul style="list-style-type: none"> <li>• The output can be used to verify if the real autonomous system number or local-as number is configured.</li> </ul>                                                                                                    |
| Step 3 | <b>show ip bgp neighbors</b> [ <i>neighbor-address</i> ] [ <b>received-routes</b>   <b>routes</b>   <b>advertised-routes</b>   <b>paths</b> <i>regex</i>   <b>dampened-routes</b>   <b>received</b> <i>prefix-filter</i> ]<br><br><b>Example:</b><br>Router(config)# show ip bgp neighbors | Displays information about TCP and BGP connections to neighbors. <ul style="list-style-type: none"> <li>• The output will display <b>local AS</b>, <b>no-prepend</b>, <b>replace-as</b>, and <b>dual-as</b> with the corresponding autonomous system number when these options are configured.</li> </ul> |

# Configuration Examples for Autonomous-System Migration

The following examples show how to configure and verify this feature:

- [Dual-AS Configuration: Example, page 321](#)
- [Dual-AS Confederation Configuration: Example, page 322](#)
- [Replace-AS Configuration: Example, page 322](#)

## Dual-AS Configuration: Example

The following examples shows how this feature is used to merge two autonomous systems without interrupting peering arrangements with the customer network. The **neighbor local-as** command is configured to allow Router1 to maintain peering sessions through autonomous-system 100 and autonomous-system 200. Router2 is a customer router that runs a BGP routing process in autonomous system 300 and is configured to peer with autonomous-system 200:

### Autonomous System 100 (provider network):

```
Router1(config)# interface Serial3/0
Router1(config-int)# ip address 10.3.3.11 255.255.255.0
Router1(config-int)# !
Router1(config)# router bgp 100
Router1(config-router)# no synchronization
Router1(config-router)# bgp router-id 100.0.0.11
Router1(config-router)# neighbor 10.3.3.33 remote-as 300
Router1(config-router)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

### Autonomous System 200 (provider network):

```
Router1(config)# interface Serial3/0
Router1(config-int)# ip address 10.3.3.11 255.255.255.0
Router1(config-int)# !
Router1(config)# router bgp 200
Router1(config-router)# bgp router-id 100.0.0.11
Router1(config-router)# neighbor 10.3.3.33 remote-as 300
```

### Autonomous System 300 (customer network):

```
Router2(config)# interface Serial3/0
Router2(config-int)# ip address 10.3.3.33 255.255.255.0
Router2(config-int)# !
Router2(config)# router bgp 300
Router2(config-router)# bgp router-id 100.0.0.3
Router2(config-router)# neighbor 10.3.3.11 remote-as 200
```

After the transition is complete, the configuration on router 3 can be updated to peer with autonomous-system 100 during a normal maintenance window or during other scheduled downtime.

```
Router2(config-router)# neighbor 10.3.3.11 remote-as 100
```

## Dual-AS Confederation Configuration: Example

The following example can be used in place of the Router 1 configuration in the previous example. The only difference between these configurations is that Router 1 is configured to be part of a confederation.

```
Router1(config)# interface Serial13/0
Router1(config-int)# ip address 10.3.3.11 255.255.255.0
Router1(config-int)# !
Router1(config)# router bgp 65534
Router1(config-router)# no synchronization
Router1(config-router)# bgp confederation identifier 100
Router1(config-router)# bgp router-id 100.0.0.11
Router1(config-router)# neighbor 10.3.3.33 remote-as 300
Router1(config-router)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

## Replace-AS Configuration: Example

The following example strips private autonomous-system 64512 from outbound routing updates for the 10.3.3.33 neighbor and replaces it with autonomous-system 300:

```
Router(config)# router bgp 64512
Router(config-router)# neighbor 10.3.3.33 local-as 300 no-prepend replace-as
```

## Additional References

The following sections provide references related to the BGP Support for Dual AS Configuration for Network AS Migrations feature.

## Related Documents

| Related Topic                            | Document Title                                                                                                                                    |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands                             | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| BGP configuration tasks                  | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                  |
| BGP Hide Local-Autonomous System feature | <ul style="list-style-type: none"> <li><a href="#">BGP Hide Local-Autonomous System</a></li> </ul>                                                |
| BGP Local-AS feature                     | <ul style="list-style-type: none"> <li><a href="#">Configuring the BGP Local-AS Feature (</a></li> </ul>                                          |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |



## MIBs

| MIBs                                                                                                                                  | MIBs Link |
|---------------------------------------------------------------------------------------------------------------------------------------|-----------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —         |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **neighbor local-as**





# BGP Support for IP Prefix Import from Global Table into a VRF Table

The BGP Support for IP Prefix Import from Global Table into a VRF Table feature introduces the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding instance (VRF) table using an import route map.

## Feature History for the BGP Support for IP Prefix Import from Global Table into a VRF Table feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(29)S | This feature was introduced.                                  |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S. |
| 12.3(14)T | This feature was integrated into Cisco IOS Release 12.3(14)T. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Support for IP Prefix Import from Global Table into a VRF Table, page 326](#)
- [Restrictions for BGP Support for IP Prefix Import from Global Table into a VRF Table, page 326](#)
- [Information About BGP Support for IP Prefix Import from Global Table into a VRF Table, page 326](#)
- [How to Import IP Prefixes from Global Table into a VRF Table, page 327](#)
- [Configuration Examples for Importing IP Prefixes from the Global Table into a VRF Table, page 334](#)
- [Additional References, page 335](#)
- [Command Reference, page 337](#)

## Prerequisites for BGP Support for IP Prefix Import from Global Table into a VRF Table

- Border Gateway Protocol peering sessions are established.
- CEF or dCEF (for distributed platforms) is enabled on all participating routers.

## Restrictions for BGP Support for IP Prefix Import from Global Table into a VRF Table

- Only IPv4 unicast and multicast prefixes can be imported to a VRF with this feature.
- A maximum of 5 VRF instances per router can be created to import IPv4 prefixes from the global routing table.
- IPv4 prefixes imported into a VRF, using this feature, cannot be imported into a VPNv4 VRF.

## Information About BGP Support for IP Prefix Import from Global Table into a VRF Table

- [Importing IPv4 Prefixes into a VRF, page 326](#)
- [Black Hole Routing, page 327](#)
- [Classifying Global Traffic, page 327](#)

## Importing IPv4 Prefixes into a VRF

The BGP Support for IP Prefix Import from Global Table into a VRF Table feature introduces the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding instance (VRF) table using an import map. This feature extends the functionality of VRF import-map configuration to allow IPv4 prefixes to be imported into a VRF based on a standard community. Both IPv4 unicast and multicast prefixes are supported. No Multiprotocol Label Switching (MPLS) or route target (import/export) configuration is required.

IP prefixes are defined as match criteria for the import map through standard Cisco IOS filtering mechanisms. For example, an IP access-list, an IP prefix-list, or an IP as-path filter is created to define an IP prefix or IP prefix range, and then the prefix or prefixes are processed through a match clause in a route map. Prefixes that pass through the route map are imported into the specified VRF per the import map configuration.

## Black Hole Routing

This feature can be configured to support Black Hole Routing (BHR). BHR is method that allows the administrator to block undesirable traffic, such as traffic from illegal sources or traffic generated by a Denial of Service (DoS) attack, by dynamically routing the traffic to a dead interface or to a host designed to collect information for investigation, mitigating the impact of the attack on the network. Prefixes are looked up, and packets that come from unauthorized sources are blackholed by the ASIC at line rate.

## Classifying Global Traffic

This feature can be used to classify global IP traffic based on physical location or class of service. Traffic is classified based on administration policy and then imported into different VRFs. On a college campus, for example, network traffic could be divided into an academic network and residence network traffic, a student network and faculty network, or a dedicated network for multicast traffic. After the traffic is divided along administration policy, routing decisions can be configured with the *MPLS VPN—VRF Selection using Policy Based Routing* or the *MPLS VPN—VRF Selection Based on Source IP address* features.

## How to Import IP Prefixes from Global Table into a VRF Table

This section contains the following tasks:

- [Defining IPv4 IP Prefixes to Import, page 327](#)
- [Creating the VRF and the Import Route Map, page 328](#)
- [Filtering on the Ingress Interface, page 331](#)
- [Verifying Global IP Prefix Import, page 332](#)

## Defining IPv4 IP Prefixes to Import

IPv4 unicast or multicast prefixes are defined as match criteria for the import route map using standard Cisco IOS filtering mechanisms. This task uses an IP access-list and an IP prefix-list.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* { **deny** | **permit** } *source* [*source-wildcard*] [**log**]
4. **ip prefix-list** *prefix-list-name* [**seq** *seq-value*] { **deny** *network/length* | **permit** *network/length* } [**ge** *ge-value*] [**le** *le-value*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                             |
| Step 3 | <b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } <i>source</i> [ <i>source-wildcard</i> ] [ <b>log</b> ]<br><br><b>Example:</b><br>Router(config)# access-list 50 permit 10.1.1.0 0.0.0.255 permit                                                                                | Creates an access list and defines a range of IP prefixes to import into the VRF table. <ul style="list-style-type: none"> <li>The example creates a standard access list numbered 50. This filter will permit traffic from any host with an IP address in the 10.1.1.0/24 subnet.</li> </ul> |
| Step 4 | <b>ip prefix-list</b> <i>prefix-list-name</i> [ <b>seq</b> <i>seq-value</i> ] { <b>deny</b> <i>network/length</i>   <b>permit</b> <i>network/length</i> } [ <b>ge</b> <i>ge-value</i> ] [ <b>le</b> <i>le-value</i> ]<br><br><b>Example:</b><br>Router(config)# ip prefix-list COLORADO permit 10.24.240.0/22 | Creates a prefix-list and defines a range of IP prefixes to import into the VRF table. <ul style="list-style-type: none"> <li>The example creates an IP prefix list named COLORADO. This filter will permit traffic from any host with an IP address in the 10.24.240.0/24 subnet.</li> </ul> |

## What to Do Next

Proceed to the next task to create the VRF and configure the import route map.

## Creating the VRF and the Import Route Map

The IP prefixes that are defined for import are then processed through a match clause in a route map. IP Prefixes that pass through the route map are imported into the VRF. A maximum of 5 VRFs per router can be configured to import IPv4 prefixes from the global routing table. 1000 prefixes per VRF are imported by default. You can manually configure from 1 to 2147483647 prefixes for each VRF. We recommend that you use caution if you manually configure the prefix import limit. Configuring the router to import too many prefixes can interrupt normal router operation.

## MPLS and Route Target Configuration is not Required

No MPLS or route target (import/export) configuration is required.

## Import Actions

Import actions are triggered when a new routing update is received or when routes are withdrawn. During the initial BGP update period, the import action is postponed to allow BGP to converge more quickly. Once BGP converges, incremental BGP updates are evaluated immediately and qualified prefixes are imported as they are received.

## New Syslog Message

The following syslog message is introduced by this feature. It will be displayed when more prefixes are available for import than the user-defined limit:

```
00:00:33: %BGP-3-AFIMPORT_EXCEED: IPv4 Multicast prefixes imported to multicast vrf exceed the limit 2
```

You can either increase the prefix limit or fine tune the import route map filter to reduce the number of candidate routes.

## Restrictions

- Only IPv4 unicast and multicast prefixes can be imported to a VRF with this feature.
- A maximum of 5 VRF instances per router can be created to import IPv4 prefixes from the global routing table.
- IPv4 prefixes imported into a VRF using this feature cannot be imported into a VPNv4 VRF.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd *route-distinguisher***
5. **import ipv4 unicast | multicast [*prefix-limit*] map *route-map***
6. **exit**
7. **route-map *map-tag* [permit | deny] [*sequence-number*]**
8. **match ip address {*acl-number* [*acl-number* ...] *acl-name* ...] | *acl-name* [*acl-name* ...] *acl-number* ...] | prefix-list *prefix-list-name* [*prefix-list-name* ...]}**
9. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>ip vrf vrf-name</b><br><br><b>Example:</b><br>Router(config)# ip vrf GREEN                                                                                       | Creates a VRF routing table and specifies the VRF name (or tag). <ul style="list-style-type: none"> <li>The <b>ip vrf vrf-name</b> command creates a VRF routing table and a CEF table, and both are named using the <i>vrf-name</i> argument. Associated with these tables is the default route distinguisher value.</li> </ul>                                                                                                                                                                                                                                                                          |
| Step 4 | <b>rd route-distinguisher</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:10                                                                               | Creates routing and forwarding tables for the VRF instance. <ul style="list-style-type: none"> <li>There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).</li> </ul>                                                                                                                                                                                                                                     |
| Step 5 | <b>import ipv4 unicast   multicast [prefix-limit]</b><br><b>map route-map</b><br><br><b>Example:</b><br>Router(config-vrf)# import ipv4 unicast 1000<br>map UNICAST | Creates an import map to import IPv4 prefixes from the global routing table to a VRF table. <ul style="list-style-type: none"> <li>Unicast or multicast prefixes are specified.</li> <li>Up to a 1000 prefixes will be imported by default. The <i>prefix-limit</i> argument is used to specify a limit from 1 to 2147483647 prefixes.</li> <li>The route-map that defines the prefixes to import is specified after the <b>map</b> keyword is entered.</li> <li>The example creates an import map that will import up to 1000 unicast prefixes that pass through the route map named UNICAST.</li> </ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# exit                                                                                                      | Exits VRF configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>route-map map-tag [permit   deny]</b><br>[sequence-number]<br><br><b>Example:</b><br>Router(config)# route-map UNICAST permit 10                                 | Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. <ul style="list-style-type: none"> <li>The route-map name must match the route map specified in Step 5.</li> <li>The example creates a route-map named UNICAST.</li> </ul>                                                                                                                                                                                                                                                                                                            |



|        | Command or Action                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <pre><b>match ip address</b> {<i>acl-number</i> [<i>acl-number</i> ...   <i>acl-name</i> ...]   <i>acl-name</i> [<i>acl-name</i> ...   <i>acl-number</i> ...]   <b>prefix-list</b> <i>prefix-list-name</i> [<i>prefix-list-name</i> ...]}</pre> <p><b>Example:</b><br/>Router(config-route-map)# match ip address 50</p> | <p>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on matched packets.</p> <ul style="list-style-type: none"> <li>Both IP access-lists and IP prefix-lists are supported.</li> <li>The example configures the route map to use standard access list 50 to define match criteria.</li> </ul> |
| Step 9 | <pre><b>exit</b></pre> <p><b>Example:</b><br/>Router(config-route-map)# exit</p>                                                                                                                                                                                                                                         | <p>Exits route-map configuration mode, and enters global configuration mode.</p>                                                                                                                                                                                                                                                                                                                       |

## What to Do Next

Proceed to the next section to configure filtering on ingress interface.

## Filtering on the Ingress Interface

This feature can be configured globally or on a per interface basis. We recommend that you apply it to ingress interfaces to maximize performance.

## Unicast Reverse Path Forwarding

Unicast Reverse Path Forwarding (Unicast RPF) can be optionally configured. Unicast RPF is used to verify that the source address is in the Forwarding Information Base (FIB). The **ip verify unicast vrf** command is configured in interface configuration mode and is enabled for each VRF. This command has **permit** and **deny** keywords that are used to determine if the traffic is forwarded or dropped.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip policy route-map** *map-tag*
5. **ip verify unicast vrf** *vrf-name* **deny** | **permit**
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                        | Purpose                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                           | Enters global configuration mode.                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>type number</i> [ <i>name-tag</i> ]<br><br><b>Example:</b><br>Router(config)# interface Ethernet 0                                   | Configures an interface and enters interface configuration mode.                                                                                                                                                                                        |
| Step 4 | <b>ip policy route-map</b> <i>type number</i> [ <i>name-tag</i> ]<br><br><b>Example:</b><br>Router(config-if)# ip policy route-map UNICAST               | Identifies a route map to use for policy routing on an interface.<br><ul style="list-style-type: none"><li>The configuration example attaches the route map named UNICAST to the interface.</li></ul>                                                   |
| Step 5 | <b>ip verify unicast vrf</b> <i>vrf-name</i> <b>deny</b>   <b>permit</b><br><br><b>Example:</b><br>Router(config-if)# ip verify unicast vrf GREEN permit | (Optional) Enables Unicast Reverse Path Forwarding verification for the specified VRF.<br><ul style="list-style-type: none"><li>The example enables verification for the VRF named GREEN. Traffic that passes verification will be forwarded.</li></ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                              | Exits interface configuration mode and enters privileged EXEC mode.                                                                                                                                                                                     |

## What to Do Next

Proceed to the next section to see a list of commands that can be used for verification.

## Verifying Global IP Prefix Import

The **show** commands described in this section can be used to display information about the VRFs that are configured with this feature and to verify that global IP prefixes are imported into the specified VRF table.

## SUMMARY STEPS

- enable**
- show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**] [**prefix-list** *prefix-list-name* | **route-map** *route-map-name*] [**shorter prefixes** *mask-length*]

3. `show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [rib-failure] [ip-prefix/length [longer-prefixes] [network-address [mask] [longer-prefixes] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]`
4. `show ip vrf [brief | detail | interfaces | id] [vrf-name]`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                  |
| Step 2 | <b>show ip bgp</b> [network] [network-mask] [longer-prefixes] [prefix-list prefix-list-name] [route-map route-map-name] [shorter prefixes mask-length]<br><br><b>Example:</b><br>Router# show ip bgp                                                                                                                                                                                                                      | Displays entries in the BGP routing table.                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>show ip bgp vpnv4</b> {all   rd route-distinguisher   vrf vrf-name} [rib-failure] [ip-prefix/length [longer-prefixes]] [network-address [mask] [longer-prefixes]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]<br><br><b>Example:</b><br>Router# show ip bgp vpn vrf | Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>The output displays the import route map, the traffic type (unicast or multicast), the default or user-defined prefix import limit, the actual number of prefixes that are imported, and individual import prefix entries.</li> </ul> |
| Step 4 | <b>show ip vrf</b> [brief   detail   interfaces   id] [vrf-name]<br><br><b>Example:</b><br>Router# show ip vrf detail                                                                                                                                                                                                                                                                                                     | Displays defined VRFs and their associated interfaces. <ul style="list-style-type: none"> <li>The output displays the import route map, the traffic type (unicast or multicast), and the default or user-defined prefix import limit.</li> </ul>                                                                                  |

# Configuration Examples for Importing IP Prefixes from the Global Table into a VRF Table

The following examples show how to configure this feature:

- [Configuring Global IP Prefix Import: Example, page 334](#)
- [Verifying Global IP Prefix Import: Example, page 334](#)

## Configuring Global IP Prefix Import: Example

The following example, beginning in global configuration mode, imports all unicast prefixes from the 10.24.240.0/22 subnet into the VRF named GREEN. An IP prefix list is used to define the imported IPv4 prefixes. The route map is attached to the Ethernet 0 interface. Unicast RPF verification for VRF GREEN is enabled.

```
ip prefix-list COLORADO permit 10.24.240.0/22
!
ip vrf GREEN
  rd 100:10
  import ipv4 unicast 1000 map UNICAST
exit
route-map UNICAST permit 10
  match ip address prefix-list COLORADO
exit
interface Ethernet 0
  ip policy route-map UNICAST
  ip verify unicast vrf GREEN permit
end
```

## Verifying Global IP Prefix Import: Example

The **show ip vrf** command or the **show ip bgp vpnv4** command can be used to verify that prefixes are imported from the global routing table to the VRF table.

The following example from the **show ip vrf** command shows the import route map named UNICAST is importing IPv4 unicast prefixes and the prefix import limit is 1000:

```
Router# show ip vrf detail

VRF academic; default RD 100:10; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:10
  Import VPN route-target communities
    RT:100:10
  Import route-map for ipv4 unicast: UNICAST (prefix limit: 1000)

  No export route-map
```

The following example from the **show ip bgp vpv4** command shows the import route map names, the prefix import limit and the actual number of imported prefixes, and the individual import entries:

```
Router# show ip bgp vpv4 all

BGP table version is 15, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf academic)
Import Map: ACADEMIC, Address-Family: IPv4 Unicast, Pfx Count/Limit: 6/1000
*> 10.50.1.0/24        2.2.2.2                      0 2 3 ?
*> 10.50.2.0/24        2.2.2.2                      0 2 3 ?
*> 10.50.3.0/24        2.2.2.2                      0 2 3 ?
*> 10.60.1.0/24        2.2.2.2                      0 2 3 ?
*> 10.60.2.0/24        2.2.2.2                      0 2 3 ?
*> 10.60.3.0/24        2.2.2.2                      0 2 3 ?
Route Distinguisher: 200:1 (default for vrf residence)
Import Map: RESIDENCE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.30.1.0/24        2.2.2.2                      0      0 2 i
*> 10.30.2.0/24        2.2.2.2                      0      0 2 i
*> 10.30.3.0/24        2.2.2.2                      0      0 2 i
Route Distinguisher: 300:1 (default for vrf BLACKHOLE)
Import Map: BLACKHOLE, Address-Family: IPv4 Unicast, Pfx Count/Limit: 3/1000
*> 10.40.1.0/24        2.2.2.2                      0      0 2 i
*> 10.40.2.0/24        2.2.2.2                      0      0 2 i
*> 10.40.3.0/24        2.2.2.2                      0      0 2 i
Route Distinguisher: 400:1 (default for vrf multicast)
Import Map: MCAST, Address-Family: IPv4 Multicast, Pfx Count/Limit: 2/2
*> 10.70.1.0/24        2.2.2.2                      0      0 2 i
*> 10.70.2.0/24        2.2.2.2                      0      0 2 i
```

## Additional References

The following sections provide references related to the BGP Support for IP Prefix Import from Global Table into a VRF Table feature.

## Related Documents

| Related Topic                            | Document Title                                                                                                                                    |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands                             | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| BGP configuration tasks                  | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                  |
| BGP commands                             | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| MPLS VPN configuration tasks             | <ul style="list-style-type: none"> <li><a href="#">MPLS Virtual Private Networks, Cisco IOS Release 12.0(5)T</a></li> </ul>                       |
| VRF Selection using Policy Based Routing | <ul style="list-style-type: none"> <li><a href="#">MPLS VPN—VRF Selection using Policy Based Routing</a></li> </ul>                               |
| VRF Selection Based on Source IP Address | <ul style="list-style-type: none"> <li><a href="#">MPLS VPN—VRF Selection Based on Source IP Address</a></li> </ul>                               |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

# Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **import ipv4**
- **ip verify unicast vrf**
- **debug ip bgp import**







# BGP Support for Fast Peering Session Deactivation

The BGP Support for Fast Peering Session Deactivation feature introduces an event driven notification system that allows a Border Gateway Protocol (BGP) process to monitor BGP peering sessions on a per-neighbor basis. This feature improves the response time of BGP to adjacency changes by allowing BGP to detect an adjacency change and deactivate the terminated session in between standard BGP scanning intervals. Enabling this feature improves overall BGP convergence.

## Feature History for the BGP Support for Fast Peering Session Deactivation feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(29)S | This feature was introduced.                                  |
| 12.3(14)T | This feature was integrated into Cisco IOS Release 12.3(14)T. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Support for Next-Hop Address Tracking, page 340](#)
- [Restrictions for BGP Support for Fast Peering Session Deactivation, page 340](#)
- [Information About BGP Support for Fast Peering Session Deactivation, page 340](#)
- [How to Configure Fast Peering Session Deactivation, page 340](#)
- [Configuration Examples for BGP Fast Peering Session Deactivation, page 342](#)
- [Additional References, page 342](#)
- [Command Reference, page 344](#)

## Prerequisites for BGP Support for Next-Hop Address Tracking

- This document assumes that BGP is enabled and peering has been established.

## Restrictions for BGP Support for Fast Peering Session Deactivation

- This feature is not supported under the IPv6 address family.
- A host route must be available for each peering session that is configured to use BGP fast session deactivation. If a route is aggregated or is an unreachable non-host route (through a loopback interface) but still available to the peer, this feature will not be able to track the route and will be unable to close the session.

## Information About BGP Support for Fast Peering Session Deactivation

- [BGP Hold Timer, page 340](#)
- [BGP Fast Peering Session Deactivation, page 340](#)

### BGP Hold Timer

By default, the BGP hold timer is set to run every 180 seconds in Cisco IOS software. This timer value is set as default to protect the BGP routing process from instability that can be introduced by peering sessions with other routing protocols. BGP routers typically carry large routing tables, so frequent session resets are not desirable.

### BGP Fast Peering Session Deactivation

BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. This feature is event driven and configured on a per-neighbor basis. When this feature is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

## How to Configure Fast Peering Session Deactivation

This section contains the following task:

- [Configuring Fast Session Deactivation for a BGP Neighbor, page 341](#)

## Configuring Fast Session Deactivation for a BGP Neighbor

The **neighbor fall-over** command was introduced to support BGP fast session deactivation.

### Aggressively Dampen IGP Routes

Enabling this feature can significantly improve BGP convergence time. However, unstable Interior Gateway Protocol (IGP) peers can still introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpnv4** [**unicast**]
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address* **fall-over**
7. **end**

#### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                              | Enters global configuration mode.                                                                                                                                                                      |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 50000                                                                                                                                                                               | Enters router configuration mode to create or configure a BGP routing process.                                                                                                                         |
| Step 4 | <b>address-family ipv4</b> [ <b>mdt</b>   <b>multicast</b>   <b>tunnel</b>   <b>unicast</b> [ <b>vrf</b> <i>vrf-name</i> ]   <b>vrf</b> <i>vrf-name</i> ]   <b>vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router-af)# address-family ipv4 unicast | Enters address-family configuration mode to configure a BGP address-family session.<br><ul style="list-style-type: none"> <li>• The example creates an IPv4 unicast address family session.</li> </ul> |

|        | Command or Action                                                                                                                                            | Purpose                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>neighbor</b> <i>ip-address</i> <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>remote-as 50000 | Establishes a peering session with a BGP neighbor.                                                                                                                                                 |
| Step 6 | <b>neighbor</b> <i>ip-address</i> <b>fall-over</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>fall-over                                               | Configures the BGP peering to use fast session deactivation. <ul style="list-style-type: none"> <li>BGP will remove all routes learned through this peer if the session is deactivated.</li> </ul> |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                           | Exits router configuration mode, and enters privileged EXEC mode.                                                                                                                                  |

## Configuration Examples for BGP Fast Peering Session Deactivation

The following examples show how to configure and verify this feature:

- [Configuring BGP Fast Peering Session Deactivation: Example, page 342](#)

### Configuring BGP Fast Peering Session Deactivation: Example

In the following example, the BGP routing process is configured to monitor and use fast peering session deactivation for the 10.0.0.1 neighbor session:

```
router bgp 50000
 neighbor 10.0.0.1 remote-as 50000
 neighbor 10.0.0.1 fall-over
end
```

## Where to Go Next

The BGP Support for Next-Hop Address Tracking feature improves the response time of BGP to next-hop changes for routes installed in the RIB, which can also improve overall BGP convergence. For information about BGP next-hop address tracking, see the [BGP Support for Next-Hop Address Tracking](#) feature.

## Additional References

The following sections provide references related to the BGP Support for Fast Peering Session Deactivation feature.

## Related Documents

| Related Topic                             | Document Title                                                                                   |
|-------------------------------------------|--------------------------------------------------------------------------------------------------|
| BGP commands                              | <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a> , Release 12.3T |
| BGP configuration tasks                   | <a href="#">Cisco IOS IP Configuration Guide</a> , Release 12.3                                  |
| BGP Support for Next-Hop Address Tracking | <a href="#">BGP Support for Next-Hop Address Tracking</a>                                        |
| IP Event Dampening                        | <a href="#">IP Event Dampening</a>                                                               |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **neighbor fall-over**



# BGP Support for Next-Hop Address Tracking

The BGP Support for Next-Hop Address Tracking feature introduces an event driven notification system to monitor the status of routes that are installed in the Routing Information Base (RIB) and to report next-hop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the Border Gateway Protocol (BGP) process. This feature improves the overall BGP convergence time by allowing BGP to respond rapidly to next-hop changes for routes installed in the RIB.

## Feature History for the BGP Support for Next-Hop Address Tracking feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(29)S | This feature was introduced.                                  |
| 12.3(14)T | This feature was integrated into Cisco IOS Release 12.3(14)T. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for BGP Support for Next-Hop Address Tracking, page 346](#)
- [Restrictions for BGP Support for Next-Hop Address Tracking, page 346](#)
- [Information About BGP Support for Next-Hop Address Tracking, page 346](#)
- [How to Configure BGP Next-Hop Address Tracking, page 346](#)
- [Configuration Examples for BGP Next-Hop Address Tracking, page 349](#)
- [Additional References, page 350](#)
- [Command Reference, page 351](#)

# Prerequisites for BGP Support for Next-Hop Address Tracking

This document assumes that BGP is enabled and peering has been established.

## Restrictions for BGP Support for Next-Hop Address Tracking

This feature is not supported under the IPv6 address family in Cisco IOS Release 12.0 S.

## Information About BGP Support for Next-Hop Address Tracking

- [Default BGP Scanner Behavior, page 346](#)
- [BGP Support for Next-Hop Address Tracking, page 346](#)

### Default BGP Scanner Behavior

BGP monitors the next hop of installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner is used to poll the RIB for this information every 60 seconds. During the 60 second time period between scan cycles, Interior Gateway Protocol (IGP) instability or other network failures can cause black holes and routing loops to temporarily form.

### BGP Support for Next-Hop Address Tracking

The BGP Support for Next-Hop Address Tracking feature is enabled by default when a supporting Cisco IOS software image is installed. BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to the BGP routing process as they are updated in the RIB. This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a bestpath calculation is run in between BGP scanner cycles, only next-hop changes are tracked and processed.

## How to Configure BGP Next-Hop Address Tracking

The tasks in this section show how configure BGP next-hop address tracking. BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP. For more details about route dampening, see the

- [Disabling BGP Next-Hop Address Tracking, page 347](#)
- [Adjusting the Delay Interval for BGP Next-Hop Address Tracking, page 348](#)
- [Configuration Examples for BGP Next-Hop Address Tracking, page 349](#)



## Disabling BGP Next-Hop Address Tracking

Perform this task to disable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default under the IPv4 and VPNv4 address families. Disabling next hop address tracking may be useful if you the network has unstable IGP peers and route dampening is not resolving the stability issues. To reenale BGP next-hop address tracking, use the **bgp nexthop** command with the **trigger** and **enable** keywords.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp *as-number***
4. **address-family ipv4 [mdt | multicast | tunnel | unicast [*vrf vrf-name*] | vrf *vrf-name*] | vpnv4 [unicast]**
5. **no bgp nexthop trigger enable**
6. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                | Enters global configuration mode.                                                                                                                                                                                                 |
| Step 3 | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 64512                                                                                                                 | Enters router configuration mod to create or configure a BGP routing process.                                                                                                                                                     |
| Step 4 | <b>address-family ipv4 [mdt   multicast   tunnel   unicast [<i>vrf vrf-name</i>]   vrf <i>vrf-name</i>]   vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router-af)# address-family ipv4 unicast | Enter address family configuration mode to configure BGP peers to accept address family-specific configurations.<br><ul style="list-style-type: none"><li>• The example creates an IPv4 unicast address family session.</li></ul> |

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>no bgp nexthop trigger enable</b><br><br><b>Example:</b><br>Router(config-router-af)# no bgp nexthop trigger enable | Disables BGP next-hop address tracking. <ul style="list-style-type: none"> <li>Next-hop address tracking is enabled by default for IPv4 and VPNv4 address family sessions.</li> <li>The example disables next-hop address tracking.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                     | Exits address-family configuration mode, and enters Privileged EXEC mode.                                                                                                                                                                      |

## Adjusting the Delay Interval for BGP Next-Hop Address Tracking

Perform this task to adjust the delay interval between routing table walks for BGP next-hop address tracking.

### Delay Interval Tuning to Match the Interior Gateway Protocol

You can increase the performance of this feature by tuning the delay interval between full routing table walks to match the tuning parameters for the Interior Gateway protocol (IGP). The default delay interval is 5 seconds. This value is optimal for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

### Aggressive IGP Route Dampening

BGP next-hop address tracking significantly improves the response time of BGP to next-hop changes in the RIB. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP neighbor sessions. We recommend that you aggressively dampen unstable IGP peering sessions to reduce the possible impact to BGP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*] | **vpn****v4** [**unicast**]
5. **bgp nexthop trigger delay** *delay-timer*
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 64512                                                                                                         | Enters router configuration mode to create or configure a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                              |
| Step 4 | <b>address-family ipv4 [mdt   multicast   tunnel   unicast [vrf vrf-name]   vrf vrf-name]   vpv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router-af)# address-family ipv4 unicast | Enter address family configuration mode to configure BGP peers to accept address family-specific configurations. <ul style="list-style-type: none"><li>The example creates an IPv4 unicast address family session.</li></ul>                                                                                                                                                                                                                                |
| Step 5 | <b>bgp nexthop trigger delay delay-timer</b><br><br><b>Example:</b><br>Router(config-router-af)# bgp nexthop trigger delay 20                                                                  | Configures the delay interval between routing table walks for next-hop address tracking. <ul style="list-style-type: none"><li>The time period determines how long BGP will wait before starting a full routing table walk after notification is received.</li><li>The value for the <i>delay-timer</i> argument is a number from 1 to 100 seconds. The default value is 5 second.</li><li>The example configures a delay interval of 20 seconds.</li></ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                                             | Exits address-family configuration mode, and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                   |

## Configuration Examples for BGP Next-Hop Address Tracking

The following examples show how to configure and tune this feature:

- [Enabling and Disabling BGP Next-Hop Address Tracking: Example, page 349](#)
- [Adjusting the Delay Interval for BGP Next-Hop Address Tracking: Example, page 350](#)

### Enabling and Disabling BGP Next-Hop Address Tracking: Example

In the following example, next-hop address tracking is disabled under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
  no bgp nexthop trigger enable
```

## Adjusting the Delay Interval for BGP Next-Hop Address Tracking: Example

In the following example, the delay interval for next-hop tracking is configured to occur every 20 seconds under the IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
  bgp nexthop trigger delay 20
```

## Where to Go Next

The BGP Support for Fast Peering Session Deactivation feature can also be configured to improve the response time of BGP to adjacency changes, improving overall BGP convergence. For information about BGP fast session deactivation, see the [BGP Support for Fast Peering Session Deactivation](#) feature.

## Additional References

The following sections provide references related to the BGP Support for Next-Hop Address Tracking feature.

## Related Documents

| Related Topic                                     | Document Title                                                                                   |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------|
| BGP commands                                      | <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a> , Release 12.3T |
| BGP configuration tasks                           | <a href="#">Cisco IOS IP Configuration Guide</a> , Release 12.3                                  |
| BGP Support for Fast Peering Session Deactivation | <a href="#">BGP Support for Fast Peering Session Deactivation</a>                                |
| IP Event Dampening                                | <a href="#">IP Event Dampening</a>                                                               |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | TAC Home Page:<br><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a><br><br>BGP Support Page:<br><a href="http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP">http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Inter networking:BGP</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **bgp nexthop trigger enable**
- **bgp nexthop trigger delay**





# BGP Multicast Inter-AS (IAS) VPN

The BGP Multicast Inter-AS(IAS) VPN feature introduces the IPv4 multicast distribution tree (MDT) subaddress family identifier (SAFI) in Border Gateway Protocol (BGP). The MDT SAFI is a transitive multicast capable connector attribute that is defined as an IPv4 address family in BGP. The MDT SAFI is designed to support inter-autonomous system (inter-AS) Virtual Private Network (VPN) peering sessions.

## Feature History for the BGP Multicast Inter-AS (IAS) VPN feature.

| Release   | Modification                 |
|-----------|------------------------------|
| 12.0(29)S | This feature was introduced. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [How to Configure an MDT Address Family Session in BGP, page 354](#)
- [Configuration Examples for the MDT Address Family, page 357](#)
- [Additional References, page 357](#)
- [Command Reference, page 358](#)

# How to Configure an MDT Address Family Session in BGP

This section contains the following tasks:

- [Configuring the MDT Address Family in BGP, page 354](#)
- [Clearing IPv4 MDT Peering Sessions in BGP, page 355](#)
- [Displaying Information about IPv4 MDT Sessions in BGP, page 356](#)

## Configuring the MDT Address Family in BGP

The **mdt** keyword has been added to the **address-family ipv4** command to configure an MDT address-family session. The MDT address-family session is configured on a Provider Edge (PE) routers to establish VPN peering sessions with Customer Edge (CE) routers and to establish inter-AS multicast VPN peering sessions. The MDT address family must be configured on each participating PE router.

## Supported Policy

The following policy configuration parameters are supported under the MDT SAFI:

- Mandatory attributes and well-known attributes, such as the AS-path, multi-exit discriminator MED, BGP local-pref, and next hop attributes.
- Standard communities, community-lists, and route-maps.

## Prerequisites

Before Inter-AS VPN peering can be established through an MDT address family, MPLS and CEF must be configured in the BGP network and multiprotocol BGP on PE routers that provide VPN services to CE routers.

## Restrictions

The following policy configuration parameters are not supported:

- Route-originator attribute
- Network Layer Reachability Information (NLRI) prefix filtering (prefix-lists, distribute-lists)
- Extended community attributes (route target and site of origin)

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf** *vrf-name*] | **vrf** *vrf-name*]
5. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                         | Purpose                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                            | Enters global configuration mode.                                                                                                                                                                                          |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 65535                                                                                    | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                       |
| Step 4 | <b>address-family ipv4 [mdt   multicast   tunnel   unicast [vrf vrf-name]   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router-af)# address-family ipv4 mdt | Enter address family configuration mode to configure BGP peers to accept address family specific configurations. <ul style="list-style-type: none"> <li>The example creates an IPv4 MDT address family session.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                        | Exits address-family configuration mode and enters privileged EXEC mode.                                                                                                                                                   |

## Clearing IPv4 MDT Peering Sessions in BGP

The **mdt** keyword has been added to the **clear ip bgp ipv4** command to allow you to clear only MDT address-family routing tables.

## SUMMARY STEPS

1. **enable**
2. **clear ip bgp ipv4 mdt dampening [network-address] [network-mask] | flap-statistics {[network-address] [network-mask] | filter-list regexp | regexp} | table-map**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                   |
| Step 2 | <b>clear ip bgp ipv4 mdt dampening</b><br><b>[network-address] [network-mask]  </b><br><b>flap-statistics {[network-address]</b><br><b>[network-mask]   filter-list regexp   regexp}  </b><br><b>table-map</b><br><br><b>Example:</b><br>Router# clear ip bgp ipv4 mdt table-map | Resets multicast discovery tree IPv4 BGP address-family session. <ul style="list-style-type: none"> <li>The example clears the table-map for IPv4 MDT peering sessions.</li> </ul> |

## Displaying Information about IPv4 MDT Sessions in BGP

The **show ip bgp ipv4 mdt** command can be used to display MDT address-family session information.

## SUMMARY STEPS

1. **enable**
2. **show ip bgp ipv4 mdt {\* | all | rd | vrf} | multicast | tunnel | unicast**

## DETAILED STEPS

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                   |
| Step 2 | <b>show ip bgp ipv4 mdt {*   all   rd   vrf}  </b><br><b>multicast   tunnel   unicast</b><br><br><b>Example:</b><br>Router# show ip bgp ipv4 mdt all | Displays entries in the IPv4 BGP routing table. <ul style="list-style-type: none"> <li>The example displays all information about the IPv4 MDT session.</li> </ul> |

# Configuration Examples for the MDT Address Family

The following example shows how to configure and verify this feature:

- [Configuring an IPv4 MDT Address-Family Session: Example, page 357](#)

## Configuring an IPv4 MDT Address-Family Session: Example

The following example creates an IPv4 MDT address family session:

```
Router(config-router-af)# address-family ipv4 mdt
```

## Additional References

The following sections provide references related to the BGP Multicast Inter-AS (IAS) VPN feature.

## Related Documents

| Related Topic                    | Document Title                                                                                                                                    |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP commands                     | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li></ul> |
| BGP configuration tasks          | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li></ul>                                  |
| IP Multicast commands            | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Command Reference, Volume 3 of 4: Multicast, Release 12.3T</a></li></ul>         |
| IP Multicast configuration tasks | <ul style="list-style-type: none"><li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li></ul>                                  |

## Standards

| Standards | Title                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MDT SAFI  | <i>MDT SAFI</i><br><a href="http://www.ietf.org/internet-drafts/draft-nalawade-idr-mdt-safi-01.txt">http://www.ietf.org/internet-drafts/draft-nalawade-idr-mdt-safi-01.txt</a> |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **address-family ipv4 (BGP)**
- **clear ip bgp ipv4 mdt**
- **show ip bgp ipv4**



## **Part 2: EIGRP**







## Configuring EIGRP

---

This chapter describes how to configure Enhanced Interior Gateway Routing Protocol (EIGRP). For a complete description of the EIGRP commands listed in this chapter, refer to the “EIGRP Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Refer to the *Cisco IOS AppleTalk and Novell IPX Configuration Guide* for information on AppleTalk EIGRP or Internetwork Packet Exchange (IPX) EIGRP.

For protocol-independent features that work with EIGRP, see the chapter “Configuring IP Routing Protocol-Independent Features” in this document.

EIGRP is an enhanced version of the IGRP developed by Cisco. EIGRP uses the same distance vector algorithm and distance information as IGRP. However, the convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP.

The convergence technology is based on research conducted at SRI International and employs an algorithm referred to as the Diffusing Update Algorithm (DUAL). This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations. The convergence time with DUAL rivals that of any other existing routing protocol.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

## The Cisco EIGRP Implementation

EIGRP provides the following features:

- Automatic redistribution—IGRP routes can be automatically redistributed into EIGRP, and EIGRP routes can be automatically redistributed into IGRP. If desired, you can turn off redistribution. You can also completely turn off EIGRP and IGRP on the router or on individual interfaces.
- Increased network width—With IP Routing Information Protocol (RIP), the largest possible width of your network is 15 hops. When EIGRP is enabled, the largest possible width is increased to 100 hops, and the metric is large enough to support thousands of hops.

**Note**

Redistribution between EIGRP and IGRP differs from normal redistribution in that the metrics of IGRP routes are compared with the metrics of external EIGRP routes. The rules of normal administrative distances are not followed, and routes with the lowest metric are selected.

EIGRP offers the following features:

- Fast convergence—The DUAL algorithm allows routing information to converge as quickly as any currently available routing protocol.
- Partial updates—EIGRP sends incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. This feature minimizes the bandwidth required for EIGRP packets.
- Less CPU usage than IGRP—This occurs because full update packets need not be processed each time they are received.
- Neighbor discovery mechanism—This is a simple hello mechanism used to learn about neighboring routers. It is protocol-independent.
- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.
- Scaling—EIGRP scales to large networks.

EIGRP has the following four basic components:

- Neighbor discovery of neighbor recovery
- Reliable transport protocol
- DUAL finite state machine
- Protocol-dependent modules

Neighbor discovery of neighbor recovery is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery of neighbor recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can determine that a neighbor is alive and functioning. Once this status is determined, the neighboring routers can exchange routing information.

The reliable transport protocol is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet) it is not necessary to send hello packets reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, which is indicated in the packet. The reliable transport has a provision to send multicast packets quickly when unacknowledged packets are pending. This provision helps to ensure that convergence time remains low in the presence of varying speed links.

The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time required to recompute the route affects the



convergence time. Recomputation is processor-intensive; it is advantageous to avoid unneeded recomputation. When a topology change occurs, DUAL will test for feasible successors. If there are feasible successors, it will use any it finds in order to avoid unnecessary recomputation.

The protocol-dependent modules are responsible for network layer protocol-specific tasks. An example is the EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. Also, EIGRP is responsible for redistributing routes learned by other IP routing protocols.

## EIGRP Configuration Task List

To configure EIGRP, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

- [Enabling EIGRP](#) (Required)
- [Making the Transition from IGRP to EIGRP](#) (Optional)
- [Logging EIGRP Neighbor Adjacency Changes](#) (Optional)
- [Configuring the Percentage of Link Bandwidth Used](#) (Optional)
- [Adjusting the EIGRP Metric Weights](#) (Optional)
- [Applying Offsets to Routing Metrics](#) (Optional)
- [Disabling Route Summarization](#) (Optional)
- [Configuring Summary Aggregate Addresses](#) (Optional)
- [Configuring Floating Summary Routes](#) (Optional)
- [Configuring EIGRP Route Authentication](#) (Optional)
- [Configuring EIGRP Protocol-Independent Parameters](#) (Optional)
- [Configuring EIGRP Stub Routing](#) (Optional)
- [Monitoring and Maintaining EIGRP](#) (Optional)

See the section “[EIGRP Configuration Examples](#)” at the end of this chapter for configuration examples.

## Enabling EIGRP

To create an EIGRP routing process, use the following commands beginning in global configuration mode:

|        | Command                                                      | Purpose                                                                                                                          |
|--------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>router eigrp</b> <i>autonomous-system</i> | Enables an EIGRP routing process in global configuration mode.<br><br>A maximum of 30 EIGRP routing processes can be configured. |
| Step 2 | Router(config-router)# <b>network</b> <i>network-number</i>  | Associates networks with an EIGRP routing process in router configuration mode.                                                  |

EIGRP sends updates to the interfaces in the specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

## Making the Transition from IGRP to EIGRP

If you have routers on your network that are configured for IGRP, and you want to make a transition to routing EIGRP, you must designate transition routers that have both IGRP and EIGRP configured. In these cases, perform the tasks as noted in the previous section, “[Enabling EIGRP](#),” and also see the chapter “Configuring IGRP” in this document. You must use the same autonomous system number in order for routes to be redistributed automatically.

## Logging EIGRP Neighbor Adjacency Changes

You can enable the logging of neighbor adjacency changes to monitor the stability of the routing system and to help you detect problems. By default, adjacency changes are not logged. To enable such logging, use the following command in global configuration mode:

| Command                                           | Purpose                                              |
|---------------------------------------------------|------------------------------------------------------|
| Router(config)# <b>eigrp log-neighbor-changes</b> | Enables logging of EIGRP neighbor adjacency changes. |

## Configuring the Percentage of Link Bandwidth Used

By default, EIGRP packets consume a maximum of 50 percent of the link bandwidth, as configured with the **bandwidth** interface configuration command. You might want to change that value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (it may have been configured to influence route metric calculations).

To configure the percentage of bandwidth that may be used by EIGRP on an interface, use the following command in interface configuration mode:

| Command                                                      | Purpose                                                                           |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Router(config-if)# <b>ip bandwidth-percent eigrp percent</b> | Configures the percentage of bandwidth that may be used by EIGRP on an interface. |

## Adjusting the EIGRP Metric Weights

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. You can use the **eigrp metric weights** command to adjust the default behavior of EIGRP routing and metric computations. For example, this adjustment allows you to tune system behavior to allow for satellite transmission. EIGRP metric defaults have been carefully selected to provide optimal performance in most networks.



### Note

Adjusting EIGRP metric weights can dramatically affect network performance. Because of the complexity of this task, we recommend that you do not change the default values without guidance from an experienced network designer.

To adjust the EIGRP metric weights, use the following command in router configuration mode:

| Command                                                         | Purpose                                                                                                                                                                                                               |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-router)# <b>metric weights</b> tos k1 k2 k3 k4 k5 | Adjusts the EIGRP metric or K value. EIGRP uses the following formula to determine the total metric to the network:<br><br>metric = [K1*bandwidth + (K2*bandwidth)/(256 - load) + K3*delay] * [K5/(reliability + K4)] |

By default, the EIGRP composite metric is a 32-bit quantity that is a sum of the segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. For a network of homogeneous media, this metric reduces to a hop count. For a network of mixed media (FDDI, Ethernet, and serial lines running from 9600 bits per second to T1 rates), the route with the lowest metric reflects the most desirable path to a destination.

## Mismatched K Values

Mismatched K values (EIGRP metrics) can prevent neighbor relationships from being established and can negatively impact network convergence. The following example explains this behavior between two EIGRP peers (ROUTER-A and ROUTER-B).

The following error message is displayed in the console of ROUTER-B because the K values are mismatched:

```
*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1 (Ethernet0/0) is down: K-value mismatch
```

There are two scenarios where this error message can be displayed:

- The two routers are connected on the same link and configured to establish a neighbor relationship. However, each router is configured with different K values.

The following configuration is applied to ROUTER-A. The K values are changed with the **metric weights** command. A value of 2 is entered for the *k1* argument to adjust the bandwidth calculation. The value of 1 is entered for the *k3* argument to adjust the delay calculation.

```
hostname ROUTER-A!
interface serial 0
 ip address 10.1.1.1 255.255.255.0
 exit
router eigrp 100
 network 10.1.1.0 0.0.0.255
 metric weights 0 2 0 1 0 0
```

The following configuration is applied to ROUTER-B. However, the **metric weights** command is not applied and the default K values are used. The default K values are 1, 0, 1, 0, and 0.

```
hostname ROUTER-B!
interface serial 0
 ip address 10.1.1.2 255.255.255.0
 exit
router eigrp 100
 network 10.1.1.0 0.0.0.255
```

The bandwidth calculation is set to 2 on ROUTER-A and set to 1 (by default) on ROUTER-B. This configuration prevents these peers from forming a neighbor relationship.

- The K-value mismatch error message can also be displayed if one of the two peers has transmitted a “goodbye” message, and the receiving router does not support this message. In this case, the receiving router will interpret this message as a K-value mismatch.

## The Goodbye Message

The goodbye message is a feature designed to improve EIGRP network convergence. The goodbye message is broadcast when an EIGRP routing process is shutdown to inform adjacent peers about the impending topology change. This feature allows supporting EIGRP peers to synchronize and recalculate neighbor relationships more efficiently than would occur if the peers discovered the topology change after the hold timer expired.

The goodbye message is supported in Cisco IOS Release 12.3(2), 12.3(3)B, and 12.3(2)T and later releases. The following message is displayed by routers that run a supported release when a goodbye message is received:

```
*Apr 26 13:48:42.523: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1
(Ethernet0/0) is down: Interface Goodbye received
```

A Cisco router that runs a software release that does not support the goodbye message can misinterpret the message as a K-value mismatch and display the following message:

```
*Apr 26 13:48:41.811: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.1.1.1
(Ethernet0/0) is down: K-value mismatch
```



### Note

The receipt of a goodbye message by a nonsupporting peer does not disrupt normal network operation. The nonsupporting peer will terminate session when the hold timer expires. The sending and receiving routers will reconverge normally after the sender reloads.

## Applying Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via EIGRP. An offset list provides a local mechanism for increasing the value of routing metrics. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

| Command                                                                                                                                                                                      | Purpose                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Router(config-router)# <b>offset-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ] { <b>in</b>   <b>out</b> } <i>offset</i> [ <i>interface-type</i> <i>interface-number</i> ] | Applies an offset to routing metrics. |

## Disabling Route Summarization

You can configure EIGRP to perform automatic summarization of subnet routes into network-level routes. For example, you can configure subnet 172.16.1.0 to be advertised as 172.16.0.0 over interfaces that have subnets of 192.168.7.0 configured. Automatic summarization is performed when there are two or more **network** router configuration commands configured for the EIGRP process. By default, this feature is enabled.

To disable automatic summarization, use the following command in router configuration mode:

| Command                                       | Purpose                           |
|-----------------------------------------------|-----------------------------------|
| Router(config-router)# <b>no auto-summary</b> | Disables automatic summarization. |

Route summarization works in conjunction with the **ip summary-address eigrp** interface configuration command, in which additional summarization can be performed. If automatic summarization is in effect, there usually is no need to configure network level summaries using the **ip summary-address eigrp** command.

## Configuring Summary Aggregate Addresses

You can configure a summary aggregate address for a specified interface. If any more specific routes are in the routing table, EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

To configure a summary aggregate address, use the following command in interface configuration mode:

| Command                                                                                               | Purpose                                 |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Router(config-if)# <b>ip summary-address eigrp</b><br><i>autonomous-system-number ip-address mask</i> | Configures a summary aggregate address. |

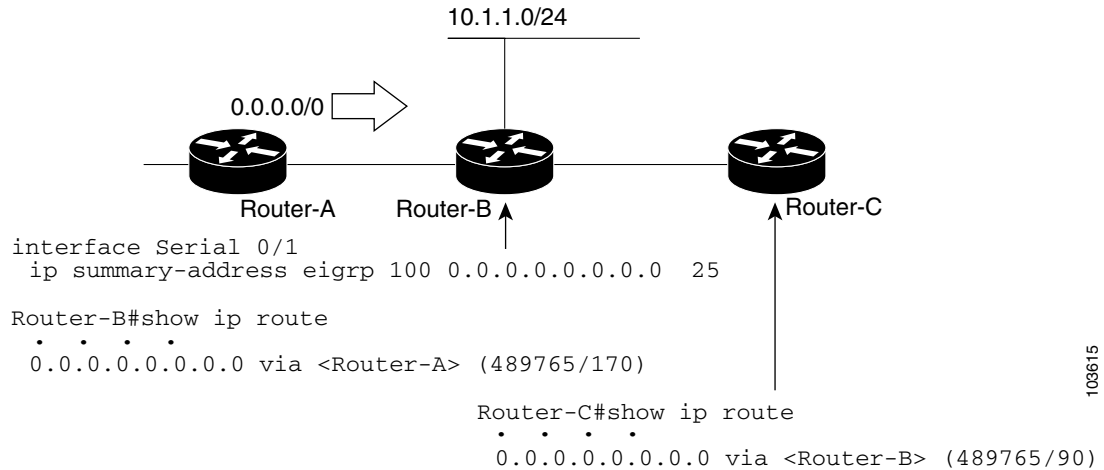
See the “[Route Summarization Example](#)” at the end of this chapter for an example of summarizing aggregate addresses.

## Configuring Floating Summary Routes

You can also use a floating summary route when configuring the **ip summary-address eigrp** command. This enhancement was introduced in Cisco IOS Release 12.2. The floating summary route is created by applying a default route and administrative distance at the interface level. The following scenarios illustrates the behavior of this enhancement.

[Figure 30](#) shows a network with three routers, Router-A, Router-B, and Router-C. Router-A learns a default route from elsewhere in the network and then advertises this route to Router-B. Router-B is configured so that only a default summary route is advertised to Router-C. The default summary route is applied to interface 0/1 on Router-B with the following configuration:

```
Router(config)# interface Serial 0/1  
Router(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
```

**Figure 30 Floating Summary Route Is Applied to Router-B**

The configuration of the default summary route on Router-B sends a 0.0.0.0/0 summary route to Router-C and blocks all other routes, including the 10.1.1.0/24 route, from being advertised to Router-C. However, this also generates a local discard route on Router-B, a route for 0.0.0.0/0 to the null 0 interface with an administrative distance of 5. When this route is created, it overrides the EIGRP learned default route. Router-B will no longer be able to reach destinations that it would normally reach through the 0.0.0.0/0 route.

This problem is resolved by applying a floating summary route to the interface on Router-B that connects to Router-C. The floating summary route is applied by applying an administrative distance to the default summary route on the interface of Router-B with the following statement:

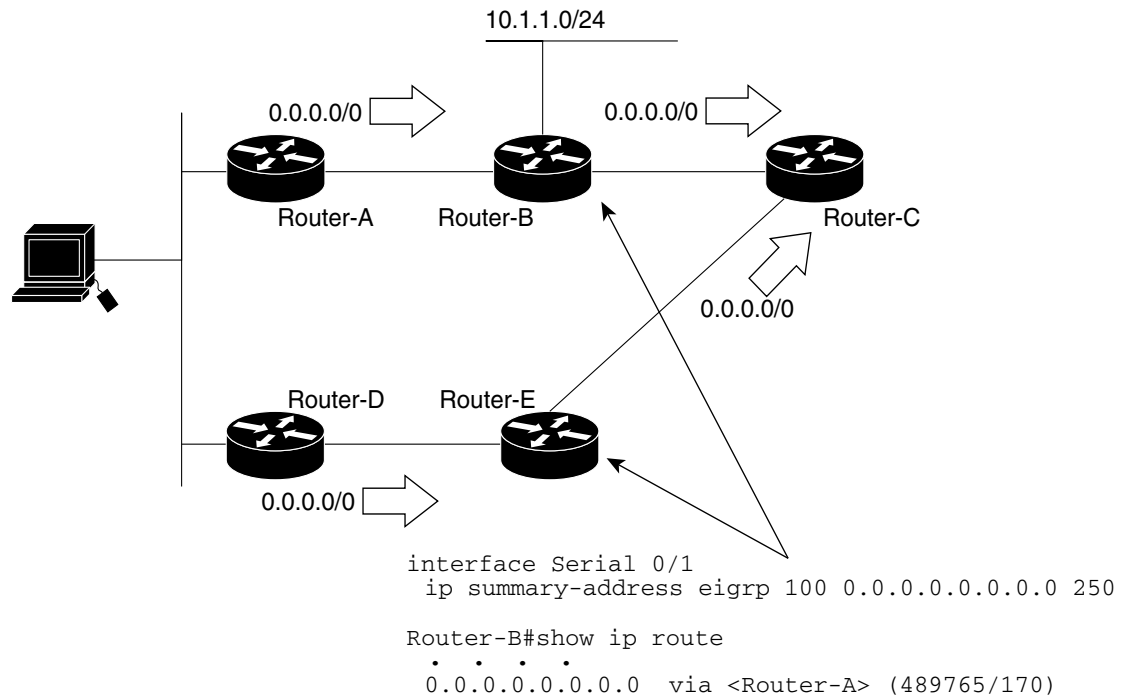
```
Router(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0 250
```

The administrative distance of 250, applied in the above statement, is now assigned to the discard route generated on Router-B. The 0.0.0.0/0, from Router-A, is learned through EIGRP and installed in the local routing table. Routing to Router-C is restored.

If Router-A loses the connection to Router-B, Router-B will continue to advertise a default route to Router-C, which allows traffic to continue to reach destinations attached to Router-B. However, traffic destined to networks to Router-A or behind Router-A will be dropped when it reaches Router-B.

Figure 31 shows a network with two connections from the core, Router-A and Router-D. Both routers have floating summary routes configured on the interfaces connected to Router-C. If the connection between Router-E and Router-C fails, the network will continue to operate normally. All traffic will flow from Router-C through Router-B to the hosts attached to Router-A and Router-D.

**Figure 31 Floating Summary Route Applied for Dual-Homed Remotes**



However, if the link between Router-D and Router-E fails, the network may blackhole traffic because Router-E will continue to advertise the default route(0.0.0.0/0) to Router-C, as long as at least one link, (other than the link to Router-C) to Router-E is still active. In this scenario, Router-C still forwards traffic to Router-E, but Router-E drops the traffic creating the black hole. To avoid this problem, you should configure the summary address with an administrative distance on only single-homed remote routers or areas where there is only one exit point between to segments of the network. If two or more exit points exist (from one segment of the network to another), configuring the floating default route can cause a black hole to be formed.

## Configuring EIGRP Route Authentication

EIGRP route authentication provides Message Digest 5 (MD5) authentication of routing updates from the EIGRP routing protocol. The MD5 keyed digest in each EIGRP packet prevents the introduction of unauthorized or false routing messages from unapproved sources.

Before you can enable EIGRP route authentication, you must enable EIGRP.

To enable authentication of EIGRP packets, use the following commands beginning in interface configuration mode:

|        | Command                                                                      | Purpose                                                            |
|--------|------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> type number                                 | Configure an interface type and enter interface configuration mode |
| Step 2 | Router(config-if)# <b>ip authentication mode eigrp autonomous-system md5</b> | Enables MD5 authentication in EIGRP packets.                       |

|        | Command                                                                                                 | Purpose                                                                    |
|--------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Step 3 | Router(config-if)# <b>ip authentication key-chain eigrp autonomous-system key-chain</b>                 | Enables authentication of EIGRP packets.                                   |
| Step 4 | Router(config-if)# <b>exit</b><br>Router(config)#                                                       | Exits to global configuration mode.                                        |
| Step 5 | Router(config)# <b>key chain name-of-chain</b>                                                          | Identifies a key chain. (Match the name configured in Step 1.)             |
| Step 6 | Router(config-keychain)# <b>key number</b>                                                              | In keychain configuration mode, identifies the key number.                 |
| Step 7 | Router(config-keychain-key)# <b>key-string text</b>                                                     | In keychain key configuration mode, identifies the key string.             |
| Step 8 | Router(config-keychain-key)# <b>accept-lifetime start-time {infinite   end-time   duration seconds}</b> | Optionally specifies the time period during which the key can be received. |
| Step 9 | Router(config-keychain-key)# <b>send-lifetime start-time {infinite   end-time   duration seconds}</b>   | Optionally specifies the time period during which the key can be sent.     |

Each key has its own key identifier (specified with the **key number** key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and MD5 authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. Note that the router needs to know the time. Refer to the Network Time Protocol (NTP) and calendar commands in the “Performing Basic System Management” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For an example of route authentication, see the section “[Route Authentication Example](#)” at the end of this chapter.

## Configuring EIGRP Protocol-Independent Parameters

EIGRP works with AppleTalk, IP, and IPX. The bulk of this chapter describes EIGRP. However, this section describes EIGRP features that work for AppleTalk, IP, and IPX. To configure such protocol-independent parameters, perform one or more of the tasks in the following sections:

- [Adjusting the Interval Between Hello Packets and the Hold Time](#)
- [Disabling Split Horizon](#)

For more protocol-independent features that work with EIGRP, see the chapter “Configuring IP Routing Protocol-Independent Features” in this document.

### Adjusting the Interval Between Hello Packets and the Hold Time

You can adjust the interval between hello packets and the hold time.

Routing devices periodically send hello packets to each other to dynamically learn of other routers on their directly attached networks. This information is used to discover neighbors and to learn when neighbors become unreachable or inoperative.



By default, hello packets are sent every 5 seconds. The exception is on low-speed, nonbroadcast multiaccess (NBMA) media, where the default hello interval is 60 seconds. Low speed is considered to be a rate of T1 or slower, as specified with the **bandwidth** interface configuration command. The default hello interval remains 5 seconds for high-speed NBMA networks. Note that for the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may or may not be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise they are not considered NBMA.

You can configure the hold time on a specified interface for a particular EIGRP routing process designated by the autonomous system number. The hold time is advertised in hello packets and indicates to neighbors the length of time they should consider the sender valid. The default hold time is three times the hello interval, or 15 seconds. For slow-speed NBMA networks, the default hold time is 180 seconds.

To change the interval between hello packets, use the following command in interface configuration mode:

| Command                                                                                      | Purpose                                                     |
|----------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Router(config-if)# <b>ip hello-interval eigrp</b><br><i>autonomous-system-number seconds</i> | Configures the hello interval for an EIGRP routing process. |

On very congested and large networks, the default hold time might not be sufficient time for all routers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

To change the hold time, use the following command in interface configuration mode:

| Command                                                                                 | Purpose                                                |
|-----------------------------------------------------------------------------------------|--------------------------------------------------------|
| Router(config-if)# <b>ip hold-time eigrp</b><br><i>autonomous-system-number seconds</i> | Configures the hold time for an EIGRP routing process. |

**Note**

Do not adjust the hold time without advising your technical support personnel.

## Disabling Split Horizon

Split horizon controls the sending of EIGRP update and query packets. When split horizon is enabled on an interface, update and query packets are not sent for destinations for which this interface is the next hop. Controlling update and query packets in this manner reduces the possibility of routing loops.

By default, split horizon is enabled on all interfaces.

Split horizon blocks route information from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and SMDS), situations can arise for which this behavior is less than ideal. For these situations, including networks in which you have EIGRP configured, you may want to disable split horizon.

To disable split horizon, use the following command in interface configuration mode:

| Command                                                                                | Purpose                 |
|----------------------------------------------------------------------------------------|-------------------------|
| Router(config-if)# <b>no ip split-horizon eigrp</b><br><i>autonomous-system-number</i> | Disables split horizon. |

## Configuring EIGRP Stub Routing

The EIGRP Stub Routing feature improves network stability, reduces resource utilization, and simplifies stub router configuration.

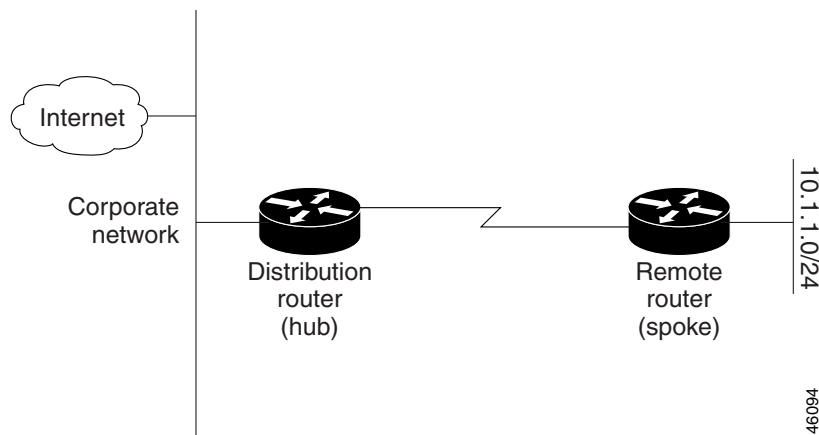
Stub routing is commonly used in a hub-and-spoke network topology. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote router (the spoke) that is connected to one or more distribution routers (the hub). The remote router is adjacent only to one or more distribution routers. The only route for IP traffic to follow into the remote router is through a distribution router. This type of configuration is commonly used in WAN topologies where the distribution router is directly connected to a WAN. The distribution router can be connected to many more remote routers. Often, the distribution router will be connected to 100 or more remote routers. In a hub-and-spoke topology, the remote router must forward all nonlocal traffic to a distribution router, so it becomes unnecessary for the remote router to hold a complete routing table. Generally, the distribution router need not send anything more than a default route to the remote router.

When using the EIGRP Stub Routing feature, you need to configure the distribution and remote routers to use EIGRP, and to configure only the remote router as a stub. Only specified routes are propagated from the remote (stub) router. The stub router responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message “inaccessible.” A router that is configured as a stub will send a special peer information packet to all neighboring routers to report its status as a stub router.

Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes, and a router that has a stub peer will not query that peer. The stub router will depend on the distribution router to send the proper updates to all peers.

Figure 32 shows a simple hub-and-spoke configuration.

**Figure 32 Simple Hub-and-Spoke Network**



The stub routing feature by itself does not prevent routes from being advertised to the remote router. In the example in Figure 32, the remote router can access the corporate network and the Internet through the distribution router only. Having a full route table on the remote router, in this example, would serve no functional purpose because the path to the corporate network and the Internet would always be through the distribution router. The larger route table would only reduce the amount of memory required by the remote router. Bandwidth and memory can be conserved by summarizing and filtering routes in the distribution router. The remote router need not receive routes that have been learned from other networks because the remote router must send all nonlocal traffic, regardless of destination, to the distribution router. If a true stub network is desired, the distribution router should be configured to send

only a default route to the remote router. The EIGRP Stub Routing feature does not automatically enable summarization on the distribution router. In most cases, the network administrator will need to configure summarization on the distribution routers.



#### Note

When configuring the distribution router to send only a default route to the remote router, you must use the **ip classless** command on the remote router. By default, the **ip classless** command is enabled in all Cisco IOS images that support the EIGRP Stub Routing feature.

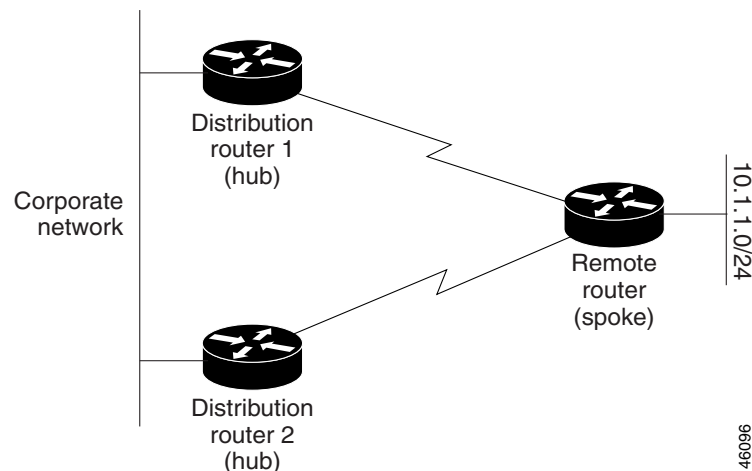
Without the stub feature, even after the routes that are sent from the distribution router to the remote router have been filtered or summarized, a problem might occur. If a route is lost somewhere in the corporate network, EIGRP could send a query to the distribution router, which in turn will send a query to the remote router even if routes are being summarized. If there is a problem communicating over the WAN link between the distribution router and the remote router, an EIGRP stuck in active (SIA) condition could occur and cause instability elsewhere in the network. The EIGRP Stub Routing feature allows a network administrator to prevent queries from being sent to the remote router.

## Dual-Homed Remote Topology

In addition to a simple hub-and-spoke network where a remote router is connected to a single distribution router, the remote router can be dual-homed to two or more distribution routers. This configuration adds redundancy and introduces unique issues, and the stub feature helps to address some of these issues.

A dual-homed remote router will have two or more distribution (hub) routers. However, the principles of stub routing are the same as they are with a hub-and-spoke topology. [Figure 33](#) shows a common dual-homed remote topology with one remote router, but 100 or more routers could be connected on the same interfaces on distribution router 1 and distribution router 2. The remote router will use the best route to reach its destination. If distribution router 1 experiences a failure, the remote router can still use distribution router 2 to reach the corporate network.

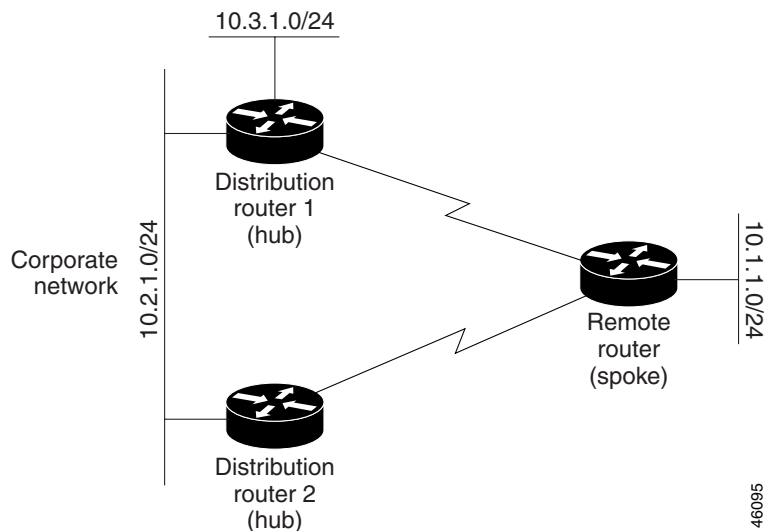
**Figure 33** Simple Dual-Homed Remote Topology



[Figure 33](#) shows a simple dual-homed remote with one remote router and two distribution routers. Both distribution routers maintain routes to the corporate network and stub network 10.1.1.0/24.

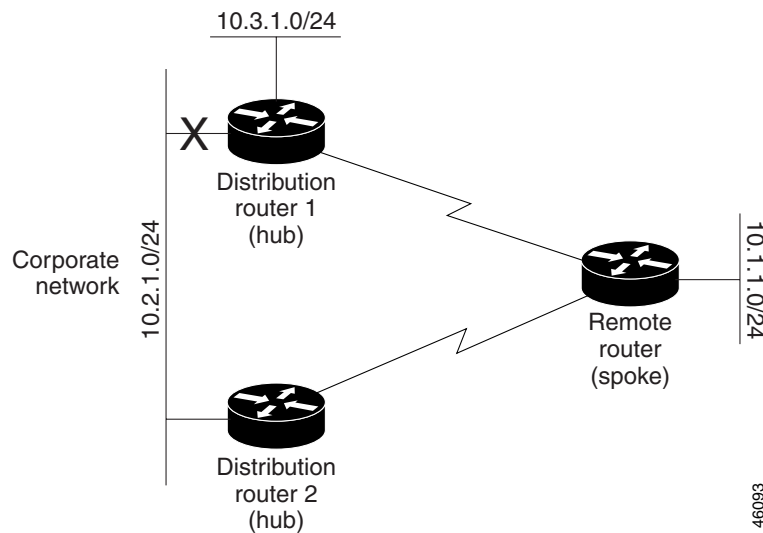
Dual-homed routing can introduce instability into an EIGRP network. In [Figure 34](#), distribution router 1 is directly connected to network 10.3.1.0/24. If summarization or filtering is applied on distribution router 1, the router will advertise network 10.3.1.0/24 to all of its directly connected EIGRP neighbors (distribution router 2 and the remote router).

**Figure 34** *Dual-Homed Remote Topology With Distribution Router 1 Connected to Two Networks*



[Figure 34](#) shows a simple dual-homed remote router where distribution router 1 is connected to both network 10.3.1.0/24 and network 10.2.1.0/24.

If the 10.2.1.0/24 link between distribution router 1 and distribution router 2 has failed, the lowest cost path to network 10.3.1.0/24 from distribution router 2 is through the remote router (see [Figure 35](#)). This route is not desirable because the traffic that was previously traveling across the corporate network 10.2.1.0/24 would now be sent across a much lower bandwidth connection. The over utilization of the lower bandwidth WAN connection can cause a number of problems that might affect the entire corporate network. The use of the lower bandwidth route that passes through the remote router might cause WAN EIGRP distribution routers to be dropped. Serial lines on distribution and remote routers could also be dropped, and EIGRP SIA errors on the distribution and core routers could occur.

**Figure 35** *Dual-Homed Remote Topology with a Failed Route to a Distribution Router*

It is not desirable for traffic from distribution router 2 to travel through any remote router in order to reach network 10.3.1.0/24. If the links are sized to handle the load, it would be acceptable to use one of the backup routes. However, most networks of this type have remote routers located at remote offices with relatively slow links. This problem can be prevented if proper summarization is configured on the distribution router and remote router.

It is typically undesirable for traffic from a distribution router to use a remote router as a transit path. A typical connection from a distribution router to a remote router would have much less bandwidth than a connection at the network core. Attempting to use a remote router with a limited bandwidth connection as a transit path would generally produce excessive congestion to the remote router. The EIGRP Stub Routing feature can prevent this problem by preventing the remote router from advertising core routes back to distribution routers. Routes learned by the remote router from distribution router 1 will not be advertised to distribution router 2. Since the remote router will not advertise core routes to distribution router 2, the distribution router will not use the remote router as a transit for traffic destined for the network core.

The EIGRP Stub Routing feature can help to provide greater network stability. In the event of network instability, this feature prevents EIGRP queries from being sent over limited bandwidth links to nontransit routers. Instead, distribution routers to which the stub router is connected answer the query on behalf of the stub router. This feature greatly reduces the chance of further network instability due to congested or problematic WAN links. The EIGRP Stub Routing feature also simplifies the configuration and maintenance of hub-and-spoke networks. When stub routing is enabled in dual-homed remote configurations, it is no longer necessary to configure filtering on remote routers to prevent those remote routers from appearing as transit paths to the hub routers.

**Caution**

EIGRP Stub Routing should only be used on stub routers. A stub router is defined as a router connected to the network core or distribution layer through which core transit traffic should not flow. A stub router should not have any EIGRP neighbors other than distribution routers. Ignoring this restriction will cause undesirable behavior.

**Note**

Multi-access interfaces, such as ATM, Ethernet, Frame Relay, ISDN PRI, and X.25, are supported by the EIGRP Stub Routing feature only when all routers on that interface, except the hub, are configured as stub routers.

## EIGRP Stub Routing Configuration Task List

To configure EIGRP Stub Routing, perform the tasks described in the following sections. The tasks in the first section are required; the task in the last section is optional.

- [Configuring EIGRP Stub Routing](#) (required)
- [Verifying EIGRP Stub Routing](#) (optional)

### Configuring EIGRP Stub Routing

To configure a remote or spoke router for EIGRP stub routing, use the following commands beginning in router configuration mode:

|               | Command                                                                                | Purpose                                                             |
|---------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Step 1</b> | router(config)# <b>router eigrp 1</b>                                                  | Configures a remote or distribution router to run an EIGRP process. |
| <b>Step 2</b> | router(config-router)# <b>network network-number</b>                                   | Specifies the network address of the EIGRP distribution router.     |
| <b>Step 3</b> | router(config-router)# <b>eigrp stub [receive-only   connected   static   summary]</b> | Configures a remote router as an EIGRP stub router.                 |

### Verifying EIGRP Stub Routing

To verify that a remote router has been configured as a stub router with EIGRP, use the **show ip eigrp neighbor detail** command from the distribution router in privileged EXEC mode. The last line of the output will show the stub status of the remote or spoke router. The following example shows output is from the **show ip eigrp neighbor detail** command:

```
Router# show ip eigrp neighbor detail
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime    SRTT    RTO  Q  Seq Type
      (sec)                (ms)
0   10.1.1.2                Se3/1       11 00:00:59    1   4500  0  7
    Version 12.1/1.2, Retrans: 2, Retries: 0
    Stub Peer Advertising ( CONNECTED SUMMARY ) Routes
```

# Monitoring and Maintaining EIGRP

To delete neighbors from the neighbor table, use the following command in EXEC mode:

| Command                                                                               | Purpose                                    |
|---------------------------------------------------------------------------------------|--------------------------------------------|
| Router# <b>clear ip eigrp neighbors</b> [ <i>ip-address</i>   <i>interface-type</i> ] | Deletes neighbors from the neighbor table. |

To display various routing statistics, use the following commands in EXEC mode, as needed:

| Command                                                                                                          | Purpose                                                                                |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Router# <b>show ip eigrp interfaces</b> [ <i>interface-type</i>   <i>interface-number</i> ] [ <i>as-number</i> ] | Displays information about interfaces configured for EIGRP.                            |
| Router# <b>show ip eigrp neighbors</b> [ <i>interface-type</i>   <i>as-number</i>   <b>static</b> ]              | Displays the EIGRP discovered neighbors.                                               |
| Router# <b>show ip eigrp topology</b> [ <i>as-number</i>   [[ <i>ip-address</i> ] <i>mask</i> ]]                 | Displays the EIGRP topology table for a given process.                                 |
| Router# <b>show ip eigrp traffic</b> [ <i>as-number</i> ]                                                        | Displays the number of packets sent and received for all or a specified EIGRP process. |

To enable EIGRP Stub Routing packet debugging, use the following command in privileged EXEC mode:

| Command                                | Purpose                                                           |
|----------------------------------------|-------------------------------------------------------------------|
| Router# <b>debug eigrp packet stub</b> | Displays debug information about the stub status of peer routers. |

## EIGRP Configuration Examples

This section contains the following examples:

- [Route Summarization Example](#)
- [Route Authentication Example](#)
- [Stub Routing Example](#)

### Route Summarization Example

The following example configures route summarization on the interface and also configures the automatic summary feature. This configuration causes EIGRP to summarize network 10.0.0.0 out Ethernet interface 0 only. In addition, this example disables automatic summarization.

```
interface Ethernet 0
 ip summary-address eigrp 1 10.0.0.0 255.0.0.0
!
router eigrp 1
 network 172.16.0.0
 no auto-summary
```

**Note**

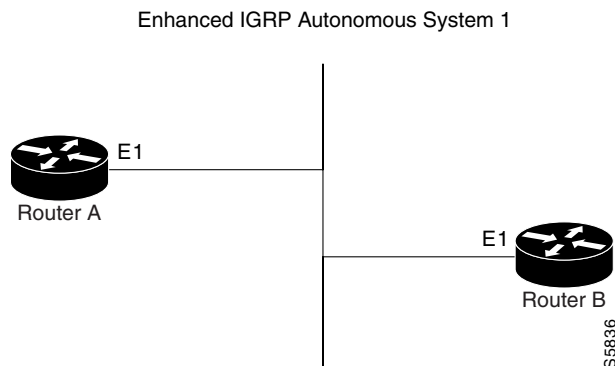
You should not use the **ip summary-address eigrp** summarization command to generate the default route (0.0.0.0) from an interface. This causes the creation of an EIGRP summary default route to the null 0 interface with an administrative distance of 5. The low administrative distance of this default route can cause this route to displace default routes learned from other neighbors from the routing table. If the default route learned from the neighbors is displaced by the summary default route, or if the summary route is the only default route present, all traffic destined for the default route will not leave the router, instead, this traffic will be sent to the null 0 interface where it is dropped.

The recommended way to send only the default route out a given interface is to use a **distribute-list** command. You can configure this command to filter all outbound route advertisements sent out the interface with the exception of the default (0.0.0.0).

## Route Authentication Example

The following example enables MD5 authentication on EIGRP packets in autonomous system 1. [Figure 36](#) shows the scenario.

**Figure 36** *EIGRP Route Authentication Scenario*



### Router A Configuration

```

interface ethernet 1
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 holly
key chain holly
key 1
 key-string 0987654321
 accept-lifetime 04:00:00 Dec 4 1996 infinite
 send-lifetime 04:00:00 Dec 4 1996 04:48:00 Dec 4 1996
exit
key 2
 key-string 1234567890
 accept-lifetime 04:00:00 Dec 4 1996 infinite
 send-lifetime 04:45:00 Dec 4 1996 infinite
  
```

### Router B Configuration

```

interface ethernet 1
 ip authentication mode eigrp 1 md5
  
```



```
ip authentication key-chain eigrp 1 mikel
key chain mikel
  key 1
    key-string 0987654321
    accept-lifetime 04:00:00 Dec 4 1996 infinite
    send-lifetime 04:00:00 Dec 4 1996 infinite
  exit
  key 2
    key-string 1234567890
    accept-lifetime 04:00:00 Dec 4 1996 infinite
    send-lifetime 04:45:00 Dec 4 1996 infinite
```

Router A will accept and attempt to verify the MD5 digest of any EIGRP packet with a key equal to 1. It will also accept a packet with a key equal to 2. All other MD5 packets will be dropped. Router A will send all EIGRP packets with key 2.

Router B will accept key 1 or key 2, and will send key 1. In this scenario, MD5 will authenticate.

## Stub Routing Example

A router that is configured as a stub with the **eigrp stub** command shares connected and summary routing information with all neighbor routers by default. Four optional keywords can be used with the **eigrp stub** command to modify this behavior:

- **receive-only**
- **connected**
- **static**
- **summary**

This section provides configuration examples for all forms of the **eigrp stub** command. The **eigrp stub** command can be modified with several options, and these options can be used in any combination except for the **receive-only** keyword. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system, and the **receive-only** keyword will not permit any other option to be specified because it prevents any type of route from being sent. The three other optional keywords (**connected**, **static**, and **summary**) can be used in any combination but cannot be used with the **receive-only** keyword. If any of these three keywords is used individually with the **eigrp stub** command, connected and summary routes will not be sent automatically.

The **connected** keyword will permit the EIGRP Stub Routing feature to send connected routes. If the connected routes are not covered by a network statement, it may be necessary to redistribute connected routes with the **redistribute connected** command under the EIGRP process. This option is enabled by default.

The **static** keyword will permit the EIGRP Stub Routing feature to send static routes. Without this option, EIGRP will not send any static routes, including internal static routes that normally would be automatically redistributed. It will still be necessary to redistribute static routes with the **redistribute static** command.

The **summary** keyword will permit the EIGRP Stub Routing feature to send summary routes. Summary routes can be created manually with the **summary address** command or automatically at a major network border router with the **auto-summary** command enabled. This option is enabled by default.

In the following example, the **eigrp stub** command is used to configure the router as a stub that advertises connected and summary routes:

```
router eigrp 1
 network 10.0.0.0
```

```
eigrp stub
```

In the following example, the **eigrp stub connected static** command is used to configure the router as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
router eigrp 1
 network 10.0.0.0
 eigrp stub connected static
```

In the following example, the **eigrp stub receive-only** command is used to configure the router as a stub, and connected, summary, or static routes will not be sent:

```
router eigrp 1
 network 10.0.0.0
 eigrp stub receive-only
```



## EIGRP Nonstop Forwarding (NSF) Awareness

Nonstop Forwarding (NSF) awareness allows an NSF-aware router to assist NSF-capable and NSF-aware neighbors to continue forwarding packets during a switchover operation or during a well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running Enhanced Interior Gateway Routing Protocol (EIGRP) to forward packets along routes that are already known for a router that is performing a switchover operation or is in a well-known failure mode. This capability allows the EIGRP peers of the failing router to retain the routing information that is advertised by the failing router and continue to use this information until the failed router has returned to normal operating behavior and is able to exchange routing information. The peering session is maintained throughout the entire NSF operation.

### History for the EIGRP Nonstop Forwarding (NSF) Awareness feature

| Release   | Modification                 |
|-----------|------------------------------|
| 12.2(15)T | This feature was introduced. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for EIGRP Nonstop Forwarding Awareness, page 382](#)
- [Restrictions for EIGRP Nonstop Forwarding Awareness, page 382](#)
- [Information About EIGRP Nonstop Forwarding Awareness, page 382](#)
- [How to Modify and Maintain EIGRP Nonstop Forwarding Awareness, page 385](#)
- [Configuration Examples for EIGRP Nonstop Forwarding Awareness, page 388](#)
- [Additional References, page 389](#)
- [Command Reference, page 390](#)

# Prerequisites for EIGRP Nonstop Forwarding Awareness

This document assumes that your network is configured to run EIGRP. The following tasks must also be completed before you can configure this feature:

- An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.
- A version of Cisco IOS that support NSF awareness or NSF capabilities must be installed.

# Restrictions for EIGRP Nonstop Forwarding Awareness

The following restrictions apply to the EIGRP Nonstop Forwarding Awareness feature:

- All neighboring devices participating in EIGRP NSF must be NSF-capable or NSF-aware.
- EIGRP NSF awareness does not support two neighbors performing an NSF restart operation at the same time. However, both neighbors will still reestablish peering sessions after the NSF restart operation is complete.

# Information About EIGRP Nonstop Forwarding Awareness

To configure this feature, you must understand the following concepts:

- [Cisco NSF Routing and Forwarding Operation, page 382](#)
- [Cisco Express Forwarding, page 383](#)
- [EIGRP Nonstop Forwarding Awareness, page 383](#)
- [EIGRP NSF Capable and NSF Aware Interoperation, page 384](#)
- [Non-NSF Aware EIGRP Neighbors, page 384](#)
- [EIGRP NSF Route-Hold Timers](#)

# Cisco NSF Routing and Forwarding Operation

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. Of the routing protocols, BGP, OSPF, and IS-IS have been enhanced with NSF-capability and awareness, which means that routers running these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the peer devices. The IS-IS protocol can be configured to use state information that has been synchronized between the active and the standby RP to recover route information following a switchover instead of information received from peer devices.

In this document, a networking device is said to be NSF-aware if it is running NSF-compatible software. A device is said to be NSF-capable if it has been configured to support NSF; therefore, it would rebuild routing information from NSF-aware or NSF-capable neighbors.

Each protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once the routing protocols have converged, CEF updates the FIB table and removes stale route entries. CEF, in turn, updates the line cards with the new FIB information.

## Cisco Express Forwarding

A key element of NSF is packet forwarding. In a Cisco networking device, packet forwarding is provided by CEF. CEF maintains the FIB, and uses the FIB information that was current at the time of the switchover to continue forwarding packets during a switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards will maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF will keep the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines will be able to continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the routing protocols start to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates for CEF, which it uses to update the FIB and adjacency databases. Existing and new entries will receive the new version (“epoch”) number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engine during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The routing protocols run only on the active RP, and they receive routing updates from their neighbor routers. Routing protocols do not run on the standby RP. Following a switchover, the routing protocols request that the NSF-aware neighbor devices send state information to help rebuild the routing tables.

**Note**

For NSF operation, the routing protocols depend on CEF to continue forwarding packets while the routing protocols rebuild the routing information.

## EIGRP Nonstop Forwarding Awareness

NSF awareness allows a router that is running EIGRP to assist NSF-capable neighbors to continue forwarding packets during a switchover operation or well-known failure condition. The EIGRP Nonstop Forwarding Awareness feature provides EIGRP with the capability to detect a neighbor that is undergoing an NSF restart event (route processor [RP] switchover operation) or well-known failure condition, maintain the peering session with this neighbor, retain known routes, and continue to forward packets for these routes. The deployment of EIGRP NSF awareness can minimize the affects of the following:

- Well-known failure conditions (for example, a stuck-in-active event).
- Unexpected events (for example, an RP switchover operation).
- Scheduled events (for example, a hitless software upgrade).

EIGRP NSF awareness is enabled by default, and its operation is transparent to the network operator and EIGRP peers that do not support NSF capabilities.

**Note**

An NSF-aware router must be up and completely converged with the network before it can assist an NSF-capable router in an NSF restart operation.

## EIGRP NSF Capable and NSF Aware Interoperation

EIGRP NSF capabilities are exchanged by EIGRP peers in hello packets. The NSF-capable router notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware router receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, the NSF-capable and NSF-aware routers immediately exchange their topology tables. The NSF-aware router sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware router then performs the following actions to assist the NSF-capable router:

- The router expires the EIGRP hello hold timer to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware router to reply to the NSF-capable router more quickly and reduces the amount of time required for the NSF-capable router to rediscover neighbors and rebuild the topology table.
- The router starts the route-hold timer. This timer is used to set the period of time that the NSF-aware router will hold known routes for the NSF-capable neighbor. This timer is configured with the **timers nsf route-hold** command. The default time period is 240 seconds.
- The router notes in the peer list that the NSF-capable neighbor is restarting, maintains adjacency, and holds known routes for the NSF-capable neighbor until the neighbor signals that it is ready for the NSF-aware router to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware router, the NSF-aware router will discard held routes and treat the NSF-capable router as a new router joining the network and reestablishing adjacency accordingly.

When the switchover operation is complete, the NSF-capable router notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting routers. The NSF-capable then returns to normal operation. The NSF-aware router will look for alternate paths (go active) for any routes that are not refreshed by the NSF-capable (restarting router). The NSF-aware router will then return to normal operation. If all paths are refreshed by the NSF-capable router, the NSF-aware router will immediately return to normal operation.

## Non-NSF Aware EIGRP Neighbors

NSF-aware routers are completely compatible with non-NSF aware or capable neighbors in an EIGRP network. A non-NSF aware neighbor will ignore NSF capabilities and reset the adjacency when they are received.

The NSF-capable router will drop any queries that are received while converging to minimize the number of transient routes that are sent to neighbors. But the NSF-capable router will still acknowledge these queries to prevent these neighbors from resetting adjacency.



### Note

NSF-aware router will continue to send queries to the NSF-capable router which is still in the process of converging after switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.

## EIGRP NSF Route-Hold Timers

The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

The route-hold timer is configured with the **timers nsf route-hold** router configuration command. The default time period for the route-hold timer is 240 seconds. The configurable range is from 10 to 300 seconds.

# How to Modify and Maintain EIGRP Nonstop Forwarding Awareness

This section contains the following procedures for configuring the EIGRP Nonstop Forwarding Awareness feature:

- [Adjusting NSF Route-Hold Timers, page 385](#)
- [Monitoring EIGRP NSF Debug Events and Notifications, page 386](#)
- [Verifying the Local Configuration of EIGRP NSF Awareness, page 387](#)

## Adjusting NSF Route-Hold Timers

Use the following steps to configure NSF route-hold timers on an NSF-aware router:

### Route-Hold Timers

The route-hold timer is configurable so that you can tune network performance and avoid undesired effects, such as “black holing” routes if the switchover operation takes too much time. When this timer expires, the NSF-aware router scans the topology table and discards any stale routes, allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation.

#### SUMMARY STEPS

1. **enable**
2. **configure {terminal | memory | network}**
3. **router eigrp as-number**
4. **timers nsf route-hold seconds**
5. **exit**

#### DETAILED STEPS

|        | Command or Action                              | Purpose                                                                              |
|--------|------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                  | Enables higher privilege levels, such as privileged EXEC mode.                       |
|        | <b>Example:</b><br>Router> enable              | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure {terminal   memory   network}</b> | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal  |                                                                                      |

|        | Command or Action                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>router eigrp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# <b>router eigrp</b> 101                        | Enters router configuration mode and creates an EIGRP routing process.                                                                                                                                                                                                                                                     |
| Step 4 | <b>timers nsf route-hold</b> <i>seconds</i><br><br><b>Example:</b><br>Router(config-router)# <b>timers nsf route-hold</b> 120 | Sets the maximum period of time that an NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation. The configurable range of time for the <i>seconds</i> argument is from 20 to 300 seconds. The default value is 240 seconds. The example sets the route-hold timer to 2 minutes. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# <b>exit</b>                                                      | Exits router configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                      |

## Troubleshooting Tips

Neighbor adjacencies are maintained during NSF switchover operations. If adjacencies between NSF-capable and NSF-aware neighbors are being reset too often, the route-hold timers may need to be adjusted. The **show ip eigrp neighbor detail** command can be used to help determine if the route-hold timer value should be set to a longer time period. The output will display the time that adjacency is established with specific neighbors. This time will tell you if adjacencies are being maintained or reset and when the last time that specific neighbors have been restarted.

## Monitoring EIGRP NSF Debug Events and Notifications

Use the following steps to monitor EIGRP NSF debug events and notifications on an NSF-aware router:

### Debug Commands

The **debug eigrp nsf** and **debug ip eigrp notifications** commands do not need to be issued together or even in the same session as there are differences in the information that is provided. These commands are provided together for example purposes.

The output of debug commands can be very verbose. These commands should not be deployed in a production network unless you are troubleshooting a problem.

### SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug eigrp ip notifications**



## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                    |
| Step 2 | <b>debug eigrp nsf</b><br><br><b>Example:</b><br>Router# debug eigrp nsf                           | Displays NSF notifications and information about NSF events in an EIGRP network on the console of the router.                                                        |
| Step 3 | <b>debug ip eigrp notifications</b><br><br><b>Example:</b><br>Router# debug ip eigrp notifications | Displays EIGRP events and notifications in the console of the router. The output from this command also includes NSF notifications and information about NSF events. |

## Verifying the Local Configuration of EIGRP NSF Awareness

Use the following steps to verify the local configuration of NSF-awareness on a router that is running EIGRP:

### SUMMARY STEPS

1. enable
2. show ip protocols

### DETAILED STEPS

|        | Command or Action                                                            | Purpose                                                                                                                                                 |
|--------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                       | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>       |
| Step 2 | <b>show ip protocols</b><br><br><b>Example:</b><br>Router# show ip protocols | Displays the parameters and current state of the active routing protocol process. The output of this command can be used to verify EIGRP NSF-awareness. |

# Configuration Examples for EIGRP Nonstop Forwarding Awareness

- [EIGRP Route-Hold Timer Configuration Example, page 388](#)
- [Monitoring EIGRP NSF Debug Events and Notifications Configuration Example, page 388](#)
- [Verifying Local Configuration of EIGRP NSF Awareness, page 388](#)

## EIGRP Route-Hold Timer Configuration Example

The **timers nsf route-hold** command is used to set the maximum period of time that an NSF-aware router will hold known routes for an NSF-capable neighbor during a switchover operation. The following example sets the route-hold timer to 2 minutes:

```
Router(config-router)# timers nsf route-hold 120
```

## Monitoring EIGRP NSF Debug Events and Notifications Configuration Example

The following example output shows that the NSF-aware router has received the restart notification. The NSF-aware router will now wait for EOT to be sent from the restarting neighbor (NSF-capable).

```
Router# debug ip eigrp notifications
*Oct  4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 135.100.10.1,
00:00:00. Wait for EOT.
*Oct  4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor
135.100.10.1 (POS3/0) is up:peer NSF restarted
```

## Verifying Local Configuration of EIGRP NSF Awareness

The following is example output from the **show ip protocols** command. The output from this command can be used to verify the local configuration of the EIGRP NSF awareness. The output below shows that the router is NSF-aware and that the route-hold timer is set to 240 seconds, which is the default value for the route-hold timer.

```
Router# show ip protocols
Routing Protocol is "eigrp 101"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 101
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.4.9.0/24
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: internal 90 external 170
```

# Additional References

For additional information related to EIGRP Nonstop Forwarding Awareness feature, refer to the following references:

## Related Documents

| Related Topic             | Document Title                                                                         |
|---------------------------|----------------------------------------------------------------------------------------|
| CEF commands              | <i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.2                 |
| CEF configuration tasks   | <i>Cisco IOS Switching Services Command Reference</i> , Release 12.2                   |
| EIGRP commands            | <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2 |
| EIGRP configuration tasks | <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                                 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                          | Title                                     |
|-------------------------------|-------------------------------------------|
| draft-ietf-idr-restart-06.txt | <i>Graceful Restart Mechanism for BGP</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **debug eigrp nsf**
- **debug ip eigrp notifications**
- **show ip eigrp neighbors**
- **show ip protocols**
- **timers nsf route-hold**



# MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge

The MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature introduces the capability to redistribute Enhanced Interior Gateway Routing Protocol (EIGRP) routes through a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) over a Border Gateway Protocol (BGP) core network. This feature is configured only on PE routers and requires no upgrade or configuration changes to customer equipment. This feature also introduces EIGRP support for MPLS and support for EIGRP extended community attributes.

## Feature History for the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer (CE) feature

| Release   | Modification                                                                                                                                                                                                                |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(22)S | This feature was introduced.                                                                                                                                                                                                |
| 12.2(15)T | This feature was integrated into Cisco IOS Release 12.2(15)T.                                                                                                                                                               |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S.                                                                                                                                                               |
| 12.0(27)S | EIGRP back door link support was introduced. This support is provided by a new POI in the BGP Cost Community (Updated in this release) and EIGRP MPLS VPN PE-CE Site of Origin (SoO) (Introduced in this release) features. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for MPLS VPN Support for EIGRP Between PE and CE, page 392](#)
- [Restrictions for MPLS VPN Support for EIGRP Between PE and CE, page 392](#)
- [Information About MPLS VPN Support for EIGRP Between PE and CE, page 392](#)
- [How to Configure an MPLS VPN Using EIGRP, page 395](#)
- [Configuration Examples for the EIGRP MPLS VPN, page 405](#)
- [Additional References, page 410](#)

- [Command Reference, page 411](#)

## Prerequisites for MPLS VPN Support for EIGRP Between PE and CE

This document assumes that BGP is configured in the network core. You will also need to complete the following tasks before you can configure this feature:

- MPLS and Cisco Express Forwarding (CEF) must be configured in the BGP core network. EIGRP and multiprotocol BGP (mBGP) must be configured on all PE routers that provide VPN services to the CE routers at the customer sites.
- The metric must be configured for routes from external EIGRP autonomous systems and non-EIGRP networks before these routes can be redistributed into an EIGRP CE router. The metric can be configured in the redistribute statement using the **redistribute (IP)** command or configured with the **default-metric (EIGRP)** command.

## Restrictions for MPLS VPN Support for EIGRP Between PE and CE

### **Metric Must Be Configured for Routes from Other Autonomous Systems and Non-EIGRP Networks**

If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE router. The metric can be configured in the redistribute statement using the **redistribute** command or configured with the **default-metric** command.

### **Native EIGRP VRF to VRF Redistribution is Not Supported**

Redistribution between native EIGRP VRFs is not supported. This is designed behavior.

## Information About MPLS VPN Support for EIGRP Between PE and CE

To configure this feature, you must understand the following concepts:

- [MPLS VPN Support for EIGRP, page 392](#)
- [EIGRP Extended Community Attributes, page 394](#)
- [Benefits of MPLS VPN Support for EIGRP, page 395](#)

## MPLS VPN Support for EIGRP

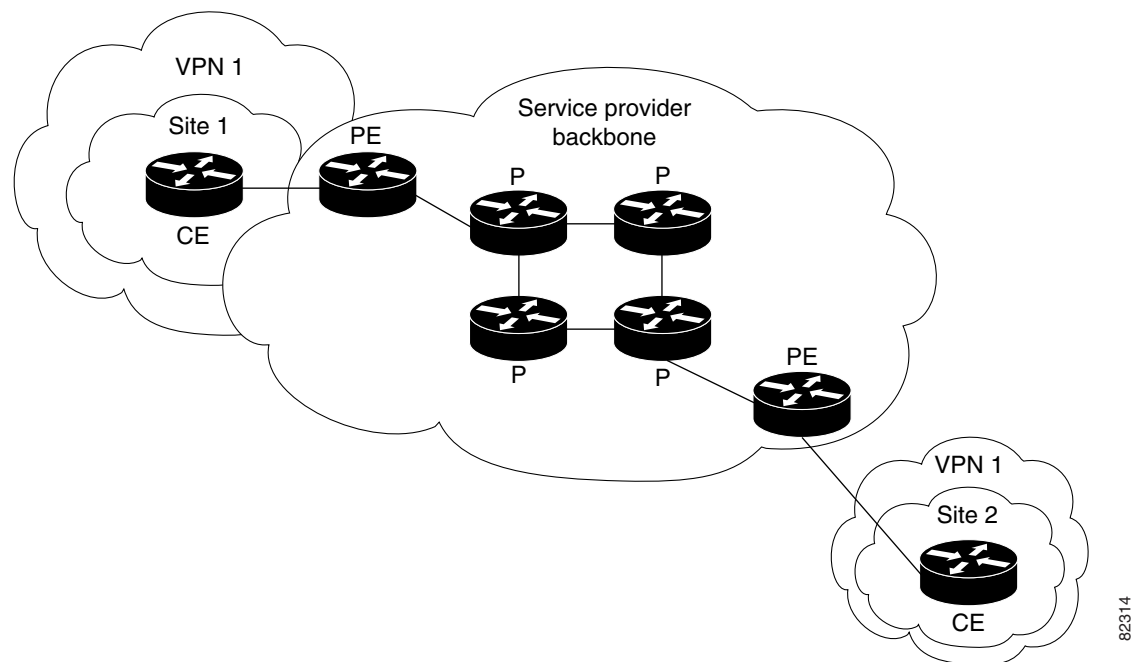
The MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature provides the capability to transparently connect EIGRP customer networks through an MPLS-enabled BGP core network so that EIGRP routes are redistributed through the VPN across the BGP network as internal

BGP (iBGP) routes. The configuration of this feature does not require any customer equipment upgrades or configuration changes; this feature is configured only on PE routers within the service provider network.

Customer networks and remote sites are connected to each other through the MPLS VPN. The configuration of this feature allows several EIGRP sites to connect seamlessly and appear as a single network. This integration is transparent to the customer sites. When this feature is enabled, EIGRP routes are converted to iBGP routes and transported through the BGP core network. EIGRP extended community attributes are used to define EIGRP routes and preserve internal metrics. These attributes are carried across the core network by multiprotocol BGP.

Figure 37 shows 2 customer EIGRP networks that are connected by the VPN over a service provider backbone: "Site 1" and "Site 2."

**Figure 37** *EIGRP Connectivity Between VPN Client Sites over a Service Provider Backbone*



In Figure 37, the EIGRP routes in Site 1 are carried through the BGP core network as iBGP routes. The EIGRP routes in "Site 1" and "Site 2" are converted to iBGP routes and EIGRP extended community attributes are appended to the iBGP routes. (See Table 13 for a description of these attributes.) The EIGRP extended community attributes are appended to the EIGRP routes when they are redistributed into BGP as iBGP routes, and VPN routing information is redistributed between the PE routers by multiprotocol BGP.

The routes that originate in "Site 1" travel to the PE router that is connected to the CE router in "Site 2" of the VPN and are then converted back to EIGRP routes using the EIGRP extended community attributes. EIGRP routes are treated the same in "Site 1" and "Site 2." If the route is internal in "Site 1", it will be internal in "Site 2", and if the route is external in "Site 1", it will be external in "Site 2." All EIGRP metrics are preserved, and EIGRP metric information, along with the autonomous system, tag, and external data, is carried across the VPN over the BGP core network.

82314

**Note**

EIGRP adjacencies, EIGRP updates, and EIGRP queries are not sent across the VPN. If a route is received from another EIGRP autonomous system without a configured metric, the route is not advertised to the CE router.

Each VPN is associated with a single VPN routing or forwarding instance (VRF). A VRF consists of an IP routing table, a CEF table, and a set of interfaces that use the CEF forwarding table. The router maintains a separate routing and CEF table for each VRF, which prevents information being sent outside the VPN and allows the same addresses to be used in several VPNs without causing problems that are associated with duplicate IP addresses.

A single EIGRP routing process can support multiple VRFs. This support is limited only by the available system resources on the router, which are determined by the number of configured VRF instances, running processes, and amount of available memory. However, only a single VRF can be supported by each VPN. Separate VRFs are unique and do not share neighbor, routing, or topology information. Redistribution between native EIGRP VRFs is not supported. An EIGRP process must be created for the default VRF even if it is not used for establishing EIGRP neighbors, and a separate VRF address family must be configured in BGP for each EIGRP VRF.

## EIGRP Extended Community Attributes

EIGRP routes are converted to iBGP routes on the PE router by appending EIGRP extended community attributes. The PE router uses multiprotocol BGP to distribute the VPN routing information using the these extended community attributes. The BGP routes are converted back to EIGRP routes using the extended community attribute information when the iBGP routes reach the PE router that is connected to the destination CE router.

[Table 13](#) describes the extended community attributes that are appended to BGP routes and used to carry EIGRP information across the service provider backbone.

**Table 13 EIGRP-Specific Extended Community Attribute Descriptions**

| EIGRP Appended Attributes        | Usage                                                | Values                                 |
|----------------------------------|------------------------------------------------------|----------------------------------------|
| Type 0x8800                      | EIGRP General Route Information                      | Route Flag and Tag                     |
| EIGRP Metric Information         | Usage                                                | Values                                 |
| Type 0x8801                      | EIGRP Route Metric Information and Autonomous System | Autonomous System and Delay            |
| Type 0x8802                      | EIGRP Route Metric Information                       | Reliability, Next Hop, and Bandwidth   |
| Type 0x8803                      | EIGRP Route Metric Information                       | Reserve, Load and MTU                  |
| EIGRP External Route Information | Usage                                                | Values                                 |
| Type 0x8804                      | EIGRP External Route Information                     | Remote Autonomous System and Remote ID |
| Type 0x8805                      | EIGRP External Route Information                     | Remote Protocol and Remote Metric      |



## Benefits of MPLS VPN Support for EIGRP

### Multiple VRFs Are Supported

A single EIGRP routing process can support multiple VRFs. This support is limited only by the available system resources on the router, which are determined by the number of configured VRF instances, running processes, and amount of available memory. However, only a single VRF can be supported by each VPN.

### Seamless Integration of Existing Customer EIGRP Deployments

This feature is configured only on PE routers that provide VPN services across the service provider network. The customer need not upgrade their version of Cisco IOS software or make any changes to their equipment or configurations.

### Secure, Scalable, and Cost-Effective Alternative

Remote sites can be seamlessly and securely connected through VPNs to customer networks. This feature provides a cost-effective alternative to traditional methods, such as WAN leased lines.

## How to Configure an MPLS VPN Using EIGRP

This section contains the following procedures:

- [Configuring the VRF for the EIGRP MPLS VPN, page 395](#) (required)
- [Configuring EIGRP Redistribution in the MPLS VPN, page 397](#) (required)
- [Configuring the PE Routers to Support the EIGRP MPLS VPN, page 401](#) (required)
- [Verifying the VPN Configuration, page 13](#) (optional)
- [Verifying PE-to-PE Connectivity, page 13](#) (optional)
- [Verifying EIGRP VRF Configuration, page 14](#) (optional)

## Configuring the VRF for the EIGRP MPLS VPN

### Creating a VRF

A VRF must be created, and a route distinguisher and route target must be configured in order for the PE routers in the BGP network to carry EIGRP routes to the EIGRP CE site. The VRF must also be associated with an interface in order for the PE router to send routing updates to the CE router. Use the following steps to create and configure the VRF and associate the VRF with an interface.

### Prerequisites

Before this feature can be configured, MPLS and CEF must be configured in the BGP network, and multiprotocol BGP and EIGRP must be configured on all PE routers that provide VPN services to CE routers.

## Restrictions

Native EIGRP VRF to VRF redistribution is not supported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **exit**
7. **interface** *type number*
8. **ip vrf forwarding** *vrf-name*
9. **ip address** *ip-address subnet-mask*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf RED          | Creates a VRF routing table and specifies the VRF name (or tag).<br><ul style="list-style-type: none"><li>The <b>ip vrf</b> <i>vrf-name</i> command creates a VRF routing table and a CEF table, and both are named using the <i>vrf-name</i> argument. Associated with these tables is the default route distinguisher value.</li></ul>                                                 |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1 | Creates routing and forwarding tables for the VRF instance created in step 3.<br><ul style="list-style-type: none"><li>There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).</li></ul> |

|         | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <b>route-target</b> {import   export   both}<br><i>route-target-extcommunity</i><br><br><b>Example:</b><br>Router(config-vrf)# route-target both 100:1 | Creates a list of import and/or export route target communities for the specified VRF. <ul style="list-style-type: none"> <li>There are two formats for configuring the route target extcommunity argument. It can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).</li> </ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# exit                                                                                         | Exits VRF configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                     |
| Step 7  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface FastEthernet 0/0                                               | Enters interface configuration mode to configure the specified interface.                                                                                                                                                                                                                                                                                                                              |
| Step 8  | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding RED                                            | Associates the VRF with an interface or subinterface. <ul style="list-style-type: none"> <li>The VRF name configured in this step should match the VRF name created in step 3.</li> </ul>                                                                                                                                                                                                              |
| Step 9  | <b>ip address</b> <i>ip-address subnet-mask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.0.0.1 255.255.255.0                         | Configures the IP address for the interface. <ul style="list-style-type: none"> <li>The IP address needs to be reconfigured after enabling VRF forwarding.</li> </ul>                                                                                                                                                                                                                                  |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                            | Exits interface configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                    |

## What to Do Next

The next task is to configure the EIGRP redistribution in the MPLS VPN. Use the steps in the following section.

# Configuring EIGRP Redistribution in the MPLS VPN

## Creating the MPLS VPN

Perform this task to enable EIGRP redistribution in the MPLS VPN. This task should be applied to every PE router that provides VPN services.

## Prerequisites

Before EIGRP SoO BGP Cost Community support was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Back door links in an EIGRP MPLS VPN topology will be preferred by BGP if the back door link is learned first. (A back door link or a route is a connection that is configured outside of the VPN between a remote and main site. For example, a WAN leased line that connects a remote site to the corporate network).

The “pre-bestpath” point of insertion (POI) has been introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-best path” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by configuring BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when Cisco IOS Release 12.0(27)S is installed to a PE, CE, or back door router.

For more information about the BGP Cost Community feature and the absolute value POI, refer to the BGP Cost Community feature documentation in Cisco IOS Release 12.0(27)S.

For more information about the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature, refer to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature documentation in Cisco IOS Release 12.0(27)S.

## Restrictions

Metrics must be configured for routes from other EIGRP autonomous systems and non-EIGRP networks. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE router. The metric can be configured in the redistribute statement using the **redistribute** command or configured with the **default-metric** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **network** *ip-address wildcard-mask*
6. **redistribute bgp** [*autonomous-system-number*] [**metric** *bandwidth delay reliability load mtu*]
7. **autonomous-system** *autonomous-system-number*
8. **exit-address-family**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>router eigrp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                                                                       | Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>The EIGRP routing process for the PE router is created in this step.</li> </ul>                                                                                                                                                                                  |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                                                         | Enters address-family configuration mode and creates a VRF. <ul style="list-style-type: none"> <li>The VRF name (or tag) must match the VRF name that was created in Step 3 of the previous section.</li> </ul>                                                                                                                                                                |
| Step 5 | <b>network</b> <i>ip-address wildcard-mask</i><br><br><b>Example:</b><br>Router(config-router-af)# network 172.16.0.0 0.0.255.255                                                                                                                                  | Specifies the network for the VRF. <ul style="list-style-type: none"> <li>The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement.</li> </ul>                                                                                              |
| Step 6 | <b>redistribute bgp</b> [ <i>autonomous-system-number</i> ] [ <b>metric</b> <i>bandwidth delay reliability load mtu</i> ] [ <b>route-map</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500 | Redistributes BGP into the EIGRP. <ul style="list-style-type: none"> <li>The autonomous system number and metric of the BGP network is configured in this step. BGP must be redistributed into EIGRP for the CE site to accept the BGP routes that carry the EIGRP information. A metric must also be specified for the BGP network and is configured in this step.</li> </ul> |
| Step 7 | <b>autonomous-system</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config-router-af)# autonomous-system 101                                                                                                                                 | Specifies the autonomous system number of the EIGRP network for the customer site.                                                                                                                                                                                                                                                                                             |
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                                                                                                 | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                                                                                                                                  |

## Troubleshooting Tips

If the MPLS VPN is not working properly, verify the following:

- Verify the configurations on each router. Make sure that the VRF and route distinguisher have been correctly configured. Check the VRF routing table and VRF CEF table.
- Verify that there is connectivity between both PE routers. Check the PE router and other neighbors that carry the VPN. The network operator should be able to ping between the PE routers that carry the VPN to verify the neighbor relationships.

The commands in the following table can also be useful for monitoring and troubleshooting the configuration of this feature:

| Command                                                     | Purpose                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>clear ip eigrp vrf <i>vrf-name</i> neighbor</b>  | Clears EIGRP neighbors from the VRF table.                                                                                                                                                                                                                                              |
| Router# <b>debug ip eigrp vrf <i>vrf-name</i></b>           | Specifies a VRF for trace debugging. <ul style="list-style-type: none"> <li>• A VRF name must be specified with the <i>vrf-name</i> argument, or the "*" can be used as a wildcard to specify all configured VRFs.</li> </ul>                                                           |
| Router# <b>show ip eigrp vrf <i>vrf-name</i> interfaces</b> | Displays EIGRP interfaces that are defined under the specified VRF. <ul style="list-style-type: none"> <li>• If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running as part of the specified VRF are displayed.</li> </ul> |
| Router# <b>show ip eigrp vrf <i>vrf-name</i> neighbors</b>  | Displays when VRF neighbors become active and inactive. <ul style="list-style-type: none"> <li>• This command can be used to help debug transport problems.</li> </ul>                                                                                                                  |
| Router# <b>show ip eigrp vrf <i>vrf-name</i> topology</b>   | Displays VRF entries in the EIGRP topology table. <ul style="list-style-type: none"> <li>• This command can be used to determine Diffusing Update Algorithm (DUAL) states and to troubleshoot possible DUAL problems.</li> </ul>                                                        |
| Router# <b>show ip vrf</b>                                  | Displays the set of defined VRFs and associated interfaces. <ul style="list-style-type: none"> <li>• This command is used to verify that the correct route distinguishers (RDs) are configured for the VRF.</li> </ul>                                                                  |
| Router# <b>show mpls interfaces</b>                         | Displays information about one or more interfaces that have been configured for label switching. <ul style="list-style-type: none"> <li>• This command is used to verify that MPLS is configured for interfaces that are used with this feature.</li> </ul>                             |

## What to Do Next

The next task is to configure the PE routers to support the EIGRP MPLS VPN. Use the steps in the following section.

# Configuring the PE Routers to Support the EIGRP MPLS VPN

## Basic BGP Configuration

The BGP configuration provided in this section includes the minimum required elements necessary to configure this feature. Steps 11 through 13 will need to be repeated on a per EIGRP VRF basis if multiple EIGRP VRFs need to be configured.

## Prerequisites

Before this feature can be configured, MPLS and CEF must be enabled in the BGP network, and multiprotocol BGP must be enabled on all PE routers that provide VPN services to CE routers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **no synchronization**
5. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
6. **neighbor** *ip-address* **update-source** **loopback** *interface-number*
7. **address-family** **vpn4**
8. **neighbor** *ip-address* **activate**
9. **neighbor** *ip-address* **send-community** **extended**
10. **exit-address-family**
11. **address-family** **ipv4** **vrf** *vrf-name*
12. **redistribute** **eigrp** *autonomous-system-number*
13. **no synchronization**
14. **exit-address-family**
15. **end**

## DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|         | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3  | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 10                                                             | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                                                                    |
| Step 4  | <b>no synchronization</b><br><br><b>Example:</b><br>Router(config-router)# no synchronization                                                                         | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                                                                                                                      |
| Step 5  | <b>neighbor ip-address remote-as</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 remote-as 10                  | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are establishing an iBGP session with the PE router that is connected to the CE router at the other CE site.</li> </ul>                         |
| Step 6  | <b>neighbor ip-address update-source loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 update-source loopback 0 | Configures BGP to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>This configuration step is not required. However, the BGP routing process will be less susceptible to the affects of interface or link flapping.</li> </ul> |
| Step 7  | <b>address-family vpnv4</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                     | Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes, such as BGP, RIP, and static routing sessions.                                                                                                       |
| Step 8  | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1 activate                                                    | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are activating the exchange of VPNv4 routing information between the PE routers.</li> </ul>                                                     |
| Step 9  | <b>neighbor ip-address send-community extended</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1 send-community extended                      | Configures the local router to send extended community attribute information to the specified neighbor. <ul style="list-style-type: none"> <li>This step is required for the exchange of EIGRP extended community attributes.</li> </ul>                                |
| Step 10 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                    | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                           |
| Step 11 | <b>address-family ipv4 vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                           | Configures an IPv4 address-family for the EIGRP VRF. <ul style="list-style-type: none"> <li>An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE routers.</li> </ul>                                                         |



|         | Command or Action                                                                                                                                                                                                  | Purpose                                                                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 12 | <b>redistribute eigrp</b> <i>autonomous-system-number</i><br>[ <b>metric</b> <i>metric-value</i> ] [ <b>route-map</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# redistribute eigrp 101 | Redistributes the EIGRP VRF into BGP. <ul style="list-style-type: none"> <li>The autonomous system number from the CE network is configured in this step.</li> </ul> |
| Step 13 | <b>no synchronization</b><br><br><b>Example:</b><br>Router(config-router-af)# no synchronization                                                                                                                   | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                   |
| Step 14 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                                                 | Exits address family configuration mode and enters router configuration mode.                                                                                        |
| Step 15 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                                                    | Exits address family configuration mode and enters privileged EXEC mode.                                                                                             |

## Verifying the VPN Configuration

A route distinguisher must be configured for the VRF, and MPLS must be configured on the interfaces that carry the VRF. Use the **show ip vrf** command to verify the route distinguisher (RD) and interface that are configured for the VRF.

### SUMMARY STEPS

1. **show ip vrf**

### DETAILED STEPS

|        | Command or Action                                                | Purpose                                                                                                                                                                                              |
|--------|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>show ip vrf</b><br><br><b>Example:</b><br>Router> show ip vrf | Displays the set of defined VRF instances and associated interfaces. <ul style="list-style-type: none"> <li>The output also maps the VRF instances to the configured route distinguisher.</li> </ul> |

## Verifying PE-to-PE Connectivity

Perform this task to verify PE-to-PE connectivity in the service provider network.

### SUMMARY STEPS

1. **enable**
2. **ping** *ip-address*
3. **show ip route vrf** *vrf-name*
4. **show ip cef vrf** *vrf-name*

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> <b>Note</b> The <b>ping</b> command can be issued only from privileged EXEC mode. The other commands in this table can be issued from both user EXEC and privileged EXEC mode.                                                     |
| Step 1 | <b>ping</b> <i>ip-address</i><br><br><b>Example:</b><br>Router# ping 172.16.0.1                                                                                                                                                                                                                                                                                                                                                                                                                              | The <b>ping</b> command can be used to verify PE to PE connectivity within the service provider network. <ul style="list-style-type: none"> <li>• If a PE router cannot be reached with the <b>ping</b> command, use the commands in the following steps to isolate the problem.</li> </ul>                                                           |
| Step 2 | <b>show ip route vrf</b> <i>vrf-name</i> [ <b>connected</b> ] [ <b>protocol</b> [ <i>as-number</i> ] [ <i>tag</i> ] [ <i>output-modifiers</i> ]] [ <i>ip-prefix</i> ] [ <b>list number</b> [ <i>output-modifiers</i> ]] [ <b>profile</b> ] [ <b>static</b> [ <i>output-modifiers</i> ]] [ <b>summary</b> [ <i>output-modifiers</i> ]] [ <b>supernets-only</b> [ <i>output-modifiers</i> ]] [ <b>traffic-engineering</b> [ <i>output-modifiers</i> ]]<br><br><b>Example:</b><br>Router# show ip route vrf RED | Displays the IP routing table associated with a VRF instance. <ul style="list-style-type: none"> <li>• The <b>show ip route vrf</b> command is used to verify that the VRF is in the routing table. If the VRF is in the routing table but the PE router still cannot be reached with the <b>ping</b> command, proceed to the next step.</li> </ul>   |
| Step 3 | <b>show ip cef</b> [ <i>vrf vrf-name</i> ] [[ <b>unresolved</b> [ <i>detail</i> ]]   [ <i>detail</i>   <b>summary</b> ]]<br><br><b>Example:</b><br>Router# show ip cef vrf RED                                                                                                                                                                                                                                                                                                                               | Displays the CEF forwarding table associated with a VRF instance. <ul style="list-style-type: none"> <li>• The <b>show ip cef vrf</b> command is used to verify that the interfaces and networks associated with the VRF are not in the global CEF database. If the VRF route is in the global CEF table, deconfigure and reconfigure CEF.</li> </ul> |

## Verifying EIGRP VRF Configuration

Use the following steps to verify EIGRP VRF configuration.

### SUMMARY STEPS

1. **enable**
1. **show ip eigrp vrf vrf-name topology**
2. **show ip bgp vpnv4 vrf vrf-name**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                    |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                           |
| Step 1 | <b>show ip eigrp vrf vrf-name topology</b><br><br><b>Example:</b><br>Router# show ip eigrp vrf RED topology                                                                                                                                                                                                                                                                                                                                             | The <b>show ip eigrp vrf</b> command verifies that the correct VRF routes are in the EIGRP topology table. <ul style="list-style-type: none"> <li>If the VRF route is not in the EIGRP topology table, proceed to the next step.</li> </ul>                                                |
| Step 1 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [ip-prefix/length] [[longer-prefixes] [output-modifiers]] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [tags]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 vrf RED | Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>The <b>show ip bgp vpnv4</b> command is used to verify that the route is in the BGP VRF table. If the VRF route is not in the BGP VRF, reconfigure the VRF and route distinguisher.</li> </ul> |

## Configuration Examples for the EIGRP MPLS VPN

- [EIGRP MPLS VPN Configuration Example, page 406](#)
- [BGP Network Configuration Example, page 406](#)
- [EIGRP Redistribution Example, page 406](#)
- [EIGRP MPLS VPN Verification Examples, page 406](#)

## EIGRP MPLS VPN Configuration Example

The following configuration example in global configuration mode creates a VRF named RED and associates it with an interface:

```
ip vrf RED
 rd 100:1
 route-target both 100:1
 exit
interface FastEthernet 0/0
 ip vrf forwarding RED
 ip address 10.0.0.1 255.255.255.0
 end
```

## BGP Network Configuration Example

The following configuration example shows the minimum BGP configuration required on the PE routers to support the EIGRP MPLS VPN:

```
router bgp 10
 no synchronization
 neighbor 10.0.0.1 remote-as 10
 neighbor 10.0.0.1 update-source loopback 0
 address-family vpnv4
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-community extended
 exit-address-family
 address-family ipv4 vrf RED
 redistribute eigrp 101
 no synchronization
 exit-address-family
```

## EIGRP Redistribution Example

The following configuration example configures EIGRP redistribution through the MPLS VPN over the BGP core network:

```
router eigrp 1
 address-family ipv4 vrf RED
 network 172.16.0.0 0.0.255.255
 redistribute bgp 10 metric 10000 100 255 1 1500
 autonomous-system 101
 exit-address-family
```

## EIGRP MPLS VPN Verification Examples

The examples in the following section show how to verify the configuration of the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature:

- [Verifying Route Distinguisher and MPLS Configuration Example, page 407](#)
- [Verifying PE-to-PE Connectivity Example, page 407](#)
- [Verifying EIGRP VRF Configuration Example, page 409](#)

## Verifying Route Distinguisher and MPLS Configuration Example

A route distinguisher must be configured for the VRF, and MPLS must be configured on the interfaces that carry the VRF.

Use the **show ip vrf** command to verify the route distinguisher (RD) and interface that are configured for the VRF. The VRF name, RD, and configured interface are displayed in the output. The following sample output is similar to the output that will be displayed when the **show ip vrf** command is issued:

```
Router# show ip vrf
```

| Name   | Default RD | Interfaces  |
|--------|------------|-------------|
| BLUE   | 120:1      |             |
| PINK   | 130:1      | Ethernet3/0 |
| RED    | 100:1      |             |
| YELLOW | 110:1      | Serial12/0  |

Use the **show ip eigrp vrf interfaces** command to display and verify specific information about VRFs configured under EIGRP. The interface to VRF mapping that is displayed in the output of this command should match the mapping that is displayed for the **show ip vrf** command. The following sample output is similar to the output that will be displayed when the **show ip eigrp vrf interfaces** command is issued:

```
Router# show ip eigrp vrf PINK interfaces
```

```
IP-EIGRP interfaces for process 1
      Xmit Queue  Mean   Pacing Time   Multicast   Pending
Interface    Peers Un/Reliable  SRTT  Un/Reliable   Flow Timer  Routes
Et3/0         1      0/0         131      0/10         528        0
```

Use the **show mpls interfaces** command to verify that MPLS is configured for interfaces that need to carry any configured VRFs. The following sample output is similar to the output that will be displayed when the **show mpls interfaces** command is issued:

```
Router# show mpls interfaces
```

| Interface   | IP        | Tunnel | Operational |
|-------------|-----------|--------|-------------|
| Ethernet2/0 | Yes (tdp) | No     | Yes         |

## Verifying PE-to-PE Connectivity Example

The **ping** command can be used to verify PE-to-PE connectivity within the service provider network. If a PE router cannot be reached with the **ping** command, use the following steps to isolate the problem:

- Step 1** Verify that the VRF is in the routing table with the **show ip route vrf vrf-name** command.

```
Router# show ip route vrf PINK
```

```
Routing Table:PINK
Codes:C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
D       172.16.17.0 [90/409600] via 10.10.10.2, 1d15h, Ethernet3/0
      10.0.0.0/24 is subnetted, 1 subnets
```

```

C      10.10.10.0 is directly connected, Ethernet3/0
      10.19.0.0/24 is subnetted, 1 subnets
D      10.19.19.0 [90/409600] via 10.10.10.2, 1d15h, Ethernet3/0
      192.168.0.0/24 is subnetted, 1 subnets
B      192.168.10.0 [200/0] via 10.14.14.14, 1d15h

```

- Step 2** If the VRF is in the routing table but the PE router still cannot be reached with the **ping** command, verify that the VRF is in the CEF table with the **show ip cef vrf vrf-name** command.

```

Router# show ip cef vrf PINK
Prefix                Next Hop                Interface
0.0.0.0/0             drop                    Null0 (default route handler
entry)
0.0.0.0/32            receive
172.16.17.0/24        10.10.10.2             Ethernet3/0
10.19.19.0/24         10.10.10.2             Ethernet3/0
10.10.10.0/24         attached               Ethernet3/0
10.10.10.0/32         receive
10.10.10.1/32         receive
10.10.10.2/32         10.10.10.2             Ethernet3/0
10.10.10.255/32       receive
172.16.10.0/24        10.22.10.1             Ethernet2/0
224.0.0.0/24          receive
255.255.255.255/32   receive

```

- Step 3** If the VRF is in the CEF table but the PE router still cannot be reached with the **ping** command, verify that the interfaces and networks associated with the VRF are not in the global CEF database with the **show ip cef** command.

```

Router# show ip cef
Prefix                Next Hop                Interface
0.0.0.0/0             drop                    Null0 (default route handler
entry)
0.0.0.0/32            receive
10.14.14.14/32        10.22.10.1             Ethernet2/0
10.15.15.15/32        receive
10.16.16.16/32        10.22.10.1             Ethernet2/0
172.16.17.17/32       10.22.10.1             Ethernet2/0
10.22.10.0/24         attached               Ethernet2/0
10.22.10.0/32         receive
10.22.10.1/32         10.22.10.1             Ethernet2/0
10.22.10.2/32         receive
10.22.10.255/32       receive
10.23.10.0/24         10.22.10.1             Ethernet2/0
224.0.0.0/4           drop
224.0.0.0/24          receive
255.255.255.255/32   receive

```

---

If the VRF route is in the global CEF table, deconfigure and reconfigure CEF.

## Verifying EIGRP VRF Configuration Example

To verify EIGRP VRF configuration, perform the following steps:

- Step 1** Use the **show ip eigrp vrf vrf-name topology** command to verify that the correct VRF route is in the EIGRP topology table.

```
Router# show ip eigrp vrf PINK topology
IP-EIGRP Topology Table for AS(1)/ID(10.10.10.1) Routing Table:PINK

Codes:P - Passive, A - Active, U - Update, Q - Query, R - Reply,
      r - reply Status, s - sia Status

P 172.16.17.0/24, 1 successors, FD is 409600
    via 10.10.10.2 (409600/128256), Ethernet3/0
P 10.19.19.0/24, 1 successors, FD is 409600
    via 10.10.10.2 (409600/128256), Ethernet3/0
P 10.10.10.0/24, 1 successors, FD is 281600
    via Connected, Ethernet3/0
P 172.16.10.0/24, 1 successors, FD is 281600
    via Redistributed (281600/0)
```

- Step 2** If the VRF route is not in the EIGRP topology table, verify that the route is in the BGP VRF table with the **show ip bgp vpnv4 vrf vrf-name** command.

```
Router# show ip bgp vpnv4 vrf PINK
BGP table version is 17, local router ID is 10.15.15.15
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
Route Distinguisher:130:1 (default for vrf PINK)
*> 172.16.17.0/24    10.10.10.2             409600             32768 ?
*> 10.19.19.0/24     10.10.10.2             409600             32768 ?
*> 10.10.10.0/24     0.0.0.0                 0                 32768 ?
*>i172.16.10.0/24    10.14.14.14             0                100              0 ?
```

## Where to Go Next

For more information about the BGP Cost Community feature, refer to the BGP Cost Community feature documentation in Cisco IOS Release 12.0(27)S.

For more information about the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature, refer to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature documentation in Cisco IOS Release 12.0(27)S.

## Additional References

For additional information related to the MPLS VPN support for EIGRP between Provider Edge (PE) and Customer (CE) feature, refer to the following references:

- [Related Documents, page 410](#)
- [Standards, page 410](#)
- [MIBs, page 410](#)
- [RFCs, page 411](#)
- [Technical Assistance, page 411](#)

## Related Documents

| Related Topic             | Document Title                                                                                 |
|---------------------------|------------------------------------------------------------------------------------------------|
| BGP Cost Community        | <a href="#">BGP Cost Community, Cisco IOS Release 12.0(27)S</a>                                |
| CEF commands              | <a href="#">Cisco IOS Switching Services Configuration Guide, Release 12.3</a>                 |
| CEF configuration tasks   | <a href="#">Cisco IOS Switching Services Command Reference, Release 12.3</a>                   |
| EIGRP commands            | <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3</a> |
| EIGRP configuration tasks | <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a>                                 |
| EIGRP Site of Origin      | <a href="#">EIGRP MPLS VPN PE-CE Site of Origin (SoO), Cisco IOS Release 12.0(27)S.</a>        |
| MPLS VPNs                 | <a href="#">MPLS Virtual Private Networks, Cisco IOS Release 12.0(5)T</a>                      |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |



## RFCs

| RFCs     | Title                                                             |
|----------|-------------------------------------------------------------------|
| RFC 1163 | <i>A Border Gateway Protocol</i>                                  |
| RFC 1164 | <i>Application of the Border Gateway Protocol in the Internet</i> |
| RFC 2283 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                              |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **address-family ipv4 (EIGRP)**
- **autonomous-system (EIGRP)**
- **clear ip eigrp vrf neighbor**
- **default-metric (EIGRP)**
- **exit-address-family**
- **ip vrf**
- **network (EIGRP)**
- **rd**
- **redistribute (IP)**
- **show ip eigrp vrf interfaces**
- **show ip eigrp vrf neighbors**
- **show ip eigrp vrf topology**
- **show ip eigrp vrf traffic**
- **show ip protocols vrf**
- **show ip route vrf**
- **show ip vrf**





## EIGRP MPLS VPN PE-CE Site of Origin (SoO)

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces the capability to filter Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic on a per-site basis for Enhanced Interior Gateway Routing Protocol (EIGRP) networks. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent transient routing loops from occurring in complex and mixed network topologies. This feature is designed to support the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature. Support for back door links is provided by this feature when Cisco IOS Release 12.0(27)S is installed to PE routers that support EIGRP MPLS VPNs.

### Feature History for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(27)S   | This feature was introduced.                                    |
| 12.3(8)T    | This feature was integrated into Cisco IOS Release 12.3(8)T.    |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin \(SoO\), page 414](#)
- [Restrictions for EIGRP MPLS VPN PE-CE Site of Origin \(SoO\), page 414](#)
- [Information About EIGRP MPLS VPN PE-CE Site of Origin \(SoO\), page 414](#)
- [How to Configure EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support, page 417](#)
- [Additional References, page 422](#)
- [Command Reference, page 423](#)

## Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

This document assumes that Border Gateway Protocol (BGP) is configured in the network core (or the service provider backbone). The following tasks will also need to be completed before you can configure this feature:

- This feature was introduced to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature and should be configured after the EIGRP MPLS VPN is created.
- All PE routers that are configured to support the EIGRP MPLS VPN must run Cisco IOS Release 12.0(27)S, which provides support for the SoO extended community.

## Restrictions for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

- If a VPN site is partitioned and the SoO extended community attribute is configured on a back door router interface, the back door link cannot be used as an alternate path to reach prefixes originated in other partition of the same site.
- A unique SoO value must be configured for each individual VPN site. The same value must be configured on all PE and CE interfaces (if SoO is configured on the CE routers) that support the same VPN site.

## Information About EIGRP MPLS VPN PE-CE Site of Origin (SoO)

To configure this feature, you must understand the following concepts:

- [EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support Overview, page 414](#)
- [Site of Origin \(SoO\) Support for Back Door Links, page 415](#)
- [Router Interoperation with the Site of Origin \(SoO\) Extended Community, page 415](#)
- [Redistributing BGP VPN Routes that Carry the Site of Origin \(SoO\) into EIGRP, page 416](#)
- [BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies, page 416](#)
- [Benefits of the EIGRP MPLS VPN PE-CE Site of Origin \(SoO\) Support Feature, page 417](#)

## EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Overview

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature provides support for the MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE) feature, which provides the capability to create MPLS VPN networks that connect separate EIGRP VPN sites.

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces SoO support for EIGRP-to-BGP and BGP-to-EIGRP redistribution. The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a PE router has learned a route. SoO support provides the capability to filter MPLS VPN traffic on a per-EIGRP site basis. SoO filtering is configured at the interface level and is used to manage MPLS VPN traffic and to prevent routing loops from occurring in complex and mixed network topologies, such as EIGRP VPN sites that contain both VPN and back door links.

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface with the **ip vrf sitemap** command. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.

## Site of Origin (SoO) Support for Back Door Links

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces support for back door links. A back door link or a route is a connection that is configured outside of the VPN between a remote and main site, for example, a WAN leased line that connects a remote site to the corporate network. Back door links are typically used as back up routes between EIGRP sites if the VPN link is down or not available. A metric is set on the back door link so that the route through the back door router is not selected unless there is a VPN link failure.

The SoO extended community is defined on the interface of the back door router. It identifies the local site-ID, which should match the value that is used on the PE routers that support the same site. When the back door router receives an EIGRP update (or reply) from a neighbor across the back door link, the router checks the update for a SoO value. If the SoO value in the EIGRP update matches the SoO value on the local back door interface, the route is rejected and not installed to the EIGRP topology table. This typically occurs when the route with the local SoO valued in the received EIGRP update was learned by the other VPN site and then advertised through the back door link by the back door router in the other VPN site. SoO filtering on the back door link prevents transient routing loops from occurring by filtering out EIGRP updates that contain routes that carry the local site-ID.



### Note

If a VPN site is partitioned and the SoO extended community attribute is configured on a back door router interface, the back door link cannot be used as an alternate path to reach prefixes originated in other partition of the same site.

If this feature is enabled on the PE routers and the back door routers in the customer sites, and SoO values are defined on both the PE and back door routers, both the PE and back door routers will support convergence between the VPN sites. The other routers in the customer sites need only propagate the SoO values carried by the routes, as the routes are forwarded to neighbors. These routers do not otherwise affect or support convergence beyond normal DUAL computations.

## Router Interoperation with the Site of Origin (SoO) Extended Community

The configuration of the SoO extended community allows routers that support this feature to identify the site from which each route originated. When this feature is enabled, the EIGRP routing process on the PE or CE router checks each received route for the SoO extended community and filters based on the following conditions:

- A received route from BGP or a CE router contains a SoO value that matches the SoO value on the receiving interface.

If a route is received with an associated SoO value that matches the SoO value that is configured on the receiving interface, the route is filtered out because it was learned from another PE router or from a back door link. This behavior is designed to prevent routing loops.

- A received route from a CE router is configured with a SoO value that does not match.  
If a route is received with an associated SoO value that does not match the SoO value that is configured on the receiving interface, the route is accepted into the EIGRP topology table so that it can be redistributed into BGP.  
If the route is already installed to the EIGRP topology table but is associated with a different SoO value, the SoO value from the topology table will be used when the route is redistributed into BGP.
- A received route from a CE router does not contain a SoO value.  
If a route is received without a SoO value, the route is accepted into the EIGRP topology table, and the SoO value from the interface that is used to reach the next hop CE router is appended to the route before it is redistributed into BGP.

When BGP and EIGRP peers that support the SoO extended community receive these routes, they will also receive the associated SoO values and pass them to other BGP and EIGRP peers that support the SoO extended community. This filtering is designed to prevent transient routes from being relearned from the originating site, which prevents transient routing loops from occurring.

## Redistributing BGP VPN Routes that Carry the Site of Origin (SoO) into EIGRP

When an EIGRP routing process on the PE router redistributes BGP VPN routes into the EIGRP topology table, EIGRP extracts the SoO value (if one is present) from the appended BGP extended community attributes and appends the SoO value to the route before installing it to the EIGRP topology table. EIGRP tests the SoO value for each route before sending updates to CE routers. Routes that are associated with SoO values that match the SoO value configured on the interface are filtered out before they are passed to the CE routers. When an EIGRP routing process receives routes that are associated with different SoO values, the SoO value is passed to the CE router and carried through the CE site.

## BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies

The BGP cost community is a non-transitive extended community attribute that is passed to internal BGP (iBGP) and confederation peers but not external BGP (eBGP) peers. The cost community feature allows you to customize the local route preference and influence the BGP best path selection process.

Before EIGRP SoO BGP Cost Community support was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Back door links in an EIGRP MPLS VPN topology were preferred by BGP when the back door link was learned first. (A back door link or a route is a connection that is configured outside of the VPN between a remote and main site, for example, a WAN leased line that connects a remote site to the corporate network).

The “pre-bestpath” point of insertion (POI) has been introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and back door links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-bestpath” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when Cisco IOS Release 12.0(27)S is installed to the PE routers or the CE and back door router at the customer sites.

For more information about the BGP Cost Community feature, refer to the BGP Cost Community feature documentation in Cisco IOS Release 12.0(27)S.

## Benefits of the EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support Feature

The configuration of the EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support feature introduces per-site VPN filtering, which improves support for complex topologies, such as, MPLS VPNs with back door links, Customer Edge (CE) routers that are dual-homed to different Provider Edge (PE) routers, and PE routers that support CE routers from different sites within the same Virtual Routing and Forwarding (VRF) instance.

## How to Configure EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support

This section contains the following procedures:

- [Configuring the Site of Origin \(SoO\) Extended Community, page 417](#)
- [Verifying the Configuration of the SoO Extended Community, page 420](#)

## Configuring the Site of Origin (SoO) Extended Community

The configuration of the SoO extended community allows MPLS VPN traffic to be filtered on a per-site basis. The SoO extended community is configured in an inbound BGP route map on the PE router and is applied to the interface with the **ip vrf sitemap** command. The SoO extended community can be applied to all exit points at the customer site for more specific filtering but must be configured on all interfaces of PE routers that provide VPN services to CE routers.

### Prerequisites

- This feature was introduced to support the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature and should be configured afterwards.
- All PE routers that are configured to support the EIGRP MPLS VPN must support the SoO extended community.
- A unique SoO value must be configured for each VPN site. The same value must be used on the interface of the PE router that connects to the CE router for each VPN site.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-name* {**permit** | **deny**}[*sequence-number*]
4. **set extcommunity** {**rt** *extended-community-value* [**additive**] | **soo** *extended-community-value*}
5. **exit**
6. **interface** *interface-type*
7. **ip vrf forwarding** *vrf-name*
8. **ip vrf sitemap** *route-map-name*
9. **ip address** *ip-address subnet-mask*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                          | Enters global configuration mode.                                                                                                                                                                  |
| Step 3 | <b>route-map</b> <i>map-name</i> { <b>permit</b>   <b>deny</b> }[ <i>sequence-number</i> ]<br><br><b>Example:</b><br>Router(config)# route-map Site-of-Origin permit 10 | Enters route map configuration mode and creates a route map. <ul style="list-style-type: none"> <li>The route map is created in this step so that SoO extended community can be applied</li> </ul> |



|         | Command or Action                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <p><b>set extcommunity</b> {<b>rt</b> <i>extended-community-value</i> [<b>additive</b>]   <b>soo</b> <i>extended-community-value</i>}</p> <p><b>Example:</b><br/>Router(config-route-map)# set extcommunity soo 100:1</p> | <p>Sets BGP extended community attributes.</p> <ul style="list-style-type: none"> <li>The <b>rt</b> keyword specifies the route target extended community attribute.</li> <li>The <b>soo</b> keyword specifies the site of origin extended community attribute.</li> <li>The <i>extended-community-value</i> argument specifies the value to be set. The value can be one of the following formats: <ul style="list-style-type: none"> <li>autonomous-system-number : network-number</li> <li>ip-address : network-number</li> </ul> </li> </ul> <p>The colon is used to separate the autonomous system number and network number or IP address and network number.</p> <ul style="list-style-type: none"> <li>The <b>additive</b> keyword adds a route target to the existing route target list without replacing any existing route targets.</li> </ul> |
| Step 5  | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-route-map)# exit</p>                                                                                                                                              | Exits route-map configuration mode and enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6  | <p><b>interface</b> <i>interface-type</i></p> <p><b>Example:</b><br/>Router(config)# interface FastEthernet 0/0</p>                                                                                                       | Enters interface configuration mode to configure the specified interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 7  | <p><b>ip vrf forwarding</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config-if)# ip vrf forwarding RED</p>                                                                                                       | <p>Associates the VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The VRF name configured in this step should match the VRF name created for the EIGRP MPLS VPN with the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge feature.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 8  | <p><b>ip vrf sitemap</b> <i>route-map-name</i></p> <p><b>Example:</b><br/>Router(config-if)# ip vrf sitemap Site-of-Origin</p>                                                                                            | <p>Associates the VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The route map name configured in this step should match the route map name created to apply the SoO extended community in step 3.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 9  | <p><b>ip address</b> <i>ip-address subnet-mask</i></p> <p><b>Example:</b><br/>Router(config-if)# ip address 10.0.0.1 255.255.255.255</p>                                                                                  | <p>Configures the IP address for the interface.</p> <ul style="list-style-type: none"> <li>The IP address needs to be reconfigured after enabling VRF forwarding.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 10 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                       | Exits interface configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Examples

The following example, beginning in global configuration mode, configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

## What to Do Next

- To verify the configuration of the SoO extended community, follow the steps in the next section, “Verifying the Configuration of the SoO Extended Community.”
- For mixed EIGRP MPLS VPN network topologies that contain back door routes, the next task is to configure the “pre-bestpath” cost community for back door routes.

## Verifying the Configuration of the SoO Extended Community

Use the following steps to verify the configuration of the SoO extended community attribute.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** { all | rd *route-distinguisher* | vrf *vrf-name* } [*ip-prefix/length* [longer-prefixes] [*output-modifiers*]] [*network-address* [*mask*] [longer-prefixes] [*output-modifiers*]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [*line*]] [peer-group] [quote-regexp] [regexp] [summary] [tags]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                         |
| Step 2 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [ip-prefix/length] [longer-prefixes] [output-modifiers] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [tags]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all 10.0.0.1 | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>show ip bgp vpnv4</b> command with the <b>all</b> keyword to verify that the specified route has been configured with the SoO extended community attribute.</li> </ul> |

## Examples

This example shows VPN address information from the BGP table and verifies the configuration of the SoO extended community:

```
Router# show ip bgp vpnv4 all 10.0.0.1
BGP routing table entry for 100:1:10.0.0.1/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  100 300
    192.168.0.2 from 192.168.0.2 (172.16.13.13)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: SOO:100:1
```

## Where to Go Next

For information about configuring EIGRP MPLS VPNs, refer to the MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge document in Cisco IOS Release 12.0(27)S.

For more information about configuring the BGP cost community, refer to the BGP Cost Community document in Cisco IOS Release 12.0(27)S.

## Additional References

The following sections provide references related to the EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature.

### Related Documents

| Related Topic                                                        | Document Title                                                                                                   |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| BGP Cost Community feature and the “pre-bestpath” point of insertion | <a href="#">BGP Cost Community, Release 12.0(27)S</a>                                                            |
| CEF commands                                                         | <a href="#">Cisco IOS Switching Services Configuration Guide, Release 12.3</a>                                   |
| CEF configuration tasks                                              | <a href="#">Cisco IOS Switching Services Command Reference, Release 12.3</a>                                     |
| EIGRP commands                                                       | <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3</a>                   |
| EIGRP configuration tasks                                            | <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a>                                                   |
| EIGRP MPLS VPNs                                                      | <a href="#">MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge, Cisco IOS Release 12.0(27)S.</a> |
| MPLS VPNs                                                            | <a href="#">MPLS Virtual Private Networks, Cisco IOS Release 12.0(5)T</a>                                        |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

### RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **ip vrf sitemap**

# Glossary

**AFI**—Address Family Identifier. Carries the identity of the network layer protocol that is associated with the network address.

**Back door Router**—a router that connects two or more sites, which are also connected to each other through an MPLS VPN EIGRP PE to CE links.

**Back door link**—a link connecting two back door routers.

**BGP**—Border Gateway Protocol. An interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined by RFC 1163, *A Border Gateway Protocol (BGP)*. The current implementation of BGP is BGP Version 4 (BGP4). BGP4 is the predominant interdomain routing protocol that is used on the Internet. It supports CIDR and uses route aggregation mechanisms to reduce the size of routing tables.

**Cost Community**—an extended community attribute that can be inserted anywhere into the bestpath calculation.

**Customer Edge (CE) router**—a router that belongs to a customer network, which connects to a Provider Edge (PE) router to utilize MPLS VPN network services.

**MBGP**—multiprotocol BGP. An enhanced version of BGP that carries routing information for multiple network layer protocols and IP multicast routes. It is defined in RFC 2858, *Multiprotocol Extensions for BGP-4*.

**Provider Edge (PE) router**—the PE router is the entry point into the Service Provider network. The PE router is typically deployed on the edge of the network and is administered by the Service Provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

**Site**—a collection of routers that have well-defined exit points to other “sites.”

**Site of Origin (SoO)**—a special purpose tag or attribute that identifies the site that injects a route into the network. This attribute is used for intersite filtering in MPLS VPN PE-to-CE topologies.

**VPN**—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.



## EIGRP Route Map Support

---

The EIGRP Route Map Support feature enables Enhanced Interior Gateway Routing Protocol (EIGRP) to interoperate with other protocols by filtering inbound and outbound traffic based on complex route map options. EIGRP can process permitted set and match parameters supplied by a route-map facility and extend filtering on added EIGRP-specific set and match choices.

### Feature History for the EIGRP Route Map Support Feature

| Release  | Modification                 |
|----------|------------------------------|
| 12.3(8)T | This feature was introduced. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [How to Configure EIGRP Route Map Support, page 426](#)
- [Configuration Examples for EIGRP Route Map Support, page 429](#)
- [Additional References, page 429](#)
- [Command Reference, page 430](#)

# How to Configure EIGRP Route Map Support

This section contains the following tasks:

- [Configuring EIGRP Metrics, page 426](#) (required)
- [Verifying EIGRP Metrics, page 427](#) (optional)

## Configuring EIGRP Metrics

Perform this task to configure the EIGRP metrics.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag*
4. **match metric** {*metric-value* | **external** [**+-** *deviation-number*]}
5. **match source-protocol** *source-protocol* [*as-number*]
6. **exit**

### DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                |
| Step 3 | <b>route-map</b> <i>map-tag</i><br><br><b>Example:</b><br>Router(config)# route-map abccomp | Enters route-map configuration mode.                                                                             |



|        | Command or Action                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>match metric</b> {<i>metric-value</i>   <b>external</b> [<b>+-</b> <i>deviation-number</i>]}</p> <p><b>Example:</b><br/>Router(config-route-map)# match metric 500 +- 100</p> | <p>Specifies an internal protocol metric associated with a route. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>metric-value</i>—Route metric, which can be an EIGRP five-part metric. The range is from 0 to 4294967295.</li> <li><b>external</b>—External route metric. The range is from 0 to 4294967295.</li> <li><b>+- deviation-number</b>—(Optional) Represents a standard deviation. The deviation can be any number. There is no default.</li> </ul> <p><b>Note</b> When you specify a metric deviation with the <b>+</b> and <b>-</b> keywords, the router will match any metric that falls inclusively in that range.</p> <p><b>Note</b> This command is not the same as the EIGRP assigned route metric, a figure computed from EIGRP vectorized metric components (delay, bandwidth, reliability, load, and MTU).</p> |
| Step 5 | <p><b>match source-protocol</b> <i>source-protocol</i> [<i>as-number</i>]</p> <p><b>Example:</b><br/>Router(config-route-map)# match source-protocol bgp 2</p>                      | <p>Specifies the source protocol for EIGRP. The arguments are as follows:</p> <ul style="list-style-type: none"> <li><i>source-protocol</i>—Protocol to match. The valid keywords are <b>bgp</b>, <b>connected</b>, <b>eigrp</b>, <b>isis</b>, <b>ospf</b>, <b>rip</b>, and <b>static</b>. There is no default.</li> <li><i>as-number</i>—(Optional) Autonomous system number. The AS number is not applicable to the <b>connected</b>, <b>static</b>, and <b>rip</b> keywords. The range is from 1 to 65535. There is no default.</li> </ul>                                                                                                                                                                                                                                                                                                                    |
| Step 6 | <p><b>exit</b></p> <p><b>Example:</b><br/>Router(config-route-map)# exit</p>                                                                                                        | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Verifying EIGRP Metrics

To verify that both the EIGRP metric and the external protocol metrics have been configured, perform the following step.

### SUMMARY STEPS

1. **show ip eigrp topology ip-address**

## DETAILED STEPS

### Step 1 **show ip eigrp topology ip-address**

Use this command to display the *internal* EIGRP metrics for a specified IP address, for example:

```
Router# show ip eigrp topology 10.2.1.0/24
```

```
IP-EIGRP (AS 1): Topology entry for 10.2.1.0/24
```

```
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600 Routing Descriptor
Blocks:
0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0 Composite metric is (281600/0),
Route is Internal
Vector metric: Minimum bandwidth is 10000 Kbit
Total delay is 1000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 0
```

In the following example, the external EIGRP metrics for a specified IP address is displayed:

```
Router# show ip eigrp topology 10.4.80.0/20
```

```
IP-EIGRP (AS 1): Topology entry for 10.4.80.0/20
```

```
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
Routing Descriptor Blocks:
10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
Composite metric is (409600/128256), Route is External
Vector metric:
Minimum bandwidth is 10000 Kbit
Total delay is 6000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
External data:
Originating router is 10.89.245.1
AS number of route is 0
External protocol is Connected, external metric is 0
Administrator tag is 0 (0x00000000)
```

# Configuration Examples for EIGRP Route Map Support

This section contains the following configuration example:

- [EIGRP Route Metric Configuration: Example, page 429](#)

## EIGRP Route Metric Configuration: Example

The following example shows how to configure an EIGRP external metric route with an allowable deviation of 100:

```
route-map acbcomp
match metric external 500 +- 100
match source-protocol bgp 2
```

## Additional References

The following sections provide references related to the EIGRP Route Map Support feature.

## Related Documents

| Related Topic                                                        | Document Title                                                                                    |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| IP routing protocols overview and configuration                      | <a href="#">Cisco IOS IP Configuration Guide, Part 2: IP Routing Protocols</a> , Release 12.3     |
| IP routing commands including syntax, usage guidelines, and examples | <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a> , Release 12.3 T |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **match metric (IP)**
- **match source-protocol**
- **show ip eigrp topology**



# EIGRP Prefix Limit Support

The EIGRP Prefix Limit Support feature introduces the capability to limit the number of prefixes per VRF that are accepted from a specific peer or to limit all prefixes that are accepted by an Enhanced Interior Gateway Routing Protocol (EIGRP) process through peering and/or redistribution. This feature is designed to protect the local router from external misconfiguration that can negatively impact local system resources, for example a peer that is misconfigured to redistribute full Border Gateway Protocol (BGP) routing tables into EIGRP. This feature is enabled under the IPv4 VRF address family and can be configured to support the *MPLS VPN Support for EIGRP Between Provider Edge (PE) and Customer Edge (CE)* feature.

## Feature History for the EIGRP Prefix Limit Support Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(29)S | This feature was introduced.                                  |
| 12.3(14)T | This feature was integrated into Cisco IOS Release 12.3(14)T. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for EIGRP Prefix Limit Support, page 432](#)
- [Restrictions for EIGRP Prefix Limit Support, page 432](#)
- [Information About EIGRP Prefix Limit Support, page 432](#)
- [MPLS VPN Support for EIGRP Between Provider Edge and Customer EdgeHow to Configure the Maximum Prefix Limit, page 434](#)

- [Configuration Examples for Configuring the Maximum Prefix Limit, page 444](#)
- [Additional References, page 445](#)
- [Command Reference, page 447](#)

## Prerequisites for EIGRP Prefix Limit Support

- Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN) services have been configured between the Provider Edge (PE) routers and the Customer Edge (CE) routers at the customer sites.

## Restrictions for EIGRP Prefix Limit Support

- This feature is supported only under the IPv4 VRF address family and can be used only to limit the number of prefixes that are accepted through a VRF.
- A peer that is configured to send too many prefixes or a peer that rapidly advertises and then withdraws prefixes can cause instability in the network. This feature can be configured to automatically reestablish a disabled peering session at the default or user-defined time interval or when the maximum-prefix limit is not exceeded. However, the configuration of this feature alone cannot change or correct a peer that is sending an excessive number of prefixes. If the maximum prefix limit is exceeded, you will need to reconfigure the maximum-prefix limit or reduce the number of prefixes that are sent from the peer.

## Information About EIGRP Prefix Limit Support

To configure the EIGRP Prefix Limit Support feature, you must understand the following concepts:

- [Misconfigured VPN Peers, page 432](#)
- [EIGRP Prefix Limit Support Overview, page 433](#)
- [Warning-Only Mode, page 433](#)
- [Restart, Reset, and Dampening Timers and Counters, page 434](#)
- [Supported Only Under the IPv4 VRF Address Family, page 434](#)

## Misconfigured VPN Peers

In a Multi protocol Label Switching (MPLS) Virtual Private Network (VPN) the number of routes that are permitted in the VPN routing and forwarding instance (VRF) is configured with the **maximum routes** VRF configuration command. However, limiting the number routes permitted in the VPN does not protect the local router from a misconfigured peer that sends an excessive number of routes or prefixes. This type of external misconfiguration can have a negative affect on the local router by consuming all available system resources (CPU and memory) in processing prefix updates. Often, this type of misconfiguration can occur on a peer that is not within the control of the local administrator.

## EIGRP Prefix Limit Support Overview

The EIGRP Prefix Limit Support feature provides the ability to configure a limit on the number of prefixes that are accepted from EIGRP peers and/or learned through redistribution. This feature can be configured on per-peer or per-process basis and can be configured for all peers and processes. This feature is designed to protect the local router from misconfigured external peers by limiting the amount of system resources that can be consumed to process prefix updates.

### Protecting the Router from External Peers

This feature can be configured to protect an individual peering session or protect all peering sessions. When this feature is enabled and the maximum-prefix limit has been exceeded, the router will tear down the peering session, clear all routes that were learned from the peer, and then place the peer in a penalty state for the default or user-defined time period. After the penalty time period expires, normal peering will be reestablished.

### Limiting the Number of Redistributed Prefixes

This feature can be configured to limit the number of prefixes that are accepted into the EIGRP topology table through redistribution from the Routing Information Base (RIB). All sources of redistribution are processed cumulatively. When the maximum-prefix limit is exceeded, all routes learned through redistribution are discarded and redistribution is suspended for the default or user-defined time period. After the penalty time period expires, normal redistribution will occur.

### Protecting the Router at the EIGRP Process Level

This feature can also be configured to protect the router at the EIGRP process level. When this feature is configured at the EIGRP process level, the maximum prefix limit is applied to all peering sessions and to route redistribution. When the maximum-prefix limit is exceeded, all sessions with the remote peers are torn down, all routes learned from remote peers are removed from the topology and routing tables, all routes learned from through redistribution are discarded, and redistribution and peering are suspended for the default or user-defined time period.

## Warning-Only Mode

The EIGRP Prefix Limit Support feature has two modes of operation. This feature can control peering and redistribution per default and user-defined values or this feature can operate in warning-only mode. In warning-only mode the router will monitor the number of prefixes learned through peering and/or redistribution but will not take any action when the maximum prefix limit is exceeded. Warning-only mode is activated only when the **warning-only** keyword is configured for any of the maximum-prefix limit commands. Only syslog messages are generated when this mode of operation is enabled. Syslog messages can be sent to a syslog server or printed in the console. These messages can be buffered or rate limited per standard Cisco IOS system logging configuration options. For more information about system logging in Cisco IOS software, refer to the following document:

- [Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3](#)

## Restart, Reset, and Dampening Timers and Counters

When the maximum-prefix limit is exceeded, peering and/or redistribution is suspended for a default or user-defined time period. If the maximum-prefix limit is exceeded too often, redistribution and/or peering will be suspended until the manual intervention is taken. This feature has 3 user-configurable timers and a dampening timer.

### Restart Timer

The restart timer determines how long the router will wait to form an adjacency or accept redistributed routes from the RIB after the *maximum*-prefix limit has been exceeded. The default restart-time period is 5 minutes.

### Restart Counter

The restart counter determines the number of times a peering session can be automatically reestablished after the peering session has been torn down or after the redistributed routes have been cleared and relearned because the maximum-prefix limit has been exceeded. The default restart-count limit is 3.



#### Warning

---

**After the restart count limit has been crossed, you will need to enter the `clear ip route *` or `clear ip eigrp neighbor` command to restore normal peering and/or redistribution.**

---

### Reset Timer

The reset timer is used to configure the router to reset the restart count to 0 after the default or configured reset-time period has expired. This timer is designed to provide administrator with control over long and medium term accumulated penalties. The default reset-time period is 15 minutes.

### Dampening Mechanism

The dampening mechanism is used to apply an exponential decay penalty to the restart-time period each time the *maximum*-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This mechanism is designed to identify and suppress unstable peers. It is disabled by default.

## Supported Only Under the IPv4 VRF Address Family

This feature is enabled only under the IPv4 VRF address-family. This feature can be configured to control the number prefixes that are accepted from Customer Edge (CE) routers in an EIGRP MPLS VPN. For more information about EIGRP MPLS VPN configuration, refer to the following document:

- [MPLS VPN Support for EIGRP Between Provider Edge and Customer EdgeHow to Configure the Maximum Prefix Limit](#)

This section contains the following tasks:

- [Configuring the Maximum Number of Prefix Accepted from Peering Sessions](#), page 435
- [Configuring the Maximum Number of Prefixes Learned Through Redistribution](#), page 438
- [Configuring the Maximum Prefix Limit for an EIGRP Process](#), page 440
- [Verifying the EIGRP Maximum Prefix Limit Configuration](#), page 443



## Configuring the Maximum Number of Prefix Accepted from Peering Sessions

The maximum-prefix limit can be configured for all peering sessions or individual peering sessions with the **neighbor maximum-prefix (EIGRP)** command. When the maximum-prefix limit is exceeded, the session with the remote peer is torn down and all routes learned from the remote peer are removed from the topology and routing tables. The maximum-prefix limit that can be configured is limited only by the available system resources on the router.

**Note**

In EIGRP, **neighbor** commands have been used traditionally to configure static neighbors. In the context of this feature, however, the **neighbor maximum-prefix** command can be used to configure the maximum-prefix limit for both statically configured and dynamically discovered neighbors.

### Inherited Timer Values

Default or user-defined **restart**, **restart-count**, and **reset-time** values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

### Prerequisites

- VRFs have been created and configured. EIGRP peering is established through the MPLS VPN.

### Restrictions

- This task can be configured only in IPv4 VRF address-family configuration mode.
- When configuring the **neighbor maximum-prefix** command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, the warning-only configuration options can be configured. Session dampening, restart, and reset timers are configured on a global basis.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
5. **neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]
6. **neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>router eigrp as-number</b><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                  | Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>A maximum of 30 EIGRP routing processes can be configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>address-family ipv4 [unicast] vrf vrf-name</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                          | Enters address-family configuration mode and creates a session for the VRF.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 5 | <b>neighbor ip-address maximum-prefix maximum [threshold] [warning-only]</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 10000 80 warning-only | Limits the number of prefixes that are accepted from the specified EIGRP neighbor. <ul style="list-style-type: none"> <li>The example configures a maximum-prefix limit of 10000 for the 10.0.0.1 neighbor and warning messages to be displayed when 80 percent of the limit has been reached.</li> <li>The <i>ip-address</i> argument is configured when applying this command to a single peer.</li> <li>The <i>maximum</i> argument sets the number of prefixes allowed under the address family. The range for this argument is a number from 1 to 4294967295.</li> <li>The <i>threshold</i> argument configures the router to generate syslog warning messages when the specified percentage of the <i>maximum</i>-prefix limit has been exceeded. The prefix percentage number that can be configured for the <i>threshold</i> argument is from 1 to 100. The default threshold is 75 percent.</li> <li>The <b>warning-only</b> keyword configures the router to only generate syslog messages when the <i>maximum</i>-prefix limit is exceeded, instead of terminating the peering session.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <p><b>neighbor maximum-prefix</b> <i>maximum</i> [<i>threshold</i>]<br/> [[<i>dampened</i>][<i>reset-time</i> <i>minutes</i>] [<i>restart</i> <i>minutes</i>]<br/> [<i>restart-count</i> <i>number</i>]   [<i>warning-only</i>]]</p> <p><b>Example:</b><br/> Router(config-router-af)# neighbor<br/> maximum-prefix 10000 80 warning-only</p> | <p>Limits the number of prefixes that are accepted from all EIGRP neighbors.</p> <ul style="list-style-type: none"> <li>• The example configures maximum-prefix limit of 10000 for all neighbors and warning messages to be displayed when 80 percent of the limit has been reached. Because the <b>warning-only</b> keyword is configured, no action will occur.</li> <li>• The <i>maximum</i> argument sets the number of prefixes allowed under the address family. The range for this argument is a number from 1 to 4294967295.</li> <li>• The <i>threshold</i> argument configures the router to generate syslog warning messages when the specified percentage of the <i>maximum-prefix</i> limit has been exceeded. The prefix percentage number that can be configured for the <i>threshold</i> argument is from 1 to 100. The default threshold is 75 percent.</li> <li>• The <b>warning-only</b> keyword configures the router to only generate syslog messages when the <i>maximum-prefix</i> limit is exceeded, instead of terminating the peering session.</li> <li>• The <b>restart</b> keyword configures a time period in which the router will not form adjacencies after the <i>maximum-prefix</i> limit has been exceeded. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.</li> <li>• The <b>restart-count</b> keyword configures the number of times a peering session can automatically be reestablished after the peering session has been torn down because the <i>maximum-prefix</i> limit has been exceeded. The default restart-count limit is 3.</li> <li>• The <b>reset-time</b> keyword configures the router to reset the restart count to 0 after the default or user-defined reset-time period has expired. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.</li> <li>• The <b>dampened</b> keyword configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This function is disabled by default.</li> </ul> |
| Step 7 | <p><b>end</b></p> <p><b>Example:</b><br/> Router(config-router-af)# end</p>                                                                                                                                                                                                                                                                   | <p>Exits address-family configuration mode and enters privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Troubleshooting Tips

If an individual peer or all peers have exceeded the maximum-prefix limit the same number of times as the default or user-defined **restart-count** value, the individual session or all sessions will need to be manually reset with the **clear ip route\*** or **clear ip eigrp neighbor** command before normal peering can be reestablished.

## Configuring the Maximum Number of Prefixes Learned Through Redistribution

The maximum prefix limit can be configured for prefixes learned through redistribution with the **redistribute maximum-prefix (EIGRP)** command. When the maximum-prefix limit is exceeded, all routes learned from the Routing Information Base (RIB) will be discarded and redistribution will be suspended for the default or user-defined time period. The maximum-prefix limit that can be configured for redistributed prefixes is limited only by the available system resources on the router.

## Inherited Timer Values

Default or user-defined **restart**, **restart-count**, and **reset-time** values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

## Prerequisites

VRFs have been created and configured. EIGRP peering is established through the MPLS VPN.

## Restrictions

This task can be configured only in IPv4 VRF address-family configuration mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
5. **redistribute maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>router eigrp as-number</b><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                                                                                              | Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>A maximum of 30 EIGRP routing processes can be configured.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 4 | <b>address-family ipv4 [unicast] vrf vrf-name</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                                                                                                      | Enters address-family configuration mode and creates a session for the VRF.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>redistribute maximum-prefix maximum [threshold] [[dampened] [reset-time minutes] [restart minutes] [restart-count number]   [warning-only]]</b><br><br><b>Example:</b><br>Router(config-router-af)# redistribute maximum-prefix 10000 80 reset-time 10 restart 2 | Limits the number of prefixes redistributed into an EIGRP process. <ul style="list-style-type: none"> <li>The example configures a maximum-prefix limit of 10000 prefixes, warning message to be displayed at 80 percent of the maximum prefix limit, a reset time period of 10 minutes, and a restart time period of 2 minutes.</li> <li>The <i>maximum</i> argument sets the number of prefixes allowed under the address family. The range for this argument is a number from 1 to 4294967295.</li> <li>The <i>threshold</i> argument configures the router to generate syslog warning messages when the specified percentage of the <i>maximum</i>-prefix limit has been exceeded. The prefix percentage number that can be configured for the <i>threshold</i> argument is from 1 to 100. The default threshold is 75 percent.</li> <li>The <b>warning-only</b> keyword configures the router to only generate syslog messages when the <i>maximum</i>-prefix limit is exceeded, instead of suspending redistribution.</li> <li>The <b>restart</b> keyword configures a time period in which the router will not form adjacencies or accept redistributed routes from the RIB after the <i>maximum</i>-prefix limit has been exceeded. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.</li> </ul> |

| Command or Action                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                   | <ul style="list-style-type: none"> <li>• The <b>restart-count</b> keyword configures the number of times a peering session can automatically be reestablished after the peering session has been torn down or after the a redistribute route has been cleared and relearned because the <i>maximum-prefix</i> limit has been exceeded. The default restart-count limit is 3.</li> <li>• The <b>reset-time</b> keyword configures the router to reset the restart count to 0 after the default or user-defined reset-time period has expired. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.</li> <li>• The <b>dampened</b> keyword configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This function is disabled by default.</li> </ul> |
| <b>Step 6</b> <b>end</b><br><br><b>Example:</b><br>Router(config-router-af) # end | Exits address-family configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Troubleshooting Tips

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined **restart-count** value, the **clear ip route \*** or **clear ip eigrp neighbor** command will need to be entered before normal redistribution will occur.

## Configuring the Maximum Prefix Limit for an EIGRP Process

The maximum prefix limit can be configured for an EIGRP process to limit the number prefixes that are accepted from all sources. This task is configured with the **maximum-prefix** command. When the maximum-prefix limit is exceeded, sessions with the remote peers are brought down and all routes learned from remote peers are removed from the topology and routing tables. Also, all routes learned from the RIB are discarded and redistribution is suspended for the default or user-defined time period.

## Inherited Timer Values

Default or user-defined **restart**, **restart-count**, and **reset-time** values for the process-level configuration of this feature, configured with the **maximum-prefix** command, are inherited by the **redistribute maximum-prefix** and **neighbor maximum-prefix** command configurations by default. If a single peer is configured with the **neighbor maximum-prefix** command, a process-level configuration or a configuration that is applied to all neighbors will be inherited.

## Prerequisites

VRFs have been created and configured. EIGRP peering is established through the MPLS VPN.

## Restrictions

This task can be configured only in IPv4 VRF address-family configuration mode.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
5. **maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | [**warning-only**]]
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router eigrp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                                                                                                                                                            | Enters router configuration mode and creates an EIGRP routing process.<br><ul style="list-style-type: none"><li>• A maximum of 30 EIGRP routing processes can be configured.</li></ul>                                                                                                                                                                                   |
| Step 4 | <b>address-family ipv4</b> [ <b>unicast</b> ] <b>vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                                                                                                                                                    | Enters address-family configuration mode and creates a session for the VRF.                                                                                                                                                                                                                                                                                              |
| Step 5 | <b>maximum-prefix</b> <i>maximum</i> [ <i>threshold</i> ] [[ <b>dampened</b> ] [ <b>reset-time</b> <i>minutes</i> ] [ <b>restart</b> <i>minutes</i> ] [ <b>restart-count</b> <i>number</i> ]   [ <b>warning-only</b> ]]<br><br><b>Example:</b><br>Router(config-router-af)# maximum-prefix 10000 80 warning-only reset-time 10 restart 2 | Limits the number of prefixes that are accepted under an address family by an EIGRP process.<br><ul style="list-style-type: none"><li>• The example configures a maximum-prefix limit of 10000 prefixes, warning message to be displayed at 80 percent of the maximum prefix limit, a reset time period of 10 minutes, and a restart time period of 2 minutes.</li></ul> |

| Command or Action                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                    | <ul style="list-style-type: none"> <li>• The <i>maximum</i> argument sets the number of prefixes allowed under the address family. The range for this argument is a number from 1 to 4294967295.</li> <li>• The <i>threshold</i> argument configures the router to generate syslog warning messages when the specified percentage of the <i>maximum</i>-prefix limit has been exceeded. The prefix percentage number that can be configured for the <i>threshold</i> argument is from 1 to 100. The default threshold is 75 percent.</li> <li>• The <b>warning-only</b> keyword configures the router to only generate syslog messages when the <i>maximum</i>-prefix limit is exceeded, instead of terminating the peering session and/or suspending redistribution.</li> <li>• The <b>restart</b> keyword configures a time period in which the router will not form adjacencies or accept redistributed routes from the RIB after the <i>maximum</i>-prefix limit has been exceeded. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default restart-time period is 5 minutes.</li> <li>• The <b>restart-count</b> keyword configures the number of times a peering session can automatically be reestablished after the peering session has been torn down or after the a redistribute route has been cleared and relearned because the <i>maximum</i>-prefix limit has been exceeded. The default restart-count limit is 3.</li> <li>• The <b>reset-time</b> keyword configures the router to reset the restart count to 0 after the default or user-defined reset-time period has expired. The range of values that can be applied with the <i>minutes</i> argument is from 1 to 65535 minutes. The default reset-time period is 15 minutes.</li> <li>• The <b>dampened</b> keyword configures a decay penalty to be applied to the restart-time period each time the maximum-prefix limit is exceeded. The half-life for the decay penalty is 150 percent of the default or user-defined restart-time value in minutes. This function is disabled by default.</li> </ul> |
| <p><b>Step 6</b>    <code>end</code></p> <p><b>Example:</b><br/> Router(config-router-af)# end</p> | <p>Exits address-family configuration mode and enters privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



## Troubleshooting Tips

If the maximum-prefix limit has been exceeded for redistribution the same number of times as the default or user-defined **restart-count** value, the **clear ip route \*** or **clear ip eigrp neighbor** command will need to be entered before normal redistribution will occur.

## Verifying the EIGRP Maximum Prefix Limit Configuration

The configuration and status of route sources and prefix limit timers can be displayed in the output of the **show ip eigrp accounting** or **show ip eigrp vrf accounting** Exec commands.



### Note

Connected and summary routes are not listed individually in the output from these **show** commands but are counted in the total aggregate count per process.

### SUMMARY STEPS

1. **enable**
2. **show ip eigrp accounting** [*as-number*]
3. **show ip eigrp vrf** {*vrf-name* | \*}**accounting** [*as-number*]

### DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show ip eigrp accounting</b> [ <i>as-number</i> ]<br><br><b>Example:</b><br>Router# show ip eigrp accounting                                               | Displays prefix accounting information for EIGRP processes.                                                           |
| Step 3 | <b>show ip eigrp vrf</b> { <i>vrf-name</i>   *} <b>accounting</b> [ <i>as-number</i> ]<br><br><b>Example:</b><br>Router# show ip eigrp vrf RED accounting 100 | Displays prefix accounting information for EIGRP VRFs.                                                                |

## Example

The following is sample output from the **show ip eigrp vrf accounting** command.

```
Router# show ip eigrp vrf RED accounting
IP-EIGRP accounting for AS(100)/ID(10.0.2.1) Routing Table: RED
Total Prefix Count: 4 States: A-Adjacency, P-Pending, D-Down
State Address/Source Interface Prefix Restart Restart/
Count Count Reset(s)
P Redistributed ---- 0 3 211
A 10.0.1.2 Et0/0 2 0 84
P 10.0.2.4 Se2/0 0 2 114
D 10.0.1.3 Et0/0 0 3 0
```

## Configuration Examples for Configuring the Maximum Prefix Limit

The following examples show how to configure this feature:

- [Configuring the Maximum Prefix Limit for a Single Peer: Example, page 444](#)
- [Configuring the Maximum Prefix Limit for All Peers: Example, page 444](#)
- [Configuring the Maximum Prefix Limit for Redistributed Routes: Example, page 445](#)
- [Configuring the Maximum Prefix Limit for an EIGRP Process: Example, page 445](#)

### Configuring the Maximum Prefix Limit for a Single Peer: Example

The following example, starting in global configuration mode, configures the maximum prefix limit for a single peer. The maximum limit is set to 1000 prefixes, and the warning threshold is set to 80 percent. When the maximum prefix limit is exceeded, the session with this peer will be torn down, all routes learned from this peer will be removed from the topology and routing tables, and this peer will be placed in a penalty state for 5 minutes (default penalty value).

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# end
```

### Configuring the Maximum Prefix Limit for All Peers: Example

The following example, starting in global configuration mode, configures the maximum prefix limit for all peers. The maximum limit is set to 10000 prefixes, the warning threshold is set to 90 percent, the restart timer is set to 4 minutes, a decay penalty is configured for the restart timer with the **dampened** keyword, and all timers are configured to be reset to 0 every 60 minutes. When the maximum prefix limit is exceeded, all peering sessions will be torn down, all routes learned from all peers will be removed from the topology and routing tables, and all peers will be placed in a penalty state for 4 minutes (user-defined penalty value). A dampening exponential decay penalty will also be applied.

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60 restart4
Router(config-router-af)# end
```

## Configuring the Maximum Prefix Limit for Redistributed Routes: Example

The following example, starting in global configuration mode, configures the maximum prefix limit for routes learned through redistribution. The maximum limit is set to 5000 prefixes and the warning threshold is set to 95percent. When the number of prefixes learned through redistribution reaches 4750 (95 percent of 5000), warning messages will be displayed in the console. Because the **warning-only** keyword is configured, the topology and routing tables will not be cleared and route redistribution will not be placed in a penalty state.

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af)# end
```

## Configuring the Maximum Prefix Limit for an EIGRP Process: Example

The following example, starting in global configuration mode, configures the maximum prefix limit for an EIGRP process, which includes routes learned through redistribution and routes learned through EIGRP peering sessions. The maximum limit is set to 50000 prefixes. When the number of prefixes learned through redistribution reaches 37500 (75 percent of 50000), warning messages will be displayed in the console. When the maximum prefix limit is exceeded, all peering sessions will be reset, the topology and routing tables will be cleared and redistributed routes and all peering sessions will be placed in a penalty state.

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf RED
Router(config-router-af)# maximum-prefix 50000
Router(config-router-af)# end
```

## Additional References

The following sections provide references related to the EIGRP Prefix Limit Support feature.

## Related Documents

| Related Topic                                                   | Document Title                                                                                                                                   |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP Cost Community configuration tasks for EIGRP MPLS VPN PE-CE | <ul style="list-style-type: none"><li><a href="#">BGP Cost Community Support for EIGRP MPLS VPN PE-CE, Cisco IOS Release 12.0(27)S</a></li></ul> |
| CEF commands                                                    | <ul style="list-style-type: none"><li><a href="#">Cisco IOS Switching Services Configuration Guide, Release 12.3T</a></li></ul>                  |
| CEF configuration tasks                                         | <ul style="list-style-type: none"><li><a href="#">Cisco IOS Switching Services Command Reference, Release 12.3</a></li></ul>                     |

| Related Topic                                     | Document Title                                                                                                                                                      |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EIGRP commands                                    | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul>                 |
| EIGRP configuration tasks                         | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                                  |
| EIGRP MPLS VPN PE-CE configuration tasks          | <ul style="list-style-type: none"> <li>• <a href="#">MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge, Cisco IOS Release 12.0(27)S</a></li> </ul> |
| EIGRP MPLS VPN Site of Origin configuration tasks | <ul style="list-style-type: none"> <li>• <a href="#">EIGRP MPLS VPN PE-CE Site of Origin (SoO), Cisco IOS Release 12.0(27)S</a></li> </ul>                          |
| MPLS VPNs configuration tasks                     | <ul style="list-style-type: none"> <li>• <a href="#">MPLS Virtual Private Networks, Cisco IOS Release 12.0(5)T</a></li> </ul>                                       |
| System logging                                    | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3</a></li> </ul>   |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **maximum-prefix**
- **neighbor maximum-prefix (EIGRP)**
- **redistribute maximum-prefix (EIGRP)**
- **show ip eigrp accounting**
- **show ip eigrp vrf accounting**





## EIGRP SNMP Support

The *EIGRP SNMP Support* feature introduces an Enhanced Interior Gateway Routing Protocol (EIGRP) Management Information Base (MIB) in Cisco IOS software. This MIB is accessed through remote Simple Network Management Support (SNMP) software clients. This MIB provides full EIGRP support for GET requests and limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events.

### Feature History for the EIGRP SNMP Support feature

| Release   | Modification                 |
|-----------|------------------------------|
| 12.3(14)T | This feature was introduced. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for EIGRP SNMP Support, page 449](#)
- [Restrictions for EIGRP SNMP Support, page 450](#)
- [Information About EIGRP SNMP Support, page 450](#)
- [How to Enable EIGRP SNMP Support, page 455](#)
- [Configuration Examples for Enabling EIGRP SNMP Support, page 456](#)
- [Additional References, page 457](#)
- [Command Reference, page 458](#)

## Prerequisites for EIGRP SNMP Support

- EIGRP MIB table objects are not visible via SNMP until an EIGRP routing process is enabled and an SNMP community string is configured on at least one router.
- Support for EIGRP notifications (TRAP) is not activated until a trap destination is configured.

## Restrictions for EIGRP SNMP Support

- EIGRP MIB support has not been implemented for the *EIGRP Prefix Limit Support* feature.
- EIGRP MIB support is currently available for only IPv4.

## Information About EIGRP SNMP Support

- [EIGRP SNMP Support Overview, page 450](#)
- [EIGRP VPN Table, page 450](#)
- [EIGRP Traffic Statistics Table, page 451](#)
- [EIGRP Topology Table, page 452](#)
- [EIGRP Neighbor Table, page 453](#)
- [EIGRP Interface Table, page 454](#)
- [EIGRP Notifications, page 455](#)

## EIGRP SNMP Support Overview

This feature introduces EIGRP MIB support in Cisco IOS software. EIGRP routing processes that run over IPv4 are supported. The EIGRP MIB is accessed through remote SNMP software clients. MIB table objects are accessed as read-only through GET, GETINFO, GETMANY, GETNEXT, GETBULK, and SET requests. Counters for MIB table objects are cleared when the EIGRP routing process is reset or when routing table is refreshed by entering the **clear ip route** or **clear ip eigrp** commands. Managed objects for all EIGRP routing processes are implemented as five table objects on a per-autonomous system or per-Virtual Private Network (VPN) basis.

## EIGRP VPN Table

The *EIGRP VPN Table* contains information regarding which virtual private networks (VPN) are configured to run an EIGRP routing process. VPN routes are indexed by the VPN name and the EIGRP autonomous system number. EIGRP VPN table objects and the values populated for each object are described in [Table 14](#).

**Table 14 VPN Table Object Description**

| EIGRP VPN Table      | Description                                                                                |
|----------------------|--------------------------------------------------------------------------------------------|
| <i>cEigrpVpnName</i> | The VRF name. Only VRFs that are configured to run an EIGRP routing process are populated. |



## EIGRP Traffic Statistics Table

The *EIGRP Traffic Statistics Table* contains counters and statistics for the specific types of EIGRP packets that are sent and the related collective information that is generated. The objects in this table are populated on a per-autonomous system basis. Objects in this table are populated for adjacencies formed on all interfaces with an IP address that is configured under an EIGRP network statement. Traffic statistics table objects and the values populated for each object are described in [Table 15](#).

**Table 15 Traffic Statistics Table Object Descriptions**

| <b>EIGRP Traffic Statistics Table</b> | <b>Description</b>                                                                                                                                                                     |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpNbrCount</i>                 | Total number of live neighbors. This table object is incremented or decremented as peering sessions are established or expired.                                                        |
| <i>cEigrpHellosSent</i>               | Total number of transmitted hello packets. This table object is incremented as packets are transmitted.                                                                                |
| <i>cEigrpHellosRcvd</i>               | Total number of received hello packets. This table object is incremented as packets are received.                                                                                      |
| <i>cEigrpUpdatesSent</i>              | Total number of transmitted routing update packets. This table object is incremented as packets are transmitted.                                                                       |
| <i>cEigrpUpdatesRcvd</i>              | Total number of received routing update packets. This table object is incremented as packets are received.                                                                             |
| <i>cEigrpQueriesSent</i>              | Total number of alternate route query packets transmitted. This table object is incremented as packets are transmitted.                                                                |
| <i>cEigrpQueriesRcvd</i>              | Total number of alternate route query packets received. This table object is incremented as packets are received.                                                                      |
| <i>cEigrpRepliesSent</i>              | Total number of reply packets that are transmitted in response to received query packets. This table object is incremented as packets are transmitted.                                 |
| <i>cEigrpRepliesRcvd</i>              | Total number of reply packets that are received in response to transmitted query packets. This table object is incremented as packets are transmitted.                                 |
| <i>cEigrpAcksSent</i>                 | Total number of acknowledgement packets that are transmitted in response to received update packets. This table object is incremented as packets are transmitted.                      |
| <i>cEigrpAcksRcvd</i>                 | Total number of acknowledgement packets that are received in response to transmitted update packets. This table object is incremented as packets are received.                         |
| <i>cEigrpInputQHighMark</i>           | The highest number of packets that have been in the input queue. This table object is incremented only when the previous highest number is exceeded.                                   |
| <i>cEigrpInputQDrops</i>              | Total number of packets dropped from the input queue because the input queue was full. This table object is incremented each time a packet is dropped.                                 |
| <i>cEigrpSiaQueriesSent</i>           | Total number of query packets sent in response to a destination that is in a SIA state for a down peer. This table object is incremented each time an SIA query packet is sent.        |
| <i>cEigrpSiaQueriesRcvd</i>           | Total number of SIA query packets received from neighbors searching for an alternate path to a destination. This table object is incremented each time a SIA query packet is received. |

|                              |                                                                                                                                                                                                                                                                     |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpAsRouterIdType</i>  | The type of IP address that is used as the router ID. The value for this table object can be an IPv4 address.                                                                                                                                                       |
| <i>cEigrpAsRouterId</i>      | The configured or automatically selected router ID in the IP address format. This table object is updated if the router ID is manually reconfigured or if the IP address that was automatically selected is removed.                                                |
| <i>cEigrpTopoRoutes</i>      | Total number of EIGRP derived routes in the topology table. This table object is incremented if a route is added or removed.                                                                                                                                        |
| <i>cEigrpHeadSerial</i>      | Internal sequencing number (serial) applied to EIGRP topology table routes. Routes are sequenced starting with 1. A value of 0 is displayed when there are no routes in the topology table. The “Head” serial number is applied to the first route in the sequence. |
| <i>cEigrpNextSerial</i>      | The serial number applied to the next route in the sequence.                                                                                                                                                                                                        |
| <i>cEigrpXmitPendReplies</i> | Total number of replies expected in response to locally transmitted query packets. This table object contains a value of 0 until a route is placed in an active state.                                                                                              |
| <i>cEigrpXmitDummies</i>     | Total number of temporary entries in the topology table. Dummies are internal entries and not transmitted in routing updates.                                                                                                                                       |

## EIGRP Topology Table

The *EIGRP Topology Table* contains information regarding EIGRP routes received in updates and routes that are locally originated. EIGRP sends and receives routing updates from adjacent routers to which peering relationships (adjacencies) have been formed. The objects in this table are populated on a per-topology table entry (route) basis. Topology table objects and the values populated for each object are described in [Table 16](#).

**Table 16 Topology Table Object Descriptions**

| EIGRP Topology Table         | Description                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpActive</i>          | Displays the active status for routes in the topology table. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route has gone into an active state. A value of 2 is displayed when a route is in a passive state (normal).                        |
| <i>cEigrpStuckInActive</i>   | Displays the SIA status of a route. The value for this table object is displayed on a per-route basis. A value of 1 is displayed when a route has is in a SIA state (no reply has been received for queries for alternate paths). SIA queries are transmitted when a route is placed in this state. |
| <i>cEigrpDestSuccessors</i>  | Total number successors (a route that is the next hop to a destination network) for a topology table entry. The topology table will contain a successor for each path to a given destination. This table object is incremented each time a successor is added or removed.                           |
| <i>cEigrpFdistance</i>       | The feasible (best) distance to a destination network. This value is used to calculate the feasible successor for a topology table entry.                                                                                                                                                           |
| <i>cEigrpRouteOriginAddr</i> | The protocol type of an IP address defined the origin of the topology table entry.                                                                                                                                                                                                                  |
| <i>cEigrpRouteOriginType</i> | Displays the IP address of the router that originated the route in the topology table entry. This table is populated only if the topology table entry was not locally originated.                                                                                                                   |

|                                 |                                                                                                                    |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpNextHopAddressType</i> | Displays the protocol type for the next-hop IP address for a the route in a topology table entry.                  |
| <i>cEigrpNextHopAddress</i>     | The next-hop IP address for a route in a topology table entry.                                                     |
| <i>cEigrpNextHopInterface</i>   | The interface through which the next-hop IP address is reached to send traffic to the destination.                 |
| <i>cEigrpDistance</i>           | The computed distance to the destination network entry from the local router.                                      |
| <i>cEigrpReportDistance</i>     | The computed distance to the destination network in the topology entry as reported by the originator of the route. |

## EIGRP Neighbor Table

The *EIGRP Neighbor Table* contains information about EIGRP neighbors to which adjacencies have been established. EIGRP uses a “Hello” protocol to form neighbor relationships with directly connected EIGRP neighbors. The objects in this table are populated on a per-neighbor basis. Neighbor table objects and the values populated for each object are described in [Table 17](#).

**Table 17 Neighbor Table Object Descriptions**

| <b>EIGRP Neighbor Table</b> | <b>Description</b>                                                                                                                                                                                                                |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpPeerAddrType</i>   | The protocol type of the remote source IP address used by the neighbor to establish the EIGRP adjacency with the local router.                                                                                                    |
| <i>cEigrpPeerAddr</i>       | The source IP address used of the neighbor that was used to establish EIGRP adjacency with the local router. T                                                                                                                    |
| <i>cEigrpPeerInterface</i>  | The name of the local interface, through which the neighbor can be reached. This table object is populated on a per-neighbor basis.                                                                                               |
| <i>cEigrpPeerIfIndex</i>    | The index of the local interface, through which this neighbor can be reached.                                                                                                                                                     |
| <i>cEigrpHoldTime</i>       | The hold timer value for the adjacency with the neighbor. If this timer expires, the neighbor is declared down and removed from the neighbor table.                                                                               |
| <i>cEigrpUpTime</i>         | The length of time that the EIGRP adjacency to the neighbor has been in an up state. The time period is displayed in hours:minutes:seconds.                                                                                       |
| <i>cEigrpSrtt</i>           | The computed smooth round trip time (SRTT) for packets transmitted to and received from the neighbor.                                                                                                                             |
| <i>cEigrpRto</i>            | The computed retransmission timeout (RTO) for the neighbor. The value for this table object is computed as an aggregate average of the time required for packet delivery. This table object is populated on a per-neighbor basis. |
| <i>cEigrpPktsEnqueued</i>   | Total number of EIGRP packets (all types) currently queued for transmission to a neighbor. This table object is populated on a per-neighbor basis.                                                                                |
| <i>cEigrpLastSeq</i>        | The number of the last sequence number of a packet transmitted to a neighbor. This table object is incremented as the sequence number increases.                                                                                  |
| <i>cEigrpVersion</i>        | The EIGRP version information reported by the remote neighbor. This table object is populated on a per-neighbor basis.                                                                                                            |

|                      |                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpRetrans</i> | Cumulative number of packets retransmitted to the neighbor, while the neighbor is in an up state. This table object is populated on a per-neighbor basis. |
| <i>cEigrpRetries</i> | Total number of times an unacknowledged packet has been sent to a neighbor. This table object is populated on a per-neighbor basis.                       |

## EIGRP Interface Table

The *EIGRP Interface Table* contains information and statistics for each interface that EIGRP has been configured to run over. The objects in this table are populated on a per-interface basis. Interface table objects and the values populated for each object are described in [Table 18](#).

**Table 18 EIGRP Interface Table Objects**

| <b>EIGRP Interface Table</b>  | <b>Description</b>                                                                                                                                           |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpPeerCount</i>        | Total number of neighbor adjacencies formed through this interface.                                                                                          |
| <i>cEigrpXmitReliableQ</i>    | Total number of packets waiting in the reliable transport transmission queue (acknowledgement is required) to be sent to a neighbor.                         |
| <i>cEigrpXmitUnreliableQ</i>  | Total number of packets waiting in the unreliable transmission queue (no acknowledgement required).                                                          |
| <i>cEigrpMeanSrtt</i>         | The computed smooth round trip time (SRTT) for packets transmitted to and received from all neighbors on the interface.                                      |
| <i>cEigrpPacingReliable</i>   | The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the reliable transport used.                        |
| <i>cEigrpPacingUnreliable</i> | The configured time interval (in milliseconds) between EIGRP packet transmissions on this interface when the unreliable transport used.                      |
| <i>cEigrpMFlowTimer</i>       | The configured multicast flow control timer value (in milliseconds) for this interface.                                                                      |
| <i>cEigrpPendingRoutes</i>    | Total number of routing updates queued for transmission on this interface.                                                                                   |
| <i>cEigrpHelloInterval</i>    | The configured time interval (in seconds) between Hello packet transmissions for this interface.                                                             |
| <i>cEigrpXmitNextSerial</i>   | The serial number of the next packet that is queued for transmission on this interface.                                                                      |
| <i>cEigrpUMcasts</i>          | Total number of unreliable (no acknowledgement required) multicast packets transmitted on this interface.                                                    |
| <i>cEigrpRMcasts</i>          | Total number of reliable (acknowledgement required) multicast packets transmitted on this interface.                                                         |
| <i>cEigrpUUcasts</i>          | Total number of unreliable (no acknowledgement required) unicast packets transmitted on this interface.                                                      |
| <i>cEigrpRUcasts</i>          | Total number of reliable (acknowledgement required) unicast packets transmitted on this interface.                                                           |
| <i>cEigrpMcastExcept</i>      | The total number of EIGRP multicast exception transmissions that have occurred on this interface.                                                            |
| <i>cEigrpCRpkts</i>           | Total number conditional-receive packets sent on this interface.                                                                                             |
| <i>cEigrpAcksSuppressed</i>   | Total number of individual acknowledgement packets that have been suppressed and combined in an already enqueued outbound reliable packet on this interface. |

|                           |                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpRetranSent</i>   | Total number of packet retransmissions sent on this interface.                                                                                                                                                                               |
| <i>cEigrpOOSrvcd</i>      | Total number of out-of-sequence packets received on this interface.                                                                                                                                                                          |
| <i>cEigrpAuthMode</i>     | The authentication mode configured for traffic that uses this interface. The value of 0 is displayed when no authentication enabled. The value of 1 is displayed when MD5 authentication is enabled.                                         |
| <i>cEigrpAuthKeyChain</i> | The name of the authentication key-chain configured this interface. The key-chain is a reference to which set of secret keys are to be accessed to determine which t key string to use. The key-chain name is not the key string (password). |

## EIGRP Notifications

This MIB provides limited notification (TRAP) support for stuck-in-active (SIA) and neighbor authentication failure events. The **snmp-server enable traps eigrp** command is used to enable EIGRP notifications on a Cisco router. Support for TRAP events is not activated until a trap destination is configured with the **snmp-server host** command and a community string is defined with the **snmp-server community** command. EIGRP notifications are described in [Table 19](#).

**Table 19 EIGRP Notifications**

| EIGRP Traps (Notifications)     | Description                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>cEigrpAuthFailureEvent</i>   | When EIGRP MD5 authentication is enabled on any interface and neighbor adjacencies are formed, a notification is sent if any adjacency goes down as a result of an authentication failure. This notification will be sent once per down event. This notification includes the source IP address of the neighbor from with the authentication failure occurred.                                                                           |
| <i>cEigrpRouteStuckInActive</i> | During the query phase for a new route to a destination network, the route is placed in the active state (an alternate path is actively being sought) and a query packet is broadcast to the network. If no replies are received to the query, then a SIA query packets are broadcast. If a reply is not received for the SIA queries, then the neighbor adjacency is dropped, the route is declared SIA, and this notification is sent. |

## How to Enable EIGRP SNMP Support

The steps in task specify an SNMP server host, configure an SNMP community string, and enable EIGRP notifications.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]]] community-string [udp-port port] [notification-type] [vrrp]
4. **snmp-server community** string [view view-name] [ro | rw] [ipv6 nacl] [access-list-number]
5. **snmp-server enable traps eigrp**
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                   | Enters global configuration mode.                                                                                                                                                                                           |
| Step 3 | <b>snmp-server host</b> {hostname   ip-address} [vrf vrf-name] [traps   informs] [version {1   2c   3 [auth   noauth   priv]]] community-string [udp-port port] [notification-type] [vrrp]<br><br><b>Example:</b><br>Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp | Specifies the destination host or address for SNMP notifications.                                                                                                                                                           |
| Step 4 | <b>snmp-server community</b> string [view view-name] [ro   rw] [ipv6 nacl] [access-list-number]<br><br><b>Example:</b><br>Router(config)# snmp-server community EIGRP1NET1A                                                                                                                      | Configures a community access string to permit SNMP access to the local router by the remote SNMP software client. <ul style="list-style-type: none"> <li>Only IPv4 is supported in Cisco IOS Release 12.3(14)T.</li> </ul> |
| Step 5 | <b>snmp-server enable traps eigrp</b><br><br><b>Example:</b><br>Router(config)# snmp-server enable traps eigrp                                                                                                                                                                                   | Enables or disables SNMP support for EIGRP notifications. <ul style="list-style-type: none"> <li>Notifications can be configured for only SIA and neighbor authentication failure events.</li> </ul>                        |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                                                                                         | Exits Global configuration mode and enters Privileged EXEC mode.                                                                                                                                                            |

## Configuration Examples for Enabling EIGRP SNMP Support

The following examples show how to configure and verify this feature:

- [EIGRP SNMP Support Configuration: Example, page 457](#)
- [EIGRP SNMP Support Configuration: Example, page 457](#)

## EIGRP SNMP Support Configuration: Example

In the following example, an SNMP server host is specified, a community string is configured, and support for EIGRP notifications is enabled.

```
Router(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER eigrp
Router(config) snmp-server community EIGRP1NET1A
Router(config)# snmp-server enable traps eigrp
```

## EIGRP SNMP Support Verification: Example

In the following example, the local SNMP configuration is verified by entering the [show running-config](#) command:

```
Router# show running-config | include snmp

snmp-server community EIGRP1NET1A
snmp-server enable traps eigrp
snmp-server host 10.0.0.1 version 2c NETMANAGER
```

## Additional References

The following sections provide references related to the EIGRP SNMP Support feature.

## Related Documents

| Related Topic              | Document Title                                                                                                                                              |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EIGRP Commands             | <ul style="list-style-type: none"><li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li></ul>             |
| EIGRP Configuration Tasks  | <ul style="list-style-type: none"><li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li></ul>                                              |
| EIGRP Overview             | <ul style="list-style-type: none"><li><a href="#">Introduction to EIGRP</a></li></ul>                                                                       |
| Troubleshooting SIA Events | <ul style="list-style-type: none"><li><a href="#">What Does the EIGRP DUAL-3-SIA Error Message Mean?</a></li></ul>                                          |
| SNMP Commands              | <ul style="list-style-type: none"><li><a href="#">Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3</a></li></ul> |
| SNMP Configuration Tasks   | <ul style="list-style-type: none"><li><a href="#">Configuring SNMP Support</a></li></ul>                                                                    |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                 | MIBs Link                                                                                                                                                                                                                         |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>CISCO-EIGRP-MIB.my</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs     | Title                                                                                       |
|----------|---------------------------------------------------------------------------------------------|
| RFC-1213 | <i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Command

- snmp-server enable traps eigrp**

### Modified Command

- snmp-server host**





## **Part 3: Integrated IS-IS**







## Configuring Integrated IS-IS

---

This chapter describes how to configure Integrated Intermediate System-to-Intermediate System (IS-IS). For a complete description of the integrated IS-IS commands listed in this chapter, refer to the “Integrated IS-IS Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

IS-IS is an International Organization for Standardization (ISO) dynamic routing specification. IS-IS is described in ISO 10589. The Cisco implementation of IS-IS allows you to configure IS-IS as an IP routing protocol.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the [“Using Cisco IOS Software for Release 12.4”](#) chapter in this book.

## IS-IS Configuration Task List

To configure IS-IS, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

- [Enabling IS-IS and Assigning Areas](#) (Required)
- [Enabling IP Routing for an Area on an Interface](#) (Optional)
- [Monitoring IS-IS](#) (Optional)

In addition, you can filter routing information and specify route redistribution. For more information about these features, see the “Filter Routing Information” and “Redistribute Routing Information” sections, respectively, in the “Configuring IP Routing Protocol-Independent Features” chapter of this document.

## Enabling IS-IS and Assigning Areas

Unlike other routing protocols, enabling IS-IS requires that you create an IS-IS routing process and assign it to a specific interface, rather than to a network. You can specify more than one IS-IS routing process per Cisco router, using the multiarea IS-IS configuration syntax. You then configure the parameters for each instance of the IS-IS routing process.



### Note

---

Multiarea IS-IS is supported only for ISO CLNS.

---

Small IS-IS networks are built as a single area that includes all the routers in the network. As the network grows larger, it is usually reorganized into a backbone area made up of the connected set of all Level 2 routers from all areas, which is in turn connected to local areas. Within a local area, routers know how to reach all system IDs. Between areas, routers know how to reach the backbone, and the backbone routers know how to reach other areas.

Routers establish Level 1 adjacencies to perform routing within a local area (intra-area routing). Routers establish Level 2 adjacencies to perform routing between Level 1 areas (interarea routing).


Some networks use legacy equipment that supports only Level 1 routing. These devices are typically organized into many small areas that cannot be aggregated due to performance limitations. Cisco routers are used to interconnect each area to the Level 2 backbone.

A single Cisco router can participate in routing in up to 29 areas, and can perform Level 2 routing in the backbone. In general, each routing process corresponds to an area. By default, the first instance of the routing process configured performs both Level 1 and Level 2 routing. You can configure additional router instances, which are automatically treated as Level 1 areas. You must configure the parameters for each instance of the IS-IS routing process individually.

For IS-IS multiarea routing, you can configure only one process to perform Level 2 routing, although you can define up to 29 Level 1 areas for each Cisco router. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform Level 1 routing at the same time. If Level 2 routing is not desired for a router instance, remove the Level 2 capability using the **is-type** router configuration command. Use the **is-type** router configuration command also to configure a different router instance as a Level 2 router.

Network entity titles (NETs) define the area addresses for the IS-IS area and the system ID of the router. Refer to the “Configuring ISO CLNS” chapter in the *Cisco IOS Apollo Domain, Banyan VINES, ISO CLNS, and XNS Configuration Guide* for a more detailed discussion of NETs.

To enable IS-IS and specify the area for each instance of the IS-IS routing process, use the following commands in global configuration mode:

| Command                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b><br>Router(config)# <b>router isis</b> [area tag]   | Enables IS-IS routing for the specified routing process, and places the router in router configuration mode.<br><br>Use the <i>area tag</i> arguments to identify the area to which this IS-IS router instance is assigned. A value for <i>tag</i> is required if you are configuring multiple IS-IS areas.<br><br>The first IS-IS instance configured is Level 1-2 by default. Later instances are automatically Level 1. You can change the level of routing to be performed by a particular routing process using the <b>is-type</b> router configuration command. |
| <b>Step 2</b><br>Router(config)# <b>net</b> network-entity-title | Configures NETs for the routing process. Specify a NET for each routing process if you are configuring multiarea IS-IS. You can specify a name for a NET and for an address.<br><br><br><b>Note</b> Multiarea IS-IS is supported only for ISO CLNS.                                                                                                                                                                                                                                |

See the “[IS-IS Configuration Examples](#)” section at the end of this chapter for examples of configuring IS-IS as an IP routing protocol.

## Enabling IP Routing for an Area on an Interface

To enable IP routing and specify the area for each instance of the IS-IS routing process, use the following commands beginning in global configuration mode:

|        | Command                                                                       | Purpose                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>Router(config)# <b>interface</b> interface-type interface-number</code> | Enters interface configuration mode.                                                                                                                                            |
| Step 2 | <code>Router(config-if)# <b>ip router isis</b> [area tag]</code>              | Configures an IS-IS routing process for ISO Connectionless Network Service (CLNS) on an interface and attaches an area designator to the routing process.                       |
| Step 3 | <code>Router(config-if)# <b>ip address</b> ip-address-mask</code>             | Defines the IP address for the interface.<br><br>An IP address is required on all interfaces in an area enabled for IS-IS if any one interface is configured for IS-IS routing. |

See the “[IS-IS Configuration Examples](#)” section at the end of this chapter for examples of configuring IS-IS as an IP routing protocol.

## IS-IS Interface Parameters Configuration Task List

The Cisco IS-IS implementation allows you to alter certain interface-specific IS-IS parameters. Most interface configuration commands can be configured independently from other attached routers. The **isis password** interface configuration command should configure the same password on all routers on a network. The settings of other commands (**isis hello-interval**, **isis hello-multiplier**, **isis retransmit-interval**, **isis retransmit-throttle-interval**, **isis csnp-interval**, and so on) can be different on different routers or interfaces. However, if you decide to change certain values from the defaults, it makes sense to configure them on multiple routers and interfaces.

To alter IS-IS parameters, perform the optional tasks described in the following sections:

- [Configuring IS-IS Link-State Metrics](#) (Optional)
- [Setting the Advertised Hello Interval](#) (Optional)
- [Setting the Advertised CSNP Interval](#) (Optional)
- [Setting the Retransmission Interval](#) (Optional)
- [Setting the LSP Transmissions Interval](#) (Optional)
- [Setting the Retransmission Throttle Interval](#) (Optional)
- [Setting the Hello Multiplier](#) (Optional)
- [Specifying Designated Router Election](#) (Optional)
- [Specifying the Interface Circuit Type](#) (Optional)
- [Assigning a Password for an Interface](#) (Optional)
- [Limiting LSP Flooding](#) (Optional)

## Configuring IS-IS Link-State Metrics

You can configure a cost for a specified interface. You can configure the *default-metric* value for Level 1 or Level 2 routing. To configure the metric for the specified interface, use the following command in interface configuration mode:

| Command                                                                                            | Purpose                                                      |
|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Router(config-if)# <b>isis metric</b> <i>default-metric</i><br>[ <b>level-1</b>   <b>level-2</b> ] | Configures the metric (or cost) for the specified interface. |

## Setting the Advertised Hello Interval

You can specify the length of time (in seconds) between hello packets that the Cisco IOS software sends on the interface.

To specify the length of time between hello packets for the specified interface, use the following command in interface configuration mode:

| Command                                                                                                               | Purpose                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Router(config-if)# <b>isis hello-interval</b> { <i>seconds</i>   <b>minimal</b> } [ <b>level-1</b>   <b>level-2</b> ] | Specifies the length of time (in seconds) between hello packets the Cisco IOS software sends on the specified interface. |

The hello interval can be configured independently for Level 1 and Level 2, except on serial point-to-point interfaces. (Because only a single type of hello packet is sent on serial links, it is independent of Level 1 or Level 2.) Specify an optional level for X.25, Switched Multimegabit Data Service (SMDS), and Frame Relay multiaccess networks. X25, SMDS, ATM, and Frame Relay networks should be configured with point-to-point subinterfaces.

## Setting the Advertised CSNP Interval

Complete sequence number protocol data units (CSNPs) are sent by the designated router to maintain database synchronization. You can configure the IS-IS CSNP interval for the interface.

To configure the CSNP interval for the specified interface, use the following command in interface configuration mode:

| Command                                                                                            | Purpose                                                         |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Router(config-if)# <b>isis csnp-interval</b> <i>seconds</i><br>[ <b>level-1</b>   <b>level-2</b> ] | Configures the IS-IS CSNP interval for the specified interface. |

This feature does not apply to serial point-to-point interfaces. It applies to WAN connections if the WAN is viewed as a multiaccess meshed network.

## Setting the Retransmission Interval

You can configure the number of seconds between retransmission of IS-IS link-state packets (LSPs) for point-to-point links. To set the retransmission level, use the following command in interface configuration mode:

| Command                                                              | Purpose                                                                                         |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Router(config-if)# <b>isis retransmit-interval</b><br><i>seconds</i> | Configures the number of seconds between retransmission of IS-IS LSPs for point-to-point links. |

The value you specify should be an integer greater than the expected round-trip delay between any two routers on the attached network. The setting of this parameter should be conservative, or needless retransmission will result. The value should be larger for serial lines.

## Setting the LSP Transmissions Interval

To configure the delay between successive IS-IS LSP transmissions, use the following command in interface configuration mode:

| Command                                                            | Purpose                                                          |
|--------------------------------------------------------------------|------------------------------------------------------------------|
| Router(config-if)# <b>isis lsp-interval</b><br><i>milliseconds</i> | Configures the delay between successive IS-IS LSP transmissions. |

## Setting the Retransmission Throttle Interval

You can configure the maximum rate at which IS-IS LSPs will be re-sent on point-to-point links, in terms of the number of milliseconds between packets. This configuration is different from the retransmission interval, which is the amount of time between successive retransmissions of the same LSP.

The retransmission throttle interval is typically not necessary, except in cases of very large networks with high point-to-point neighbor counts. To set the retransmission throttle interval, use the following command in interface configuration mode:

| Command                                                                            | Purpose                                                    |
|------------------------------------------------------------------------------------|------------------------------------------------------------|
| Router(config-if)# <b>isis retransmit-throttle-interval</b><br><i>milliseconds</i> | Configures the IS-IS LSP retransmission throttle interval. |

## Setting the Hello Multiplier

To specify the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down, use the following command in interface configuration command. The default value is 3.

| Command                                                                               | Purpose                    |
|---------------------------------------------------------------------------------------|----------------------------|
| Router(config-if)# <b>isis hello-multiplier</b> <i>multiplier</i> [level-1   level-2] | Sets the hello multiplier. |

## Specifying Designated Router Election

You can configure the priority to use for designated router election. Priorities can be configured for Level 1 and Level 2 individually.

To specify the designated router election, use the following command in interface configuration mode:

| Command                                                                         | Purpose                                                        |
|---------------------------------------------------------------------------------|----------------------------------------------------------------|
| Router(config-if)# <b>isis priority</b> <i>number-value</i> [level-1   level-2] | Configures the priority to use for designated router election. |

## Specifying the Interface Circuit Type

You can specify adjacency levels on a specified interface. This parameter is also referred to as the *interface circuit type*.

To specify the interface circuit type, use the following command in interface configuration mode:

| Command                                                                          | Purpose                                                                                                         |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Router(config-if)# <b>isis circuit-type</b> [level-1   level-1-2   level-2-only] | Configures the type of adjacency desired for neighbors on the specified interface (the interface circuit type). |

## Assigning a Password for an Interface

You can assign different passwords for different routing levels. Specifying Level 1 or Level 2 configures the password for only Level 1 or Level 2 routing, respectively. If you do not specify a level, the default is Level 1. By default, authentication is disabled.

To configure a password for the specified level, use the following command in interface configuration mode:

| Command                                                                     | Purpose                                                           |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------|
| Router(config-if)# <b>isis password</b> <i>password</i> [level-1   level-2] | Configures the authentication password for a specified interface. |



## Limiting LSP Flooding

Limiting LSP flooding is important to IS-IS networks in general, and is not limited to configuring multiarea IS-IS networks. In a network with a high degree of redundancy, such as a fully meshed set of point-to-point links over a nonbroadcast multiaccess (NBMA) transport, flooding of LSPs can limit network scalability. You can reduce LSP flooding in two ways:

- [Blocking Flooding on Specific Interfaces](#)

The advantage of full blocking over mesh groups is that it is easier to configure and understand, and fewer LSPs are flooded. Blocking flooding on all links permits the best scaling performance, but results in a less robust network structure. Permitting flooding on all links results in poor scaling performance.

- [Configuring Mesh Groups](#)

The advantage of mesh groups over full blocking is that mesh groups allow LSPs to be flooded over one hop to all routers on the mesh, while full blocking allows some routers to receive LSPs over multiple hops. This relatively small delay in flooding can have an impact on convergence times, but the delay is negligible compared to overall convergence times.

## Blocking Flooding on Specific Interfaces

You can completely block flooding (full blocking) on specific interfaces, so that new LSPs will not be flooded out over those interfaces. However, if flooding is blocked on a large number of links, and all remaining links go down, routers cannot synchronize their link-state databases even though there is connectivity to the rest of the network. When the link-state database is no longer updated, routing loops usually result.

To use CSNPs on selected point-to-point links to synchronize the link-state database, configure a CSNP interval using the **isis csnp-interval** interface configuration command on selected point-to-point links over which normal flooding is blocked. You should use CSNPs for this purpose only as a last resort.

## Configuring Mesh Groups

Configuring mesh groups (a set of interfaces on a router) can help to limit redundant flooding. All routers reachable over the interfaces in a particular mesh group are assumed to be densely connected (each router has many links to other routers), where many links can fail without isolating one or more routers from the network.

Normally, when a new LSP is received on an interface, it is flooded out over all other interfaces on the router. When the new LSP is received over an interface that is part of a mesh group, the new LSP will not be flooded out over the other interfaces that are part of that same mesh group.

Mesh groups rely on a full mesh of links between a group of routers. If one or more links in the full mesh go down, the full mesh is broken, and some routers might miss new LSPs, even though there is connectivity to the rest of the network. When you configure mesh groups to optimize or limit LSP flooding, be sure to select alternative paths over which to flood in case interfaces in the mesh group go down.

To minimize the possibility of incomplete flooding, you should allow unrestricted flooding over at least a minimal set of links in the mesh. Selecting the smallest set of logical links that covers all physical paths results in very low flooding, but less robustness. Ideally you should select only enough links to ensure that LSP flooding is not detrimental to scaling performance, but enough links to ensure that under most failure scenarios no router will be logically disconnected from the rest of the network.

# Miscellaneous IS-IS Parameters Configuration Task List

The following tasks differ from the preceding interface-specific IS-IS tasks because they configure IS-IS itself, rather than the interface.

To configure optional IS-IS parameters as described in the following sections:

- [Generating a Default Route](#) (Required)
- [Specifying the System Type](#) (Optional)
- [Configuring IS-IS Authentication Passwords](#) (Optional)
- [Summarizing Address Ranges](#) (Optional)
- [Setting the Overload Bit](#) (Optional)
- [Changing the Routing Level for an Area](#) (Optional)
- [Tuning LSP Interval and Lifetime](#) (Optional)
- [Customizing IS-IS Throttling of LSP Generation, SPF Calculation, and PRC](#) (Optional)
- [Modifying the Output of show Commands](#) (Optional)

## Generating a Default Route

You can force a default route into an IS-IS routing domain. Whenever you specifically configure redistribution of routes into an IS-IS routing domain, the Cisco IOS software does not, by default, redistribute the *default route* into the IS-IS routing domain. The following command generates a default route into IS-IS, which can be controlled by a route map. You can use the route map to identify the level into which the default route is to be announced, and you can specify other filtering options configurable under a route map. You can use a route map to conditionally advertise the default route, depending on the existence of another route in the routing table of the router.

To generate a default route, use the following command in router configuration mode:

| Command                                                                                                         | Purpose                                               |
|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <code>Router(config-router)# <b>default-information originate</b><br/>[<b>route-map</b> <i>map-name</i>]</code> | Forces a default route into the IS-IS routing domain. |

See also the discussion of redistribution of routes in the “Configuring IP Routing Protocol-Independent Features” chapter of this document.

## Specifying the System Type

You can configure the router to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (interarea) router, or as an interarea router only.

To specify router level support, use the following command in router configuration mode:

| Command                                                                                                      | Purpose                                               |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <code>Router(config-router)# <b>is-type</b> {<b>level-1</b>   <b>level-1-2</b>   <b>level-2-only</b>}</code> | Configures the system type (area or backbone router). |

## Configuring IS-IS Authentication Passwords

You can assign passwords to areas and domains.

The area authentication password is inserted in Level 1 (station router level) LSPs, and the routing domain authentication password is inserted in Level 2 (area router level) LSPs.

To configure either area or domain authentication passwords, use the following commands in router configuration mode, as needed:

| Command                                                       | Purpose                                                |
|---------------------------------------------------------------|--------------------------------------------------------|
| Router(config-router)# <b>area-password</b> <i>password</i>   | Configures the area authentication password.           |
| Router(config-router)# <b>domain-password</b> <i>password</i> | Configures the routing domain authentication password. |

## Summarizing Address Ranges

You can create aggregate addresses that are represented in the routing table by a summary address. This process is called *route summarization*. One summary address can include multiple groups of addresses for a given level. Routes learned from other routing protocols also can be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes.

To create a summary of addresses for a given level, use the following command in router configuration mode:

| Command                                                                                                                  | Purpose                                           |
|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Router(config-router)# <b>summary-address</b> <i>address mask</i> { <b>level-1</b>   <b>level-1-2</b>   <b>level-2</b> } | Creates a summary of addresses for a given level. |

## Setting the Overload Bit

You can configure the router to set the overload bit (also known as the hippity bit) in its nonpseudonode LSPs. Normally the setting of the overload bit is allowed only when a router runs into problems. For example, when a router is experiencing a memory shortage, the link-state database may not be complete, resulting in an incomplete or inaccurate routing table. By setting the overload bit in their LSPs, other routers can ignore the unreliable router in their shortest path first (SPF) calculations until the router has recovered from its problems.

The result will be that no paths through this router are seen by other routers in the IS-IS area. However, IP and CLNS prefixes directly connected to this router will be still be reachable.

This command can be useful when you want to connect a router to an IS-IS network, but do not want real traffic flowing through it under any circumstances. Examples are as follows:

- A test router in the lab, connected to a production network.
- A router configured as an LSP flooding server, for example, on an NBMA network, in combination with the mesh-group feature.
- A router that is aggregating virtual circuits (VCs) used only for network management. In this case, the network management stations must be on a network directly connected to the router with the **set-overload-bit** router configuration command configured.

Unless you specify the **on-startup** keyword, this command sets the overload bit immediately and it remains set until the **no set-overload-bit** command is specified. If you specify the **on-startup** keyword, you must indicate whether it is set for a specified number of *seconds* or until BGP has converged. If BGP does not signal IS-IS that it has converged, IS-IS will turn off the overload bit after 10 minutes.

In addition to setting the overload bit, you might also want to suppress certain types of IP prefix advertisements from LSPs. For example, allowing IP prefix propagation between Level 1 and Level 2 effectively makes a node a transit node for IP traffic, which may be undesirable. The **suppress** keyword used with the **interlevel** or **external** keyword (or both) accomplishes that suppression while the overload bit is set.

To set the overload bit, use the following command in router configuration mode:

| Command                                                                                                                                                                           | Purpose                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| Router(config-router)# <b>set-overload-bit</b><br>[ <b>on-startup</b> { <i>seconds</i>   <b>wait-for-bgp</b> }]<br>[ <b>suppress</b> {[ <b>interlevel</b> ] [ <b>external</b> ]}] | Sets the overload bit. |

## Changing the Routing Level for an Area

You can change the routing level configured for an area using the **is-type** router configuration command. If the router instance has been configured for a Level 1-2 area (the default for the first instance of the IS-IS routing process in a Cisco router), you can remove Level 2 (interarea) routing for the area using the **is-type** command and change the routing level to Level 1 (intra-area). You can also configure Level 2 routing for an area using the **is-type** command, but the instance of the IS-IS router configured for Level 2 on the Cisco router must be the only instance configured for Level 2.

To change the routing level for an IS-IS routing process in a given area, use the following command in router configuration mode:

| Command                                                                                     | Purpose                                                                    |
|---------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Router (config)# <b>is-type</b> { <b>level-1</b>   <b>level-1-2</b>   <b>level-2-only</b> } | Configures the routing level for an instance of the IS-IS routing process. |

## Tuning LSP Interval and Lifetime

By default, the router sends a periodic LSP refresh every 15 minutes. LSPs remain in a database for 20 minutes by default. If they are not refreshed by that time, they are deleted. You can change the LSP refresh interval or the LSP lifetime. The LSP interval should be less than the LSP lifetime or else LSPs will time out before they are refreshed. The software will adjust the LSP refresh interval if necessary to prevent the LSPs from timing out.

To change the LSP refresh interval or lifetime, use the appropriate command in router configuration mode:

| Command                                                               | Purpose                                                                                                         |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Router (config-router)# <b>lsp-refresh-interval</b><br><i>seconds</i> | Sets the LSP refresh interval.                                                                                  |
| Router (config-router)# <b>max-lsp-lifetime</b><br><i>seconds</i>     | Sets the maximum time that link-state packets (LSPs) can remain in a router's database without being refreshed. |

## Customizing IS-IS Throttling of LSP Generation, SPF Calculation, and PRC

### Partial Route Computation (PRC)

PRC is the software's process of calculating routes without performing an SPF calculation. This is possible when the topology of the routing system itself has not changed, but a change is detected in the information announced by a particular IS or when it is necessary to attempt to reinstall such routes in the RIB.

### Benefits of Throttling IS-IS LSP Generation, SPF Calculation, and PRC

IS-IS throttles three main events: link-state PDU (LSP) generation, Shortest Path First (SPF) computation, and partial route computation (PRC). Throttling slows down the frequency of these events during times of network instability. Although throttling these events slows down network convergence, not throttling could result in a network not functioning. If network topology is unstable, throttling slows down the scheduling of these intervals until the topology becomes stable.

The throttling of LSP generation prevents flapping links from causing many LSPs to be flooded through the network. The throttling of SPF computation and PRC prevents the router from crashing from the demand of too many calculations.

### How Throttling of IS-IS LSP Generation, SPF Calculation, and PRC Works

IS-IS throttling of LSP generation, SPF calculations, and PRC occurs by default. You can customize the throttling of these events with the **lsp-gen-interval**, **spf-interval**, and **prc-interval** commands, respectively.

The arguments in each command behave similarly. For each command:

- The first argument indicates the maximum number of seconds between LSP generations or calculations.
- The second argument indicates the initial wait time (in milliseconds) before running the first LSP generation or calculation.
- The third argument indicates the minimum amount of time to wait (in milliseconds) between the first and second LSP generation or calculation. (In addition to this wait time, there might be some other system overhead between LSP generations or calculations.)

Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified, upon which the wait interval remains constant. After the network calms down and there are no triggers for 2 times the maximum interval, fast behavior is restored (the initial wait time).

Other commands are available to control the delay between successive LSPs, the retransmission of the same LSA, and the retransmission of LSPs on a point-to-point interface.

Perform this task to customize throttling of LSP generation, SPF calculation, PRC, or any combination of the three, beginning in router configuration mode:

| Command                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-router)# <b>lsp-gen-interval</b> [ <b>level-1</b>   <b>level-2</b> ] <i>lsp-max-wait</i> [ <i>lsp-initial-wait</i> <i>lsp-second-wait</i> ] | Sets IS-IS LSP generation throttling timers. <ul style="list-style-type: none"> <li>The default <i>lsp-max-wait</i> interval is 5 seconds.</li> <li>The default <i>lsp-initial-wait</i> interval is 50 milliseconds.</li> <li>The default <i>lsp-second-wait</i> interval is 5000 milliseconds.</li> </ul>               |
| Router(config-router)# <b>spf-interval</b> [ <b>level-1</b>   <b>level-2</b> ] <i>spf-max-wait</i> [ <i>spf-initial-wait</i> <i>spf-second-wait</i> ]     | Sets IS-IS SPF throttling timers. <ul style="list-style-type: none"> <li>The default <i>spf-max-wait</i> interval is 10 seconds.</li> <li>The default <i>spf-initial-wait</i> interval is 5500 milliseconds.</li> <li>The default <i>spf-second-wait</i> interval is 5500 milliseconds.</li> </ul>                       |
| Router(config-router)# <b>prc-interval</b> <i>prc-max-wait</i> [ <i>prc-initial-wait</i> <i>prc-second-wait</i> ]                                         | Sets IS-IS partial route computation throttling timers. <ul style="list-style-type: none"> <li>The default <i>prc-max-wait</i> interval is 10 seconds.</li> <li>The default <i>prc-initial-wait</i> interval is 2000 milliseconds.</li> <li>The default <i>prc-second-wait</i> interval is 5000 milliseconds.</li> </ul> |

## Modifying the Output of show Commands

To customize display output when the IS-IS multiarea feature is used, making the display easier to read, use the following command in EXEC mode:

| Command                                                                                | Purpose                                                                                              |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Router# <b>isis display delimiter</b> [ <b>return count</b>   <i>character count</i> ] | Specifies the delimiter to be used to separate displays of information about individual IS-IS areas. |

For example, the following command causes information about individual areas to be separated by 14 dashes (-) in the display:

```
isis display delimiter - 14
```

The output for a configuration with two Level 1 areas and one Level 2 area configured is as follows:

```
dtp-5# show clns neighbors
```

```
-----
```

```
Area L2BB:
```

| System Id      | Interface | SNPA        | State | Holdtime | Type | Protocol |
|----------------|-----------|-------------|-------|----------|------|----------|
| 0000.0000.0009 | Tu529     | 172.21.39.9 | Up    | 25       | L1L2 | IS-IS    |

```
-----
```

```

Area A3253-01:
System Id      Interface  SNPA                State  Holdtime  Type  Protocol
0000.0000.0053 Et1         0060.3e58.ccdb      Up     22        L1   IS-IS
0000.0000.0003 Et1         0000.0c03.6944      Up     20        L1   IS-IS
-----
Area A3253-02:
System Id      Interface  SNPA                State  Holdtime  Type  Protocol
0000.0000.0002 Et2         0000.0c03.6bc5      Up     27        L1   IS-IS
0000.0000.0053 Et2         0060.3e58.ccde      Up     24        L1   IS-IS

```

## Monitoring IS-IS

To monitor the IS-IS tables and databases, use the following commands in EXEC mode, as needed:

| Command                                                                                                                                | Purpose                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Router# <b>show isis database</b> [ <b>level-1</b> ] [ <b>level-2</b> ] [ <b>l1</b> ] [ <b>l2</b> ] [ <b>detail</b> ] [ <b>lspid</b> ] | Displays the IS-IS link-state database.                               |
| Router# <b>show isis area-tag routes</b>                                                                                               | Displays the IS-IS Level 1 routing table.                             |
| Router# <b>show isis spf-log</b>                                                                                                       | Displays how often and why the router has run a full SPF calculation. |
| Router# <b>show isis area-tag topology</b>                                                                                             | Displays a list of all connected routers in all areas.                |

## IS-IS Configuration Examples

This section includes the following examples:

- [Enabling IS-IS Configuration Example](#)
- [Multiarea IS-IS Configuration for CLNS Network Example](#)
- [IS-IS Throttle Timers Example](#)

### Enabling IS-IS Configuration Example

The following example shows how to configure three routers to run IS-IS as an IP routing protocol. [Figure 38](#) illustrates the example configuration.

#### Router A Configuration

```

router isis
 net 49.0001.0000.0000.000a.00
 interface ethernet 0
  ip router isis
 interface serial 0
  ip router isis

```

#### Router B Configuration

```

router isis
 net 49.0001.0000.0000.000b.00
 interface ethernet 0
  ip router isis
 interface ethernet 1
  ip router isis

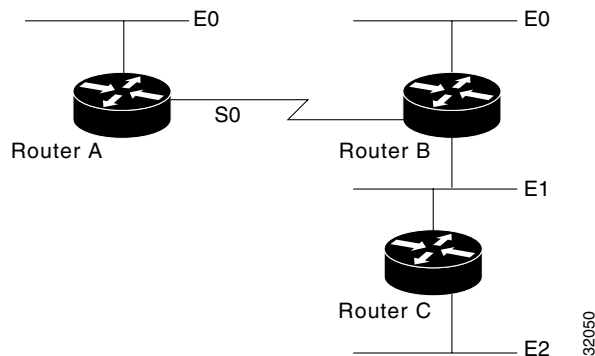
```

```
interface serial 0
 ip router isis
```

#### Router C Configuration

```
router isis
 net 49.0001.0000.0000.000c.00
interface ethernet 1
 ip router isis
interface ethernet 2
 ip router isis
```

**Figure 38 IS-IS Routing**



## Multiarea IS-IS Configuration for CLNS Network Example

The following example shows a multiarea IS-IS configuration with two Level 1 areas and one Level 1-2 area. [Figure 39](#) illustrates this configuration.

```
clns routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

.
.
.
```

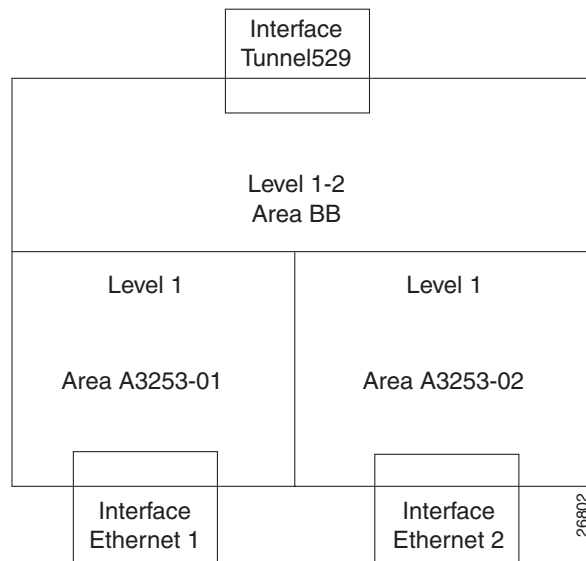


```

router isis BB                                ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1

```

**Figure 39** Multiarea IS-IS Configuration with Three Level 1 Areas and One Level 2 Area



## IS-IS Throttle Timers Example

This example shows a system configured with IS-IS throttling of LSP generations, SPF calculations and PRC:

```

router isis
 spf-interval 5 10 20
 prc-interval 5 10 20
 lsp-gen-interval 2 50 100

```





# Integrated IS-IS Point-to-Point Adjacency over Broadcast Media

## Feature History

| Release  | Modification                 |
|----------|------------------------------|
| 12.2(8)T | This feature was introduced. |

This document describes how to configure an integrated IS-IS point-to-point adjacency over broadcast media and contains the following sections:

- [Feature Overview, page 477](#)
- [Supported Platforms, page 478](#)
- [Supported Standards, MIBs, and RFCs, page 479](#)
- [Prerequisites, page 479](#)
- [Configuration Tasks, page 479](#)
- [Configuration Example, page 480](#)
- [Command Reference, page 480](#)

## Feature Overview

When a network consists of only two networking devices connected to broadcast media and uses the integrated IS-IS protocol, it is better for the system to handle the link as a point-to-point link instead of as a broadcast link. This feature introduces a new command to make IS-IS behave as a point-to-point link between the networking devices.

## Benefits

Using this feature provides performance improvements to the network convergence times of the customer's network because the feature saves the system from electing a designated router (DR), prevents flooding from using CSNPs for database synchronization, and simplifies shortest path first (SPF) computations.

## Restrictions

This feature applies only to IS-IS interfaces connected to broadcast media.

## Related Features and Technologies

This feature is part of the Integrated IS-IS protocol.

## Related Documents

- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2
- *Cisco IOS IP Configuration Guide*, Release 12.2

## Supported Platforms

This feature is supported on the following platforms:

- Cisco 2600 Series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3620
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100 Series
- Cisco 7200 Series
- Cisco 7500 Series
- Universal Router Module
- Cisco MC3810 Multiservice Access Concentrator
- Cisco uBR7200 Series Universal Broadband Router

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

### Standards

No new standards are supported by this feature.

### MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

### RFCs

No new or modified RFCs are supported by this feature.

## Prerequisites

This feature requires broadcast media connected to the interface and Integrated IS-IS configured on the interface.

## Configuration Tasks

See the following section to configure the Integrated IS-IS Point-to-Point Adjacency over Broadcast Media feature. The task is required for the feature.

- [Configuring Point-to-Point Adjacency over Broadcast Media](#) (required)

## Configuring Point-to-Point Adjacency over Broadcast Media

To configure an IS-IS point-to-point adjacency over broadcast media, use the following commands beginning in global configuration mode:

|        | Command                                               | Purpose                                                                                                                                          |
|--------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface fastethernet number</b>  | Configures a fast Ethernet interface and enters interface configuration mode.                                                                    |
| Step 2 | Router(config-if)# <b>isis network point-to-point</b> | Configures an IS-IS network of two networking devices connected to broadcast media into a point-to-point network instead of a broadcast network. |

## Configuration Example

This example configures an IS-IS point-to-point adjacency over broadcast media:

```
interface fastethernet 1/0
 isis network point-to-point
```

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **isis network point-to-point**



# IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest to each Intermediate System-to-Intermediate System (IS-IS) protocol data unit (PDU). The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing message from being injected into the network routing domain. IS-IS clear text (plain text) authentication is enhanced so that passwords are encrypted when the software configuration is displayed and passwords are easier to manage and change.

## Feature Specifications for the IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication Feature

### Feature History

| Release    | Modification                                                  |
|------------|---------------------------------------------------------------|
| 12.0(21)ST | This feature was introduced.                                  |
| 12.2(11)S  | This feature was integrated into Cisco IOS Release 12.2(11)S. |
| 12.0(22)S  | This feature was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(13)T  | This feature was integrated into Cisco IOS Release 12.2(13)T. |

### Supported Platforms

Cisco 7200 series, Cisco 7500 series, Cisco 10000 series, Cisco 10720 Internet router, Cisco 12000 series

## Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### **Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.

## **Contents**

- [Prerequisites for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 482](#)
- [Information About IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 482](#)
- [How to Configure IS-IS HMAC-MD5 Authentication or Enhanced Clear Text Authentication, page 483](#)
- [Configuration Examples for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication, page 496](#)
- [Additional References, page 497](#)
- [Command Reference, page 499](#)

## **Prerequisites for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication**

In order to use HMAC-MD5 or clear text authentication with encrypted keys, the Integrated IS-IS routing protocol must be configured.

## **Information About IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication**

Before you configure IS-IS HMAC-MD5 authentication or clear text authentication, you should understand the following concepts:

- [IS-IS HMAC-MD5 Authentication, page 483](#)
- [Benefits of IS-IS HMAC-MD5 Authentication, page 483](#)
- [Benefits of IS-IS Clear Text Authentication, page 483](#)



## IS-IS HMAC-MD5 Authentication

The IS-IS HMAC-MD5 authentication feature adds an HMAC-MD5 digest to each IS-IS PDU. HMAC is a mechanism for message authentication codes (MACs) using cryptographic hash functions. The digest allows authentication at the IS-IS routing protocol level, which prevents unauthorized routing messages from being injected into the network routing domain.

IS-IS has five packet types: link state packet (LSP), LAN Hello, Serial Hello, CSNP, and PSNP. The IS-IS HMAC-MD5 authentication or the clear text password authentication can be applied to all five types of PDU. The authentication can be enabled on different IS-IS levels independently. The interface-related PDUs (LAN Hello, Serial Hello, CSNP, and PSNP) can be enabled with authentication on different interfaces, with different levels and different passwords.

The HMAC-MD5 mode cannot be mixed with the clear text mode on the same authentication scope (LSP or interface). However, administrators can use one mode for LSP and another mode for some interfaces, for example. If mixed modes are intended, different keys should be used for different modes in order not to compromise the encrypted password in the PDUs.

## Benefits of IS-IS HMAC-MD5 Authentication

- IS-IS now supports MD5 authentication, which is more secure than clear text authentication.
- MD5 authentication or clear text authentication can be enabled on Level 1 or Level 2 independently.
- Passwords can be rolled over to new passwords without disrupting routing messages.
- For the purpose of network transition, you can configure the networking device to *accept* PDUs without authentication or with wrong authentication information, yet *send* PDUs with authentication. Such transition might be because you are migrating from no authentication to some type of authentication, you are changing authentication type, or you are changing keys.

## Benefits of IS-IS Clear Text Authentication

IS-IS clear text (plain text) authentication was formerly configured only by using the **area-password** or **domain-password** command. Clear text authentication can now be configured using new commands that cause passwords to be encrypted when the software configuration is displayed and make passwords easier to manage and change.

## How to Configure IS-IS HMAC-MD5 Authentication or Enhanced Clear Text Authentication

The following sections describe configuration tasks for IS-IS authentication. The task you perform depends on whether you are introducing authentication or migrating from an existing authentication scheme.

- [Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time](#) (optional)
- [Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication](#) (optional)
- [Migrating from Old Clear Text Authentication to the New Clear Text Authentication](#) (optional)

## Configuring HMAC-MD5 Authentication or Clear Text Authentication for the First Time

Before you can configure authentication, you must make the following decisions:

- Whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are included in this section)
- Whether to configure HMAC-MD5 authentication or clear text authentication (this decision is made with the **authentication mode** command if you are configuring an IS-IS instance, or with the **isis authentication mode** command if you are configuring an IS-IS interface)

### Configuring HMAC-MD5 or Clear Text Authentication for the IS-IS Instance

To achieve a smooth transition to authenticating IS-IS packets, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **authentication mode** {**md5** | **text**} [**level-1** | **level-2**]
11. **authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

## DETAILED STEPS

|         | Command                                                                                                                                                              | Purpose                                                                                                                                                                                                                                     |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                               | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                           |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                       | Enters global configuration mode.                                                                                                                                                                                                           |
| Step 3  | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain remote3754                                                                 | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                                                 |
| Step 4  | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 100                                                                                  | Identifies an authentication key on a key chain. <ul style="list-style-type: none"> <li>The <i>key-id</i> must be a number.</li> </ul>                                                                                                      |
| Step 5  | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string mno172                                                               | Specifies the authentication string for a key. <ul style="list-style-type: none"> <li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li> </ul>                     |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                                                              | Returns to global configuration mode.                                                                                                                                                                                                       |
| Step 7  | <b>router isis</b> <i>area-tag</i><br><br><b>Example:</b><br>Router(config)# router isis 1                                                                           | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                                          |
| Step 8  | <b>authentication send-only</b> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# authentication send-only                        | Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).                                                                                                                      |
| Step 9  | Repeat Steps 1 through 8 on each router that will communicate.                                                                                                       | Use the same key-string on each router.                                                                                                                                                                                                     |
| Step 10 | <b>authentication mode</b> { <b>md5</b>   <b>text</b> } [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# authentication mode md5 | Specifies the type of authentication used in IS-IS packets for the IS-IS instance. <ul style="list-style-type: none"> <li>Specify <b>md5</b> for MD5 authentication.</li> <li>Specify <b>text</b> for clear text authentication.</li> </ul> |

|         | Command                                                                                                                                                                       | Purpose                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>authentication key-chain</b> <i>name-of-chain</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# authentication key-chain remote3754 | Enables MD5 authentication for the IS-IS instance.                                                              |
| Step 12 | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                  | —                                                                                                               |
| Step 13 | <b>no authentication send-only</b><br><br><b>Example:</b><br>Router(config-router)# no authentication send-only                                                               | Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received. |
| Step 14 | Repeat Step 13 on each router that will communicate.                                                                                                                          | —                                                                                                               |

## Configuring HMAC-MD5 or Clear Text Authentication for an IS-IS Interface

To achieve a smooth transition to authenticating IS-IS packets, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **interface** *type number*
8. **isis authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode** {**md5** | **text** } [**level-1** | **level-2**]
11. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no isis authentication send-only**
14. Repeat Step 13 on each router that will communicate.

## DETAILED STEPS

|         | Command                                                                                                                                                                    | Purpose                                                                                                                                                                                                                 |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                     | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                       |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                             | Enters global configuration mode.                                                                                                                                                                                       |
| Step 3  | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain multistate87723                                                                  | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                             |
| Step 4  | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 201                                                                                        | Identifies an authentication key on a key chain. <ul style="list-style-type: none"> <li>The <i>key-id</i> must be a number.</li> </ul>                                                                                  |
| Step 5  | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string idaho                                                                      | Specifies the authentication string for a key. <ul style="list-style-type: none"> <li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li> </ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                                                                    | Returns to global configuration mode.                                                                                                                                                                                   |
| Step 7  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 0                                                                         | Configures an interface.                                                                                                                                                                                                |
| Step 8  | <b>isis authentication send-only</b> [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication send-only                        | Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.                                                                                                |
| Step 9  | Repeat Steps 1 through 8 on each router that will communicate.                                                                                                             | Use the same key-string on each router.                                                                                                                                                                                 |
| Step 10 | <b>isis authentication mode</b> { <i>md5</i>   <i>text</i> } [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication mode md5 | Specifies the type of authentication used for an IS-IS interface.                                                                                                                                                       |

|         | Command                                                                                                                                                                                  | Purpose                                                                                                                                                                                           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>isis authentication key-chain</b> <i>name-of-chain</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication key-chain multistate87723 | Enables MD5 authentication for an IS-IS interface. <ul style="list-style-type: none"> <li>Refer to the key management feature, which is referenced in the “Related Documents” section.</li> </ul> |
| Step 12 | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                             | —                                                                                                                                                                                                 |
| Step 13 | Router(config-if) # <b>no isis authentication send-only</b><br><br><b>Example:</b><br>Router(config-if)# no isis authentication send-only                                                | Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.                                                                                 |
| Step 14 | Repeat Step 13 on each router that will communicate.                                                                                                                                     | —                                                                                                                                                                                                 |

## Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication

When you are migrating from the old clear text authentication to HMAC-MD5 authentication, after you load the first router with an image that includes this feature, the router will continue to use the old clear text authentication with other routers on the network.



### Note

If you want HMAC-MD5 authentication, all routers in the authentication scope must have the new image before HMAC-MD5 can be configured. The scope can be either a Level 1 or Level 2 domain.

Before you can configure authentication, you must decide whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are in this section).

## Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for the IS-IS Instance

To achieve a smooth transition to authenticating IS-IS packets, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

When you configure the MD5 authentication, the **area-password** and **domain-password** command settings will be overridden automatically with the new authentication commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]

9. Repeat Steps 1 through 8 on each router that will communicate.
10. **authentication mode md5** [**level-1** | **level-2**]
11. **authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

|        | Command                                                                                                                                       | Purpose                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted.                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                       |
| Step 3 | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain dinosaur                                            | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                             |
| Step 4 | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 301                                                           | Identifies an authentication key on a key chain. <ul style="list-style-type: none"> <li>The <i>key-id</i> must be a number.</li> </ul>                                                                                  |
| Step 5 | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string pterodactyl                                   | Specifies the authentication string for a key. <ul style="list-style-type: none"> <li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li> </ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                                       | Returns to global configuration mode.                                                                                                                                                                                   |
| Step 7 | <b>router isis</b> <i>area-tag</i><br><br><b>Example:</b><br>Router(config)# router isis 1                                                    | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                      |
| Step 8 | <b>authentication send-only</b> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# authentication send-only | Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).                                                                                                  |
| Step 9 | Repeat Steps 1 through 8 on each router that will communicate.                                                                                | Use the same key-string on each router.                                                                                                                                                                                 |

|         | Command                                                                                                                                                                       | Purpose                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>authentication mode md5</b> [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-router)# authentication mode md5                                   | Specifies the type of authentication used in IS-IS packets for the IS-IS instance.                              |
| Step 11 | <b>authentication key-chain</b> <i>name-of-chain</i> [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-router)# authentication key-chain remote3754 | Enables MD5 authentication for the IS-IS instance.                                                              |
| Step 12 | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                  | —                                                                                                               |
| Step 13 | <b>no authentication send-only</b><br><br><b>Example:</b><br>Router(config-router)# no authentication send-only                                                               | Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received. |
| Step 14 | Repeat Step 13 on each router that will communicate.                                                                                                                          | —                                                                                                               |

## Migrating from Old Clear Text Authentication to HMAC-MD5 Authentication for an IS-IS Interface

### Prerequisites

Before you can migrate from the old method of clear text authentication to HMAC-MD5 authentication at the interface level, you must upgrade all the routers associated with the media of the interfaces to the new image containing the HMAC-MD5 feature.

To achieve a smooth transition to authenticating IS-IS packets, it is important to perform the steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

When you configure the MD5 authentication, the **isis password** command setting will be overridden automatically with the new authentication commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **interface** *type number*
8. **isis authentication send-only** [*level-1* | *level-2*]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode md5** [*level-1* | *level-2*]
11. **isis authentication key-chain** *name-of-chain* [*level-1* | *level-2*]



12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no isis authentication send-only**
14. Repeat Step 13 on each router that will communicate.

## DETAILED STEPS

|         | Command                                                                                                                                             | Purpose                                                                                                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                              | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                       |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                      | Enters global configuration mode.                                                                                                                                                                                     |
| Step 3  | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain dinosaur                                                  | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                           |
| Step 4  | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 301                                                                 | Identifies an authentication key on a key chain. <ul style="list-style-type: none"><li>The <i>key-id</i> must be a number.</li></ul>                                                                                  |
| Step 5  | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string pterodactyl                                         | Specifies the authentication string for a key. <ul style="list-style-type: none"><li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li></ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                                             | Returns to global configuration mode.                                                                                                                                                                                 |
| Step 7  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 0                                                  | Configures an interface.                                                                                                                                                                                              |
| Step 8  | <b>isis authentication send-only</b> [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication send-only | Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.                                                                                              |
| Step 9  | Repeat Steps 1 through 8 on each router that will communicate.                                                                                      | Use the same key-string on each router.                                                                                                                                                                               |
| Step 10 | <b>isis authentication mode md5</b> [ <i>level-1</i>   <i>level-2</i> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication mode md5   | Specifies the type of authentication used for an IS-IS interface.                                                                                                                                                     |

|         | Command                                                                                                                                                                                  | Purpose                                                                                                                                                                                           |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>isis authentication key-chain</b> <i>name-of-chain</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication key-chain multistate87723 | Enables MD5 authentication for an IS-IS interface. <ul style="list-style-type: none"> <li>Refer to the key management feature, which is referenced in the “Related Documents” section.</li> </ul> |
| Step 12 | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                             | —                                                                                                                                                                                                 |
| Step 13 | Router(config-if) # <b>no isis authentication send-only</b><br><br><b>Example:</b><br>Router(config-if)# no isis authentication send-only                                                | Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.                                                                                 |
| Step 14 | Repeat Step 13 on each router that will communicate.                                                                                                                                     | —                                                                                                                                                                                                 |

## Migrating from Old Clear Text Authentication to the New Clear Text Authentication

The benefits of migrating from the old method of clear text authentication to the new method of clear text authentication are as follows:

- Passwords are easier to change and maintain.
- Passwords can be encrypted when the system configuration is being displayed (if you use key management).

Before you can configure authentication, you must decide whether to configure authentication for the IS-IS instance or for individual IS-IS interfaces (both tasks are in this section).

## Migrating from Old Clear Text Authentication to the New Clear Text Authentication for the IS-IS Instance


To achieve a smooth transition to authenticating LSPs, perform the following steps in the order shown, which requires moving from router to router doing certain steps before all the steps are performed on any one router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **router isis** *area-tag*
8. **authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.

10. **authentication mode text** [level-1 | level-2]
11. **authentication key-chain** *name-of-chain* [level-1 | level-2]
12. Repeat Steps 10 and 11 on each router that will communicate.
13. **no authentication send-only**
14. Repeat Step 13 on each router that will communicate.

|         | Command                                                                                                                       | Purpose                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                        | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                       |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                | Enters global configuration mode.                                                                                                                                                                                     |
| Step 3  | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain dinosaur                            | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                           |
| Step 4  | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 301                                           | Identifies an authentication key on a key chain. <ul style="list-style-type: none"><li>The <i>key-id</i> must be a number.</li></ul>                                                                                  |
| Step 5  | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string pterodactyl                   | Specifies the authentication string for a key. <ul style="list-style-type: none"><li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li></ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                       | Returns to global configuration mode.                                                                                                                                                                                 |
| Step 7  | <b>router isis</b> <i>area-tag</i><br><br><b>Example:</b><br>Router(config)# router isis 1                                    | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                    |
| Step 8  | <b>authentication send-only</b> [level-1   level-2]<br><br><b>Example:</b><br>Router(config-router)# authentication send-only | Specifies for the IS-IS instance that MD5 authentication is performed only on IS-IS packets being sent (not received).                                                                                                |
| Step 9  | Repeat Steps 1 through 8 on each router that will communicate.                                                                | Use the same key-string on each router.                                                                                                                                                                               |
| Step 10 | <b>authentication mode text</b> [level-1   level-2]<br><br><b>Example:</b><br>Router(config-router)# authentication mode text | Specifies the type of authentication used in IS-IS packets for the IS-IS instance.                                                                                                                                    |

|         | Command                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>authentication key-chain</b> <i>name-of-chain</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# authentication key-chain remote3754 | Enables MD5 authentication for the IS-IS instance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 12 | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                  | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 13 | <b>no authentication send-only</b><br><br><b>Example:</b><br>Router(config-router)# no authentication send-only                                                               | Specifies for the IS-IS instance that MD5 authentication is performed on IS-IS packets being sent and received.<br><br> <b>Note</b> Do not perform this step if some of the routers sharing the media on the interface do not run the new image. In software releases prior to those on which this feature runs, authentication is not applied to SNP packets. If the router runs the new image without the <b>authentication send-only</b> command configured and with the new clear text password scheme, it will fail to authenticate the SNP packets from the router with old images. |
| Step 14 | Repeat Step 13 on each router that will communicate.                                                                                                                          | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Migrating from Old Clear Text Authentication to the New Clear Text Authentication for an IS-IS Interface

This section describes how to configure authentication on interface-related PDUs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *text*
6. **exit**
7. **interface** *type number*
8. **isis authentication send-only** [**level-1** | **level-2**]
9. Repeat Steps 1 through 8 on each router that will communicate.
10. **isis authentication mode text** [**level-1** | **level-2**]
11. **isis authentication key-chain** *name-of-chain* [**level-1** | **level-2**]
12. Repeat Steps 10 and 11 on each router that will communicate.

13. Load the new image on all the other routers that share the media that the interface uses.
14. **no isis authentication send-only**
15. Repeat Step 14 on each interface.

## DETAILED STEPS

|         | Command                                                                                                                                             | Purpose                                                                                                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                              | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                       |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                      | Enters global configuration mode.                                                                                                                                                                                     |
| Step 3  | <b>key chain</b> <i>name-of-chain</i><br><br><b>Example:</b><br>Router(config)# key chain dinosaur                                                  | Enables authentication for routing protocols and identifies a group of authentication keys.                                                                                                                           |
| Step 4  | <b>key</b> <i>key-id</i><br><br><b>Example:</b><br>Router(config-keychain)# key 301                                                                 | Identifies an authentication key on a key chain. <ul style="list-style-type: none"><li>The <i>key-id</i> must be a number.</li></ul>                                                                                  |
| Step 5  | <b>key-string</b> <i>text</i><br><br><b>Example:</b><br>Router(config-keychain-key)# key-string pterodactyl                                         | Specifies the authentication string for a key. <ul style="list-style-type: none"><li>The <i>text</i> can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a number.</li></ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-keychain-key)# exit                                                                             | Returns to global configuration mode.                                                                                                                                                                                 |
| Step 7  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 0                                                  | Configures an interface.                                                                                                                                                                                              |
| Step 8  | <b>isis authentication send-only</b> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication send-only | Specifies that MD5 authentication is performed only on packets being sent (not received) on a specified IS-IS interface.                                                                                              |
| Step 9  | Repeat Steps 1 through 8 on each router that will communicate.                                                                                      | Use the same key-string on each router.                                                                                                                                                                               |
| Step 10 | <b>isis authentication mode text</b> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication mode text | Specifies the type of authentication used for an IS-IS interface.                                                                                                                                                     |

|                | Command                                                                                                                                                                                  | Purpose                                                                                                                                                                                           |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 11</b> | <b>isis authentication key-chain</b> <i>name-of-chain</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-if)# isis authentication key-chain multistate87723 | Enables MD5 authentication for an IS-IS interface. <ul style="list-style-type: none"> <li>Refer to the key management feature, which is referenced in the “Related Documents” section.</li> </ul> |
| <b>Step 12</b> | Repeat Steps 10 and 11 on each router that will communicate.                                                                                                                             | —                                                                                                                                                                                                 |
| <b>Step 13</b> | Load the new image on all the other routers that share the media that the interface uses.                                                                                                | —                                                                                                                                                                                                 |
| <b>Step 14</b> | Router(config-if)# <b>no isis authentication send-only</b><br><br><b>Example:</b><br>Router(config-if)# no isis authentication send-only                                                 | Specifies that MD5 authentication is performed on packets being sent and received on a specified IS-IS interface.                                                                                 |
| <b>Step 15</b> | Repeat Step 14 on each interface.                                                                                                                                                        | —                                                                                                                                                                                                 |

## Configuration Examples for IS-IS HMAC-MD5 Authentication and Enhanced Clear Text Authentication

This section provides the following configuration examples:

- [Configuring IS-IS HMAC-MD5 Authentication Example, page 496](#)
- [Configuring IS-IS Clear Text Authentication Example, page 497](#)

### Configuring IS-IS HMAC-MD5 Authentication Example

The following example configures a key chain and key for IS-IS HMAC-MD5 authentication for Ethernet interface 3 (on Hello packets) and for the IS-IS instance (on LSP, CSNP, and PSNP packets):

```

!
key chain cisco
  key 100
  key-string tasman-drive
!
interface Ethernet3
  ip address 10.1.1.1 255.255.255.252
  ip router isis real_secure_network
  isis authentication mode md5 level-1
  isis authentication key-chain cisco level-1
!
router isis real_secure_network
  net 49.0000.0101.0101.0101.00
  is-type level-1
  authentication mode md5 level-1
  authentication key-chain cisco level-1
!

```

## Configuring IS-IS Clear Text Authentication Example

The following example configures a key chain and key for IS-IS clear text authentication for Ethernet interface 3 (on Hello packets) and for the IS-IS instance (on LSP, CSNP, and PSNP packets):

```
!  
key chain cisco  
  key 100  
  key-string tasman-drive  
!  
interface Ethernet3  
  ip address 10.1.1.1 255.255.255.252  
  ip router isis real_secure_network  
  isis authentication mode text level-1  
  isis authentication key-chain cisco level-1  
!  
router isis real_secure_network  
  net 49.0000.0101.0101.0101.00  
  is-type level-1  
  authentication mode text level-1  
  authentication key-chain cisco level-1  
!
```

## Additional References

For additional information related to IS-IS HMAC-MD5 authentication and clear text authentication, refer to the following references:

- [Related Documents, page 497](#)
- [MIBs, page 498](#)
- [RFCs, page 498](#)
- [Technical Assistance, page 498](#)

## Related Documents

| Related Topic                 | Document Title                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Key chains and key management | <ul style="list-style-type: none"><li>• “IP Routing Protocol-Independent Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i>, Release 12.2</li><li>• “Configuring IP Routing Protocol-Independent Features” chapter in the <i>Cisco IOS IP Configuration Guide</i>, Release 12.2</li></ul> |
| IS-IS routing protocol        | <ul style="list-style-type: none"><li>• “Integrated IS-IS Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i>, Release 12.2</li><li>• “Configuring Integrated IS-IS” chapter in the <i>Cisco IOS IP Configuration Guide</i>, Release 12.2</li></ul>                                        |

## MIBs

| MIBs <sup>1</sup>                                                                                                           | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs <sup>1</sup>           | Title                                                 |
|-----------------------------|-------------------------------------------------------|
| draft-ietf-isis-hmac-03.txt | <i>IS-IS Cryptographic Authentication</i>             |
| RFC 1321                    | <i>The MD5 Message-Digest Algorithm</i>               |
| RFC 2104                    | <i>HMAC: Keyed-Hashing for Message Authentication</i> |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |



# Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **area-password**
- **authentication key-chain**
- **authentication mode**
- **authentication send-only**
- **debug isis authentication**
- **domain-password**
- **isis authentication key-chain**
- **isis authentication mode**
- **isis authentication send-only**





# Integrated IS-IS Nonstop Forwarding (NSF) Awareness

The Integrated IS-IS Nonstop Forwarding (NSF) Awareness feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. This feature is part of the software code and requires no configuration.

## Feature Specifications for the Integrated IS-IS NSF Awareness Feature

### Feature History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.2(15)T | This feature was introduced. |

### Supported Platforms

For information about platforms supported, refer to Cisco Feature Navigator.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About IS-IS NSF Awareness, page 501](#)
- [Additional References, page 502](#)
- [Command Reference, page 503](#)

## Information About IS-IS NSF Awareness

The following concept describes the IS-IS NSF Awareness feature:

- [Benefits of IS-IS NSF Awareness, page 502](#)

## Benefits of IS-IS NSF Awareness

The Integrated IS-IS Nonstop Forwarding Awareness feature allows CPE routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. The awareness feature is part of the software code; it need not be configured.

The local router is not necessarily performing NSF; its awareness of NSF allows the integrity and accuracy of the RIB and link-state database occurring on the neighboring NSF-capable router to be maintained during the switchover process. Customers would want the IS-IS NSF Awareness feature when their routers are neighbors to NSF-capable routers.

## Additional References

For additional information related to NSF and IS-IS, see the following section:

- [Related Documents, page 502](#)
- [Standards, page 502](#)
- [MIBs, page 503](#)
- [RFCs, page 503](#)
- [Technical Assistance, page 503](#)

## Related Documents

| Related Topic                | Document Title                                                                                                                                                                                                                                                                                |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nonstop forwarding (NSF)     | <i>Cisco Nonstop Forwarding with Stateful Switchover</i><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/nsf120s.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/nsf120s.htm</a> |
| Configuring Integrated IS-IS | <i>Cisco IOS IP Configuration Guide, Release 12.2</i>                                                                                                                                                                                                                                         |
| Integrated IS-IS commands    | <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2</i>                                                                                                                                                                                                         |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.





## IS-IS Incremental SPF

---

Integrated Intermediate System-to-Intermediate System (IS-IS) can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing IS-IS to converge faster on a new routing topology in reaction to a network event.

### Feature History for the IS-IS Incremental SPF Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(24)S | This feature was introduced.                                  |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IS-IS Incremental SPF, page 505](#)
- [Information About IS-IS Incremental SPF, page 506](#)
- [How to Enable IS-IS Incremental SPF, page 506](#)
- [Configuration Examples for IS-IS Incremental SPF, page 507](#)
- [Additional References, page 508](#)
- [Command Reference, page 509](#)

## Prerequisites for IS-IS Incremental SPF

It is presumed that you have IS-IS configured in your network.

# Information About IS-IS Incremental SPF

Before you enable the IS-IS Incremental SPF feature, you should understand the concept described in this section.

- [Benefits of IS-IS Incremental SPF, page 506](#)

## Benefits of IS-IS Incremental SPF

IS-IS uses Dijkstra's SPF algorithm to compute the shortest path tree (SPT). During the computation of the SPT, the shortest path to each node is discovered. The topology tree is used to populate the routing table with routes to IP networks. When changes occur, the entire SPT is recomputed. In many cases, the entire SPT need not be recomputed because most of the tree remains unchanged. Incremental SPF allows the system to recompute only the affected part of the tree. Recomputing only a portion of the tree rather than the entire tree results in faster IS-IS convergence and saves CPU resources.

Incremental SPF computes only the steps needed to apply the changes in the network topology diagram. That process requires that the system keep more information about the topology in order to apply the incremental changes. Also, more processing must be done on each node for which the system receives a new LSP. However, incremental SPF typically reduces demand on CPU.

## How to Enable IS-IS Incremental SPF

This section contains the following procedure:

- [Enabling Incremental SPF, page 506](#)

## Enabling Incremental SPF

This section describes how to enable incremental SPF.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [tag]**
4. **ispf [level-1 | level-2 | level-1-2] [seconds]**
5. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                        | Purpose                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                           | Enters global configuration mode.                                                                                                                     |
| Step 3 | <b>router isis</b> [tag]<br><br><b>Example:</b><br>Router(config)# router isis                                           | Configures an IS-IS routing process.                                                                                                                  |
| Step 4 | <b>ispf</b> [level-1   level-2   level-1-2] [seconds]<br><br><b>Example:</b><br>Router(config-router)# ispf level-1-2 60 | Enables incremental SPF. <ul style="list-style-type: none"> <li>The default number of seconds for incremental SPF to begin is 120 seconds.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                          | Exits router configuration mode.                                                                                                                      |

## Configuration Examples for IS-IS Incremental SPF

This section contains an example of configuring IS-IS incremental SPF.

- [Incremental SPF: Example, page 507](#)

### Incremental SPF: Example

This example enables incremental SPF:

```
router isis
 ispf level-1 60
```

# Additional References

The following sections provide references related to IS-IS.

## Related Documents

| Related Topic             | Document Title                                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------|
| IS-IS commands            | “Integrated IS-IS Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0       |
| IS-IS configuration tasks | “Configuring Integrated IS-IS ” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **ispf**





# IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

This document describes two Integrated Intermediate System-to-Intermediate System (IS-IS) mechanisms to exclude IP prefixes of connected networks from link-state packet (LSP) advertisements, thereby reducing IS-IS convergence time.

## Feature History for the IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(22)S | This feature was introduced.                                  |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements, page 512](#)
- [Information About IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements, page 512](#)
- [How to Exclude Connected IP Prefixes from IS-IS LSP Advertisements, page 513](#)

- [Configuration Examples of IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements, page 517](#)
- [Where to Go Next, page 518](#)
- [Additional References, page 519](#)
- [Command Reference, page 520](#)

## Prerequisites for IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

Before you can use either mechanism to exclude IP prefixes of connected networks from IS-IS LSP advertisements, the integrated IS-IS routing protocol must be configured.

## Information About IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

To exclude IP prefixes of connected networks from LSP advertisements, you should understand the following concepts:

- [Convergence, page 512](#)
- [Two Alternative Methods to Reduce IS-IS Convergence Time, page 512](#)
- [Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements, page 513](#)

### Convergence

Convergence is the process of all routers coming to agreement on optimal routes in a network. When a network event causes routes to become available or unavailable, routers send routing update messages through the network that cause routing algorithms to recalculate optimal routes. Eventually all the routers agree on the routes. Fast convergence benefits the network performance. Routing algorithms that converge slowly may cause routing loops or network unavailability.

### Two Alternative Methods to Reduce IS-IS Convergence Time

In order to speed up IS-IS convergence, the number of IP prefixes carried in LSPs needs to be limited. Configuring interfaces as unnumbered would limit the prefixes. However, for network management reasons, you might want to have numbered interfaces and also want to prevent advertising interface addresses into IS-IS.

The IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements feature provides two methods to avoid the overpopulation of routing tables and thereby reduce IS-IS convergence time. These methods are described in the following sections.

## Small-Scale Method to Reduce IS-IS Convergence Time

You can explicitly configure an IS-IS interface not to advertise its IP network to the neighbors (by using the **no isis advertise-prefix** command). This method is feasible for a small network; it does not scale well. If you have dozens or hundreds of routers in your network, with possibly ten times as many physical interfaces involved, it would be difficult to add this command to each router's configuration.

## Large-Scale Method to Reduce IS-IS Convergence Time

An easier way to reduce IS-IS convergence is to configure the IS-IS instance on a router to advertise only passive interfaces (by configuring the **advertise-passive-only** command). This command relies on the fact that when enabling IS-IS on a loopback interface, you usually configure the loopback as passive (to prevent sending unnecessary hello packets out through it because there is no chance of finding a neighbor behind it). Thus, if you want to advertise only the loopback and if it has already been configured as passive, configuring the **advertise-passive-only** command per IS-IS instance would prevent the overpopulation of the routing tables.

## Benefit of Excluding IP Prefixes of Connected Networks in LSP Advertisements

Whether you choose to prevent the advertising of IS-IS interface subnetworks or advertise only the IS-IS prefixes that belong to passive (loopback) interfaces, you will reduce IS-IS convergence time. The IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements feature is recommended in any case where fast convergence is required.

# How to Exclude Connected IP Prefixes from IS-IS LSP Advertisements

This section provides two alternative IS-IS mechanisms to exclude connected IP prefixes from LSP advertisements:

- [Excluding Connected IP Prefixes on a Small Scale](#), page 513 (optional)
- [Excluding Connected IP Prefixes on a Large Scale](#), page 515 (optional)

## Excluding Connected IP Prefixes on a Small Scale

This section provides the steps necessary to exclude connected IP prefixes from IS-IS LSP advertisements in a small network.

For a configuration example of this feature where IS-IS acts as the MPLS backbone, see the [“Excluding Connected IP Prefixes on a Small Scale: Example”](#) section on page 518.

### SUMMARY STEPS

1. **enable**
2. **configure** { **terminal** | **memory** | **network** }
3. **interface** *type number*
4. **ip address** *ip-address netmask*

5. **no ip directed-broadcast**
6. **ip router isis** *[area-tag]*
7. **no isis advertise-prefix**
8. **exit**
9. Repeat Steps 3 through 8 for each interface on which you do not want to advertise IP prefixes.
10. **router isis** *area-tag*
11. **net** *network-entity-title*
12. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                         | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted.                                                                                                                               |
| Step 2 | <b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }<br><br><b>Example:</b><br>Router# configure terminal     | Enters global configuration mode.                                                                                                                                                                                                    |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0                             | Configures an interface type and enters interface configuration mode.                                                                                                                                                                |
| Step 4 | <b>ip address</b> <i>ip-address netmask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 192.168.20.1 255.255.255.0 | Sets a primary IP address for an interface. <ul style="list-style-type: none"> <li>The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.</li> </ul> |
| Step 5 | <b>no ip directed-broadcast</b><br><br><b>Example:</b><br>Router(config-if)# no ip directed-broadcast                          | (Optional) Disables the translation of a directed broadcast to physical broadcasts.                                                                                                                                                  |
| Step 6 | <b>ip router isis</b> <i>[area-tag]</i><br><br><b>Example:</b><br>Router(config-if)# ip router isis                            | Configures an IS-IS routing process on an interface and attaches an area designator to the routing process.                                                                                                                          |
| Step 7 | <b>no isis advertise-prefix</b><br><br><b>Example:</b><br>Router(config-if)# no isis advertise-prefix                          | Prevents the advertising of IP prefixes of connected networks in LSP advertisements per IS-IS interface.                                                                                                                             |



|         | Command or Action                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                               | Returns to global configuration mode.                                                                                                                                                                                                                                                                                           |
| Step 9  | Repeat Steps 3 through 8 for each interface on which you do not want to advertise IP prefixes.                              | (Optional)                                                                                                                                                                                                                                                                                                                      |
| Step 10 | <b>router isis area-tag</b><br><br><b>Example:</b><br>Router(config)# router isis                                           | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                                                                                                                              |
| Step 11 | <b>net network-entity-title</b><br><br><b>Example:</b><br>Router(config-router)# net<br>47.0004.004d.0001.0001.0c11.1111.00 | Configures an IS-IS network entity title (NET) for the routing process.                                                                                                                                                                                                                                                         |
| Step 12 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                             | (Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode.<br><br><ul style="list-style-type: none"> <li>Use this command when you are ready to exit configuration mode and save the configuration to the running configuration file.</li> </ul> |

## Excluding Connected IP Prefixes on a Large Scale

This section provides the steps necessary to exclude connected IP prefixes from LSP advertisements in a large network where IS-IS acts as the MPLS backbone.

### SUMMARY STEPS

1. **enable**
2. **configure {terminal | memory | network}**
3. **interface loopback number**
4. **ip address ip-address netmask**
5. **no ip directed-broadcast**
6. **exit**
7. **interface type number**
8. **ip address ip-address netmask**
9. **no ip directed-broadcast**
10. **ip router isis [area-tag]**
11. **exit**
12. **router isis area-tag**
13. **passive-interface [default] {type number}**

14. **net** *network-entity-title*
15. **advertise-passive-only**
16. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted.                                                                                                                               |
| Step 2 | <b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }<br><br><b>Example:</b><br>Router# configure terminal       | Enters global configuration mode.                                                                                                                                                                                                    |
| Step 3 | <b>interface</b> <i>loopback number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                           | Configures a loopback interface and enters interface configuration mode.                                                                                                                                                             |
| Step 4 | <b>ip address</b> <i>ip-address netmask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 192.168.10.1 255.255.255.255 | Sets a primary IP address for an interface. <ul style="list-style-type: none"> <li>The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.</li> </ul> |
| Step 5 | <b>no ip directed-broadcast</b><br><br><b>Example:</b><br>Router(config-if)# no ip directed-broadcast                            | (Optional) Disables the translation of a directed broadcast to physical broadcasts.                                                                                                                                                  |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                    | Returns to global configuration mode.                                                                                                                                                                                                |
| Step 7 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0                               | Configures an interface type and enters interface configuration mode.                                                                                                                                                                |
| Step 8 | <b>ip address</b> <i>ip-address netmask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 192.168.20.1 255.255.255.0   | Sets a primary IP address for an interface. <ul style="list-style-type: none"> <li>The network mask can be indicated as a 4-part dotted decimal address or as a prefix. This example uses a 4-part dotted decimal number.</li> </ul> |
| Step 9 | <b>no ip directed-broadcast</b><br><br><b>Example:</b><br>Router(config-if)# no ip directed-broadcast                            | (Optional) Disables the translation of a directed broadcast to physical broadcasts.                                                                                                                                                  |

|         | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                      |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>ip router isis</b> <i>[area-tag]</i><br><br><b>Example:</b><br>Router(config-if)# ip router isis                                            | Configures an IS-IS routing process on an interface and attaches an area designator to the routing process.                                                                                                                                                                                                                  |
| Step 11 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                  | Returns to global configuration mode.                                                                                                                                                                                                                                                                                        |
| Step 12 | <b>router isis</b> <i>area-tag</i><br><br><b>Example:</b><br>Router(config)# router isis                                                       | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                                                                                                                           |
| Step 13 | <b>passive-interface</b> [ <b>default</b> ] <i>{type number}</i><br><br><b>Example:</b><br>Router(config-router)# passive-interface loopback 0 | Disables sending routing updates on an interface.                                                                                                                                                                                                                                                                            |
| Step 14 | <b>net</b> <i>network-entity-title</i><br><br><b>Example:</b><br>Router(config-router)# net 47.0004.004d.0001.0001.0c11.1111.00                | Configures an IS-IS NET for the routing process.                                                                                                                                                                                                                                                                             |
| Step 15 | <b>advertise-passive-only</b><br><br><b>Example:</b><br>Router(config-router)# advertise-passive-only                                          | Configures IS-IS to advertise only prefixes that belong to passive interfaces.                                                                                                                                                                                                                                               |
| Step 16 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                       | (Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns you to privileged EXEC mode. <ul style="list-style-type: none"> <li>Use this command when you are ready to exit configuration mode and save the configuration to the running configuration file.</li> </ul> |

## Configuration Examples of IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements

This section provides the following examples:

- [Excluding Connected IP Prefixes on a Small Scale: Example, page 518](#)
- [Excluding Connected IP Prefixes on a Large Scale: Example, page 518](#)

## Excluding Connected IP Prefixes on a Small Scale: Example

The following example uses the **no isis advertise-prefix** command on Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
interface loopback 0
 ip address 192.168.10.1 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet 0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
 ip router isis
 no isis advertise-prefix
!
!.
!.
!.
!
router isis
 passive-interface loopback 0
 net 47.0004.004d.0001.0001.0c11.1111.00
 log-adjacency-changes
!
```

## Excluding Connected IP Prefixes on a Large Scale: Example

The following example uses the **advertise-passive-only** command, which applies to the entire IS-IS instance, thereby preventing IS-IS from advertising the IP network of Ethernet interface 0. Only the IP address of loopback interface 0 is advertised.

```
!
interface loopback 0
 ip address 192.168.10.1 255.255.255.255
 no ip directed-broadcast
!
!
interface Ethernet0
 ip address 192.168.20.1 255.255.255.0
 no ip directed-broadcast
 ip router isis
!.
!.
!.
!
router isis
 passive-interface Loopback0
 net 47.0004.004d.0001.0001.0c11.1111.00
 advertise-passive-only
 log-adjacency-changes
!
```

## Where to Go Next

You might want to propagate the prefixes configured on interfaces by means other than IS-IS, such as internal BGP (iBGP), because fast convergence is not requested for interface addresses. If so, refer to

the “Configuring BGP” chapter in the *Cisco IOS IP Configuration Guide*, Release 12.2.

## Additional References

The following sections provide references related to the IS-IS Mechanisms to Exclude Connected IP Prefixes from LSP Advertisements feature.

### Related Documents

| Related Topic             | Document Title                                                                                                                    |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Integrated IS-IS commands | “Integrated IS-IS Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2 |
| IS-IS configuration tasks | “Configuring Integrated IS-IS” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                              |
| BGP configuration tasks   | “Configuring BGP” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                                           |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **advertise-passive-only**
- **isis advertise-prefix**



## IS-IS Support for Route Tags

The IS-IS Support for Route Tags feature provides the capability to tag IS-IS route prefixes and use those tags in a route map to control Intermediate System-to-Intermediate System (IS-IS) route redistribution or route leaking.

### Feature History for the IS-IS Support for Route Tags Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.3(2)T  | This feature was introduced.                                  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites to Using IS-IS Route Tags, page 521](#)
- [Information About IS-IS Route Tags, page 522](#)
- [How to Use IS-IS Route Tags, page 523](#)
- [Configuration Examples for IS-IS Support for Route Tags, page 532](#)
- [Additional References, page 535](#)
- [Command Reference, page 536](#)

## Prerequisites to Using IS-IS Route Tags

- You must have integrated IS-IS configured.
- Because the IS-IS route tag will be used in a route map, you must understand how to configure a route map.

- In order to use the route tag, you must configure the **metric-style wide** command. (The **metric-style narrow** command is configured by default). The tag value is set into sub-TLV 1 for TLV (Type Length Value) Type 135.
- You must understand the task for which you are using the route tag, such as route redistribution, route summarization, or route leaking.

## Information About IS-IS Route Tags

You should understand at least the first two concepts before implementing IS-IS route tags, and you should understand the third concept if you plan to configure route leaking:

- [Benefits of IS-IS Route Tags, page 522](#)
- [IS-IS Route Tag Characteristics, page 522](#)
- [IS-IS Route Leaking Based on a Route Tag, page 523](#)

## Benefits of IS-IS Route Tags

- The IS-IS Support for Route Tags feature allows you to tag IP addresses of an interface and use the tag to apply administrative policy with a route map.
- You can tag IS-IS routes to control their redistribution. You can configure a route map to set a tag for an IS-IS IP prefix (route) and/or match on the tag (perhaps on a different router) to redistribute IS-IS routes. Although the **match tag** and **set tag** commands existed for other protocols before this feature, they were not implemented for IS-IS, so they did nothing when specified in an IS-IS network until now.
- You can tag a summary route and then use a route map to match the tag and set one or more attributes for the route.

## IS-IS Route Tag Characteristics

An IS-IS route tag number can be up to 4 bytes long. The tag value is set into a sub-TLV 1 for TLV (Type Length Value) Type 135. For more information about TLV Type 135, refer to the “*Intermediate System-to-Intermediate System (IS-IS) TLVs*” document referenced in the “[Additional References](#)” section.

Only one tag can be set to an IS-IS IP route (prefix). The tag is sent out in link-state packets (LSPs) advertising the route. Setting a tag to a route alone does nothing for your network. You can use the route tag at area or Level 1/Level 2 boundaries by matching on the tag and then applying administrative policies such as redistribution, route summarization, or route leaking.

Configuring a tag for an interface (with the **isis tag** command) triggers the generation of new LSPs from the router because the tag is new information for the packets.



## IS-IS Route Leaking Based on a Route Tag

The IS-IS Support for Route Tags feature provides a new way to configure route leaking (redistribution). If you configure route leaking and you want to match on a tag, use a route map (not a distribute list). For more information on route leaking, refer to *IS-IS Route Leaking Overview* at: <http://www.cisco.com/warp/public/97/route-leak.html>

## How to Use IS-IS Route Tags

There are two general steps to using IS-IS route tags: tagging routes and referencing the tag to set values for the routes and/or redistribute routes. This section describes the following tasks:

- [Tagging IS-IS Routes, page 523](#) (required)
- [Using the Tag to Set Values and/or Redistribute Routes, page 529](#) (required)

### Tagging IS-IS Routes

There are three ways to tag IS-IS routes: tag routes for networks directly connected to an interface, set a tag in a route map, or tag a summary route. All three methods are described in this section. The tagging method is independent of how you use the tag.

After you tag the routes, you can use the tag to set values (such as a metric or next hop, and so on) and/or redistribute routes. You might tag routes on one router, but reference the tag on other routers, depending on what you want to achieve. For example, you could tag the interface on Router A with a tag, match the tag on Router B to set values, and redistribute routes on Router C based on values using a route map.

### Prerequisites

Before you tag any IS-IS routes, you need to decide on the following:

1. Your goal to set values for routes or redistribute routes (or both).
2. Where in your network you want to tag routes.
3. Where in your network you want to reference the tags.
4. Which tagging method you will use, which determines which task in this section to perform.

After you know which tagging method suits your need, proceed to one of the following tasks:

- [Tagging Routes for Networks Directly Connected to an Interface, page 523](#)
- [Tagging Routes Using a Route Map, page 525](#)
- [Tagging a Summary Address, page 528](#)

### Tagging Routes for Networks Directly Connected to an Interface

Perform this task if you want to tag routes for networks directly connected to an interface.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip address** *ip-address mask secondary*
6. **isis tag** *tag-number*
7. **end**
8. **show isis database verbose**
9. **show ip route** *[[ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name]]*

## DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                           |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                              | Enters global configuration mode.                                                                                                                                                                 |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 0                                          | Configures an interface.                                                                                                                                                                          |
| Step 4 | <b>ip address</b> <i>ip-address mask</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.1.1.1 255.255.255.0                     | Sets a primary IP address for an interface.<br><ul style="list-style-type: none"> <li>In this example, the network 10.1.1.0 will be tagged.</li> </ul>                                            |
| Step 5 | <b>ip address</b> <i>ip-address mask secondary</i><br><br><b>Example:</b><br>Router(config-if)# ip address 10.2.2.1 255.255.255.0 secondary | (Optional) Sets a secondary IP address for an interface.<br><ul style="list-style-type: none"> <li>In this example, the network 10.2.2.0 will be tagged.</li> </ul>                               |
| Step 6 | <b>isis tag</b> <i>tag-number</i><br><br><b>Example:</b><br>Router(config-if)# isis tag 120                                                 | Sets a tag on the IP addresses configured under this interface when those IP prefixes are put into an IS-IS LSP.<br><ul style="list-style-type: none"> <li>The tag must be an integer.</li> </ul> |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                 | (Optional) Exits configuration mode and returns to privileged EXEC mode.                                                                                                                          |

|        | Command or Action                                                                                                                                                                                                   | Purpose                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <b>show isis database verbose</b><br><br><b>Example:</b><br>Router# show isis database verbose                                                                                                                      | (Optional) Displays details about the IS-IS link-state database, including the route tag. <ul style="list-style-type: none"> <li>Perform this step if you want to verify the tag.</li> </ul> |
| Step 9 | <b>show ip route</b> <i>[[ip-address [mask] [longer-prefixes]]   [protocol [process-id]]   [list access-list-number   access-list-name]]</i><br><br><b>Example:</b><br>Router# show ip route 10.1.1.1 255.255.255.0 | (Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> <li>Perform this step if you want to verify the tag.</li> </ul>                               |

## What to Do Next

Applying the tag does nothing for your network until you use the tag by referencing it in a route map, either to set values, to redistribute routes, or to do both. Proceed to the section, “[Using the Tag to Set Values and/or Redistribute Routes, page 529.](#)”

## Tagging Routes Using a Route Map

Perform this task when you want to redistribute connected routes, static routes or routes from other routing protocols using a route map. You can optionally set some new values for the redistributed routes. You should create the route map first, and then reference the tag (shown in a separate task).

It is possible that you might configure some commands on one router and other commands on another router. For example, you might have a route map that matches on a tag and sets a different tag on a router at the edge of a network, and on different routers configure the redistribution of routes based on the route map.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* **[permit | deny]** *[sequence-number]*
4. **match tag** *tag-number* *[...tag-number]*
5. Use an additional **match** command for each match criterion you want.
6. **set tag** *tag-number*
7. Set another value, depending on what else you want to do with the tagged routes.
8. Repeat Step 7 for each value you want to set.
9. Repeat Steps 3 through 8 for each route-map statement you want.
10. **end**
11. **show isis database verbose**
12. **show ip route** *[[ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name]]*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                          |
| Step 3 | <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ]<br>[ <i>sequence-number</i> ]<br><br><b>Example:</b><br>Router(config)# route-map static-color permit 15 | Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another. <ul style="list-style-type: none"> <li>This command causes the router to enter route-map configuration mode.</li> </ul>                                                        |
| Step 4 | <b>match tag</b> <i>tag-number</i> [... <i>tag-number</i> ]<br><br><b>Example:</b><br>Router(config-route-map)# match tag 15                                             | (Optional) Matches routes tagged with the specified tag numbers. <ul style="list-style-type: none"> <li>If you are setting a tag for the first time, you cannot match on tag; this step is an option if you are changing tags.</li> </ul>                                                                  |
| Step 5 | Use an additional <b>match</b> command for each match criterion you want.                                                                                                | (Optional) Refer to the appropriate <b>match</b> commands in the “IP Routing Protocol-Independent Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> . <ul style="list-style-type: none"> <li>Repeat this step for each match criterion you want.</li> </ul> |
| Step 6 | <b>set tag</b> <i>tag-number</i><br><br><b>Example:</b><br>Router(config-route-map)# set tag 10                                                                          | Specifies the tag number to set.                                                                                                                                                                                                                                                                           |

|         | Command or Action                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | Set another value, depending on what else you want to do with the tagged routes.                                                                                                                                                                                              | (Optional) Reference the appropriate <b>set</b> commands in the “IP Routing Protocol-Independent Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> , such as: <ul style="list-style-type: none"> <li>• <b>set default interface</b></li> <li>• <b>set interface</b></li> <li>• <b>set ip default next-hop</b></li> <li>• <b>set default interface</b></li> <li>• <b>set ip next-hop</b></li> <li>• <b>set ip next-hop verify-availability</b></li> <li>• <b>set ip precedence</b></li> <li>• <b>set level</b></li> <li>• <b>set local-preference</b></li> <li>• <b>set metric</b></li> <li>• <b>set metric-type</b></li> <li>• <b>set next-hop</b></li> </ul> |
| Step 8  | Repeat Step 7 for each value you want to set.                                                                                                                                                                                                                                 | (Optional)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 9  | Repeat Steps 3 through 8 for each route-map statement you want.                                                                                                                                                                                                               | (Optional)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-route-map)# end                                                                                                                                                                                                            | (Optional) Exits configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 11 | <b>show isis database verbose</b><br><br><b>Example:</b><br>Router# show isis database verbose                                                                                                                                                                                | (Optional) Displays details about the IS-IS link-state database, including the route tag. <ul style="list-style-type: none"> <li>• Perform this step if you want to verify the tag.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 12 | <b>show ip route</b> [[ <i>ip-address</i> [ <i>mask</i> ]<br>[ <i>longer-prefixes</i> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]  <br>[ <i>list access-list-number</i>   <i>access-list-name</i> ]]<br><br><b>Example:</b><br>Router# show ip route 10.1.1.1 255.255.255.0 | (Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> <li>• Perform this step if you want to verify the tag.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## What to Do Next

Applying the tag does nothing for your network until you use the tag by referencing it in a route map, either to set values, to redistribute routes, or to do both. Proceed to the section, “[Using the Tag to Set Values and/or Redistribute Routes, page 529.](#)”

## Tagging a Summary Address

Perform this task if you want to summarize IS-IS routes at an area boundary or level boundary and tag the summarized route. You will later use the tag to set values for the summarized route.



### Note

If a tagged route is summarized and the tag is not explicitly configured in the **summary-address** command, then the tag is lost.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **summary-address** *address mask* {**level-1** | **level-1-2** | **level-2**} [**tag** *tag-number*] [**metric** *metric-value*]
6. **end**
7. **show isis database verbose**
8. **show ip route** [[*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]]

## DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                             |
| Step 3 | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis                    | Enables the IS-IS routing protocol and specifies an IS-IS process.                                                            |
| Step 4 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide | Configures a router running IS-IS so that it generates and accepts Type, Length, and Value object (TLV) 135 for IP addresses. |

|        | Command or Action                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>summary-address</b> <i>address mask</i> { <b>level-1</b>   <b>level-1-2</b>   <b>level-2</b> } [ <b>tag</b> <i>tag-number</i> ] [ <b>metric</b> <i>metric-value</i> ]<br><br><b>Example:</b><br>Router(config-router)# summary-address 192.168.0.0 255.255.0.0 tag 12345 metric 321 | Creates aggregate addresses for IS-IS.                                                                                                                                                       |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                                                                                                                        | (Optional) Exits configuration mode and returns to privileged EXEC mode.                                                                                                                     |
| Step 7 | <b>show isis database verbose</b><br><br><b>Example:</b><br>Router# show isis database verbose                                                                                                                                                                                         | (Optional) Displays details about the IS-IS link-state database, including the route tag. <ul style="list-style-type: none"> <li>Perform this step if you want to verify the tag.</li> </ul> |
| Step 8 | <b>show ip route</b> [[ <i>ip-address</i> [ <i>mask</i> ] [ <i>longer-prefixes</i> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]   [ <i>list</i> <i>access-list-number</i>   <i>access-list-name</i> ]]<br><br><b>Example:</b><br>Router# show ip route 10.1.1.1 255.255.255.0         | (Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> <li>Perform this step if you want to verify the tag.</li> </ul>                               |

## What to Do Next

Applying the tag does nothing for your network until you use the tag by referencing it in a route map to set value. It is unlikely that you will redistribute summary routes. Proceed to the section, “[Using the Tag to Set Values and/or Redistribute Routes, page 529](#).”

## Using the Tag to Set Values and/or Redistribute Routes

Now that you have applied a tag to one or more routes, you can use that tag to set various values for routes or to redistribute the routes, or both. This task shows you how to set values and redistribute routes. Note that it is likely you are using the tag on a different router from the router on which you applied the tag.

## Prerequisites

You must have already applied a tag either on the interface, in a route map, or on a summary route. See the section “[Tagging IS-IS Routes, page 523](#).”

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match tag** *tag-number*

5. Specify a **match** command for each match criterion you want.
6. Set a value, depending on what you want to do with the tagged routes.
7. Repeat Step 6 for each value you want to set.
8. Repeat Steps 3 through 7 for each route-map statement you want.
9. **exit**
10. **exit**
11. **router isis**
12. **metric-style wide**
13. **redistribute protocol** [*process-id*] [**level-1** | **level-1-2** | **level-2**] [**metric metric-value**] [**metric-type type-value**] [**route-map map-tag**]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                    | Enters global configuration mode.                                                                                                                                                                                                            |
| Step 3 | <b>route-map map-tag</b> [ <b>permit</b>   <b>deny</b> ]<br>[ <i>sequence-number</i> ]<br><br><b>Example:</b><br>Router(config)# route-map static-color permit 15 | Defines the conditions for redistributing routes from one routing protocol into another or from one IS-IS level to another. <ul style="list-style-type: none"><li>• This command causes you to enter route-map configuration mode.</li></ul> |
| Step 4 | <b>match tag tag-number</b><br><br><b>Example:</b><br>Router(config-route-map)# match tag 120                                                                     | (Optional) Applies the subsequent set commands to routes that match routes tagged with this tag number.                                                                                                                                      |
| Step 5 | Specify a <b>match</b> command for each match criterion you want.                                                                                                 | (Optional) Reference the appropriate <b>match</b> commands in the “IP Routing Protocol-Independent Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> .                                        |



|                | Command or Action                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b>  | Set a value, depending on what you want to do with the tagged routes.    | (Optional) Reference the appropriate <b>set</b> commands in the “IP Routing Protocol-Independent Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> , such as <ul style="list-style-type: none"> <li>• <b>set default interface</b></li> <li>• <b>set interface</b></li> <li>• <b>set ip default next-hop</b></li> <li>• <b>set default interface</b></li> <li>• <b>set ip next-hop</b></li> <li>• <b>set ip next-hop verify-availability</b></li> <li>• <b>set ip precedence</b></li> <li>• <b>set level</b></li> <li>• <b>set local-preference</b></li> <li>• <b>set metric</b></li> <li>• <b>set metric-type</b></li> <li>• <b>set next-hop</b></li> <li>• <b>set tag</b></li> </ul> |
| <b>Step 7</b>  | Repeat Step 6 for each value you want to set.                            | (Optional)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 8</b>  | Repeat Steps 3 through 7 for each route-map statement you want.          | (Optional)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config-route-map)# exit     | (Optional) Returns to the next higher configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 10</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit        | (Optional) Returns to the next higher configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 11</b> | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis | (Optional) Enables the IS-IS routing protocol and specifies an IS-IS process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                                                                                                                    | Purpose                                                                                                                       |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Step 12 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                                                                                                                                                          | Configures a router running IS-IS so that it generates and accepts Type, Length, and Value object (TLV) 135 for IP addresses. |
| Step 13 | <b>redistribute protocol [process-id] [level-1   level-1-2   level-2] [metric metric-value] [metric-type type-value] [route-map map-tag]</b><br><br><b>Example:</b><br>Router(config-router)# redistribute static ip metric 2 route-map static-color | (Optional) Redistributes routes from one routing domain into another routing domain.                                          |

## Configuration Examples for IS-IS Support for Route Tags

This section provides the following examples:

- [Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them: Example, page 532](#)
- [Redistributing IS-IS Routes Using a Route-Map: Example, page 533](#)
- [Tagging a Summary Address and Applying a Route Map: Example, page 533](#)
- [Filtering and Redistributing IS-IS Routes Using an Access List and a Route Map: Example, page 534](#)

### Tagging Routes for Networks Directly Connected to an Interface and Redistributing Them: Example

In this example, two interfaces are tagged with different tag values. By default, these two IP addresses would have been put into the IS-IS Level 1 and Level 2 database. However, by using the **redistribute** command with a route map to match tag 110, only IP address 20.1.1.1 255.255.255.0 is put into the Level 2 database.

```
interface ethernet 1/0
ip address 10.1.1.1 255.255.255.0
ip router isis
isis tag 120
interface ethernet 1/1
ip address 20.1.1.1 255.255.255.0
ip router isis
isis tag 110
router isis
net 49.0001.0001.0001.0001.00
redistribute isis ip level-1 into level-2 route-map match-tag
route-map match-tag permit 10
match tag 110
```

## Redistributing IS-IS Routes Using a Route-Map: Example

In a scenario using route tags, you might configure some commands on one router and other commands on another router. For example, you might have a route map that matches on a tag and sets a different tag on a router at the edge of a network, and on different routers configure the redistribution of routes based on a tag in a different route map.

**Figure 40** Example of Redistributing IS-IS Routes Using a Route Tag

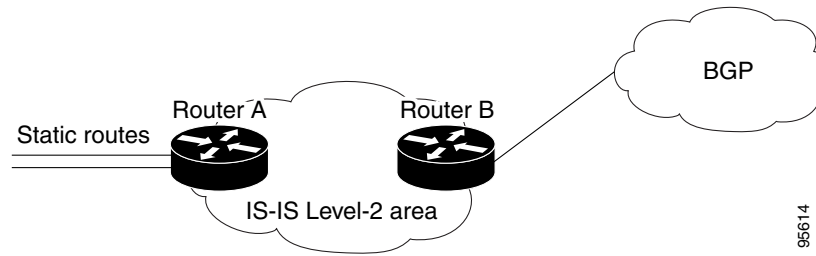


Figure 40 illustrates a flat Level 2 IS-IS area. On the left edge are static routes from Router A to reach some IP prefixes. Router A redistributes the static routes into IS-IS. Router B runs BGP and redistributes IS-IS routes into BGP and then uses the tag to apply different administrative policy based on different tag values.

### Router A

```
router isis
 net 49.0000.0000.0001.00
 metric-style wide
 redistribute static ip route-map set-tag
!
route-map set-tag permit 5
 set tag 10
```

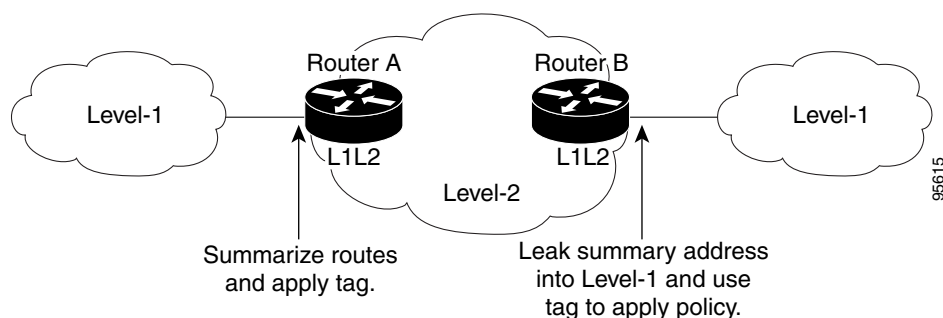
### Router B

```
router bgp 100
 redistribute isis level-2 route-map tag-policy
route-map tag-policy permit 20
 match tag 10
 set metric 1000
```

## Tagging a Summary Address and Applying a Route Map: Example

Figure 2 illustrates two Level 1 areas and a Level 2 area between them. Router A and Router B are Level 1/Level 2 edge routers in the Level 2 area. On edge Router A, a summary address is configured to reduce the number of IP addresses put into the Level 2 IS-IS database. Also, a tag value of 100 is set to the summary address.

On Router B, the summary address is leaked into the Level 1 area and administrative policy is applied based on the tag value.

**Figure 41** Tag on a Summary Address**Router A**

```
router isis
 net 49.0001.0001.0001.00
 metric-style wide
 summary-address 10.0.0.0 255.0.0.0 tag 100
```

**Router B**

```
router isis
 net 49.0002.0002.0002.0002.0
 metric-style wide
 redistribute isis ip level-2 into level-1 route-map match-tag
 route-map match-tag permit 10
 match tag 100
```

## Filtering and Redistributing IS-IS Routes Using an Access List and a Route Map: Example

In this example, the first **redistribute isis ip** command controls the redistribution of Level 1 routes into Level 2. Only the routes with the tag of 90 and whose IP prefix is not 3.3.3.3/32 will be redistributed from Level 1 into Level 2.

The second **redistribute isis ip** command controls the route leaking from Level 2 into Level 1 domain. Only the routes tagged with 60 or 50 will be redistributed from Level 2 into Level 1.

```
interface ethernet 1
 ip address 3.3.3.3 255.255.255.0
 ip router isis
 isis tag 60
!
interface ethernet 2
 ip address 10.10.10.1 255.255.255.0
 ip router isis
 isis tag 90
!
interface ethernet 3
 ip address 20.20.20.20 255.255.255.0
 ip router isis
 isis tag 50
!
```

```

router isis
 net 49.0001.0001.0001.00
 metric-style wide
 redistribute isis ip level-1 into level-2 route-map redist1-2
 redistribute isis ip level-2 into level-1 route-map leak2-1
 !
 access-list 102 deny ip host 3.3.3.3 host 255.255.255.255
 access-list 102 permit ip any any
 !
 route-map leak2-1 permit 10
  match tag 60
 !
 route-map leak2-1 permit 20
  match tag 50
 !
 route-map redist1-2 permit 10
  match ip address 102
  match tag 90

```

## Additional References

The following sections provide references related to IS-IS Support for Route Tags.

## Related Documents

| Related Topic                                              | Document Title                                                                                                                                                                            |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS configuration tasks                                  | “Configuring Integrated IS-IS” chapter of the <i>Cisco IOS IP Configuration Guide, Release 12.3</i>                                                                                       |
| IS-IS commands                                             | “Integrated IS-IS Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> .                                                                      |
| Route redistribution                                       | <i>Redistributing Routing Protocols</i> at:<br><a href="http://www.cisco.com/warp/public/105/redist.html">http://www.cisco.com/warp/public/105/redist.html</a>                            |
| Redistribute Routing Information configuration tasks       | “Configuring Routing Protocol-Independent Features” chapter of the <i>Cisco IOS IP Configuration Guide, Release 12.3</i>                                                                  |
| The <b>route-map</b> and <b>redistribute</b> (IP) commands | “IP Routing Protocol-Independent Commands” chapter of the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> .                                                       |
| IS-IS route leaking                                        | <i>IS-IS Route Leaking Overview</i> at:<br><a href="http://www.cisco.com/warp/public/97/route-leak.html">http://www.cisco.com/warp/public/97/route-leak.html</a>                          |
| IS-IS TLVs                                                 | <i>Intermediate System-to-Intermediate System (IS-IS) TLVs</i> at:<br><a href="http://www.cisco.com/warp/public/97/tlvs_5739.html">http://www.cisco.com/warp/public/97/tlvs_5739.html</a> |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Commands

- **isis tag**
- **redistribute isis**

### Modified Commands

- **show ip route**
- **show isis database verbose**
- **summary-address (IS-IS)**



## Integrated IS-IS Global Default Metric

The Integrated IS-IS Global Default Metric feature allows you to change the global Intermediate System-to-Intermediate System (IS-IS) default metric for interfaces so that you need not change the metric values for the interfaces one by one. All interfaces that had the original IS-IS default metric 10 will be configured with the new default value.

### Feature History for the Integrated IS-IS Global Default Metric Feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(4)T    | This feature was introduced.                                    |
| 12.0(27)S   | This feature was integrated into Cisco IOS Release 12.0(27)S.   |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Integrated IS-IS Global Default Metric, page 537](#)
- [Restrictions for Integrated IS-IS Global Default Metric, page 538](#)
- [Information About Integrated IS-IS Global Default Metric, page 538](#)
- [How to Configure the Integrated IS-IS Global Default Metric Feature, page 538](#)
- [Configuration Examples for the Integrated IS-IS Global Default Metric Feature, page 541](#)
- [Additional References, page 545](#)
- [Command Reference, page 546](#)

## Prerequisites for Integrated IS-IS Global Default Metric

- You must have IS-IS configured in your network.
- You must be familiar with IPv4. Refer to the publications referenced in the “[Related Documents](#)” section for IPv4 configuration and command reference information.

- You must be familiar with IPv6 addressing and basic configuration. Refer to the publications referenced in the “[Related Documents](#)” section for implementing basic connectivity for IPv6.

## Restrictions for Integrated IS-IS Global Default Metric

If you have already configured a metric for a specific interface by entering either the **isis metric** command or the **isis ipv6 metric** command, the metric that has been configured for that specific interface will take precedence over any global default set by the **metric** command introduced by this feature.

## Information About Integrated IS-IS Global Default Metric

Before you enable the Integrated IS-IS Global Default Metric feature, you should understand the following concept:

- [Benefits of Using the Integrated IS-IS Global Default Metric Feature, page 538](#)

## Benefits of Using the Integrated IS-IS Global Default Metric Feature

IS-IS has a default active interface metric value of 10 in Cisco IOS software. If the interface is passive, the default value is zero. You can change the metric value for a specific interface by using the **isis metric** command or the **isis ipv6 metric** command. If all IS-IS interfaces metric values need to be changed to some value other than the default value, the change needs to be made one by one on all IS-IS interfaces.

The Integrated IS-IS Global Default Metric feature allows you to use one command to change the metric value globally for all IS-IS interfaces. Besides offering the user the convenience of being able to globally configure the value for all IS-IS interfaces, the feature helps prevent errors that occur when interfaces are individually configured to change the metric value: user can remove metrics from an interface and then add the interface back into IS-IS without a set metric, thereby allowing the default metric 10—unintentionally making that interface a highly preferred one in the network. Such an occurrence on the wrong interface could mean the rerouting of traffic across the network on an undesirable path.

## How to Configure the Integrated IS-IS Global Default Metric Feature

This section contains the following procedures:

- [Changing the Global IS-IS IPv4 Default Metric for IPv4 Networks, page 538](#)
- [Changing the Global IS-IS IPv6 Default Metric for IPv6 Networks, page 540](#)

## Changing the Global IS-IS IPv4 Default Metric for IPv4 Networks

This section describes how to change the global IS-IS IPv4 default metric for interfaces for networks using IPv4.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*tag*]
4. **net** *network-entity-title*
5. **metric-style wide**
6. **metric** *default-value* [**level-1** | **level-2**]
7. **end**
8. **show clns interface** *type number*

## DETAILED STEPS

|        | Command                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>router isis</b> [ <i>tag</i> ]<br><br><b>Example:</b><br>Router(config)# router isis 1                                                 | Enables the IS-IS routing protocol and specifies an IS-IS process. Enters router configuration mode.                                                                                                                                                                                                                                              |
| Step 4 | <b>net</b> <i>network-entity-title</i><br><br><b>Example:</b><br>Router(config-router)# net 01.0000.0309.1234.0                           | Configures an IS-IS network entity title (NET) for a Connectionless Network Service (CLNS) routing process.                                                                                                                                                                                                                                       |
| Step 5 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                                               | (Optional) Configures a router running IS-IS so that it generates and accepts type, length, and value (TLV) object 135 for IP addresses.<br><ul style="list-style-type: none"><li>• If you do not enter the <b>metric-style wide</b> command, the default metric style is narrow.</li></ul>                                                       |
| Step 6 | <b>metric</b> <i>default-value</i> [ <b>level-1</b>   <b>level-2</b> ]<br><br><b>Example:</b><br>Router(config-router)# metric 25 level-2 | Globally sets a new default metric value for all IS-IS interfaces.<br><ul style="list-style-type: none"><li>• The value 25 shown in the example will apply only to Level 2 IS-IS interfaces. If you do not enter the <b>level-1</b> or <b>level-2</b> keyword, the metric will be applied to both Level 1 and Level 2 IS-IS interfaces.</li></ul> |

|        | Command                                                                                                          | Purpose                                                                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                  | Exits router configuration mode.                                                                                                                                                          |
| Step 8 | <b>show clns interface</b> <i>type number</i><br><br><b>Example:</b><br>Router# show clns interface ethernet 0/1 | Optional. Lists the CLNS-specific information about each interface. <ul style="list-style-type: none"> <li>Enter this command if you want to verify the global default metric.</li> </ul> |

## Changing the Global IS-IS IPv6 Default Metric for IPv6 Networks

This section describes how to change the global IS-IS IPv6 default metric for interfaces for IS-IS IPv6 networks.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **router isis** [*tag*]
5. **net** *network-entity-title*
6. **metric-style wide**
7. **address-family ipv6** [*unicast*]
8. **metric** *default-value* [*level-1* | *level-2*]
9. **exit-address-family**
10. **end**
11. **show clns interface** *type number*

### DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|         | Command                                                                                                     | Purpose                                                                                                                                                                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3  | <b>ipv6 unicast-routing</b><br><br><b>Example:</b><br>Router(config)# ipv6 unicast-routing                  | Enables the forwarding of IPv6 unicast datagrams.                                                                                                                                                                                                                |
| Step 4  | <b>router isis</b> [tag]<br><br><b>Example:</b><br>Router(config)# router isis 1                            | Enables the IS-IS routing protocol and specifies an IS-IS process. Enters router configuration mode.                                                                                                                                                             |
| Step 5  | <b>net</b> network-entity-title<br><br><b>Example:</b><br>Router(config-router)# net 01.0000.0309.1234.0    | Configures an IS-IS NET for a CLNS routing process.                                                                                                                                                                                                              |
| Step 6  | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                 | Configures a router running IS-IS so that it generates and accepts TLV object 135 for IP addresses.<br><ul style="list-style-type: none"><li>For IS-IS IPv6, the <b>metric-style wide</b> command must be entered.</li></ul>                                     |
| Step 7  | <b>address-family ipv6</b> [unicast]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv6   | Enters address family configuration mode for configuring IS-IS routing sessions that use standard IPv6 address prefixes.                                                                                                                                         |
| Step 8  | <b>metric default-value</b> [level-1   level-2]<br><br><b>Example:</b><br>Router(address-family)# metric 25 | Globally sets a new default metric value for all IS-IS interfaces.<br><ul style="list-style-type: none"><li>If you do not enter the <b>level-1</b> or <b>level-2</b> keyword, the metric will be applied to both Level 1 and Level 2 IS-IS interfaces.</li></ul> |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(address-family)# exit-address-family            | Exits address family configuration mode.                                                                                                                                                                                                                         |
| Step 10 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                           | (Optional) Returns to privileged EXEC mode.                                                                                                                                                                                                                      |
| Step 11 | <b>show clns interface</b> type number<br><br><b>Example:</b><br>Router# show clns interface ethernet 0/1   | Optional. Lists the CLNS-specific information about each interface.<br><ul style="list-style-type: none"><li>Enter this command if you want to verify the global default metric.</li></ul>                                                                       |

## Configuration Examples for the Integrated IS-IS Global Default Metric Feature

This section contains the following configuration examples:

- [Setting a Global Default Metric for IPv4: Example, page 542](#)
- [Setting a Global Default Metric for IPv6: Example, page 544](#)

## Setting a Global Default Metric for IPv4: Example

The following example sets a global default metric of 111 for the IS-IS interfaces.

```
interface Ethernet3/1
ip address 172.16.10.2 255.255.0.0
ip router isis areal
no ip route-cache
duplex half
!
interface Ethernet3/2
ip address 192.10.168.10 255.255.255.0
ip router isis areal
no ip route-cache
duplex half
router isis areal
net 01.0000.0309.1234.00
metric-style wide
metric 111
```

In the following example, the **show clns interface** command confirms that the IS-IS IPv4 interface metric for both Level 1 and Level 2 interfaces is assigned the new default metric value 111:

```
Router# show clns interface

Ethernet3/1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 39 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 922 milliseconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
Ethernet3/2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 20 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x1, local circuit ID 0x2
    Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
    Level-2 IPv6 Metric: 10
```

```

Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-1 Hello in 2 seconds
Next IS-IS LAN Level-2 Hello in 1 seconds

```

In the following example, the **isis metric** command is entered so that it will assign a metric value of 10. The metric value that is set with the **isis metric** command for the specific Ethernet interface 3/1 will take precedence over the metric value that was previously set with the **metric** command.

```

interface Ethernet3/1
 ip address 172.30.10.2 255.255.0.0
 ip router isis area1
 no ip route-cache
 duplex half
 isis metric 10
!
interface Ethernet3/2
 ip address 168.200.10.10 255.255.255.0
 ip router isis area1
 no ip route-cache
 duplex half
router isis area1
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111

```

When the **show clns** command is entered, the router output confirms that the interface has an assigned IS-IS IPv4 metric value of 10:

```

show clns interface
Ethernet3/1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 53 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
      Interface number 0x0, local circuit ID 0x1
      Level-1 Metric: 10, Priority: 64, Circuit ID: mekong.01
      Level-1 IPv6 Metric: 10
      Number of active level-1 adjacencies: 0
      Level-2 Metric: 10, Priority: 64, Circuit ID: mekong.01
      Level-2 IPv6 Metric: 10
      Number of active level-2 adjacencies: 0
      Next IS-IS LAN Level-1 Hello in 4 seconds
      Next IS-IS LAN Level-2 Hello in 4 seconds
Ethernet3/2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 30 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
      Interface number 0x1, local circuit ID 0x2
      Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
      Level-1 IPv6 Metric: 10
      Number of active level-1 adjacencies: 1
      Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
      Level-2 IPv6 Metric: 10
      Number of active level-2 adjacencies: 1
      Next IS-IS LAN Level-1 Hello in 2 seconds

```

Next IS-IS LAN Level-2 Hello in 922 milliseconds

## Setting a Global Default Metric for IPv6: Example

The following example changes the IS-IS IPv6 metric to 10 for Ethernet interface 3/2:

```
interface Ethernet3/1
 ip address 172.19.10.2 255.255.0.0
 ip router isis areal
 no ip route-cache
 duplex half
 isis metric 10
!
interface Ethernet3/2
 ip address 172.29.10.10 255.255.255.0
 ip router isis areal
 no ip route-cache
 duplex half
 isis ipv6 metric 10
!
router isis areal
 net 01.0000.0309.1234.00
 metric-style wide
 metric 111
!
 address-family ipv6
 metric 222
 exit-address-family
!
```

In the following example, the **show clns interface** command is entered and the router output shows that, for IPv6 interfaces, the metric value of 10 that was entered with the **isis ipv6 metric** command takes precedence over the metric value of 222 that has been set with the **metric** command:

```
Router# show clns interface

Ethernet3/1 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 9 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: mekong.01
    Level-1 IPv6 Metric: 222
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: mekong.01
    Level-2 IPv6 Metric: 222
    Number of active level-2 adjacencies: 0
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 3 seconds
Ethernet3/2 is up, line protocol is up
  Checksums enabled, MTU 1497, Encapsulation SAP
  ERPDUs enabled, min. interval 10 msec.
  CLNS fast switching enabled
  CLNS SSE switching disabled
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 36 seconds
  Routing Protocol: IS-IS
```

```

Circuit Type: level-1-2
Interface number 0x1, local circuit ID 0x2
Level-1 Metric: 111, Priority: 64, Circuit ID: mekong.02
Level-1 IPv6 Metric: 10
Number of active level-1 adjacencies: 1
Level-2 Metric: 111, Priority: 64, Circuit ID: mekong.02
Level-2 IPv6 Metric: 10
Number of active level-2 adjacencies: 1
Next IS-IS LAN Level-1 Hello in 482 milliseconds
Next IS-IS LAN Level-2 Hello in 932 milliseconds

```

## Additional References

The following sections provide references related to the Integrated IS-IS Global Default Metric feature.

## Related Documents

| Related Topic                                    | Document Title                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS routing protocol                           | <ul style="list-style-type: none"> <li>“Integrated IS-IS Commands” chapter in the <a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a>, Release 12.3 T</li> <li>“Configuring Integrated IS-IS” chapter in the <a href="#">Cisco IOS IP Configuration Guide</a>, Release 12.3</li> </ul> |
| Configuring IPv6                                 | “Implementing Basic connectivity for IPv6” chapter in the <a href="#">Cisco IOS IPv6 Configuration Library</a>                                                                                                                                                                                                      |
| Configuring the IS-IS protocol for IPv6 networks | “Implementing Multitopology IS-IS for IPv6” chapter in the <a href="#">Integrated IS-IS Multi-Topology for IS-IS IPv6</a> , Release 12.3                                                                                                                                                                            |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **metric**





# Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

This feature allows you to disable the Integrated Intermediate System-to-Intermediate System (IS-IS) protocol at the interface level or at the global IS-IS process level without removing the IS-IS configuration parameters.

## Feature History for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(4)T    | This feature was introduced.                                    |
| 12.0(27)S   | This feature was integrated into Cisco IOS Release 12.0(27)S.   |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, page 548](#)
- [Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, page 548](#)
- [How to Configure Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters, page 549](#)
- [Configuration Examples for the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature, page 551](#)
- [Additional References, page 552](#)
- [Command Reference, page 554](#)

# Prerequisites for Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

It is presumed that you have IS-IS configured in your network.

## Information About Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

Before you enable the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature, you should understand the following concept:

- [Benefits of Using the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature, page 548](#)

## Benefits of Using the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature

Before the introduction of the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature, there was no nondestructive way to disable IS-IS operation. The only way to disable IS-IS at the router level was to issue the **no router isis** command, which removes the IS-IS configuration. At the interface level there are two ways to disable IS-IS operation. You can enter the **no ip router isis** command to either remove IS-IS from the specified interface or you can put the interface into passive mode such that the IP address of the specified interface will still be advertised. In either case, the current IS-IS configuration will be removed.

The Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature allows users to set the IS-IS protocol into an administrative state. If the router was rebooted when the protocol was turned off, the protocol would be expected to come back up in the disabled state. When the protocol is set to the administrative state, network administrators are allowed to administratively turn off the operation of the IS-IS protocol without losing the protocol configuration, to make a series of changes to the protocol configuration without having the operation of the protocol transition through intermediate—and perhaps undesirable—states, and then reenabling the protocol at a suitable time.

At the interface level, the feature will disable the operation of the protocol on the interface, no IS-IS protocol data unit (PDU) will be sent out on the specified interface, and the received IS-IS PDU will be discarded. Any existing adjacencies will be removed and no new adjacencies will be formed. A link-state packet (LSP) will rebuild its IS-IS LSP database to remove the IP address of the specified interface.

At the router level, the feature will completely disable the operation of the protocol by internally controlling timers and other variables. However, IS-IS updates and router processes will remain functioning. The LSP database will be cleared, and all IS-IS routes that have been added to the Routing Information Database (RIB) will be removed, and all adjacencies associated with the IS-IS instance will be deleted.

# How to Configure Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters

- This section contains the following procedures:
- [Shutting Down the IS-IS Protocol in Interface Mode, page 549](#) (optional)
  - [Shutting Down the IS-IS Protocol and Maintaining IS-IS Configuration Parameters in Router Mode, page 550](#) (optional)

## Shutting Down the IS-IS Protocol in Interface Mode

This task describes how to disable the IS-IS protocol in interface configuration mode so that it will not form adjacencies in the specified interface. The IP address of the specified interface will be placed into the LSP that is generated by the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **isis protocol shutdown**
5. **end**

### DETAILED STEPS

|        | Command                                                                                            | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0 | Configures an interface and enters interface configuration mode.                                                 |

|        | Command                                                                                           | Purpose                                                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>isis protocol shutdown</b><br><br><b>Example:</b><br>Router(config-if)# isis protocol shutdown | Disables the IS-IS protocol so that it cannot form adjacencies on a specified interface and places the IP address of the interface into the LSP that is generated by the router. |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                       | (Optional) Saves configuration commands to the running configuration file, exits interface configuration mode, and returns the router to privileged EXEC mode.                   |

## Shutting Down the IS-IS Protocol and Maintaining IS-IS Configuration Parameters in Router Mode

This task describes how to disable the IS-IS protocol in router configuration mode so that no adjacencies are formed on any interface and that the IS-IS LSP database is cleared while IS-IS still runs on the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis area-tag**
4. **protocol shutdown**
5. **end**

### DETAILED STEPS

|        | Command                                                                             | Purpose                                                                                                            |
|--------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal      | Enters global configuration mode.                                                                                  |
| Step 3 | <b>router isis area-tag</b><br><br><b>Example:</b><br>Router(config)# router isis 1 | Enables the IS-IS routing protocol and specifies an IS-IS process. Enters router configuration mode.               |

|        | Command                                                                                     | Purpose                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>protocol shutdown</b><br><br><b>Example:</b><br>Router(config-router)# protocol shutdown | Prevents IS-IS from forming any adjacency on any interface and clears the IS-IS LSP database, without actually removing the IS-IS configuration. |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                             | (Optional) Saves configuration commands to the running configuration file, exits router configuration mode, and returns to privileged EXEC mode. |

## Configuration Examples for the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters Feature

This section contains the following configuration examples:

- [Shutting Down the IS-IS Protocol in Interface Mode: Example, page 551](#)
- [Shutting Down the IS-IS Protocol in Router Mode: Example, page 552](#)

### Shutting Down the IS-IS Protocol in Interface Mode: Example

The following router output shows that the router has two IS-IS adjacencies:

```
Router# show clns neighbors
```

| System Id | Interface | SNPA           | State | Holdtime | Type | Protocol |
|-----------|-----------|----------------|-------|----------|------|----------|
| first     | Et3/1     | 0002.7dd6.1c21 | Up    | 25       | L1L2 | IS-IS    |
| second    | Et3/2     | 0004.6d25.c056 | Up    | 29       | L1L2 | IS-IS    |

When the **isis protocol shutdown** command is entered for Ethernet interface 3/1, the IS-IS protocol will be disabled for the specified interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e3/1
Router(config-if)# isis protocol shutdown
Router(config-if)# end
```

The following router output shows that the adjacency for interface 3/1 has not formed:

```
Router# show clns neighbors
```

| System Id | Interface | SNPA           | State | Holdtime | Type | Protocol |
|-----------|-----------|----------------|-------|----------|------|----------|
| second    | Et3/2     | 0004.6d25.c056 | Up    | 27       | L1L2 | IS-IS    |

## Shutting Down the IS-IS Protocol in Router Mode: Example

The following router output shows that the router has two IS-IS adjacencies:

| System Id | Interface | SNPA           | State | Holdtime | Type | Protocol |
|-----------|-----------|----------------|-------|----------|------|----------|
| south     | Et3/1     | 0002.7dd6.1c21 | Up    | 29       | L1L2 | IS-IS    |
| north     | Et3/2     | 0004.6d25.c056 | Up    | 28       | L1L2 | IS-IS    |

The **protocol shutdown** command is entered so that IS-IS is disabled and no adjacencies will be formed on any interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# router isis area1
Router(config-router)# protocol shutdown
Router(config-router)# end
```

The following router output now shows that both adjacencies are gone.

| System Id | Interface | SNPA | State | Holdtime | Type | Protocol |
|-----------|-----------|------|-------|----------|------|----------|
|-----------|-----------|------|-------|----------|------|----------|

When the **no protocol shutdown** command is entered, the adjacencies will again be formed on both interfaces:

```
Router(config)# router isis area1
Router(config-router)# no protocol shutdown
Router(config-router)# end
Router# show clns neighbors
```

| System Id | Interface | SNPA           | State | Holdtime | Type | Protocol |
|-----------|-----------|----------------|-------|----------|------|----------|
| south     | Et3/1     | 0002.7dd6.1c21 | Up    | 24       | L1L2 | IS-IS    |
| north     | Et3/2     | 0004.6d25.c056 | Up    | 24       | L1L2 | IS-IS    |

## Additional References

The following sections provide references related to the Integrated IS-IS Protocol Shutdown Support Maintaining Configuration Parameters feature.

## Related Documents

| Related Topic          | Document Title                                                                                                                                                                                                                                                                   |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS routing protocol | <ul style="list-style-type: none"><li>“Integrated IS-IS Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i>, Release 12.3 T</li><li>“Configuring Integrated IS-IS” chapter in the <i>Cisco IOS IP Configuration Guide</i></li></ul> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

# Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **isis protocol shutdown**
- **protocol shutdown**





# IS-IS Caching of Redistributed Routes

The IS-IS Caching of Redistributed Routes feature improves Intermediate System-to-Intermediate System (IS-IS) convergence time when routes are being redistributed into IS-IS. This document introduces new commands for monitoring and maintaining IS-IS redistributed routes.

## Feature History for the IS-IS Caching of Redistributed Routes Feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(27)S   | This feature was introduced.                                    |
| 12.3(7)T    | This feature was integrated into Cisco IOS Release 12.3(7)T.    |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About IS-IS Caching of Redistributed Routes, page 556](#)
- [How to Use the IS-IS Caching of Redistributed Routes Feature, page 556](#)
- [Additional References, page 557](#)
- [Command Reference, page 558](#)

# Information About IS-IS Caching of Redistributed Routes

The IS-IS Caching of Redistributed Routes feature is enabled by default. However, you should understand the concept in the following section:

- [Benefits of Caching of Redistributed Routes, page 556](#)

## Benefits of Caching of Redistributed Routes

Beginning with Cisco IOS Release 12.0(27)S, IS-IS caches routes that are redistributed from other routing protocols or from another IS-IS level into a local redistribution cache that is maintained by IS-IS. Caching occurs automatically and requires no configuration. The caching of redistributed routes improves IS-IS convergence time when routes are being redistributed into IS-IS.

## How to Use the IS-IS Caching of Redistributed Routes Feature

This section contains the following procedure:

- [Monitoring the IS-IS Caching of Redistributed Routes Feature, page 556](#) (optional)

## Monitoring the IS-IS Caching of Redistributed Routes Feature

This task monitors the IS-IS Caching of Redistributed Routes feature. The commands in steps 2 through four of this task can be entered in any order, as needed.

### SUMMARY STEPS

1. **enable**
2. **clear isis rib redistribution** [level-1 | level-2] [network-prefix] [network-mask]
3. **debug isis rib redistribution** [level-1 | level-2] [access-list]
4. **show isis rib redistribution** [level-1 | level-2] [network-prefix]

### DETAILED STEPS

|        | Command or Action                                                                                                                                                | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>clear isis rib redistribution</b> [level-1   level-2] [network-prefix] [network-mask]<br><br><b>Example:</b><br>Router# clear isis rib redistribution level-2 | Clears some or all prefixes in the local redistribution cache.                                                   |

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                         |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>debug isis rib redistribution [level-1   level-2] [access-list]</pre> <p><b>Example:</b><br/>Router# debug isis rib redistribution level-2</p>  | Debugs the local redistribution cache events.                                                                                                                                   |
| Step 4 | <pre>show isis rib redistribution [level-1   level-2] [network-prefix]</pre> <p><b>Example:</b><br/>Router# show isis rib redistribution level-2</p> | Displays the prefixes in the local redistribution cache. <ul style="list-style-type: none"> <li>You can verify if desired routes have been redistributed into IS-IS.</li> </ul> |

## Additional References

The following sections provide references related to the IS-IS Caching of Redistributed Routes feature.

## Related Documents

| Related Topic             | Document Title                                                                                                          |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------|
| IS-IS commands            | “Integrated IS-IS Commands” chapter in the <a href="#">Network Protocols Command Reference</a> , Part 1, Release 12.3 T |
| IS-IS configuration tasks | “Configuring Integrated IS-IS” chapter in the <a href="#">Network Protocols Configuration Guide</a>                     |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                 |
|----------|-----------------------|
| RFC 2328 | <i>OSPF Version 2</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **clear isis rib redistribution**
- **debug isis rib redistribution**
- **show isis rib redistribution**



# IS-IS Fast-Flooding of LSPs Using the fast-flood Command

The IS-IS Fast-Flooding of LSPs Using the fast-flood Command feature improves Intermediate System-to-Intermediate System (IS-IS) convergence time when new link-state packets (LSPs) are generated in the network and shortest path first (SPF) is triggered by the new LSPs. This document introduces the new **fast-flood** command.

## Feature History for the IS-IS Fast-Flooding of LSPs Using the fast-flood Command Feature

| Release   | Modification                                                 |
|-----------|--------------------------------------------------------------|
| 12.0(27)S | This feature was introduced.                                 |
| 12.3(7)T  | This feature was integrated into Cisco IOS Release 12.3(7)T. |



### Note

Software images for Cisco 12000 series Internet routers have been deferred to Cisco IOS Release 12.0(27)S1.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About IS-IS Fast-Flooding of LSPs Using the fast-flood Command](#), page 560
- [How to Use the IS-IS Fast-Flooding of LSPs Using the fast-flood Command Feature](#), page 560
- [Additional References](#), page 561
- [Command Reference](#), page 562

# Information About IS-IS Fast-Flooding of LSPs Using the fast-flood Command

Before using the **fast-flood** command, you should understand the concept in the following section:

- [Benefits of Fast-Flooding, page 560](#)

## Benefits of Fast-Flooding

If you are using the SPF and if very short values are used for the initial delay required (less than 40 milliseconds), SPF may start before the LSP that triggered SPF is flooded to neighbors. The router should always flood (at least) the LSP that triggered SPF before the router runs the SPF computation.

We recommend that you enable the fast-flooding of LSPs before the router runs the SPF computation, to ensure that the whole network achieves a faster convergence time.

## How to Use the IS-IS Fast-Flooding of LSPs Using the fast-flood Command Feature

This section contains the following procedure:

- [Enabling Fast-Flooding, page 560](#) (optional)

## Enabling Fast-Flooding

Perform this task to enable fast-flooding.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [tag]**
4. **fast-flood *lsp-number***
5. **end**
6. **show running-configuration**

## DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                         | Enters global configuration mode.                                                                                |
| Step 3 | <b>router isis tag</b><br><br><b>Example:</b><br>Router(config)# router isis first                     | Configures an IS-IS routing process and enters router configuration mode.                                        |
| Step 4 | <b>fast-flood lsp-number</b><br><br><b>Example:</b><br>Router(config-router)# fast-flood 12            | Fast-floods LSPs.                                                                                                |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                        | Exits router configuration mode.                                                                                 |
| Step 6 | <b>show running-configuration</b><br><br><b>Example:</b><br>Router(config)# show running-configuration | Verifies that fast-flooding has been enabled.                                                                    |

## Additional References

The following sections provide references related to the IS-IS Fast-Flooding of LSPs Using the fast-flood Command feature.

## Related Documents

| Related Topic             | Document Title                                                                                                                      |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS commands            | “Integrated IS-IS Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.3 T |
| IS-IS configuration tasks | “Configuring Integrated IS-IS” chapter in the <i>Cisco IOS IP Configuration Guide</i>                                               |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                 |
|----------|-----------------------|
| RFC 2328 | <i>OSPF Version 2</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **fast-flood**





## **Part 4: ODR**







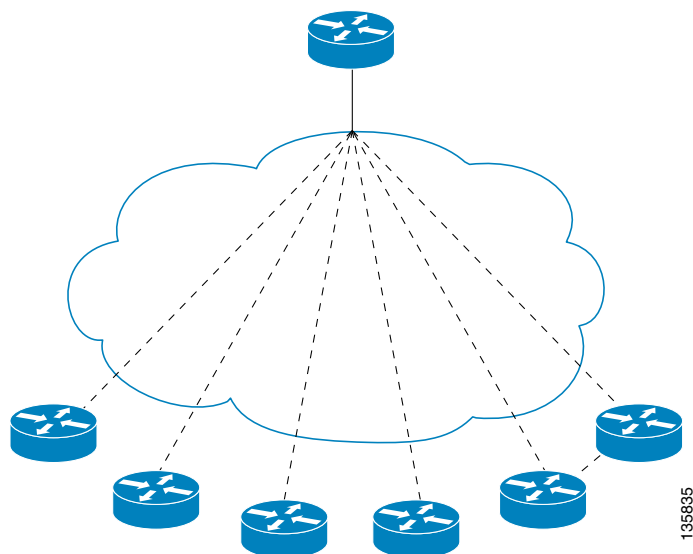
## Configuring On-Demand Routing

This chapter describes how to configure On-Demand Routing (ODR). For a complete description of the ODR commands in this chapter, refer to the “On-Demand Routing Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands in this chapter, use the command reference master index or search online.

ODR is a feature that provides IP routing for stub sites, with minimum overhead. The overhead of a general, dynamic routing protocol is avoided without incurring the configuration and management overhead of static routing.

A *stub router* can be thought of as a spoke router in a hub-and-spoke network topology—as shown in [Figure 42](#)—where the only router to which the spoke is adjacent is the hub router. In such a network topology, the IP routing information required to represent this topology is fairly simple. These stub routers commonly have a WAN connection to the hub router, and a small number of LAN network segments (*stub networks*) are directly connected to the stub router.

**Figure 42** Hub-And-Spoke Network Topology Example



These stub networks might consist only of end systems and the stub router, and thus do not require the stub router to learn any dynamic IP routing information.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

## On-Demand Routing Configuration Task List

To configure ODR, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

- [Enabling ODR](#) (Required)
- [Filtering ODR Information](#) (Optional)
- [Redistributing ODR Information into the Dynamic Routing Protocol of the Hub](#) (Optional)
- [Reconfiguring CDP or ODR Timers](#) (Optional)
- [Using ODR with Dialer Mappings](#) (Optional)

## Enabling ODR

ODR allows you to easily install IP stub networks where the hubs dynamically maintain routes to the stub networks. This installation is accomplished without requiring the configuration of an IP routing protocol on the stubs.

On stub routers that support the ODR feature, the stub router advertises IP prefixes corresponding to the IP networks configured on all directly connected interfaces. If the interface has multiple logical IP networks configured, only the primary IP network is advertised through ODR. Because ODR advertises IP prefixes and not simply IP network numbers, ODR is able to carry variable-length subnet mask (VSLM) information.

To enable ODR, use the following command in global configuration mode:

| Command                           | Purpose                        |
|-----------------------------------|--------------------------------|
| Router(config)# <b>router odr</b> | Enables ODR on the hub router. |

Once ODR is enabled on a hub router, the hub router begins installing stub network routes in the IP forwarding table. The hub router also can be configured to redistribute these routes into any configured dynamic IP routing protocols.

On the stub router, no IP routing protocol must be configured. In fact, from the standpoint of ODR, a router is automatically considered to be a stub when no IP routing protocols have been configured.

ODR uses the Cisco Discovery Protocol (CDP) to carry minimal routing information between the hub and stub routers. The stub routers send IP prefixes to the hub router. The hub router provides default route information to the stub routers, thereby eliminating the need to configure a default route on each stub router.

Using the **no cdp run** global configuration command disables the propagation of ODR stub routing information entirely. Using the **no cdp enable** interface configuration command disables the propagation of ODR information on a particular interface.

## Filtering ODR Information

The hub router will attempt to populate the IP routing table with ODR routes as they are learned dynamically from stub routers. The IP next hop for these routes is the IP address of the neighboring router as advertised through CDP.

Use IP filtering to limit the network prefixes that the hub router will permit to be learned dynamically through ODR.

To filter ODR information, use the following command in router configuration mode:

| Command                                                                                                                                                                                                         | Purpose                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| Router(config-router)# <b>distribute-list</b> <i>access-list-number</i>   <i>access-list-name</i>   <b>prefix</b> <i>list-name</i> { <b>in</b>   <b>out</b> } [ <i>interface-type</i> <i>interface-number</i> ] | Filters ODR information on the hub router. |

For example, the following configuration causes the hub router to only accept advertisements for IP prefixes about (or subnets of) the Class C network 192.168.1.0:

```
Router(config)# access-list 101 permit ip any 192.168.1.0 0.0.0.255
Router(config)# !
Router(config)# router odr
Router(config-router)# distribute-list 101 in
Router(config)# end
```

## Redistributing ODR Information into the Dynamic Routing Protocol of the Hub

This task may be performed by using the **redistribute** router configuration command. The exact syntax depends upon the routing protocol into which ODR is being redistributed.

See the “Redistribute Routing Information” section in the “Configuring IP Routing Protocol-Independent Features” chapter.

## Reconfiguring CDP or ODR Timers

By default, CDP sends updates every 60 seconds. This update interval may not be frequent enough to provide speedy reconvergence of IP routes on the hub router side of the network. A faster reconvergence rate may be necessary if the stub connects to one of several hub routers via asynchronous interfaces such as modem lines.

ODR expects to receive periodic CDP updates containing IP prefix information. When ODR fails to receive such updates for routes that it has installed in the routing table, these ODR routes are first marked invalid and eventually removed from the routing table. (By default, ODR routes are marked invalid after 180 seconds and are removed from the routing table after 240 seconds.) These defaults are based on the default CDP update interval. Configuration changes made to either the CDP or ODR timers should be reflected through changes made to both.

To configure CDP or ODR timers, use the following commands beginning in global configuration mode:

|               | Command                                                                                     | Purpose                                                                  |
|---------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>cdp timer</b> <i>seconds</i>                                             | Changes the rate at which CDP updates are sent.                          |
| <b>Step 2</b> | Router(config)# <b>router odr</b>                                                           | Enables ODR.                                                             |
| <b>Step 3</b> | Router(config-router)# <b>timers basic</b> <i>update invalid holddown flush [sleeptime]</i> | Changes the rate at which ODR routes are expired from the routing table. |

Other CDP features are described in the *Cisco IOS Configuration Fundamentals Configuration Guide*, in the “Monitoring the Router and Network” chapter.

## Using ODR with Dialer Mappings

For interfaces that specify dialer mappings, CDP packets will make use of dialer map configuration statements that pertain to the IP protocol. Because CDP packets are always broadcast packets, these dialer map statements must handle broadcast packets, typically through use of the dialer map **broadcast** keyword. The **dialer string** interface configuration command may also be used.

On DDR interfaces, certain kinds of packets can be classified as interesting. These interesting packets can cause a DDR connection to be made or cause the idle timer of a DDR interface to be reset. For the purposes of DDR classification, CDP packets are considered uninteresting. This classification occurs even while CDP is making use of dialer map statements for IP, where IP packets are classified as interesting.



## **Part 5: OSPF**









## Configuring OSPF

---

This chapter describes how to configure Open Shortest Path First (OSPF). For a complete description of the OSPF commands in this chapter, refer to the “OSPF Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

OSPF is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

We support RFC 1253, *Open Shortest Path First (OSPF) MIB*, August 1991. The OSPF MIB defines an IP routing protocol that provides management information related to OSPF and is supported by Cisco routers.

For protocol-independent features that include OSPF, see the chapter “Configuring IP Routing Protocol-Independent Features” in this book.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

## The Cisco OSPF Implementation

The Cisco implementation conforms to the OSPF Version 2 specifications detailed in the Internet RFC 2328. The list that follows outlines key features supported in the Cisco OSPF implementation:

- Stub areas—Definition of stub areas is supported.
- Route redistribution—Routes learned via any IP routing protocol can be redistributed into any other IP routing protocol. At the intradomain level, OSPF can import routes learned via Interior Gateway Routing Protocol (IGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS). OSPF routes can also be exported into IGRP, RIP, and IS-IS. At the interdomain level, OSPF can import routes learned via Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP). OSPF routes can be exported into BGP and EGP.
- Authentication—Plain text and Message Digest 5 (MD5) authentication among neighboring routers within an area is supported.
- Routing interface parameters—Configurable parameters supported include interface output cost, retransmission interval, interface transmit delay, router priority, router “dead” and hello intervals, and authentication key.

- Virtual links—Virtual links are supported.
- Not so stubby area (NSSA)—RFC 1587.
- OSPF over demand circuit—RFC 1793.

## OSPF Configuration Task List

OSPF typically requires coordination among many internal routers: Area Border Routers (ABRs), which are routers connected to multiple areas, and Autonomous System Boundary Routers (ASBRs). At a minimum, OSPF-based routers or access servers can be configured with all default parameter values, no authentication, and interfaces assigned to areas. If you intend to customize your environment, you must ensure coordinated configurations of all routers.

To configure OSPF, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional, but might be required for your application.

- [Enabling OSPF](#) (Required)
- [Configuring OSPF Interface Parameters](#) (Optional)
- [Configuring OSPF over Different Physical Networks](#) (Optional)
- [Configuring OSPF Area Parameters](#) (Optional)
- [Configuring OSPF NSSA](#) (Optional)
- [Configuring Route Summarization Between OSPF Areas](#) (Optional)
- [Configuring Route Summarization When Redistributing Routes into OSPF](#) (Optional)
- [Creating Virtual Links](#) (Optional)
- [Generating a Default Route](#) (Optional)
- [Configuring Lookup of DNS Names](#) (Optional)
- [Forcing the Router ID Choice with a Loopback Interface](#) (Optional)
- [Controlling Default Metrics](#) (Optional)
- [Changing the OSPF Administrative Distances](#) (Optional)
- [Configuring OSPF on Simplex Ethernet Interfaces](#) (Optional)
- [Configuring Route Calculation Timers](#) (Optional)
- [Configuring OSPF over On-Demand Circuits](#) (Optional)
- [Logging Neighbors Going Up or Down](#) (Optional)
- [Changing the LSA Group Pacing](#) (Optional)
- [Blocking OSPF LSA Flooding](#) (Optional)
- [Reducing LSA Flooding](#) (Optional)
- [Ignoring MOSPF LSA Packets](#) (Optional)
- [Displaying OSPF Update Packet Pacing](#) (Optional)
- [Monitoring and Maintaining OSPF](#) (Optional)

In addition, you can specify route redistribution; see the task “Redistribute Routing Information” in the chapter “Configuring IP Routing Protocol-Independent Features” for information on how to configure route redistribution.

## Enabling OSPF

As with other routing protocols, enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses. To do so, use the following commands beginning in global configuration mode:

|               | Command                                                                                   | Purpose                                                                            |
|---------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                                      | Enables OSPF routing, which places you in router configuration mode.               |
| <b>Step 2</b> | Router(config-router)# <b>network</b> <i>ip-address wildcard-mask area</i> <i>area-id</i> | Defines an interface on which OSPF runs and define the area ID for that interface. |

## Configuring OSPF Interface Parameters

Our OSPF implementation allows you to alter certain interface-specific OSPF parameters, as needed. You are not required to alter any of these parameters, but some interface parameters must be consistent across all routers in an attached network. Those parameters are controlled by the **ip ospf hello-interval**, **ip ospf dead-interval**, and **ip ospf authentication-key** interface configuration commands. Therefore, be sure that if you do configure any of these parameters, the configurations for all routers on your network have compatible values.

To specify interface parameters for your network, use the following commands in interface configuration mode, as needed:

| Command                                                              | Purpose                                                                                                                                       |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-if)# <b>ip ospf cost</b> <i>cost</i>                   | Explicitly specifies the cost of sending a packet on an OSPF interface.                                                                       |
| Router(config-if)# <b>ip ospf retransmit-interval</b> <i>seconds</i> | Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.        |
| Router(config-if)# <b>ip ospf transmit-delay</b> <i>seconds</i>      | Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.                                        |
| Router(config-if)# <b>ip ospf priority</b> <i>number-value</i>       | Sets priority to help determine the OSPF designated router for a network.                                                                     |
| Router(config-if)# <b>ip ospf hello-interval</b> <i>seconds</i>      | Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.                                |
| Router(config-if)# <b>ip ospf dead-interval</b> <i>seconds</i>       | Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet. |
| Router(config-if)# <b>ip ospf authentication-key</b> <i>key</i>      | Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.         |

| Command                                                                                  | Purpose                                                                                                                                                          |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-if)# <b>ip ospf message-digest-key</b> <i>key-id</i> <b>md5</b> <i>key</i> | Enables OSPF MD5 authentication. The values for the <i>key-id</i> and <i>key</i> arguments must match values specified for other neighbors on a network segment. |
| Router(config-if)# <b>ip ospf authentication</b> [ <b>message-digest</b>   <b>null</b> ] | Specifies the authentication type for an interface.                                                                                                              |

## Configuring OSPF over Different Physical Networks

OSPF classifies different media into the following three types of networks by default:

- Broadcast networks (Ethernet, Token Ring, and FDDI)
- Nonbroadcast multiaccess (NBMA) networks (Switched Multimegabit Data Service (SMDS), Frame Relay, and X.25)
- Point-to-point networks (High-Level Data Link Control [HDLC], PPP)

You can configure your network as either a broadcast or an NBMA network.

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. Refer to the **x25 map** and **frame-relay map** command descriptions in the *Cisco IOS Wide-Area Networking Command Reference* publication for more detail.

## Configuring Your OSPF Network Type

You have the choice of configuring your OSPF network type as either broadcast or NBMA, regardless of the default media type. Using this feature, you can configure broadcast networks as NBMA networks when, for example, you have routers in your network that do not support multicast addressing. You also can configure NBMA networks (such as X.25, Frame Relay, and SMDS) as broadcast networks. This feature saves you from needing to configure neighbors, as described in the section “[Configuring OSPF for Nonbroadcast Networks](#)” later in this chapter.

Configuring NBMA, multiaccess networks as either broadcast or nonbroadcast assumes that there are virtual circuits (VCs) from every router to every router or fully meshed network. This is not true for some cases, for example, because of cost constraints, or when you have only a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers not directly connected will go through the router that has VCs to both routers. Note that you need not configure neighbors when using this feature.

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes. An OSPF point-to-multipoint network has the following benefits compared to NBMA and point-to-point networks:

- Point-to-multipoint is easier to configure because it requires no configuration of neighbor commands, it consumes only one IP subnet, and it requires no designated router election.
- It costs less because it does not require a fully meshed topology.
- It is more reliable because it maintains connectivity in the event of VC failure.

To configure your OSPF network type, use the following command in interface configuration mode:

| Command                                                                                                                                                                | Purpose                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Router(config-if)# <b>ip ospf network</b> { <b>broadcast</b>   <b>non-broadcast</b>   { <b>point-to-multipoint</b> [ <b>non-broadcast</b> ]   <b>point-to-point</b> }} | Configures the OSPF network type for a specified interface. |

See the “[OSPF Point-to-Multipoint Example](#)” section at the end of this chapter for an example of an OSPF point-to-multipoint network.

## Configuring Point-to-Multipoint, Broadcast Networks

On point-to-multipoint, broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the **neighbor** router configuration command, in which case you should specify a cost to that neighbor.

Before the **point-to-multipoint** keyword was added to the **ip ospf network** interface configuration command, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the **neighbor** router configuration command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hello, update, and acknowledgment messages were sent using multicast. In particular, multicast hello messages discovered all neighbors dynamically.

On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumed that the cost to each neighbor was equal. The cost was configured with the **ip ospf cost** interface configuration command. In reality, the bandwidth to each neighbor is different, so the cost should differ. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat an interface as point-to-multipoint broadcast and assign a cost to each neighbor, use the following commands beginning in interface configuration mode:

|               | Command                                                       | Purpose                                                                  |
|---------------|---------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config-if)# <b>ip ospf network point-to-multipoint</b> | Configures an interface as point-to-multipoint for broadcast media.      |
| <b>Step 2</b> | Router(config-if)# <b>exit</b>                                | Enters global configuration mode.                                        |
| <b>Step 3</b> | Router(config)# <b>router ospf process-id</b>                 | Configures an OSPF routing process and enters router configuration mode. |
| <b>Step 4</b> | Router(config-router)# <b>neighbor ip-address cost number</b> | Specifies a neighbor and assigns a cost to the neighbor.                 |

Repeat Step 4 for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the **ip ospf cost** interface configuration command.

## Configuring OSPF for Nonbroadcast Networks

Because many routers might be attached to an OSPF network, a *designated router* is selected for the network. Special configuration parameters are needed in the designated router selection if broadcast capability is not configured.

These parameters need only be configured in those devices that are themselves eligible to become the designated router or backup designated router (in other words, routers with a nonzero router priority value).

To configure routers that interconnect to nonbroadcast networks, use the following command in router configuration mode:

| Command                                                                                                                               | Purpose                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Router(config-router)# <b>neighbor</b> <i>ip-address</i><br>[ <b>priority</b> <i>number</i> ] [ <b>poll-interval</b> <i>seconds</i> ] | Configures a router interconnecting to nonbroadcast networks. |

You can specify the following neighbor parameters, as required:

- Priority for a neighboring router
- Nonbroadcast poll interval

On point-to-multipoint, nonbroadcast networks, you now use the **neighbor** router configuration command to identify neighbors. Assigning a cost to a neighbor is optional.

Prior to Cisco IOS Release 12.0, some customers were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), so their routers could not dynamically discover their neighbors. This feature allows the **neighbor** router configuration command to be used on point-to-multipoint interfaces.

On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumed the cost to each neighbor was equal. The cost was configured with the **ip ospf cost** interface configuration command. In reality, the bandwidth to each neighbor is different, so the cost should differ. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

To treat the interface as point-to-multipoint when the media does not support broadcast, use the following commands beginning in interface configuration mode:

|               | Command                                                                                | Purpose                                                                  |
|---------------|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config-if)# <b>ip ospf network point-to-multipoint non-broadcast</b>            | Configures an interface as point-to-multipoint for nonbroadcast media.   |
| <b>Step 2</b> | Router(config-if)# <b>exit</b>                                                         | Enters global configuration mode.                                        |
| <b>Step 3</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                                   | Configures an OSPF routing process and enters router configuration mode. |
| <b>Step 4</b> | Router(config-router)# <b>neighbor</b> <i>ip-address</i> [ <b>cost</b> <i>number</i> ] | Specifies a neighbor and assigns a cost to the neighbor.                 |

Repeat Step 4 for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the **ip ospf cost** interface configuration command.

## Configuring OSPF Area Parameters

Our OSPF software allows you to configure several area parameters. These area parameters, shown in the following task table, include authentication, defining stub areas, and assigning specific costs to the default summary route. *Authentication* allows password-based protection against unauthorized access to an area.

*Stub areas* are areas into which information on external routes is not sent. Instead, there is a default external route generated by the ABR, into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, *default routing* must be used in the stub area. To further reduce the number of LSAs sent into a stub area, you can configure the **no-summary** keyword of the **area stub** router configuration command on the ABR to prevent it from sending summary link advertisement (LSAs type 3) into the stub area.

To specify an area parameter for your network, use the following commands in router configuration mode as needed:

| Command                                                                  | Purpose                                                                      |
|--------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Router(config-router)# <b>area area-id authentication</b>                | Enables authentication for an OSPF area.                                     |
| Router(config-router)# <b>area area-id authentication message-digest</b> | Enables MD5 authentication for an OSPF area.                                 |
| Router(config-router)# <b>area area-id stub [no-summary]</b>             | Defines an area to be a stub area.                                           |
| Router(config-router)# <b>area area-id default-cost cost</b>             | Assigns a specific cost to the default summary route used for the stub area. |

## Configuring OSPF NSSA

The OSPF implementation of NSSA is similar to OSPF stub area. NSSA does not flood type 5 external LSAs from the core into the area, but it can import autonomous system external routes in a limited fashion within the area.

NSSA allows importing of type 7 autonomous system external routes within NSSA area by redistribution. These type 7 LSAs are translated into type 5 LSAs by NSSA ABRs, which are flooded throughout the whole routing domain. Summarization and filtering are supported during the translation.

Use NSSA to simplify administration if you are an Internet service provider (ISP) or a network administrator that must connect a central site using OSPF to a remote site that is using a different routing protocol.

Prior to NSSA, the connection between the corporate site border router and the remote router could not be run as OSPF stub area because routes for the remote site could not be redistributed into stub area, and two routing protocols needed to be maintained. A simple protocol like RIP was usually run and handled the redistribution. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

To specify area parameters as needed to configure OSPF NSSA, use the following command in router configuration mode:

| Command                                                                                             | Purpose                     |
|-----------------------------------------------------------------------------------------------------|-----------------------------|
| Router(config-router)# <b>area area-id nssa [no-redistribution] [default-information-originate]</b> | Defines an area to be NSSA. |

To control summarization and filtering of type 7 LSAs into type 5 LSAs, use the following command in router configuration mode on the ABR:

| Command                                                                                              | Purpose                                                          |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Router(config-router)# <b>summary</b> address prefix mask [ <b>not advertise</b> ] [ <b>tag</b> tag] | Controls the summarization and filtering during the translation. |

## Implementation Considerations

Evaluate the following considerations before you implement this feature:

- You can set a type 7 default route that can be used to reach external destinations. When configured, the router generates a type 7 default into the NSSA or the NSSA ABR.
- Every router within the same area must agree that the area is NSSA; otherwise, the routers will not be able to communicate.

## Configuring Route Summarization Between OSPF Areas

*Route summarization* is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

To specify an address range, use the following command in router configuration mode:

| Command                                                                                                                                | Purpose                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Router(config-router)# <b>area</b> area-id <b>range</b> ip-address mask [ <b>advertise</b>   <b>not-advertise</b> ][ <b>cost</b> cost] | Specifies an address range for which a single route will be advertised. |

## Configuring Route Summarization When Redistributing Routes into OSPF

When routes from other protocols are redistributed into OSPF (as described in the chapter “Configuring IP Routing Protocol-Independent Features”), each route is advertised individually in an external LSA. However, you can configure the Cisco IOS software to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. Doing so helps decrease the size of the OSPF link-state database.



To have the software advertise one summary route for all redistributed routes covered by a network address and mask, use the following command in router configuration mode:

| Command                                                                                                                                                | Purpose                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-router)# <b>summary-address</b> {{ <i>ip-address mask</i> }   { <i>prefix mask</i> }} [ <b>not-advertise</b> ] [ <b>tag</b> <i>tag</i> ] | Specifies an address and mask that covers redistributed routes, so only one summary route is advertised. Use the optional <b>not-advertise</b> keyword to filter out a set of routes. |

## Creating Virtual Links

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a *virtual link*. The two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the nonbackbone area that the two routers have in common (called the *transit area*). Note that virtual links cannot be configured through stub areas.

To establish a virtual link, use the following command in router configuration mode:

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                        | Purpose                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Router(config-router)# <b>area</b> <i>area-id</i> <b>virtual-link</b> <i>router-id</i> [ <b>authentication</b> [ <b>message-digest</b>   <b>null</b> ]] [ <b>hello-interval</b> <i>seconds</i> ] [ <b>retransmit-interval</b> <i>seconds</i> ] [ <b>transmit-delay</b> <i>seconds</i> ] [ <b>dead-interval</b> <i>seconds</i> ] [[ <b>authentication-key</b> <i>key</i> ]   [ <b>message-digest-key</b> <i>key-id</i> <b>md5</b> <i>key</i> ]] | Establishes a virtual link. |

To display information about virtual links, use the **show ip ospf virtual-links** EXEC command. To display the router ID of an OSPF router, use the **show ip ospf** EXEC command.

## Generating a Default Route

You can force an ASBR to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a *default route* into the OSPF routing domain.

To force the ASBR to generate a default route, use the following command in router configuration mode:

| Command                                                                                                                                                                                           | Purpose                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Router(config-router)# <b>default-information originate</b> [ <b>always</b> ] [ <b>metric</b> <i>metric-value</i> ] [ <b>metric-type</b> <i>type-value</i> ] [ <b>route-map</b> <i>map-name</i> ] | Forces the autonomous system boundary router to generate a default route into the OSPF routing domain. |

For a discussion of redistribution of routes, see the “Configuring IP Routing Protocol-Independent Features” chapter.

## Configuring Lookup of DNS Names

You can configure OSPF to look up Domain Naming System (DNS) names for use in all OSPF **show EXEC** command displays. This feature makes it easier to identify a router, because the router is displayed by name rather than by its router ID or neighbor ID.

To configure DNS name lookup, use the following command in global configuration mode:

| Command                                    | Purpose                     |
|--------------------------------------------|-----------------------------|
| Router(config)# <b>ip ospf name-lookup</b> | Configures DNS name lookup. |

## Forcing the Router ID Choice with a Loopback Interface

OSPF uses the largest IP address configured on the interfaces as its router ID. If the interface associated with this IP address is ever brought down, or if the address is removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces.

If a loopback interface is configured with an IP address, the Cisco IOS software will use this IP address as its router ID, even if other interfaces have larger IP addresses. Because loopback interfaces never go down, greater stability in the routing table is achieved.

OSPF automatically prefers a loopback interface over any other kind, and it chooses the highest IP address among all loopback interfaces. If no loopback interfaces are present, the highest IP address in the router is chosen. You cannot tell OSPF to use any particular interface.

To configure an IP address on a loopback interface, use the following commands beginning in global configuration mode:

|        | Command                                              | Purpose                                                                                |
|--------|------------------------------------------------------|----------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface loopback 0</b>          | Creates a loopback interface, which places the router in interface configuration mode. |
| Step 2 | Router(config-if)# <b>ip address ip-address mask</b> | Assigns an IP address to this interface.                                               |

## Controlling Default Metrics

In Cisco IOS Release 10.3 and later releases, by default OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64-kbps link gets a metric of 1562, while a T1 link gets a metric of 64.

The OSPF metric is calculated as the *ref-bw* value divided by the *bandwidth* value, with the *ref-bw* value equal to  $10^8$  by default, and the *bandwidth* value determined by the **bandwidth** interface configuration command. The calculation gives FDDI a metric of 1. If you have multiple links with high bandwidth, you might want to specify a larger number to differentiate the cost on those links. To do so, use the following command in router configuration mode:

| Command                                                            | Purpose                              |
|--------------------------------------------------------------------|--------------------------------------|
| Router(config-router)# <b>auto-cost reference-bandwidth ref-bw</b> | Differentiates high bandwidth links. |

## Changing the OSPF Administrative Distances

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, interarea, and external. Routes within an area are intra-area; routes to another area are interarea; and routes from another routing domain learned via redistribution are external. The default distance for each type of route is 110.

To change any of the OSPF distance values, use the following command in router configuration mode:

| Command                                                                                                           | Purpose                           |
|-------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <code>Router(config-router)# <b>distance ospf</b> {[intra-area dist1] [inter-area dist2] [external dist3]}</code> | Changes the OSPF distance values. |

For an example of changing administrative distance, see the section “[Changing OSPF Administrative Distance Example](#)” at the end of this chapter.

## Configuring OSPF on Simplex Ethernet Interfaces

Because simplex interfaces between two devices on an Ethernet represent only one network segment, for OSPF you must configure the sending interface to be a passive interface. This configuration prevents OSPF from sending hello packets for the sending interface. Both devices are able to see each other via the hello packet generated for the receiving interface.

To configure OSPF on simplex Ethernet interfaces, use the following command in router configuration mode:

| Command                                                                                      | Purpose                                                                  |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <code>Router(config-router)# <b>passive-interface</b> interface-type interface-number</code> | Suppresses the sending of hello packets through the specified interface. |

## Configuring Route Calculation Timers

You can configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation. You can also configure the hold time between two consecutive SPF calculations. To do so, use the following command in router configuration mode:

| Command                                                                      | Purpose                              |
|------------------------------------------------------------------------------|--------------------------------------|
| <code>Router(config-router)# <b>timers spf</b> spf-delay spf-holdtime</code> | Configures route calculation timers. |

## Configuring OSPF over On-Demand Circuits

The OSPF on-demand circuit is an enhancement to the OSPF protocol that allows efficient operation over on-demand circuits like ISDN, X.25 switched virtual circuits (SVCs), and dialup lines. This feature supports RFC 1793, *Extending OSPF to Support Demand Circuits*.

Prior to this feature, OSPF periodic hello and LSA updates would be exchanged between routers that connected the on-demand link, even when no changes occurred in the hello or LSA information.

With this feature, periodic hellos are suppressed and the periodic refreshes of LSAs are not flooded over the demand circuit. These packets bring up the link only when they are exchanged for the first time, or when a change occurs in the information they contain. This operation allows the underlying data link layer to be closed when the network topology is stable.

This feature is useful when you want to connect telecommuters or branch offices to an OSPF backbone at a central site. In this case, OSPF for on-demand circuits allows the benefits of OSPF over the entire domain, without excess connection costs. Periodic refreshes of hello updates, LSA updates, and other protocol overhead are prevented from enabling the on-demand circuit when there is no “real” data to send.

Overhead protocols such as hellos and LSAs are transferred over the on-demand circuit only upon initial setup and when they reflect a change in the topology. This means that critical changes to the topology that require new SPF calculations are sent in order to maintain network topology integrity. Periodic refreshes that do not include changes, however, are not sent across the link.

To configure OSPF for on-demand circuits, use the following commands beginning in global configuration mode:

|        | Command                                                                           | Purpose                                  |
|--------|-----------------------------------------------------------------------------------|------------------------------------------|
| Step 1 | Router(config)# <b>router ospf</b> <i>process-id</i>                              | Enables OSPF operation.                  |
| Step 2 | Router(config)# <b>interface</b> <i>interface-type</i><br><i>interface-number</i> | Enters interface configuration mode.     |
| Step 3 | Router(config-if)# <b>ip ospf demand-circuit</b>                                  | Configures OSPF on an on-demand circuit. |

If the router is part of a point-to-point topology, then only one end of the demand circuit must be configured with this command. However, all routers must have this feature loaded.

If the router is part of a point-to-multipoint topology, only the multipoint end must be configured with this command.

For an example of OSPF over an on-demand circuit, see the section “[OSPF over On-Demand Routing Example](#)” at the end of this chapter.

## Implementation Considerations

Evaluate the following considerations before implementing this feature:

- Because LSAs that include topology changes are flooded over an on-demand circuit, we recommend that you put demand circuits within OSPF stub areas or within NSSAs to isolate the demand circuits from as many topology changes as possible.
- To take advantage of the on-demand circuit functionality within a stub area or NSSA, every router in the area must have this feature loaded. If this feature is deployed within a regular area, all other regular areas must also support this feature before the demand circuit functionality can take effect because type 5 external LSAs are flooded throughout all areas.
- Hub-and-spoke network topologies that have a point-to-multipoint (p2mp) OSPF interface type on a hub might not revert back to non-demand circuit mode when needed. You must simultaneously reconfigure OSPF on all interfaces on the p2mp segment when reverting them from demand circuit mode to non-demand circuit mode.
- Do not implement this feature on a broadcast-based network topology because the overhead protocols (such as hello and LSA packets) cannot be successfully suppressed, which means the link will remain up.
- Configuring the router for an OSPF on-demand circuit with an asynchronous interface is not a supported configuration. The supported configuration is to use dialer interfaces on both ends of the circuit. For more information, refer to the following TAC URL:

<http://www.cisco.com/warp/public/104/dcprob.html#reason5>

## Logging Neighbors Going Up or Down

By default, the system sends a syslog message when an OSPF neighbor goes up or down. If you turned off this feature and want to restore it, use the following command in router configuration mode:

| Command                                                                  | Purpose                                                     |
|--------------------------------------------------------------------------|-------------------------------------------------------------|
| Router(config-router)# <b>log-adjacency-changes</b><br>[ <b>detail</b> ] | Sends syslog message when an OSPF neighbor goes up or down. |

Configure this command if you want to know about OSPF neighbors going up or down without turning on the **debug ip ospf adjacency** EXEC command. The **log-adjacency-changes** router configuration command provides a higher level view of the peer relationship with less output. Configure **log-adjacency-changes detail** if you want to see messages for each state change.

## Changing the LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, checksumming, and aging functions. The group pacing results in more efficient use of the router.

The router groups OSPF LSAs and paces the refreshing, checksumming, and aging functions so that sudden increases in CPU usage and network resources are avoided. This feature is most beneficial to large OSPF networks.

OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

## Original LSA Behavior

Each OSPF LSA has an age, which indicates whether the LSA is still valid. Once the LSA reaches the maximum age (1 hour), it is discarded. During the aging process, the originating router sends a refresh packet every 30 minutes to refresh the LSA. Refresh packets are sent to keep the LSA from expiring, whether there has been a change in the network topology or not. Checksumming is performed on all LSAs every 10 minutes. The router keeps track of LSAs it generates and LSAs it receives from other routers. The router refreshes LSAs it generated; it ages the LSAs it received from other routers.

Prior to the LSA group pacing feature, the Cisco IOS software would perform refreshing on a single timer, and checksumming and aging on another timer. In the case of refreshing, for example, the software would scan the whole database every 30 minutes, refreshing every LSA the router generated, no matter how old it was. [Figure 43](#) illustrates all the LSAs being refreshed at once. This process wasted CPU resources because only a small portion of the database needed to be refreshed. A large OSPF database (several thousand LSAs) could have thousands of LSAs with different ages. Refreshing on a single timer resulted in the age of all LSAs becoming synchronized, which resulted in much CPU processing at once. Furthermore, a large number of LSAs could cause a sudden increase of network traffic, consuming a large amount of network resources in a short period of time.

**Figure 43** *OSPF LSAs on a Single Timer Without Group Pacing*

All LSAs refreshed, 120 external LSAs on Ethernet need three packets



## LSA Group Pacing With Multiple Timers

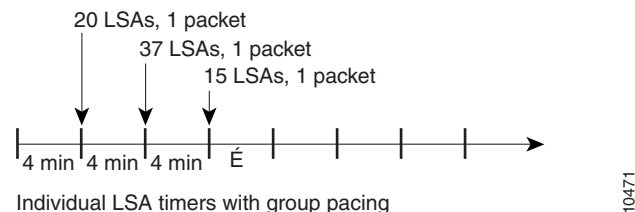
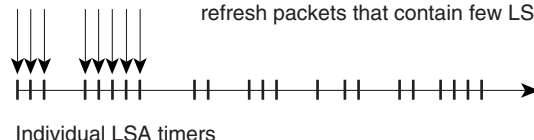
This problem is solved by configuring each LSA to have its own timer. To again use the example of refreshing, each LSA gets refreshed when it is 30 minutes old, independent of other LSAs. So the CPU is used only when necessary. However, LSAs being refreshed at frequent, random intervals would require many packets for the few refreshed LSAs the router must send out, which would be inefficient use of bandwidth.

Therefore, the router delays the LSA refresh function for an interval of time instead of performing it when the individual timers are reached. The accumulated LSAs constitute a group, which is then refreshed and sent out in one packet or more. Thus, the refresh packets are paced, as are the checksumming and aging. The pacing interval is configurable; it defaults to 4 minutes, which is randomized to further avoid synchronization.

[Figure 44](#) illustrates the case of refresh packets. The first timeline illustrates individual LSA timers; the second timeline illustrates individual LSA timers with group pacing.

**Figure 44** OSPF LSAs on Individual Timers with Group Pacing

Without group pacing, LSAs need to be refreshed frequently and at random intervals. Individual LSA timers require many refresh packets that contain few LSAs.



The group pacing interval is inversely proportional to the number of LSAs the router is refreshing, checksumming, and aging. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

The default value of pacing between LSA groups is 240 seconds (4 minutes). The range is from 10 seconds to 1800 seconds (30 minutes). To change the LSA group pacing interval, use the following command in router configuration mode:

| Command                                                          | Purpose                           |
|------------------------------------------------------------------|-----------------------------------|
| Router(config-router)# <b>timers lsa-group-pacing</b><br>seconds | Changes the group pacing of LSAs. |

For an example, see the section “[LSA Group Pacing Example](#)” at the end of this chapter.

## Blocking OSPF LSA Flooding

By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. Some redundancy is desirable, because it ensures robust flooding. However, too much redundancy can waste bandwidth and might destabilize the network due to excessive link and CPU usage in certain topologies. An example would be a fully meshed topology.

You can block OSPF flooding of LSAs two ways, depending on the type of networks:

- On broadcast, nonbroadcast, and point-to-point networks, you can block flooding over specified OSPF interfaces.
- On point-to-multipoint networks, you can block flooding to a specified neighbor.

On broadcast, nonbroadcast, and point-to-point networks, to prevent flooding of OSPF LSAs, use the following command in interface configuration mode:

| Command                                                | Purpose                                                   |
|--------------------------------------------------------|-----------------------------------------------------------|
| Router(config-if)# <b>ospf database-filter all out</b> | Blocks the flooding of OSPF LSA packets to the interface. |

On point-to-multipoint networks, to prevent flooding of OSPF LSAs, use the following command in router configuration mode:

| Command                                                                   | Purpose                                                            |
|---------------------------------------------------------------------------|--------------------------------------------------------------------|
| Router(config-router)# <b>neighbor ip-address database-filter all out</b> | Blocks the flooding of OSPF LSA packets to the specified neighbor. |

For an example of blocking LSA flooding, see the section “[Block LSA Flooding Example](#)” at the end of this chapter.

## Reducing LSA Flooding

The explosive growth of the Internet has placed the focus on the scalability of IGPs such as OSPF. By design, OSPF requires LSAs to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to about 50 minutes. This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF flooding reduction solution works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set. The LSAs are now set as “do not age.”

To reduce unnecessary refreshing and flooding of LSAs on your network, use the following command in interface configuration mode:

| Command                                           | Purpose                                                           |
|---------------------------------------------------|-------------------------------------------------------------------|
| Router(config-if)# <b>ip ospf flood-reduction</b> | Suppresses the unnecessary flooding of LSAs in stable topologies. |

## Ignoring MOSPF LSA Packets

Cisco routers do not support LSA type 6 Multicast OSPF (MOSPF), and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages. To do so, use the following command in router configuration mode:

| Command                                        | Purpose                                                                                 |
|------------------------------------------------|-----------------------------------------------------------------------------------------|
| Router(config-router)# <b>ignore lsa mospf</b> | Prevents the router from generating syslog messages when it receives MOSPF LSA packets. |

For an example of suppressing MOSPF LSA packets, see the section “[Ignore MOSPF LSA Packets Example](#)” at the end of this chapter.



## Displaying OSPF Update Packet Pacing

The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates quickly enough, or the router was out of buffer space. For example, packets might be dropped if either of the following topologies existed:

- A fast router was connected to a slower router over a point-to-point link.
- During flooding, several neighbors sent updates to a single router at the same time.

OSPF update packets are now automatically paced so they are not sent less than 33 milliseconds apart. Pacing is also added between resends to increase efficiency and minimize lost retransmissions. Also, you can display the LSAs waiting to be sent out an interface. The benefit of the pacing is that OSPF update and retransmission packets are sent more efficiently.

There are no configuration tasks for this feature; it occurs automatically.

To observe OSPF packet pacing by displaying a list of LSAs waiting to be flooded over a specified interface, use the following command in EXEC mode:

| Command                                                                          | Purpose                                                          |
|----------------------------------------------------------------------------------|------------------------------------------------------------------|
| Router# <b>show ip ospf flood-list</b><br><i>interface-type interface-number</i> | Displays a list of LSAs waiting to be flooded over an interface. |

## Monitoring and Maintaining OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that your device packets are taking through the network.

To display various routing statistics, use the following commands in EXEC mode, as needed:

| Command                                           | Purpose                                                               |
|---------------------------------------------------|-----------------------------------------------------------------------|
| Router# <b>show ip ospf</b> [ <i>process-id</i> ] | Displays general information about OSPF routing processes.            |
| Router# <b>show ip ospf border-routers</b>        | Displays the internal OSPF routing table entries to the ABR and ASBR. |

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b><br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>database-summary</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>router</i> ] [ <i>self-originate</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>router</i> ] [ <i>adv-router</i> [ <i>ip-address</i> ]]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>router</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>network</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>summary</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>asbr-summary</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>external</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>nssa-external</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>opaque-link</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>opaque-area</i> ] [ <i>link-state-id</i> ]<br><br>Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> [ <i>opaque-as</i> ] [ <i>link-state-id</i> ] | Displays lists of information related to the OSPF database.                                         |
| Router# <b>show ip ospf flood-list interface</b><br><i>interface-type</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Displays a list of LSAs waiting to be flooded over an interface (to observe OSPF packet pacing).    |
| Router# <b>show ip ospf interface</b> [ <i>interface-type</i><br><i>interface-number</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Displays OSPF-related interface information.                                                        |
| Router# <b>show ip ospf neighbor</b> [ <i>interface-name</i> ]<br>[ <i>neighbor-id</i> ] <b>detail</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Displays OSPF neighbor information on a per-interface basis.                                        |
| Router# <b>show ip ospf request-list</b> [ <i>neighbor</i> ]<br>[ <i>interface</i> ] [ <i>interface-neighbor</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Displays a list of all LSAs requested by a router.                                                  |
| Router# <b>show ip ospf retransmission-list</b><br>[ <i>neighbor</i> ] [ <i>interface</i> ] [ <i>interface-neighbor</i> ]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Displays a list of all LSAs waiting to be resent.                                                   |
| Router# <b>show ip ospf</b> [ <i>process-id</i> ] <b>summary-address</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Displays a list of all summary address redistribution information configured under an OSPF process. |
| Router# <b>show ip ospf virtual-links</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Displays OSPF-related virtual links information.                                                    |

To restart an OSPF process, use the following command in EXEC mode:

| Command                                                                                                                                                                         | Purpose                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>clear ip ospf</b> [ <i>pid</i> ] { <b>process</b>   <b>redistribution</b>   <b>counters</b> [ <b>neighbor</b> [ <i>neighbor-interface</i> ] [ <i>neighbor-id</i> ]]} | Clears redistribution based on the OSPF routing process ID. If the <i>pid</i> option is not specified, all OSPF processes are cleared. |

## OSPF Configuration Examples

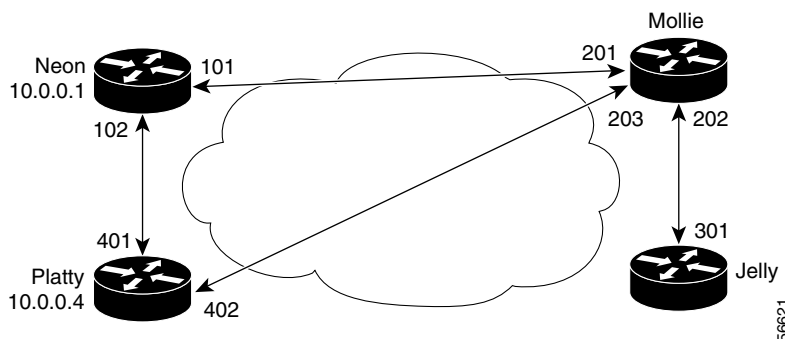
The following sections provide OSPF configuration examples:

- [OSPF Point-to-Multipoint Example](#)
- [OSPF Point-to-Multipoint, Broadcast Example](#)
- [OSPF Point-to-Multipoint, Nonbroadcast Example](#)
- [Variable-Length Subnet Masks Example](#)
- [OSPF Routing and Route Redistribution Examples](#)
- [Route Map Examples](#)
- [Changing OSPF Administrative Distance Example](#)
- [OSPF over On-Demand Routing Example](#)
- [LSA Group Pacing Example](#)
- [Block LSA Flooding Example](#)
- [Ignore MOSPF LSA Packets Example](#)

### OSPF Point-to-Multipoint Example

In [Figure 45](#), the router named Mollie uses data-link connection identifier (DLCI) 201 to communicate with the router named Neon, DLCI 202 to the router named Jelly, and DLCI 203 to the router named Platty. Neon uses DLCI 101 to communicate with Mollie and DLCI 102 to communicate with Platty. Platty communicates with Neon (DLCI 401) and Mollie (DLCI 402). Jelly communicates with Mollie (DLCI 301). Configuration examples follow the figure.

**Figure 45**      **OSPF Point-to-Multipoint Example**



**Mollie Configuration**

```

hostname mollie
!
interface serial 1
 ip address 10.0.0.2 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 201 broadcast
 frame-relay map ip 10.0.0.3 202 broadcast
 frame-relay map ip 10.0.0.4 203 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0

```

**Neon Configuration**

```

hostname neon
!
interface serial 0
 ip address 10.0.0.1 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.2 101 broadcast
 frame-relay map ip 10.0.0.4 102 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0

```

**Platty Configuration**

```

hostname platty
!
interface serial 3
 ip address 10.0.0.4 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 1000000
 frame-relay map ip 10.0.0.1 401 broadcast
 frame-relay map ip 10.0.0.2 402 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0

```

**Jelly Configuration**

```

hostname jelly
!
interface serial 2
 ip address 10.0.0.3 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 2000000
 frame-relay map ip 10.0.0.2 301 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0

```

## OSPF Point-to-Multipoint, Broadcast Example

The following example illustrates a point-to-multipoint network with broadcast:

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

The following example shows the configuration of the neighbor at 10.0.1.3:

```
interface serial 0
 ip address 10.0.1.3 255.255.255.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300 broadcast
 no shut
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration is as follows:

Router# **show ip ospf neighbor**

| Neighbor ID | Pri | State   | Dead Time | Address  | Interface |
|-------------|-----|---------|-----------|----------|-----------|
| 4.1.1.1     | 1   | FULL/ - | 00:01:50  | 10.0.1.5 | Serial0   |
| 3.1.1.1     | 1   | FULL/ - | 00:01:47  | 10.0.1.4 | Serial0   |
| 2.1.1.1     | 1   | FULL/ - | 00:01:45  | 10.0.1.3 | Serial0   |

The route information in the first configuration is as follows:

Router# **show ip route**

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    1.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O    10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
C    10.0.1.0/24 is directly connected, Serial0
O    10.0.1.5/32 [110/5] via 10.0.1.5, 00:39:08, Serial0
O    10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0
```

## OSPF Point-to-Multipoint, Nonbroadcast Example

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
ip address 10.0.1.1 255.255.255.0
ip ospf network point-to-multipoint non-broadcast
encapsulation frame-relay
no keepalive
frame-relay local-dlci 200
frame-relay map ip 10.0.1.3 202
frame-relay map ip 10.0.1.4 203
frame-relay map ip 10.0.1.5 204
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.3 cost 5
neighbor 10.0.1.4 cost 10
neighbor 10.0.1.5 cost 15
```

The following example is the configuration for the router on the other side:

```
interface Serial9/2
ip address 10.0.1.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint non-broadcast
no ip mroute-cache
no keepalive
no fair-queue
frame-relay local-dlci 301
frame-relay map ip 10.0.1.1 300
no shut
!
router ospf 1
network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration is as follows:

Router# **show ip ospf neighbor**

| Neighbor ID | Pri | State   | Dead Time | Address  | Interface |
|-------------|-----|---------|-----------|----------|-----------|
| 4.1.1.1     | 1   | FULL/ - | 00:01:52  | 10.0.1.5 | Serial0   |
| 3.1.1.1     | 1   | FULL/ - | 00:01:52  | 10.0.1.4 | Serial0   |
| 2.1.1.1     | 1   | FULL/ - | 00:01:52  | 10.0.1.3 | Serial0   |

## Variable-Length Subnet Masks Example

OSPF, static routes, and IS-IS support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space.

In the following example, a 30-bit subnet mask is used, leaving two bits of address space reserved for serial line host addresses. There is sufficient host address space for two host endpoints on a point-to-point serial link.

```
interface ethernet 0
ip address 131.107.1.1 255.255.255.0
! 8 bits of host address space reserved for ethernet

interface serial 0
ip address 131.107.254.1 255.255.255.252
```

```

! 2 bits of address space reserved for serial lines

! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
network 131.107.0.0 0.0.255.255 area 0.0.0.0

```

## OSPF Routing and Route Redistribution Examples

OSPF typically requires coordination among many internal routers, ABRs, and ASBRs. At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three types of examples follow:

- The first is a simple configuration illustrating basic OSPF commands.
- The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
- The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

### Basic OSPF Configuration Examples

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches Ethernet interface 0 to area 0.0.0.0, and redistributes RIP into OSPF, and OSPF into RIP:

```

interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 9000
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 10.94.0.0
 redistribute ospf 9000
 default-metric 1

```

### Basic OSPF Configuration Example for Internal Router, ABR, and ASBRs

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for *all other* networks.

```

router ospf 109
 network 131.108.20.0 0.0.0.255 area 10.9.50.0
 network 131.108.0.0 0.0.255.255 area 2
 network 131.109.10.0 0.0.0.255 area 3
 network 0.0.0.0 255.255.255.255 area 0
!
! Interface Ethernet0 is in area 10.9.50.0:
interface ethernet 0

```

```

ip address 131.108.20.5 255.255.255.0
!
! Interface Ethernet1 is in area 2:
interface ethernet 1
ip address 131.108.1.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
interface ethernet 2
ip address 131.108.2.5 255.255.255.0
!
! Interface Ethernet3 is in area 3:
interface ethernet 3
ip address 131.109.10.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
interface ethernet 4
ip address 131.109.1.1 255.255.255.0
!
! Interface Ethernet5 is in area 0:
interface ethernet 5
ip address 10.1.0.1 255.255.0.0

```

Each **network area** router configuration command is evaluated sequentially, so the order of these commands in the configuration is important. The Cisco IOS software sequentially evaluates the address/wildcard-mask pair for each interface. See the “OSPF Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication for more information.

Consider the first **network area** command. Area ID 10.9.50.0 is configured for the interface on which subnet 131.108.20.0 is located. Assume that a match is determined for Ethernet interface 0. Ethernet interface 0 is attached to area 10.9.50.0 only.

The second **network area** command is evaluated next. For area 2, the same process is then applied to all interfaces (except Ethernet interface 0). Assume that a match is determined for interface Ethernet 1. OSPF is then enabled for that interface and Ethernet interface 1 is attached to area 2.

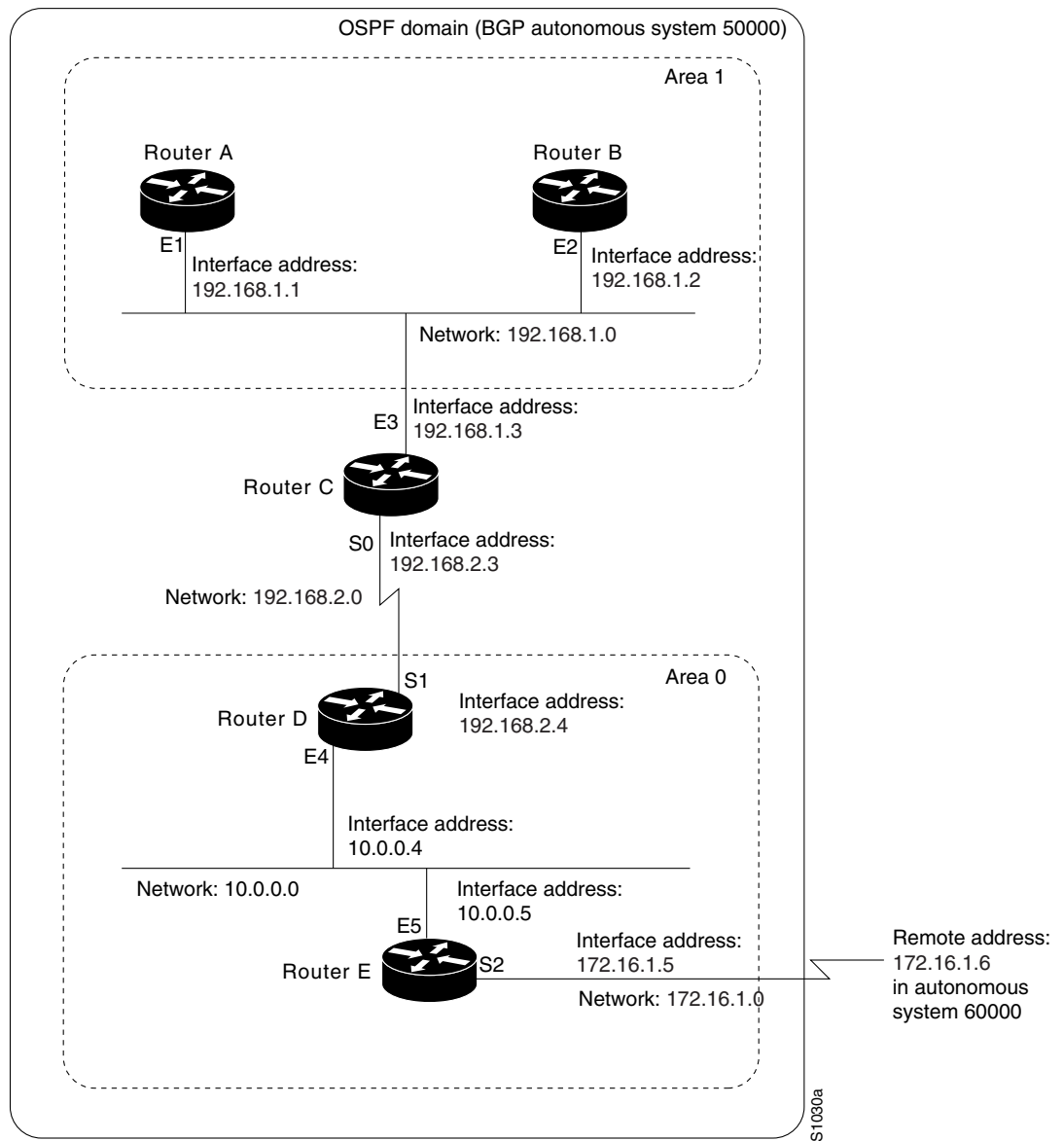
This process of attaching interfaces to OSPF areas continues for all **network area** commands. Note that the last **network area** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to area 0.

## Complex Internal Router, ABR, and ASBRs Example

The following example outlines a configuration for several routers within a single OSPF autonomous system. [Figure 46](#) provides a general network map that illustrates this example configuration.



**Figure 46** Sample OSPF Autonomous System Network Map



In this configuration, five routers are configured with OSPF:

- Router A and Router B are both internal routers within area 1.
- Router C is an OSPF ABR. Note that for Router C, Area 1 is assigned to E3 and area 0 is assigned to S0.
- Router D is an internal router in area 0 (backbone area). In this case, both **network** router configuration commands specify the same area (area 0, or the backbone area).
- Router E is an OSPF ASBR. Note that BGP routes are redistributed into OSPF and that these routes are advertised by OSPF.

**Note**

It is not necessary to include definitions of all areas in an OSPF autonomous system in the configuration of all routers in the autonomous system. You must only define the *directly* connected areas. In the example that follows, routes in area 0 are learned by the routers in area 1 (Router A and Router B) when the ABR (Router C) injects summary LSAs into area 1.

The OSPF domain in BGP autonomous system 109 is connected to the outside world via the BGP link to the external peer at IP address 11.0.0.6. Example configurations follow.

Following is the sample configuration for the general network map shown in [Figure 46](#).

**Router A Configuration—Internal Router**

```
interface ethernet 1
 ip address 131.108.1.1 255.255.255.0

router ospf 1
 network 131.108.0.0 0.0.255.255 area 1
```

**Router B Configuration—Internal Router**

```
interface ethernet 2
 ip address 131.108.1.2 255.255.255.0

router ospf 202
 network 131.108.0.0 0.0.255.255 area 1
```

**Router C Configuration—ABR**

```
interface ethernet 3
 ip address 131.108.1.3 255.255.255.0

interface serial 0
 ip address 131.108.2.3 255.255.255.0

router ospf 999
 network 131.108.1.0 0.0.0.255 area 1
 network 131.108.2.0 0.0.0.255 area 0
```

**Router D Configuration—Internal Router**

```
interface ethernet 4
 ip address 10.0.0.4 255.0.0.0

interface serial 1
 ip address 131.108.2.4 255.255.255.0

router ospf 50
 network 131.108.2.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

**Router E Configuration—ASBR**

```
interface ethernet 5
 ip address 10.0.0.5 255.0.0.0

interface serial 2
 ip address 11.0.0.5 255.0.0.0

router ospf 65001
 network 10.0.0.0 0.255.255.255 area 0
 redistribute bgp 109 metric 1 metric-type 1
```

```

router bgp 109
network 131.108.0.0
network 10.0.0.0
neighbor 11.0.0.6 remote-as 110

```

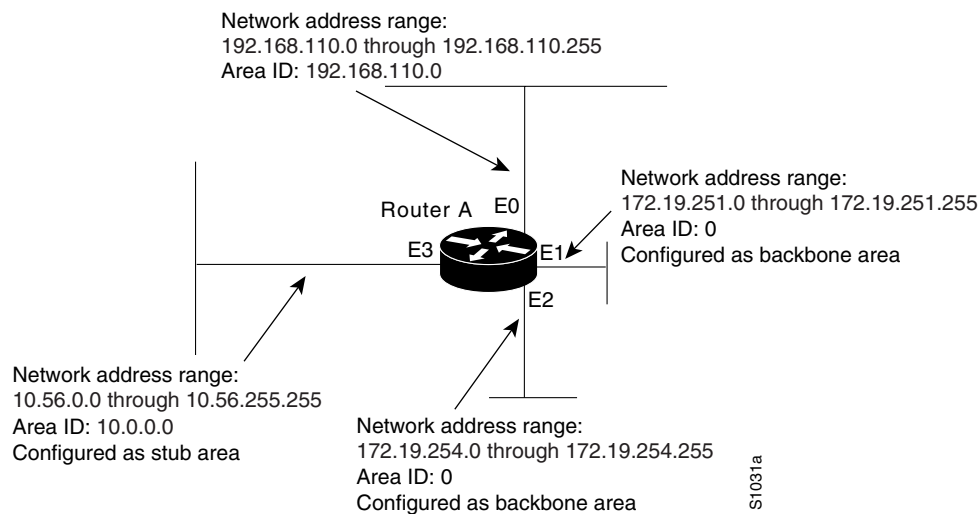
## Complex OSPF Configuration for ABR Examples

The following example configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

- Basic OSPF configuration
- Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. [Figure 47](#) illustrates the network address ranges and area assignments for the interfaces.

**Figure 47** Interface and Area Specifications for OSPF Example Configuration



The basic configuration tasks in this example are as follows:

- Configure address ranges for Ethernet interface 0 through Ethernet interface 3.
- Enable OSPF on each interface.
- Set up an OSPF authentication password for each area and network.
- Assign link-state metrics and other OSPF interface configuration options.
- Create a *stub area* with area ID 36.0.0.0. (Note that the **authentication** and **stub** options of the **area** router configuration command are specified with separate **area** command entries, but can be merged into a single **area** command.)
- Specify the backbone area (area 0).

Configuration tasks associated with redistribution are as follows:

- Redistribute IGRP and RIP into OSPF with various options set (including **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```

interface ethernet 0
 ip address 192.42.110.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 1
 ip address 131.119.251.201 255.255.255.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf retransmit-interval 10
 ip ospf transmit-delay 2
 ip ospf priority 4
!
interface ethernet 2
 ip address 131.119.254.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 3
 ip address 36.56.0.201 255.255.0.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf dead-interval 80

```

In the following configuration OSPF is on network 131.119.0.0:

```

router ospf 201
 network 36.0.0.0 0.255.255.255 area 36.0.0.0
 network 192.42.110.0 0.0.0.255 area 192.42.110.0
 network 131.119.0.0 0.0.255.255 area 0
 area 0 authentication
 area 36.0.0.0 stub
 area 36.0.0.0 authentication
 area 36.0.0.0 default-cost 20
 area 192.42.110.0 authentication
 area 36.0.0.0 range 36.0.0.0 255.0.0.0
 area 192.42.110.0 range 192.42.110.0 255.255.255.0
 area 0 range 131.119.251.0 255.255.255.0
 area 0 range 131.119.254.0 255.255.255.0
 redistribute igmp 200 metric-type 2 metric 1 tag 200 subnets
 redistribute rip metric-type 2 metric 1 tag 200

```

In the following configuration IGRP autonomous system 200 is on 131.119.0.0:

```

router igrp 200
 network 131.119.0.0
!
! RIP for 192.42.110
!
router rip
 network 192.42.110.0
 redistribute igrp 200 metric 1
 redistribute ospf 201 metric 1

```

## Route Map Examples

The examples in this section illustrate the use of redistribution, with and without route maps. Examples from both the IP and Connectionless Network Service (CLNS) routing protocols are given.

The following example redistributes all OSPF routes into IGRP:

```

router igrp 109
 redistribute ospf 110

```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a metric of 5, a metric type of type 1, and a tag equal to 1.

```
router ospf 109
 redistribute rip route-map rip-to-ospf
!
route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

The following example redistributes OSPF learned routes with tag 7 as a RIP metric of 15:

```
router rip
 redistribute ospf 109 route-map 5
!
route-map 5 permit
 match tag 7
 set metric 15
```

The following example redistributes OSPF intra-area and interarea routes with next hop routers on serial interface 0 into BGP with an INTER\_AS metric of 5:

```
router bgp 109
 redistribute ospf 109 route-map 10
!
route-map 10 permit
 match route-type internal
 match interface serial 0
 set metric 5
```

The following example redistributes two types of routes into the integrated IS-IS routing table (supporting both IP and CLNS). The first type is OSPF external IP routes with tag 5; these routes are inserted into Level 2 IS-IS LSPs with a metric of 5. The second type is ISO-IGRP derived CLNS prefix routes that match CLNS access list 2000; these routes will be redistributed into IS-IS as Level 2 LSPs with a metric of 30.

```
router isis
 redistribute ospf 109 route-map 2
 redistribute iso-igrp nsfnet route-map 3
!
route-map 2 permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
route-map 3 permit
 match address 2000
 set metric 30
```

With the following configuration, OSPF external routes with tags 1, 2, 3, and 5 are redistributed into RIP with metrics of 1, 1, 5, and 5, respectively. The OSPF routes with a tag of 4 are not redistributed.

```
router rip
 redistribute ospf 109 route-map 1
!
route-map 1 permit
 match tag 1 2
 set metric 1
!
```

```

route-map 1 permit
  match tag 3
  set metric 5
!
route-map 1 deny
  match tag 4
!
route map 1 permit
  match tag 5
  set metric 5

```

In the following configuration, a RIP learned route for network 160.89.0.0 and an ISO-IGRP learned route with prefix 49.0001.0002 will be redistributed into an IS-IS Level 2 LSP with a metric of 5:

```

router isis
  redistribute rip route-map 1
  redistribute iso-igrp remote route-map 1
!
route-map 1 permit
  match ip address 1
  match clns address 2
  set metric 5
  set level level-2
!
access-list 1 permit 160.89.0.0 0.0.255.255
clns filter-set 2 permit 49.0001.0002...

```

The following configuration example illustrates how a route map is referenced by the **default-information** router configuration command. This type of reference is called *conditional default origination*. OSPF will originate the default route (network 0.0.0.0) with a type 2 metric of 5 if 140.222.0.0 is in the routing table.

**Note**


---

Only routes external to the OSPF process can be used for tracking, such as non-OSPF routes or OSPF routes from a separate OSPF process.

---

```

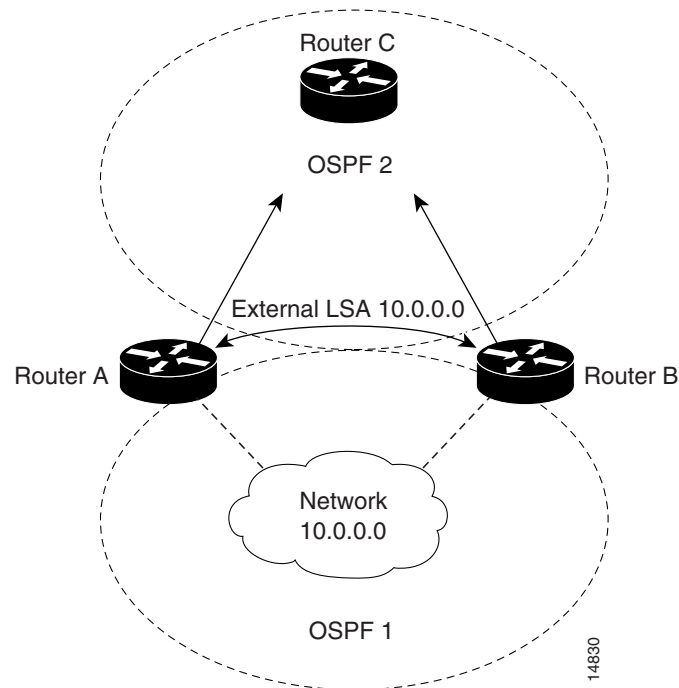
route-map ospf-default permit
  match ip address 1
  set metric 5
  set metric-type type-2
!
access-list 1 permit 140.222.0.0 0.0.255.255
!
router ospf 109
  default-information originate route-map ospf-default

```

## Changing OSPF Administrative Distance Example

The following configuration changes the external distance to 200, making it less trustworthy. [Figure 48](#) illustrates the example.

**Figure 48** OSPF Administrative Distance



### Router A Configuration

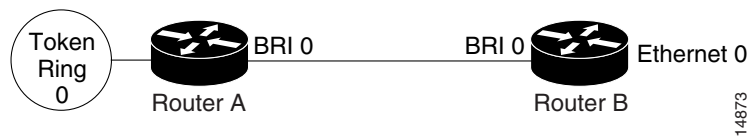
```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

### Router B Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

## OSPF over On-Demand Routing Example

The following configuration allows OSPF over an on-demand circuit, as shown in [Figure 49](#). Note that the on-demand circuit is defined on one side only (BRI 0 on Router A). It is not required to be configured on both sides.

**Figure 49**      **OSPF over On-Demand Circuit****Router A Configuration**

```

username RouterB password 7 060C1A2F47
isdn switch-type basic-5ess
ip routing
!
interface TokenRing0
 ip address 140.10.20.7 255.255.255.0
 no shut
!
interface BRI0
 no cdp enable
 description connected PBX 1485
 ip address 140.10.10.7 255.255.255.0
 encapsulation ppp
 ip ospf demand-circuit
 dialer map ip 140.10.10.6 name RouterB broadcast 61484
 dialer-group 1
 ppp authentication chap
 no shut
!
router ospf 100
 network 140.10.10.0 0.0.0.255 area 0
 network 140.10.20.0 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit

```

**Router B Configuration**

```

username RouterA password 7 04511E0804
isdn switch-type basic-5ess
ip routing
!
interface Ethernet0
 ip address 140.10.60.6 255.255.255.0
 no shut
!
interface BRI0
 no cdp enable
 description connected PBX 1484
 ip address 140.10.10.6 255.255.255.0
 encapsulation ppp
 dialer map ip 140.10.10.7 name RouterA broadcast 61485
 dialer-group 1
 ppp authentication chap
 no shut
!
router ospf 100
 network 140.10.10.0 0.0.0.255 area 0
 network 140.10.60.0 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit

```



## LSA Group Pacing Example

The following example changes the OSPF pacing between LSA groups to 60 seconds:

```
router ospf
 timers lsa-group-pacing 60
```

## Block LSA Flooding Example

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ospf database-filter all out
```

The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 1.2.3.4:

```
router ospf 109
 neighbor 1.2.3.4 database-filter all out
```

## Ignore MOSPF LSA Packets Example

The following example configures the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
router ospf 109
 ignore lsa mospf
```





## OSPF ABR Type 3 LSA Filtering

### Feature History

| Release   | Modification                                                                            |
|-----------|-----------------------------------------------------------------------------------------|
| 12.0(15)S | This feature was introduced.                                                            |
| 12.2(4)T  | This feature was integrated into Cisco IOS Release 12.2(4)T.                            |
| 12.2(4)T3 | Support for the Cisco 7500 series was added in Cisco IOS Release 12.2(4)T3.             |
| 12.2(8)T  | Support for the Cisco 1721, 3631, 3745 and URM was added in Cisco IOS Release 12.2(8)T. |

This feature module describes filtering interarea routes on an Area Border Router (ABR) with the Open Shortest Path First (OSPF) protocol. It includes the following sections:

- [Feature Overview, page 605](#)
- [Benefits, page 606](#)
- [Restrictions, page 606](#)
- [Related Features and Technologies, page 606](#)
- [Supported Platforms, page 606](#)
- [Supported Standards, MIBs, and RFCs, page 607](#)
- [Configuration Tasks, page 607](#)
- [Configuration Examples, page 609](#)
- [Command Reference, page 609](#)

## Feature Overview

The OSPF ABR Type 3 LSA Filtering feature extends the ability of an ABR that is running the OSPF protocol to filter type 3 link-state advertisements (LSAs) that are sent between different OSPF areas. This feature allows only packets with specified prefixes to be sent from one area to another area and restricts all packets with other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time. This feature is supported by the addition of the **area filter-list** command in router configuration mode.

## Benefits

The OSPF ABR Type 3 LSA Filtering feature gives the administrator improved control of route distribution between OSPF areas.

## Restrictions

Only type 3 LSAs that originate from an ABR are filtered.

## Related Features and Technologies

This feature is an extension of the OSPF routing protocol. For more information about configuring OSPF and configuring route summarization and filtering, refer to the “OSPF” chapter of the Release 12.2 *Cisco IOS IP Configuration Guide* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

## Supported Platforms

The OSPF ABR Type 3 LSA Filtering feature is supported for the following platforms in Cisco IOS Release 12.2(4)T:

- Cisco 1400 series
- Cisco 1600 series
- Cisco 1600R series
- Cisco 1720
- Cisco 1721 (Supported in Cisco IOS Release 12.2(8)T and above.)
- Cisco 1750
- Cisco 1751
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3631 (Supported in Cisco IOS Release 12.2(8)T and above.)
- Cisco 3640
- Cisco 3745 (Supported in Cisco IOS Release 12.2(8)T and above.)
- Cisco 3660
- Cisco MC3810
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (Supported in Cisco IOS Release 12.2(4)T3 and above.)
- Cisco uBR7200 series
- Universal Router Module (Supported in Cisco IOS Release 12.2(8)T.)

### Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

### Standards

No new or modified standards are supported by this feature.

### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

### RFCs

No new or modified standards are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the OSPF ABR Type 3 LSA Filtering feature. Each task in the list is identified as either required or optional:

- [Configuring OSPF ABR Type 3 LSA Filtering](#) (required)
- [Verifying OSPF ABR Type 3 LSA Filtering](#) (optional)

## Configuring OSPF ABR Type 3 LSA Filtering

To filter interarea routes into a specified area, use the following commands beginning in router configuration mode:

|               | Command                                                                                                                      | Purpose                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf process-id</b>                                                                                | Configures the router to run an OSPF process.                                    |
| <b>Step 2</b> | Router(config-router)# <b>area area-id filter-list prefix prefix-list-name in</b>                                            | Configures the router to filter interarea routes into the specified area.        |
| <b>Step 3</b> | Router(config-router)# <b>ip prefix-list list-name [seq seq-value] deny   permit network/len [ge ge-value] [le le-value]</b> | Creates a prefix list with the name specified for the <i>list-name</i> argument. |

To filter interarea routes out of a specified area, use the following commands beginning in router configuration mode:

|               | Command                                                                                                                      | Purpose                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf process-id</b>                                                                                | Configures the router to run an OSPF process.                                    |
| <b>Step 2</b> | Router(config-router)# <b>area area-id filter-list prefix prefix-list-name out</b>                                           | Configures the router to filter interarea routes out of the specified area.      |
| <b>Step 3</b> | Router(config-router)# <b>ip prefix-list list-name [seq seq-value] deny   permit network/len [ge ge-value] [le le-value]</b> | Creates a prefix list with the name specified for the <i>list-name</i> argument. |

## Verifying OSPF ABR Type 3 LSA Filtering

To verify that the OSPF ABR Type 3 LSA Filtering feature has been configured, use the **show ip ospf EXEC** command. The **show ip ospf** command will show that this feature has been enabled by listing the area filter as “in” or “out.” The following is sample output from the **show ip ospf** command:

```
router# show ip ospf 1
Routing Process "ospf 1" with ID 172.16.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an area border router
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 6 times
    Area ranges are
      10.0.0.0/8 Passive Advertise
    Area-filter AREA_0_IN in
    Area-filter AREA_0_OUT out
    Number of LSA 5. Checksum Sum 0x29450
```

```

Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
Area 1
Number of interfaces in this area is 1
Area has no authentication
SPF algorithm executed 4 times
Area ranges are
Area-filter AREA_1_IN in
Area-filter AREA_1_OUT out
Number of LSA 6. Checksum Sum 0x30100
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

## Monitoring and Maintaining OSPF ABR Type 3 LSA Filtering

| Command                            | Purpose                                                          |
|------------------------------------|------------------------------------------------------------------|
| Router# <b>show ip prefix-list</b> | Displays information about a prefix list or prefix list entries. |

## Configuration Examples

The following configuration example output shows interarea filtering that is applied to both incoming and outgoing routes:

```

Router(config)# router ospf 1
log-adjacency-changes
area 1 filter-list prefix AREA_1_OUT out
area 3 filter-list prefix AREA_3_IN in
network 10.0.0.0 0.255.255.255 area 3
network 172.16.1.0 0.0.0.255 area 0
network 192.168.0.0 0.255.255.255 area 1
!
ip prefix-list AREA_1_OUT seq 10 permit 10.25.0.0/8 ge 16
ip prefix-list AREA_1_OUT seq 20 permit 172.20.20.0/24
!
ip prefix-list AREA_3_IN seq 10 permit 172.31.0.0/16
!

```

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **area filter-list**







# OSPF Stub Router Advertisement

## Feature History

| Release    | Modification                                                                                         |
|------------|------------------------------------------------------------------------------------------------------|
| 12.1(8)E   | This feature was introduced.                                                                         |
| 12.0(15)S  | This feature was integrated into Cisco IOS Release 12.0(15)S.                                        |
| 12.0(15)SC | This feature was integrated into Cisco IOS Release 12.0(15)SC.                                       |
| 12.0(16)ST | This feature was integrated into Cisco IOS Release 12.0(16)ST.                                       |
| 12.2(4)T   | This feature was integrated into Cisco IOS Release 12.2(4)T.                                         |
| 12.2(4)T3  | Support for the Cisco 7500 series was added in Cisco IOS Release 12.2(4)T3.                          |
| 12.2(8)T   | Support for the Cisco 1710, 1721, 3631, 3725, 3745, and URM was added in Cisco IOS Release 12.2(8)T. |
| 12.2(8)T1  | Support for the Cisco 2691 was added in Cisco IOS Release 12.2(8)T1.                                 |

This document describes the OSPF Stub Router Advertisement feature. It includes the following sections:

- [Feature Overview, page 612](#)
- [Benefits, page 613](#)
- [Related Features and Technologies, page 613](#)
- [Supported Platforms, page 613](#)
- [Supported Standards, MIBs, and RFCs, page 614](#)
- [Configuration Tasks, page 615](#)
- [Monitoring and Maintaining OSPF Stub Router Advertisement, page 618](#)
- [Configuration Examples, page 619](#)
- [Command Reference, page 619](#)

## Feature Overview

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors.

When any of these three configuration options are enabled on a router, the router will originate link-state advertisements (LSAs) with a maximum metric (LSInfinity: 0xFFFF) through all non-stub links. The advertisement of a maximum metric causes other routers to assign a cost to the new router that is higher than the cost of using an alternate path. Because of the high cost assigned to paths that pass through the new router, other routers will not use a path through the new router as a transit path to forward traffic that is destined for other networks, which allows switching and routing functions to be up and running and routing tables to converge before transit traffic is routed through the new router.

**Note**

Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

## Allowing Routing Tables to Converge

Two configuration options introduced by the OSPF Stub Router Advertisement feature allow you to bring a new router into a network without immediately routing traffic through the new router. These configuration options are useful because Interior Gateway Protocols (IGPs) converge very quickly upon a router during startup or after a reload, often before Border Gateway Protocol (BGP) routing tables have completely converged. If neighbor routers forward traffic through a router while that router is building BGP routing tables, packets that have been received for other destinations may be dropped. Advertising a maximum metric during startup will allow routing tables to converge before traffic that is destined for other networks is sent through the router. The following two configuration options enable a router to advertise a maximum metric at startup:

- You can configure a timer to advertise a maximum metric when the router is started or reloaded. When this option is configured, the router will advertise a maximum metric, which forces neighbor routers to select alternate paths until the timer expires. When the timer expires, the router will advertise accurate (normal) metrics, and other routers will send traffic to this router depending on the cost. The configurable range of the timer is from 5 to 86,400 seconds.
- You can configure a router to advertise a maximum metric at startup until BGP routing tables converge or until the default timer expires (600 seconds). Once BGP routing tables converge or the default timer expires, the router will advertise accurate (normal) metrics and other routers will send traffic to this router, depending on the cost.

## Configuring a Graceful Shutdown

The third configuration option introduced by the OSPF Stub Router Advertisement feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down. There are many situations where you may need to remove a router from the network. If a router is removed from a network and neighbor routers cannot detect that the physical interface is down,

neighbors will need to wait for dead timers to expire before the neighbors will remove the adjacency and routing tables will reconverge. This situation may occur when there is a switch between other routers and the router that is shut down. Packets may be dropped while the neighbor routing tables reconverge.

When this third option is configured, the router advertises a maximum metric, which allows neighbor routers to select alternate paths before the router is shut down. This configuration option could also be used to remove a router that is in a critical condition from the network without affecting traffic that is destined for other networks.

**Note**

You should not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

## Benefits

### Improved Stability and Availability

Advertising a maximum metric through all links at startup or during a reload will prevent neighbor routers from using a path through the router as a transit path, thereby reducing the number of packets that are dropped and improving the stability and availability of the network.

### Graceful Removal from the Network

Advertising a maximum metric before shutdown allows other routers to select alternate paths before the transit path through a router becomes inaccessible.

## Related Features and Technologies

The OSPF Stub Router Advertisement feature is an extension of the OSPF routing protocol. For more information about configuring OSPF and BGP, refer to the Release 12.2 *Cisco IOS IP Routing Configuration Guide* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

## Supported Platforms

The OSPF Stub Router Advertisement feature is supported by the following platforms in Cisco IOS Release 12.2(4)T that support OSPF:

- Cisco 1400 series
- Cisco 1600 series
- Cisco 1600R series
- Cisco 1710 (Supported in Release 12.2(8)T and above.)
- Cisco 1720
- Cisco 1721 (Supported in Release 12.2(8)T and above.)
- Cisco 1750
- Cisco 1751
- Cisco 2500 series
- Cisco 2600 series

- Cisco 2691 (Supported in Release 12.2(8)T1 and above.)
- Cisco 3620
- Cisco 3631 (Supported in Release 12.2(8)T and above.)
- Cisco 3640
- Cisco 3660
- Cisco 3725 (Supported in Release 12.2(8)T and above.)
- Cisco 3745 (Supported in Release 12.2(8)T and above.)
- Cisco 7100 series
- Cisco 7200 series
- Cisco 7500 series (Supported in Release 12.2(4)T3 and above.)
- Cisco uBR7200 series
- Universal Router Module (Supported in Release 12.2(8)T and above.)

#### Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

#### Standards

No new or modified standards are supported by this feature.

#### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

#### RFCs

- RFC 3137 *OSPF Stub Router Advertisement*

# Configuration Tasks

See the following sections for configuration tasks to configure OSPF to advertise a maximum metric. This feature has three different configuration options. All tasks are optional and should be individually configured.

- [Configuring Advertisement on Startup](#) (optional)
- [Configuring Advertisement Until Routing Tables Converge](#) (optional)
- [Configuring Advertisement for a Graceful Shutdown](#) (optional)
- [Verifying the Advertisement of a Maximum Metric](#) (optional)

## Configuring Advertisement on Startup

To configure a router that is running OSPF to advertise a maximum metric during startup, use the following commands beginning in global configuration mode:

|        | Command                                                                             | Purpose                                                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>router ospf</b> <i>process-id</i>                                | Places the router in router configuration mode and enables an OSPF routing process.                                                                                                                                                                                                                                |
| Step 2 | Router(config-router)# <b>max-metric router-lsa on-startup</b> <i>announce-time</i> | Configures OSPF to advertise a maximum metric during startup for a configured period of time. The <i>announce-time</i> argument is a configurable timer that must follow the <b>on-startup</b> keyword to be configured. There is no default timer value. The configurable time range is from 5 to 86,400 seconds. |

## Configuring Advertisement Until Routing Tables Converge

To configure a router that is running OSPF to advertise a maximum metric until BGP routing tables converge, use the following commands beginning in global configuration mode:

|        | Command                                                                     | Purpose                                                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>router ospf</b> <i>process-id</i>                        | Places the router in router configuration mode and enables an OSPF routing process.                                                                                                                                                                               |
| Step 2 | Router(config-router)# <b>max-metric router-lsa on-startup wait-for-bgp</b> | Configures OSPF to advertise a maximum metric until BGP routing tables have converged or until the default timer has expired. The <b>wait-for-bgp</b> keyword must follow the <b>on-startup</b> keyword to be configured. The default timer value is 600 seconds. |

## Configuring Advertisement for a Graceful Shutdown

To configure a router that is running OSPF to advertise a maximum metric for a graceful shutdown or removal from the network, use the following commands beginning in global configuration mode:

|        | Command                                              | Purpose                                                                                                                                                                                                                             |
|--------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>router ospf</b> <i>process-id</i> | Places the router in router configuration mode and enables an OSPF routing process.                                                                                                                                                 |
| Step 2 | Router(config-router)# <b>max-metric router-lsa</b>  | Configures OSPF to advertise a maximum metric, which causes neighbor routers to select alternate paths for transit traffic before the router is shut down.                                                                          |
| Step 3 | Router(config-router)# <b>exit</b>                   | Exits router configuration mode.                                                                                                                                                                                                    |
| Step 4 | Router(config)# <b>exit</b>                          | Exits configuration mode and places the router in privileged EXEC mode.                                                                                                                                                             |
| Step 5 | Router# <b>show ip ospf</b>                          | Displays general information about OSPF routing processes. The <b>show ip ospf</b> command is entered in order to verify that the <b>max-metric router-lsa</b> command has been enabled before the router is shut down or reloaded. |



### Note

You should not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

## Verifying the Advertisement of a Maximum Metric

To verify that the advertisement of a maximum metric has been configured correctly, use the **show ip ospf** or **show ip ospf database** command.

The output of the **show ip ospf** command will display the condition, state, and remaining time delay of the advertisement of a maximum metric, depending on which options were configured with the **max-metric router-lsa** command.

The following sample output is similar to the output that will be displayed when the **on-startup** keyword and *announce-time* argument are configured with the **max-metric router-lsa** command:

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
    static, includes subnets in redistribution
  Originating router-LSAs with maximum metric, Time remaining: 00:01:18
  Condition: on startup for 300 seconds, State: active
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  Number of external LSA 7. Checksum Sum 0x47261
```

```

Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 1 normal 0 stub 1 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm executed 3 times
    Area ranges are
    Number of LSA 8. Checksum Sum 0x474AE
    Number of opaque link LSA 0. Checksum Sum 0x0

```

The following sample output is similar to the output that will be displayed when the **on-startup** and **wait-for-bgp** keywords are configured with the **max-metric router-lsa** command:

```

Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
    static, includes subnets in redistribution
  Originating router-LSAs with maximum metric, Time remaining: 00:01:18
    Condition: on startup while BGP is converging, State: active
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  Number of external LSA 7. Checksum Sum 0x47261
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 2. 1 normal 0 stub 1 nssa
  External flood list length 0
    Area BACKBONE(0)
      Number of interfaces in this area is 1
      Area has no authentication
      SPF algorithm executed 3 times
      Area ranges are
      Number of LSA 8. Checksum Sum 0x474AE
      Number of opaque link LSA 0. Checksum Sum 0x0

```

The following sample output is similar to the output that will be displayed when the **max-metric router-lsa** command is configured without any keywords or arguments:

```

Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
    static, includes subnets in redistribution
  Originating router-LSAs with maximum metric
    Condition: always, State: active
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  Number of external LSA 7. Checksum Sum 0x47261
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 2. 1 normal 0 stub 1 nssa
  External flood list length 0

```

```

Area BACKBONE(0)
  Number of interfaces in this area is 1
  Area has no authentication
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 8. Checksum Sum 0x474AE
  Number of opaque link LSA 0. Checksum Sum 0x0

```

The output of the **show ip ospf database** command will display information about OSPF LSAs and indicate if the router is announcing maximum cost links. The following sample output is similar to the output that will be displayed when any form of the **max-metric router-lsa** command is configured:

Router# **show ip ospf database**

```

Exception Flag: Announcing maximum link costs
LS age: 68
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 172.18.134.155
Advertising Router: 172.18.134.155
LS Seq Number: 80000002
Checksum: 0x175D
Length: 60
Area Border Router
AS Boundary Router
Number of Links: 3

Link connected to: a Transit Network
(Link ID) Designated Router address: 192.168.1.11
(Link Data) Router Interface address: 192.168.1.14
Number of TOS metrics: 0
  TOS 0 Metrics: 65535 (metric used for local calculation: 10)

Link connected to: a Transit Network
(Link ID) Designated Router address: 10.1.145.11
(Link Data) Router Interface address: 10.1.145.14
Number of TOS metrics: 0
  TOS 0 Metrics: 65535 (metric used for local calculation: 10)

Link connected to: a Stub Network
(Link ID) Network/subnet number: 10.11.12.0
(Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
  TOS 0 Metrics: 1

```

## Monitoring and Maintaining OSPF Stub Router Advertisement

To monitor and maintain the advertisement of a maximum metric, use the following EXEC commands:

| Command                                     | Purpose                                                                                                                                                                       |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip ospf</b>                 | Displays general information about OSPF routing processes and provides information about the configuration settings and status of the OSPF Stub Router Advertisement feature. |
| Router# <b>show ip ospf database router</b> | Displays information about router LSAs, and indicates if a router is announcing maximum link costs.                                                                           |



# Configuration Examples

This section provides the following configuration examples:

- [Advertisement on Startup Example](#)
- [Advertisement Until Routing Tables Converge Example](#)
- [Graceful Shutdown Example](#)

## Advertisement on Startup Example

In the following example, a router that is running OSPF is configured to advertise a maximum metric at startup for 300 seconds:

```
Router(config)# router ospf 100  
Router(config-router)# max-metric router-lsa on-startup 300
```

## Advertisement Until Routing Tables Converge Example

In the following example, a router that is running OSPF is configured to advertise a maximum metric until BGP routing tables converge or until the default timer expires (600 seconds):

```
Router(config)# router ospf 100  
Router(config-router)# max-metric router-lsa on-startup wait-for-bgp
```

## Graceful Shutdown Example

In the following example, a router that is running OSPF is configured to advertise a maximum metric, which causes neighbor routers to select alternate paths for transit traffic before the router is shut down:

```
Router(config)# router ospf 100  
Router(config-router)# max-metric router-lsa  
Router(config-router)# exit  
Router(config)# exit  
Router# show ip ospf
```

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Command

- **max-metric router-lsa**

### Modified Command

- **show ip ospf**





# OSPF Update Packet-Pacing Configurable Timers

## Feature History

| Release   | Modification                                                                                   |
|-----------|------------------------------------------------------------------------------------------------|
| 12.2(4)T  | This feature was introduced.                                                                   |
| 12.2(4)T3 | Support for the Cisco 7500 series was added in Cisco IOS Release 12.2(4)T3.                    |
| 12.2(8)T  | Support for the Cisco 1710, 3631, 3725, 3745, and URM was added in Cisco IOS Release 12.2(8)T. |
| 12.2(8)T1 | Support for the Cisco 2691 was added in Cisco IOS Release 12.2(8)T1.                           |

This feature module describes the OSPF Update Packet-Pacing Configurable Timers feature. It includes the following sections:

- [Feature Overview, page 621](#)
- [Benefits, page 622](#)
- [Related Features and Technologies, page 622](#)
- [Supported Platforms, page 622](#)
- [Supported Standards, MIBs, and RFCs, page 623](#)
- [Configuration Tasks, page 624](#)
- [Monitoring and Maintaining OSPF Packet-Pacing Timers, page 626](#)
- [Configuration Examples, page 626](#)
- [Command Reference, page 627](#)

## Feature Overview

In rare situations, you might need to change Open Shortest Path First (OSPF) packet-pacing default timers to mitigate CPU or buffer utilization issues associated with flooding very large numbers of link-state advertisements (LSAs). The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which OSPF LSA flood pacing, retransmission pacing, and group pacing updates occur.

Configuring OSPF flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF transmission queue. Configuring OSPF retransmission pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue. Cisco IOS software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval used for group LSA refreshment; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh occurs every 30 minutes).

**Note**

The default settings for OSPF packet pacing timers are suitable for the majority of OSPF deployments. You should change the default timers only as a last resort.

## Benefits

The OSPF Update Packet-Pacing Configurable Timers feature provides the administrator with a mechanism to control the rate at which LSA updates occur in order to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

## Restrictions

Do not change the packet pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default timers. Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks associated with changing the default timer values.

## Related Features and Technologies

The OSPF Update Packet-Pacing Configurable Timers feature is an extension of the OSPF routing protocol. For more information about configuring OSPF, packet pacing, area border router (ABR) and autonomous system boundary router (ASBR) summarization, and stub router configuration, refer to the Release 12.2 *Cisco IOS IP Routing Configuration Guide* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

## Supported Platforms

The OSPF Update Packet-Pacing Configurable Timers feature is supported by the following platforms in Cisco IOS Release 12.2(4)T that support OSPF:

- Cisco 1710 (Supported in Release 12.2(8)T and above.)
- Cisco 2500 series
- Cisco 2600 series
- Cisco 2691 (Supported in Release 12.2(8)T1 and above.)
- Cisco 3620
- Cisco 3631 (Supported in Release 12.2(8)T and above.)

- Cisco 3640
- Cisco 3725 (Supported in Release 12.2(8)T and above.)
- Cisco 3745 (Supported in Release 12.2(8)T and above.)
- Cisco 7200 series
- Cisco 7500 series (Supported in Release 12.2(4)T3 and above.)
- Universal Router Module (Supported in Release 12.2(8)T and above.)

#### Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. As of May 2001, Feature Navigator supports M, T, E, S, and ST releases. You can access Feature Navigator at the following URL:

<http://www.cisco.com/go/fn>

## Supported Standards, MIBs, and RFCs

#### Standards

No new or modified standards are supported by this feature.

#### MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

#### RFCs

No new or modified RFCs are supported by this feature.

## Configuration Tasks

See the following sections for configuration tasks for the OSPF Update Packet-Pacing Configurable Timers feature. Each task in the list is identified as either required or optional:

- [Configuring OSPF Packet-Pacing Timers](#) (required)
- [Verifying OSPF Packet-Pacing Timers](#) (optional)

### Configuring OSPF Packet-Pacing Timers

To configure a flood packet pacing timer, use the following commands beginning in router configuration mode:

|               | Command                                                               | Purpose                                                                             |
|---------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                  | Places the router in router configuration mode and enables an OSPF routing process. |
| <b>Step 2</b> | Router(config-router)# <b>timers pacing flood</b> <i>milliseconds</i> | Configures a flood packet pacing timer delay (in milliseconds).                     |

To configure a retransmission packet pacing timer, use the following commands beginning in router configuration mode:

|               | Command                                                                        | Purpose                                                                             |
|---------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                           | Places the router in router configuration mode and enables an OSPF routing process. |
| <b>Step 2</b> | Router(config-router)# <b>timers pacing retransmission</b> <i>milliseconds</i> | Configures a retransmission packet pacing timer delay (in milliseconds).            |

To configure a group packet pacing timer, use the following commands beginning in router configuration mode:

|               | Command                                                              | Purpose                                                                             |
|---------------|----------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                 | Places the router in router configuration mode and enables an OSPF routing process. |
| <b>Step 2</b> | Router(config-router)# <b>timers pacing lsa-group</b> <i>seconds</i> | Configures an LSA group packet pacing timer delay (in seconds).                     |

## Verifying OSPF Packet-Pacing Timers

To verify that OSPF packet pacing has been configured, use the **show ip ospf** privileged EXEC command. The output of the **show ip ospf** command will display the type and delay time of the configurable pacing timers (flood, retransmission, group). The following example output is from the **show ip ospf** command:

```
Router# show ip ospf

Routing Process "ospf 1" with ID 10.0.0.1 and Domain ID 10.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 100 secs
Interface flood pacing timer 55 msec
Retransmission pacing timer 100 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has message digest authentication
    SPF algorithm executed 4 times
    Area ranges are
      Number of LSA 4. Checksum Sum 0x29BEB
      Number of opaque link LSA 0. Checksum Sum 0x0
      Number of DCbitless LSA 3
      Number of indication LSA 0
      Number of DoNotAge LSA 0
      Flood list length 0
  Area 172.16.26.0
    Number of interfaces in this area is 0
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
      192.168.0.0/16 Passive Advertise
      Number of LSA 1. Checksum Sum 0x44FD
      Number of opaque link LSA 0. Checksum Sum 0x0
      Number of DCbitless LSA 1
      Number of indication LSA 1
      Number of DoNotAge LSA 0
      Flood list length 0
```

## Troubleshooting Tips

If the number of OSPF packet retransmissions rapidly increases, increase the value of the packet pacing timers. The number of OSPF packet retransmissions is displayed in the output of the **show ip ospf neighbor** command.

# Monitoring and Maintaining OSPF Packet-Pacing Timers

To monitor and maintain OSPF packet-pacing timers, use the following commands in privileged EXEC mode:

| Command                                     | Purpose                                                           |
|---------------------------------------------|-------------------------------------------------------------------|
| Router# <b>show ip ospf</b>                 | Displays general information about OSPF routing processes.        |
| router# <b>show ip ospf neighbor</b>        | Displays OSPF neighbor information on a per-interface basis.      |
| Router# <b>clear ip ospf redistribution</b> | Clears route redistribution based on the OSPF routing process ID. |

## Configuration Examples

This section provides the following configuration examples:

- [Flood Pacing Example](#)
- [Retransmission Pacing Example](#)
- [Group Pacing Example](#)

### Flood Pacing Example

The following example configures LSA flood pacing updates to occur in 50-millisecond intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing flood 50
```

### Retransmission Pacing Example

The following example configures LSA flood pacing updates to occur in 100-millisecond intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing retransmission 100
```

### Group Pacing Example

The following example configures OSPF group pacing updates between LSA groups to occur in 75-second intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing lsa-group 75
```



# Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

## New Commands

- **timers pacing flood**
- **timers pacing lsa-group**
- **timers pacing retransmission**

## Modified Commands

- **show ip ospf**





# OSPF Sham-Link Support for MPLS VPN

## Feature History

| Release  | Modification                 |
|----------|------------------------------|
| 12.2(8)T | This feature was introduced. |

This document describes how to configure and use a sham-link to connect Virtual Private Network (VPN) client sites that run the Open Shortest Path First (OSPF) protocol and share backdoor OSPF links in a Multiprotocol Label Switching (MPLS) VPN configuration.

This document includes the following sections:

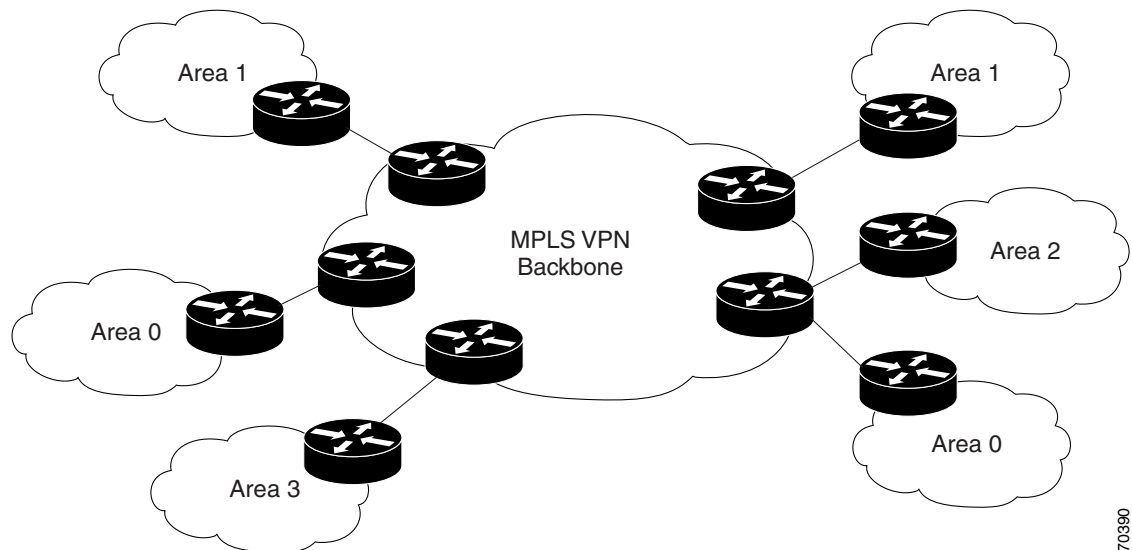
- [Feature Overview, page 629](#)
- [Supported Platforms, page 636](#)
- [Supported Standards, MIBs, and RFCs, page 638](#)
- [Prerequisites, page 638](#)
- [Configuration Tasks, page 638](#)
- [Configuration Examples, page 640](#)
- [Command Reference, page 640](#)
- [Glossary, page 641](#)

## Feature Overview

### Using OSPF in PE-CE Router Connections

In an MPLS VPN configuration, the OSPF protocol is one way you can connect customer edge (CE) routers to service provider edge (PE) routers in the VPN backbone. OSPF is often used by customers that run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone.

[Figure 50](#) shows an example of how VPN client sites that run OSPF can connect over an MPLS VPN backbone.

**Figure 50** *OSPF Connectivity Between VPN Client Sites and an MPLS VPN Backbone*

When OSPF is used to connect PE and CE routers, all routing information learned from a VPN site is placed in the VPN routing and forwarding (VRF) instance associated with the incoming interface. The PE routers that attach to the VPN use the Border Gateway Protocol (BGP) to distribute VPN routes to each other. A CE router can then learn the routes to other sites in the VPN by peering with its attached PE router. The MPLS VPN superbackbone provides an additional level of routing hierarchy to interconnect the VPN sites running OSPF.

When OSPF routes are propagated over the MPLS VPN backbone, additional information about the prefix in the form of BGP extended communities (route type, domain ID extended communities) is appended to the BGP update. This community information is used by the receiving PE router to decide the type of link-state advertisement (LSA) to be generated when the BGP route is redistributed to the OSPF PE-CE process. In this way, internal OSPF routes that belong to the same VPN and are advertised over the VPN backbone are seen as interarea routes on the remote sites.

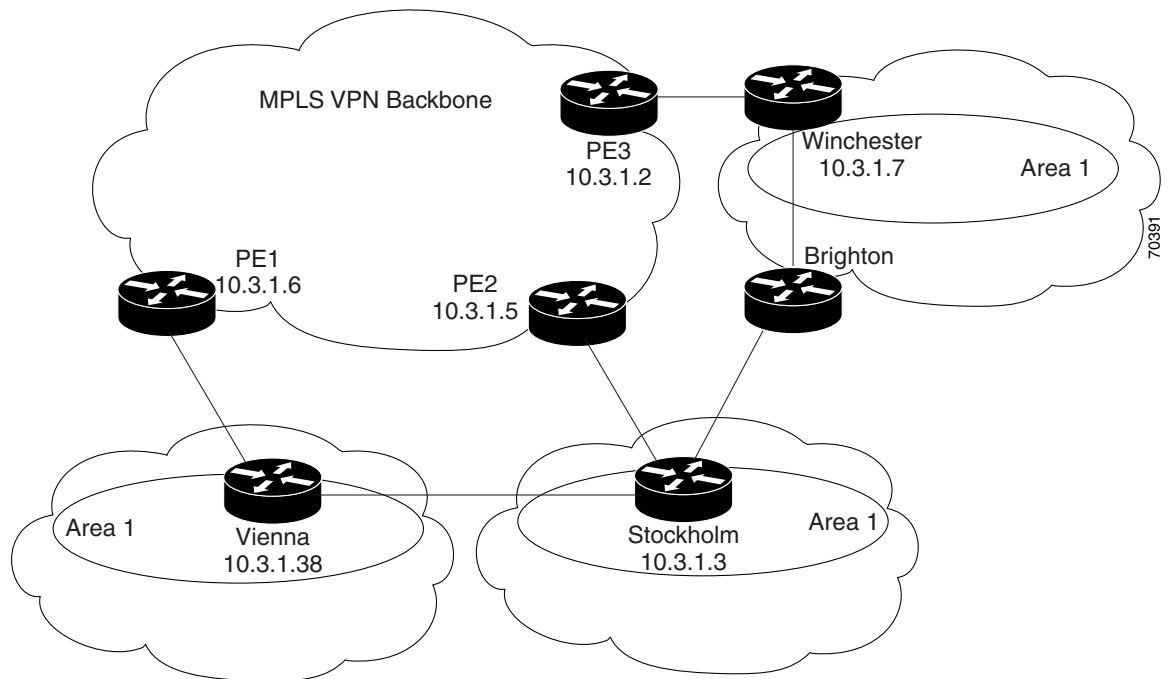
For basic information about how to configure an MPLS VPN, refer to:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm>

## Using a Sham-Link to Correct OSPF Backdoor Routing

Although OSPF PE-CE connections assume that the only path between two client sites is across the MPLS VPN backbone, backdoor paths between VPN sites (shown in grey in [Figure 51](#)) may exist. If these sites belong to the same OSPF area, the path over a backdoor link will always be selected because OSPF prefers intraarea paths to interarea paths. (PE routers advertise OSPF routes learned over the VPN backbone as interarea paths.) For this reason, OSPF backdoor links between VPN sites must be taken into account so that routing is performed based on policy.

**Figure 51 Backdoor Paths Between OSPF Client Sites**



For example, [Figure 51](#) shows three client sites, each with backdoor links. Because each site runs OSPF within the same Area 1 configuration, all routing between the three sites follows the intraarea path across the backdoor links, rather than over the MPLS VPN backbone.

The following example shows BGP routing table entries for the prefix 10.3.1.7/32 in the PE-1 router in [Figure 51](#). This prefix is the loopback interface of the Winchester CE router. As shown in bold in this example, the loopback interface is learned via BGP from PE-2 and PE-3. It is also generated through redistribution into BGP on PE-1.

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 58
Paths: (3 available, best #2)
  Advertised to non peer-group peers:
    10.3.1.2 10.3.1.5
  Local
    10.3.1.5 (metric 30) from 10.3.1.5 (10.3.1.5)
      Origin incomplete, metric 22, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.2.1.38 from 0.0.0.0 (10.3.1.6)
      Origin incomplete, metric 86, localpref 100, weight 32768,
      valid, sourced, best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

Within BGP, the locally generated route (10.2.1.38) is considered to be the best route. However, as shown in bold in the next example, the VRF routing table shows that the selected path is learned via OSPF with a next hop of 10.2.1.38, which is the Vienna CE router.

```

PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100", distance 110, metric 86, type intra area
  Redistributing via bgp 215
  Advertised by bgp 215
  Last update from 10.2.1.38 on Serial0/0/0, 00:00:17 ago
  Routing Descriptor Blocks:
  * 10.2.1.38, from 10.3.1.7, 00:00:17 ago, via Serial0/0/0
    Route metric is 86, traffic share count is 1

```

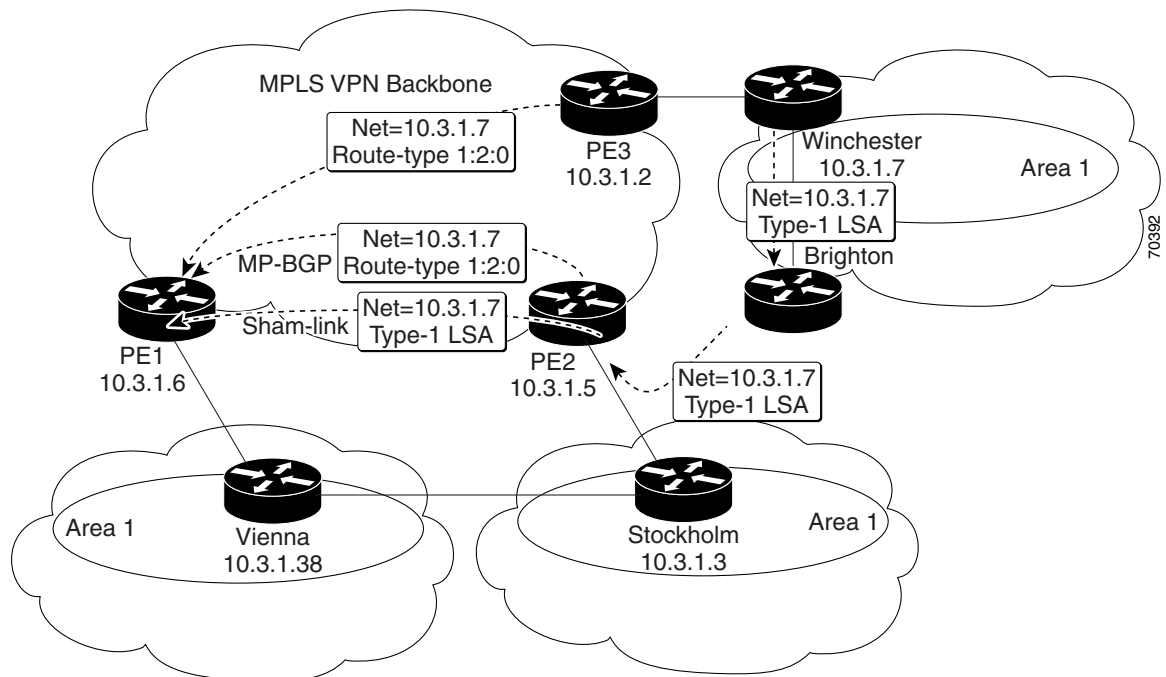
This path is selected because:

- The OSPF intra-area path is preferred over the interarea path (over the MPLS VPN backbone) generated by the PE-1 router.
- OSPF has a lower administrative distance (AD) than internal BGP (BGP running between routers in the same autonomous system).

If the backdoor links between sites are used only for backup purposes and do not participate in the VPN service, then the default route selection shown in the preceding example is not acceptable. To reestablish the desired path selection over the MPLS VPN backbone, you must create an additional OSPF intra-area (logical) link between ingress and egress VRFs on the relevant PE routers. This link is called a sham-link.

A sham-link is required between any two VPN sites that belong to the same OSPF area and share an OSPF backdoor link. If no backdoor link exists between the sites, no sham-link is required.

[Figure 52](#) shows a sample sham-link between PE-1 and PE-2. A cost is configured with each sham-link and is used to decide whether traffic will be sent over the backdoor path or the sham-link path. When a sham-link is configured between PE routers, the PEs can populate the VRF routing table with the OSPF routes learned over the sham-link.

**Figure 52** Using a Sham-Link Between PE Routers to Connect OSPF Client Sites

Because the sham-link is seen as an intra-area link between PE routers, an OSPF adjacency is created and database exchange (for the particular OSPF process) occurs across the link. The PE router can then flood LSAs between sites from across the MPLS VPN backbone. As a result, the desired intra-area connectivity is created.

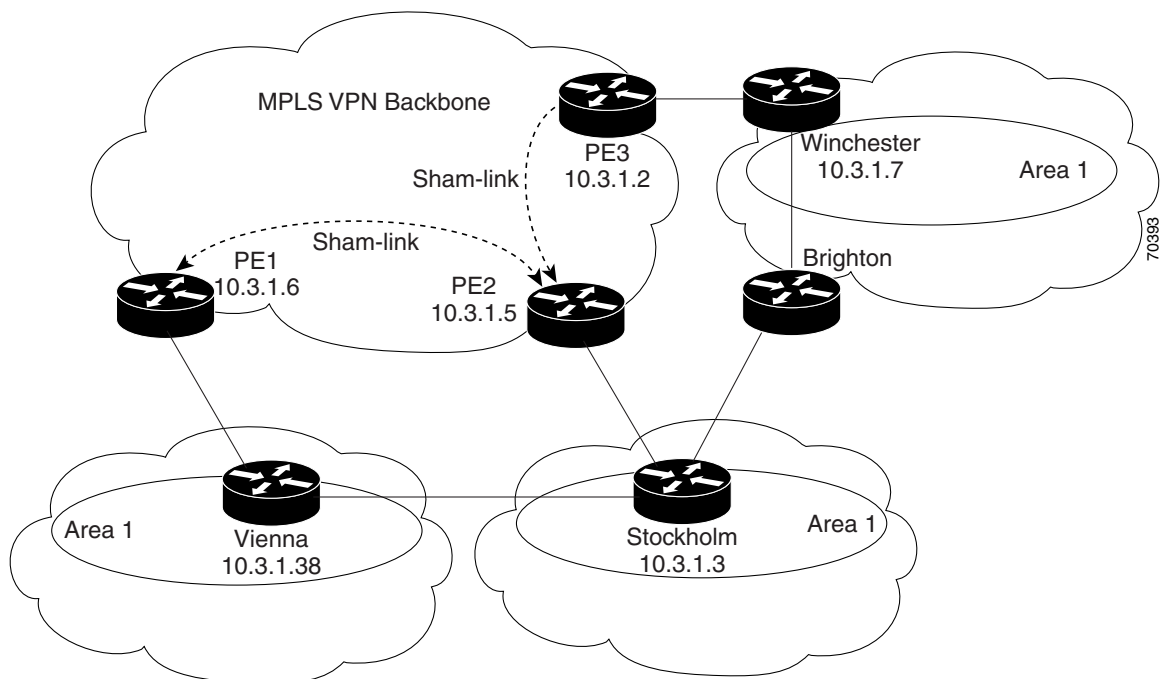
The section, “[Creating a Sham-Link](#)”, describes how to configure a sham-link between two PE routers. For more information about how to configure OSPF, refer to:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1\\_c/1cp1/1cospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/np1_c/1cp1/1cospf.htm)

## Sham-Link Configuration Example

The example in this section is designed to show how a sham-link is used only to affect the OSPF intra-area path selection of the PE and CE routers. The PE router also uses the information received from MP-BGP to set the outgoing label stack of incoming packets, and to decide to which egress PE router to label switch the packets.

[Figure 53](#) shows a sample MPLS VPN topology in which a sham-link configuration is necessary. A VPN client has three sites, each with a backdoor link. Two sham-links have been configured, one between PE-1 and PE-2, and another between PE-2 and PE-3. A sham-link between PE-1 and PE-3 is not necessary in this configuration because the Vienna and Winchester sites do not share a backdoor link.

**Figure 53 Sham-Link Example**

The following example shows the forwarding that occurs between sites from the standpoint of how PE-1 views the 10.3.1.7/32 prefix, the loopback1 interface of the Winchester CE router in [Figure 53](#).

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 124
Paths: (1 available, best #1)
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2

PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100", distance 110, metric 13, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:12:59 ago
  Routing Descriptor Blocks:
    10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:12:59 ago
```

The next example shows forwarding information in which the next hop for the route, 10.3.1.2, is the PE-3 router rather than the PE-2 router (which is the best path according to OSPF). The reason the OSPF route is not redistributed to BGP on the PE is because the other end of the sham-link already redistributed the route to BGP and there is no need for duplication. The OSPF sham-link is used only to influence intra-area path selection. When sending traffic to a particular destination, the PE router uses the MP-BGP forwarding information.

```
PE-1# show ip bgp vpnv4 all tag | begin 10.3.1.7
10.3.1.7/32      10.3.1.2      notag/38

PE-1# show tag-switching forwarding 10.3.1.2
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC  or Tunnel Id    switched  interface
31     42        10.3.1.2/32     0         PO3/0/0   point2point
```



```

PE-1# show ip cef vrf ospf 10.3.1.7
10.3.1.7/32, version 73, epoch 0, cached adjacency to POS3/0/0
0 packets, 0 bytes
tag information set
  local tag: VPN-route-head
  fast tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}
via 10.3.1.2, 0 dependencies, recursive
  next hop 10.1.1.17, POS3/0/0 via 10.3.1.2/32
  valid cached adjacency
  tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}

```

If a prefix is learned across the sham-link and the path via the sham-link is selected as the best, the PE router does not generate an MP-BGP update for the prefix. It is not possible to route traffic from one sham-link over another sham-link.

In the following example, PE-2 shows how an MP-BGP update for the prefix is not generated. Although 10.3.1.7/32 has been learned via OSPF across the sham-link as shown in bold, no local generation of a route into BGP is performed. The only entry within the BGP table is the MP-BGP update received from PE-3 (the egress PE router for the 10.3.1.7/32 prefix).

```

PE-2# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100", distance 110, metric 12, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:00:10 ago
  Routing Descriptor Blocks:
    * 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:00:10 ago
      Route metric is 12, traffic share count is 1

```

```

PE-2# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 166
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2

```

The PE router uses the information received from MP-BGP to set the ongoing label stack of incoming packets, and to decide to which egress PE router to label switch the packets.

## Benefits

### Client Site Connection Across the MPLS VPN Backbone

A sham-link overcomes the OSPF default behavior for selecting an intra-area backdoor route between VPN sites instead of an interarea (PE-to-PE) route. A sham-link ensures that OSPF client sites that share a backdoor link can communicate over the MPLS VPN backbone and participate in VPN services.

### Flexible Routing in an MPLS VPN Configuration

In an MPLS VPN configuration, the OSPF cost configured with a sham-link allows you to decide if OSPF client site traffic will be routed over a backdoor link or through the VPN backbone.

## Restrictions

When OSPF is used as a protocol between PE and CE routers, the OSPF metric is preserved when routes are advertised over the VPN backbone. The metric is used on the remote PE routers to select the correct route. For this reason, you should not modify the metric value when OSPF is redistributed to BGP, and when BGP is redistributed to OSPF. If you modify the metric value, routing loops may occur.

## Related Features and Technologies

- MPLS
- OSPF
- BGP

## Related Documents

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2
- *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp\\_r/1rfospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfospf.htm)
- *MPLS Virtual Private Networks*  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm>
- *Configuring OSPF*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcprt2/1cfospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfospf.htm)
- *Configuring BGP*  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcprt2/1cfbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt2/1cfbgp.htm)
- RFC 1163, *A Border Gateway Protocol*
- RFC 1164, *Application of the Border Gateway Protocol in the Internet*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2328, *Open Shortest Path First, Version 2*
- RFC 2547, *BGP/MPLS VPNs*

## Supported Platforms

- Cisco 1400 series
- Cisco 1600
- Cisco 1600R
- Cisco 1710
- Cisco 1720

- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 2420
- Cisco 2600
- Cisco 2691
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3660
- Cisco 3725
- Cisco 3745
- Cisco 7100
- Cisco 7200
- Cisco 7500
- Cisco 7700
- URM
- Cisco uBR7200

#### **Determining Platform Support Through Cisco Feature Navigator**

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

# Supported Standards, MIBs, and RFCs

## Standards

No new or modified standards are supported by this feature.

## MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

## RFCs

No new or modified RFCs are supported by this feature.

## Prerequisites

Before you can configure a sham-link in an MPLS VPN, you must first enable OSPF as follows:

- Create an OSPF routing process.
- Specify the range of IP addresses to be associated with the routing process.
- Assign area IDs to be associated with the range of IP addresses.

For more information on these OSPF configuration procedures, go to:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp\\_r/1rfospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprrp_r/1rfospf.htm)

## Configuration Tasks

See the following sections for configuration tasks for the sham-link feature. Each task in the list is identified as either required or optional.

- [Creating a Sham-Link](#) (required)
- [Verifying Sham-Link Creation](#) (optional)

## Creating a Sham-Link

Before you create a sham-link between PE routers in an MPLS VPN, you must:

- Configure a separate /32 address on the remote PE so that OSPF packets can be sent over the VPN backbone to the remote end of the sham-link. The /32 address must meet the following criteria:
  - Belong to a VRF.
  - Not be advertised by OSPF.
  - Be advertised by BGP.

You can use the /32 address for other sham-links.

- Associate the sham-link with an existing OSPF area.

To create a sham-link, use the following commands starting in EXEC mode:

|         | Command                                                                                                                                          | Purpose                                                                                                                                                                                                                                                               |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | Router1# <b>configure terminal</b>                                                                                                               | Enters global configuration mode on the first PE router.                                                                                                                                                                                                              |
| Step 2  | Router1(config)# <b>interface loopback</b><br><i>interface-number</i>                                                                            | Creates a loopback interface to be used as an endpoint of the sham-link on PE-1 and enters interface configuration mode.                                                                                                                                              |
| Step 3  | Router1(config-if)# <b>ip vrf forwarding</b><br><i>vrf-name</i>                                                                                  | Associates the loopback interface with a VRF. Removes the IP address.                                                                                                                                                                                                 |
| Step 4  | Router1(config-if)# <b>ip address</b> <i>ip-address</i><br><i>mask</i>                                                                           | Reconfigures the IP address of the loopback interface on PE-1.                                                                                                                                                                                                        |
| Step 5  | Router1(config-if)# <b>end</b>                                                                                                                   | Returns to global configuration mode.                                                                                                                                                                                                                                 |
| Step 6  | Router1(config)# <b>end</b>                                                                                                                      | Returns to EXEC mode.                                                                                                                                                                                                                                                 |
| Step 7  | Router2# <b>configure terminal</b>                                                                                                               | Enters global configuration mode on the second PE router.                                                                                                                                                                                                             |
| Step 8  | Router2(config)# <b>interface loopback</b><br><i>interface-number</i>                                                                            | Creates a loopback interface to be used as the endpoint of the sham-link on PE-2 and enters interface configuration mode.                                                                                                                                             |
| Step 9  | Router2(config-if)# <b>ip vrf forwarding</b><br><i>vrf-name</i>                                                                                  | Associates the second loopback interface with a VRF. Removes the IP address.                                                                                                                                                                                          |
| Step 10 | Router2(config-if)# <b>ip address</b> <i>ip-address</i><br><i>mask</i>                                                                           | Reconfigures the IP address of the loopback interface on PE-2.                                                                                                                                                                                                        |
| Step 11 | Router2(config-if)# <b>end</b>                                                                                                                   | Returns to global configuration mode.                                                                                                                                                                                                                                 |
| Step 12 | Router1(config)# <b>end</b>                                                                                                                      | Returns to EXEC mode.                                                                                                                                                                                                                                                 |
| Step 13 | Router1(config)# <b>router ospf</b> <i>process-id</i><br><b>vrf</b> <i>vrf-name</i>                                                              | Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-1 and enters interface configuration mode.                                                                                                                           |
| Step 14 | Router1(config-if)# <b>area</b> <i>area-id</i><br><b>sham-link</b> <i>source-address</i><br><i>destination-address</i> <b>cost</b> <i>number</i> | Configures the sham-link on the PE-1 interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. <b>cost</b> <i>number</i> configures the OSPF cost for sending an IP packet on the PE-1 sham-link interface. |
| Step 15 | Router2(config)# <b>router ospf</b> <i>process-id</i><br><b>vrf</b> <i>vrf-name</i>                                                              | Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-2 and enters interface configuration mode.                                                                                                                           |
| Step 16 | Router2(config-if)# <b>area</b> <i>area-id</i><br><b>sham-link</b> <i>source-address</i><br><i>destination-address</i> <b>cost</b> <i>number</i> | Configures the sham-link on the PE-2 interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. <b>cost</b> <i>number</i> configures the OSPF cost for sending an IP packet on the PE-2 sham-link interface. |

## Verifying Sham-Link Creation

To verify that the sham-link was successfully created and is operational, use the **show ip ospf sham-links** command in EXEC mode:

```
Router1# show ip ospf sham-links
```

```
Sham Link OSPF_SL0 to address 10.2.1.2 is up
Area 1 source address 10.2.1.1
Run as demand circuit
DoNotAge LSA allowed. Cost of using 40 State POINT_TO_POINT,
```

```

Timer intervals configured, Hello 10, Dead 40, Wait 40,
Hello due in 00:00:04
Adjacency State FULL (Hello suppressed)
Index 2/2, retransmission queue length 4, number of
retransmission 0
First 0x63311F3C(205)/0x63311FE4(59) Next
0x63311F3C(205)/0x63311FE4(59)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
Link State retransmission due in 360 msec

```

## Monitoring and Maintaining a Sham-Link

To monitor a sham-link, use the following **show** commands in EXEC mode:

| Command                                                   | Purpose                                                                                                                       |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip ospf sham-links</b>                    | Displays the operational status of all sham-links configured for a router.                                                    |
| Router# <b>show ip ospf data router</b> <i>ip-address</i> | Displays information about how the sham-link is advertised as an unnumbered point-to-point connection between two PE routers. |

## Configuration Examples

The following example shows how to configure a sham-link between two PE routers:

```

Router1(config)# interface loopback 1
Router1(config-if)# ip vrf forwarding ospf
Router1(config-if)# ip address 10.2.1.1 255.255.255.255
!
Router2(config)# interface loopback 1
Router2(config-if)# ip vrf forwarding ospf
Router2(config-if)# ip address 10.2.1.2 255.255.255.255
!
Router1(config)# router ospf 100 vrf ospf
Router1(config-if)# area 1 sham-link 10.2.1.1 10.2.1.2 cost 40
!
Router2(config)# router ospf 100 vrf ospf
Router2(config-if)# area 1 sham-link 10.2.1.2 10.2.1.1 cost 40

```

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **area sham-link cost**
- **show ip ospf sham-links**

# Glossary

**BGP**—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined in RFC 1163.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers are not aware of associated VPNs.

**CEF**—Cisco Express Forwarding. An advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns.

**OSPF**—Open Shortest Path First protocol.

**IGP**—Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common IGP include IGRP, OSPF, and RIP.

**LSA**—link-state advertisement. A broadcast packet used by link-state protocols. The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

**MPLS**—Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

**PE router**—provider edge router. A router that is part of a service provider network connected to a customer edge (CE) router. All VPN processing occurs in the PE router.

**SPF**—shortest path first calculation.

**VPN**—Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

**VRF**—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.







# OSPF Retransmissions Limit

## Feature History

| Release   | Modification                 |
|-----------|------------------------------|
| 12.2(11)T | This feature was introduced. |

This feature module describes the change in how the Open Shortest Path First (OSPF) protocol handles retransmissions and includes the following sections:

- [Feature Overview, page 643](#)
- [Benefits, page 643](#)
- [Restrictions, page 644](#)
- [Related Features and Technologies, page 644](#)
- [Supported Platforms, page 644](#)
- [Configuration Tasks, page 645](#)
- [Command Reference, page 646](#)

## Feature Overview

Cisco IOS Release 12.2(4)T added a limit to the number of retransmissions of database exchange and update packets for both demand and non-demand circuits. The retransmission of these packets stops once this retry limit is reached, thus preventing unnecessary use of the link in continual retransmission of the packets if, for some reason, a neighbor is not responding during adjacency forming.

The limit for both demand circuit and non-demand circuit retransmissions is 24.

The **limit-retransmissions** command allows you to either remove (disable) the limit or change the maximum number of retransmissions to be a number from 1 to 255.

## Benefits

The **limit-retransmissions** command provides for backward compatibility for previous or other releases of Cisco IOS or other routers that do not have this feature.

## Restrictions

The limit to the number of retransmissions does not apply for update packets on nonbroadcast multiaccess (NBMA) point-to-multipoint direct circuits. In this situation, the dead timer is used to end communication with non-responding neighbors and thus stop the retransmissions.

## Related Features and Technologies

This feature is an extension of the OSPF routing protocol. For more information about configuring OSPF and configuring route summarization and filtering, refer to the “[Configuring OSPF](#)” chapter of the *Cisco IOS IP Configuration Guide* and the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*.

## Supported Platforms

The **limit-retransmissions** command is supported for the following platforms in Cisco IOS Release 12.2(11)T:

- Cisco AS5300
- Cisco AS5400
- Cisco AS5800
- Cisco 1400 series
- Cisco 1600 series
- Cisco 1600R series
- Cisco 1710
- Cisco 1720
- Cisco 1721
- Cisco 1750
- Cisco 1751
- Cisco 2500 series
- Cisco 2600 series
- Cisco 3620
- Cisco 3631
- Cisco 3640
- Cisco 3725
- Cisco 3745
- Cisco 3660
- Cisco IGX 8400 Series URM
- Cisco MC3810
- Cisco 7100 series
- Cisco 7200 series

- Cisco 7500 series
- Cisco uBR7200 series

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Configuration Tasks

See the following sections for configuration tasks for the OSPF retransmission limits feature. Each task in the list is identified as either required or optional:

- [Setting OSPF Retransmission Limits](#) (required)

## Setting OSPF Retransmission Limits

To set OSPF retransmission limits, use the following commands beginning in router configuration mode:

|               | Command                                                                                                                                                           | Purpose                                                                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router ospf</b> <i>process-id</i>                                                                                                              | Configures the router to run an OSPF process.                                                                                    |
| <b>Step 2</b> | Router(config-router)# <b>limit retransmissions</b> {[ <b>dc</b> { <i>max-number</i>   <b>disable</b> }] [ <b>non-dc</b> { <i>max-number</i>   <b>disable</b> }]} | Sets the limit in the number of retransmissions of database exchange and update packets for both demand and non-demand circuits. |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **limit retransmissions**



## OSPF Support for Multi-VRF on CE Routers

The OSPF Support for Multi-VRF on CE Routers feature provides the capability of suppressing provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VPN routing and forward (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

OSPF multi-VRF allows you to split the router into multiple virtual routers, where each router contains its own set of interfaces, routing table, and forwarding table.

### Feature Specifications for the OSPF Support for Multi-VRF on CE Routers Feature

#### Feature History

| Release    | Modification                                                  |
|------------|---------------------------------------------------------------|
| 12.0(21)ST | This feature was introduced.                                  |
| 12.0(22)S  | This feature was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(8)B   | This feature was integrated into Cisco IOS Release 12.2(8)B.  |
| 12.2(13)T  | This feature was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(14)S  | This feature was integrated into Cisco IOS Release 12.2(14)S. |

#### Supported Platforms

For information about platforms supported in Cisco IOS Release 12.0(21)ST, 12.0(22)S, 12.2(13)T, and 12.2(14)S, refer to Cisco Feature Navigator. Cisco Feature Navigator does not support Cisco IOS Release 12.2(8)B.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

#### **Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Contents

- [Information About OSPF Support for Multi-VRF on CE Routers, page 648](#)
- [How to Configure OSPF Support for Multi-VRF on CE Routers, page 649](#)
- [Configuration Examples for OSPF Support for Multi-VRF on CE Routers, page 650](#)
- [Additional References, page 651](#)
- [Command Reference, page 653](#)
- [Glossary, page 654](#)

## Information About OSPF Support for Multi-VRF on CE Routers

Before you configure OSPF support for multi-VRF on CE routers, you should understand the following concepts:

- [Benefits of OSPF Multi-VRF Support, page 648](#)

## Benefits of OSPF Multi-VRF Support

The OSPF Support for Multi-VRF on CE Routers feature provides the capability of suppressing provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VPN routing and forward (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

OSPF multi-VRF allows you to split the router into multiple virtual routers, where each router contains its own set of interfaces, routing table, and forwarding table. OSPF multi-VRF gives you the ability to segment parts of your network and configure those segments to perform specific functions, yet still maintain correct routing information.

# How to Configure OSPF Support for Multi-VRF on CE Routers

This section contains the following procedures:

- [Configuring the Multi-VRF Capability for OSPF Routing, page 649](#)
- [Verifying the OSPF Multi-VRF Configuration, page 650](#)

## Configuring the Multi-VRF Capability for OSPF Routing

This section describes how to configure the multi-VRF for OSPF routing.

### SUMMARY STEPS

1. **enable**
2. **show ip ospf** [*process-id*]
3. **configure terminal**
4. **router ospf** *process-id* [**vrf** *vpn-name*]
5. **capability vrf-lite**

### DETAILED STEPS

|        | Command or Action                                                                                                                   | Purpose                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                              | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <b>show ip ospf</b> [ <i>process-id</i> ]<br><br><b>Example:</b><br>Router> show ip ospf 1                                          | Displays the status of the router. If the display indicates that the router is connected to the VPN backbone, you can use the <b>capability vrf-lite</b> command to decouple the PE router from the VPN backbone.                                                |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                      | Enters global configuration mode.                                                                                                                                                                                                                                |
| Step 4 | <b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vpn-name</i> ]<br><br><b>Example:</b><br>Router(config)# router ospf 1 vrf grc | Enables OSPF routing and enters router configuration mode. <ul style="list-style-type: none"> <li>• The <i>process-id</i> argument identifies the OSPF process.</li> <li>• Use the <b>vrf</b> keyword and <i>vpn-name</i> argument to identify a VPN.</li> </ul> |
| Step 5 | <b>capability vrf-lite</b><br><br><b>Example:</b><br>Router(config)# capability vrf-lite                                            | Applies the multi-VRF capability to the OSPF process.                                                                                                                                                                                                            |

## Verifying the OSPF Multi-VRF Configuration

No specific **debug** or **show** commands are associated with this feature. You can verify the success of the OSPF multi-VRF configuration by using the **show ip ospf** [*process-id*] command to verify that the router is not connected to the VPN backbone.

This output from the **show ip ospf process** command indicates that the PE router is currently connected to the backbone.

```
Router# show ip ospf 12

Routing Process "ospf 12" with ID 151.1.1.1 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
Connected to MPLS VPN Superbackbone
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

When the OSPF VRF process is configured with the **capability vrf-lite** command under the **router ospf** command, the “Connected to MPLS VPN Superbackbone” line will not be present in the display.

## Configuration Examples for OSPF Support for Multi-VRF on CE Routers

This section provides the following configuration examples:

- [Configuring the Multi-VRF Capability Example, page 650](#)
- [Verifying the OSPF Multi-VRF Configuration Example, page 651](#)

### Configuring the Multi-VRF Capability Example

This example shows a basic OSPF configuration using the **capability vrf-lite** command to suppress the PE checks.

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 9000 vrf grc
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
 capability vrf-lite
!
router rip
 network 10.94.0.0
```



```
redistribute ospf 9000
default-metric 1
```

## Verifying the OSPF Multi-VRF Configuration Example

This example illustrates the output display from the **show ip ospf process** command after OSPF multi-VRF has been configured on the router. Notice that in this display the indication that the router is connected to the VPN backbone is not present.

Router# **show ip ospf 12**

```
Routing Process "ospf 12" with ID 151.1.1.1 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA

SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DChitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

## Additional References

For additional information related to OSPF support for multi-VRF on CE routers, refer to the following references:

## Related Documents

| Related Topic                        | Document Title                                                         |
|--------------------------------------|------------------------------------------------------------------------|
| Configuring OSPF                     | <i>Cisco IOS IP Routing Configuration Guide</i> , Release 12.2         |
| Multiprotocol Label Switching (MPLS) | <i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.2 |

## Standards

| Standards <sup>1</sup>                                                                                                                | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

1. Not all supported standards are listed.

## MIBs

| MIBs <sup>1</sup>                                                                                                           | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs <sup>1</sup>                                                                                                           | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

1. Not all supported RFCs are listed.

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

# Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **capability vrf-lite**

# Glossary

**CE Router**—Customer Edge router, an edge router in the C network, defined as a C router which attaches directly to a P router.

**C Network**—Customer (enterprise or service provider) network.

**C Router**—Customer router, a router in the C network.

**LSA**—link-state advertisement. Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.

**PE Router**—Provider Edge router, an edge router in the P network, defined as a P router which attaches directly to a C router.

**P Network**—MPLS-capable service provider core network. P routers perform MPLS.

**P Router**—Provider router, a router in the P network.

**SPF**—shortest path first. A routing algorithm that iterates on length of path to determine a shortest-path spanning tree.

**VPN**—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

**VRF**—VPN Routing and Forwarding.



## OSPF Nonstop Forwarding (NSF) Awareness

The OSPF Nonstop Forwarding (NSF) Awareness feature allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets.

### Feature Specifications for the OSPF NSF Awareness Feature

| Feature History                                                              |                              |
|------------------------------------------------------------------------------|------------------------------|
| Release                                                                      | Modification                 |
| 12.2(15)T                                                                    | This feature was introduced. |
| Supported Platforms                                                          |                              |
| For information about platforms supported, refer to Cisco Feature Navigator. |                              |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About OSPF NSF Awareness, page 655](#)
- [How to Control OSPF NSF Awareness, page 656](#)
- [Additional References, page 659](#)
- [Command Reference, page 661](#)

## Information About OSPF NSF Awareness

The following concept describes the OSPF NSF Awareness feature:

- [Benefits of OSPF NSF Awareness, page 656](#)

## Benefits of OSPF NSF Awareness

The OSPF Nonstop Forwarding (NSF) Awareness feature allows customer premise equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets. The awareness feature is part of the software code; it need not be configured.

The local router is not necessarily performing NSF; its awareness of NSF allows the integrity and accuracy of the RIB and link state database occurring on the neighboring NSF-capable router to be maintained during the switchover process.

## How to Control OSPF NSF Awareness

OSPF NSF awareness is a feature that is part of the system's software code and need not be specifically enabled. However, there are a few optional tasks related to OSPF NSF awareness. This section contains the following tasks:

- [Setting the OSPF Resynchronization Timeout Timer, page 656](#) (optional)
- [Disabling OSPF NSF Awareness, page 657](#) (optional)
- [Displaying OSPF Neighbor NSF Information, page 659](#) (optional)

## Setting the OSPF Resynchronization Timeout Timer

The user can configure a timer that sets the out-of-band resynchronization timer, which is a optional task described in this section.

### Prerequisites

This task presumes that OSPF is already configured before you configure the out-of-band resynchronization timer. It also presumes that the local router is a neighbor to a router that is NSF-capable.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf resync-timeout** *seconds*
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                              | Enables higher privilege levels, such as privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 0                  | Configures the interface type and number.                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>ip ospf resync-timeout</b> <i>seconds</i><br><br><b>Example:</b><br>Router(config-if)# ip ospf resync-timeout 60 | Configures how long the router will wait before taking a neighbor adjacency down if the out-of-band resynchronization has not taken place since the time a restart signal was received from the neighbor. <ul style="list-style-type: none"> <li>The default is 40 seconds or the value of the OSPF dead interval, whichever is greater.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                         | Exits the configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                   |

## Disabling OSPF NSF Awareness

OSPF NSF awareness is enabled by default. You might want to disable NSF awareness by disabling the use of the Link-Local Signalling (LLS) data block in originated OSPF packets. You might want to disable NSF awareness if the router has no applications using LLS. Disabling NSF awareness is described in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **no capability lls**
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables higher privilege levels, such as privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                         |
| Step 3 | <b>router ospf process-id</b><br><br>Router(config)# router ospf 1                          | Enables OSPF routing and enters router configuration mode.<br><ul style="list-style-type: none"><li>The <i>process-id</i> argument identifies the OSPF process.</li></ul> |
| Step 4 | <b>no capability lls</b><br><br><b>Example:</b><br>Router(config-router)# no capability lls | Disables the use of the LLS data block and NSF awareness.                                                                                                                 |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                             | Exits the configuration mode and returns to privileged EXEC mode.                                                                                                         |

## Configuration Examples for OSPF NSF Awareness

This section provides the following configuration examples:

- [Setting OSPF Resynchronization Timeout Example, page 658](#)
- [Displaying OSPF Neighbor NSF Information, page 659](#)

### Setting OSPF Resynchronization Timeout Example

This example configures a 60-second resync timeout for OSPF on Ethernet interface 1:

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
 ip ospf resync-timeout 60
```



## Displaying OSPF Neighbor NSF Information

You can issue the **show ip ospf neighbor detail** command and display a new line of output about an NSF-capable neighbor. The command displays the last successful out-of-band resynchronization with the NSF-capable router.

This document presumes that OSPF is configured and that the local router has a neighbor that is NSF-capable.

The following is sample output from the **show ip ospf neighbor detail** command. The bold line is the new output about the NSF-capable neighbor, which indicates Link-local Signaling and Out-of-band (oob) link-state database resynchronization was performed *hours:minutes:seconds* ago. The command displays the last successful out-of-band resynchronization with the NSF-capable router.

```
Router> show ip ospf neighbor detail

Neighbor 192.168.5.2, interface address 10.225.200.28
  In the area 0 via interface GigabitEthernet1/0/0
  Neighbor priority is 1, State is FULL, 6 state changes
  DR is 10.225.200.28 BDR is 10.225.200.30
  Options is 0x42
  LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
  Dead timer due in 00:00:36
  Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```

## Additional References

For additional information related to NSF and OSPF, see the following sections:

- [Related Documents, page 659](#)
- [Standards, page 660](#)
- [MIBs, page 660](#)
- [RFCs, page 660](#)
- [Technical Assistance, page 661](#)

## Related Documents

| Related Topic      | Document Title                                                                                                                                                                                                                                                                                |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nonstop forwarding | <i>Cisco Nonstop Forwarding with Stateful Switchover</i><br><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/nsf120s.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s22/nsf120s.htm</a> |
| Configuring OSPF   | <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                                                                                                                                                                                                                                        |
| OSPF commands      | <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2                                                                                                                                                                                                        |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Commands

- `capability lls`
- `ip ospf resync-timeout`

### Modified Command

- `show ip ospf neighbor`





# OSPF Forwarding Address Suppression in Translated Type-5 LSAs

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes a not-so-stubby area (NSSA) area border router (ABR) to translate Type-7 link state advertisements (LSAs) to Type-5 LSAs, but use the address 0.0.0.0 for the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ABRs.

## Feature Specifications for the OSPF Forwarding Address Suppression in Translated Type-5 LSAs Feature

### Feature History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.2(15)T | This feature was introduced.                                  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Supported Platforms

For information about platforms supported, refer to Cisco Feature Navigator.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 664](#)
- [Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 664](#)
- [How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs, page 665](#)
- [Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 667](#)
- [Additional References, page 667](#)
- [Command Reference, page 669](#)

# Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

This document presumes you have OSPF configured on the networking device; it does not document other steps to configure OSPF.

## Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs

Before you configure the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature, you should understand the following concepts:

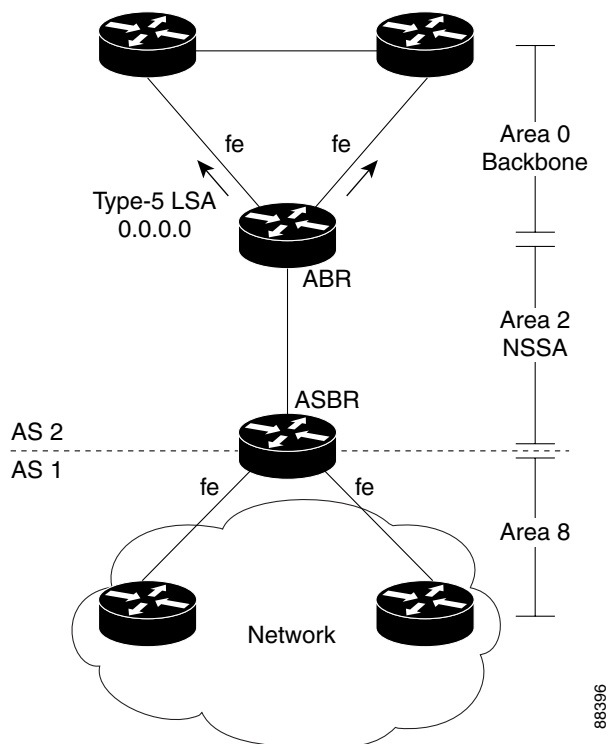
- [Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 664](#)
- [When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs, page 664](#)

## Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes an NSSA ABR to translate Type-7 LSAs to Type-5 LSAs, but use the 0.0.0.0 as the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ASBRs.

## When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs

In [Figure 54](#), it would be advantageous to filter Area 2 addresses from Area 0 to minimize the number of routes introduced into the backbone (Area 0). However, using **area range** commands to filter addresses will not work because Area 2 addresses include forwarding addresses for Type-7 LSAs generated by the ASBR, and without those forwarding addresses present in Area 0, the backbone routers cannot reach the prefixes advertised in the translated Type-5 LSAs (autonomous system external LSAs).

**Figure 54** *OSPF Forwarding Address Suppression in Translated Type-5 LSAs*

This problem is solved by suppressing the forwarding address on the ABR so that the forwarding address is set to 0.0.0.0 in the Type-5 LSAs that were translated from Type-7 LSAs. A forwarding address set to 0.0.0.0 indicates that packets for the external destination should be forwarded to the advertising OSPF router, in this case, the translating NSSA ABR.

Before configuring this feature, consider the following caution.



#### Caution

Configuring this feature causes the router to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

## How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs

This section contains the following procedure:

- [Suppressing OSPF Forwarding Address in Translated Type-5 LSAs, page 665](#)

### Suppressing OSPF Forwarding Address in Translated Type-5 LSAs

This task describes how to suppress OSPF forwarding address in translated Type-5 LSAs. Before configuring this feature, consider the following caution.

**Caution**

Configuring this feature causes the router to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router ospf *process-id***
4. **area *area-id* nssa translate type7 suppress-fa**
5. **end**

**DETAILED STEPS**

|        | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                | Enables higher privilege levels, such as privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                        | Enters global configuration mode.                                                                                                                                           |
| Step 3 | <b>router ospf <i>process-id</i></b><br><br><b>Example:</b><br>Router(config-router)# router ospf 1                                                   | Enables OSPF routing and enters router configuration mode.<br><ul style="list-style-type: none"><li>• The <i>process-id</i> argument identifies the OSPF process.</li></ul> |
| Step 4 | <b>area <i>area-id</i> nssa translate type7 suppress-fa</b><br><br><b>Example:</b><br>Router(config-router)# area 10 nssa translate type7 suppress-fa | Configures an area as a not-so-stubby-area (NSSA) and suppresses the forwarding address in translated Type-7 LSAs.                                                          |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                       | Exits configuration mode and returns to privileged EXEC mode.                                                                                                               |



# Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

This section provides the following configuration example:

- [Suppressing OSPF Forwarding Address in Translated Type-5 LSAs Example, page 667](#)

## Suppressing OSPF Forwarding Address in Translated Type-5 LSAs Example

This example suppresses the forwarding address in translated Type-5 LSAs:

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 1
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 network 10.94.0.0 0.0.255.255 area 10
 area 10 nssa translate type7 suppress-fa
```

## Additional References

For additional information related to OSPF, see the following sections:

- [Related Documents, page 667](#)
- [Standards, page 667](#)
- [MIBs, page 668](#)
- [RFCs, page 668](#)
- [Technical Assistance, page 668](#)

## Related Documents

| Related Topic    | Document Title                                                                         |
|------------------|----------------------------------------------------------------------------------------|
| Configuring OSPF | <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                                 |
| OSPF commands    | <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs                                                                                                                                      | Title                       |
|-------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587. | <i>The OSPF NSSA Option</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

# Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **area nssa translate**
- **show ip ospf**





# OSPF Inbound Filtering Using Route Maps with a Distribute List

The OSPF Inbound Filtering Using Route Maps with a Distribute List feature allows users to define a route map to prevent Open Shortest Path First (OSPF) routes from being added to the routing table. In the route map, the user can match on any attribute of the OSPF route.

## Feature Specifications for the OSPF Inbound Filtering Using Route Maps with a Distribute List Feature

### Feature History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(24)S | This feature was introduced.                                  |
| 12.2(15)T | This feature was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Supported Platforms

Use Cisco Feature Navigator as described below.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites, page 672](#)
- [Information About OSPF Inbound Filtering Using Route Maps with a Distribute List, page 672](#)
- [How to Configure OSPF Inbound Filtering Using Route Maps, page 673](#)
- [Configuration Examples for OSPF Inbound Filtering Using Route Maps with a Distribute List, page 674](#)
- [Additional References, page 675](#)
- [Command Reference, page 676](#)

## Prerequisites

It is presumed that you have OSPF configured in your network.

## Information About OSPF Inbound Filtering Using Route Maps with a Distribute List

Before you configure filtering based on an OSPF route map, you should understand the concept described in this section.

- [Benefits of OSPF Route Map-Based Filtering, page 672](#)

## Benefits of OSPF Route Map-Based Filtering

Users can define a route map to prevent OSPF routes from being added to the routing table. This filtering happens at the moment when OSPF is installing the route in the routing table. This feature has no effect on LSA flooding. In the route map, the user can match on any attribute of the OSPF route. That is, the route map could be based on the following **match** options:

- **match interface**
- **match ip address**
- **match ip next-hop**
- **match ip route-source**
- **match metric**
- **match route-type**
- **match tag**

This feature can be useful during redistribution if the user tags prefixes when they get redistributed on ASBRs and later uses the tag to filter the prefixes from being installed in the routing table on other routers.

### Filtering Based on Route Tag

Users can assign tags to external routes when they are redistributed to OSPF. Then the user can deny or permit those routes in the OSPF domain by identifying that tag in the **route-map** and **distribute-list in** commands.

### Filtering Based on Route Type

In OSPF, the external routes could be Type 1 or Type 2. Users can create route maps to match either Type 1 or Type 2 and then use the **distribute-list in** command to filter certain prefixes. Also, route maps can identify internal routes (interarea and intra-area) and then those routes can be filtered.

### Filtering Based on Route Source

When a match is done on the route source, the route source represents the OSPF Router ID of the LSA originator of the LSA in which the prefix is advertised.

### Filtering Based on Interface

When a match is done on the interface, the interface represents the outgoing interface for the route that OSPF is trying to install in the routing table.

### Filtering Based on Next-Hop

When a match is done on the next hop, the next hop represents the next hop for the route that OSPF is trying to install in the routing table.

## How to Configure OSPF Inbound Filtering Using Route Maps

This section describes enabling OSPF filtering based on a route map.

- [Configuring OSPF Route Map-Based Filtering, page 673](#)

## Configuring OSPF Route Map-Based Filtering

This section describes how to configure OSPF route map-based filtering. Step 4 is simply an example of a route map; other **match** commands could be used.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match tag** *tag-name*  
or other **match** commands.
5. Repeat Steps 3 and 4 with other **route-map** and **match** commands if you choose.
6. **exit**
7. **router ospf** *process-id*
8. **distribute-list route-map** *map-tag* **in**
9. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ]<br><i>[sequence-number]</i><br><br><b>Example:</b><br>Router(config)# route-map tag-filter deny 10 | Defines a route map to control filtering.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 4 | <b>match tag</b> <i>tag-name</i><br><br>or other <b>match</b> command(s)<br><br><b>Example:</b><br>Router(config-router)# match tag 777                            | Matches routes with a specified name, to be used as the route map is referenced. <ul style="list-style-type: none"> <li>At least one <b>match</b> command is required, but it need not be this <b>match</b> command. This is just an example.</li> <li>The list of <b>match</b> commands available to be used in this type of route map appears on the <b>distribute-list in</b> command reference page.</li> <li>This type of route map will have no <b>set</b> commands.</li> </ul> |
| Step 5 | Repeat Steps 3 and 4 with other <b>route-map</b> and <b>match</b> commands if you choose.                                                                          | Optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                  | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 7 | <b>router ospf</b> <i>process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                       | Configures an OSPF routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <b>distribute-list route-map</b> <i>map-tag</i> <b>in</b><br><br><b>Example:</b><br>Router(config-router)# distribute-list route-map tag-filter in                 | Enables filtering based on an OSPF route map.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                    | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Configuration Examples for OSPF Inbound Filtering Using Route Maps with a Distribute List

This section contains an example of filtering based on an OSPF route map.

- [OSPF Route Map-Based Filtering Example, page 675](#)



## OSPF Route Map-Based Filtering Example

In this example, OSPF external LSAs have a tag. The value of the tag is examined before the prefix is installed in the routing table. All OSPF external prefixes that have the tag value of 777 are filtered (prevented from being installed in the routing table). The permit statement with sequence number 20 has no match conditions, and there are no other route-map statements after sequence number 20, so all other conditions are permitted.

```
route-map tag-filter deny 10
  match tag 777
route-map tag-filter permit 20
!
router ospf 1
  router-id 10.0.0.2
  log-adjacency-changes
  network 172.16.2.1 0.0.0.255 area 0
  distribute-list route-map tag-filter in
```

## Additional References

For additional information related to OSPF, refer to the following references:

- [Related Documents, page 675](#)
- [Standards, page 675](#)
- [MIBs, page 676](#)
- [RFCs, page 676](#)
- [Technical Assistance, page 676](#)

## Related Documents

| Related Topic            | Document Title                                                                                        |
|--------------------------|-------------------------------------------------------------------------------------------------------|
| OSPF commands            | “OSPF Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0      |
| OSPF configuration tasks | “Configuring OSPF” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **distribute-list in (IP)**



# OSPF Shortest Path First Throttling

The OSPF Shortest Path First Throttling feature makes it possible to configure SPF scheduling in millisecond intervals and to potentially delay shortest path first (SPF) calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events.

The interval at which the SPF calculations occur is chosen dynamically and is based on the frequency of topology changes in the network. The chosen interval is within the boundary of the user-specified value ranges. If network topology is unstable, SPF throttling calculates SPF scheduling intervals to be longer until topology becomes stable.

## Feature Specifications for OSPF Shortest Path First Throttling

### Feature History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.2(14)S | This feature was introduced.                                  |
| 12.0(23)S | This feature was integrated into Cisco Release 12.0(23)S.     |
| 12.2(15)T | This feature was integrated into Cisco IOS Release 12.2(15)T. |

### Supported Platforms

For information about platforms supported, refer to Cisco Feature Navigator.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About OSPF SPF Throttling, page 678](#)
- [How to Configure OSPF SPF Throttling, page 679](#)
- [Configuration Examples for OSPF SPF Throttling, page 681](#)
- [Additional References, page 682](#)
- [Command Reference, page 683](#)

# Information About OSPF SPF Throttling

To use SPF throttling, you should understand the following concepts:

- [Shortest Path First Calculations, page 678](#)

## Shortest Path First Calculations

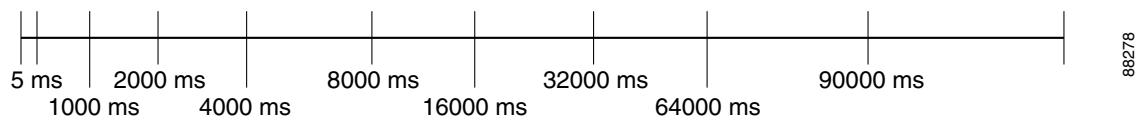
SPF calculations occur at the interval set by the **timers throttle spf** command. The wait interval indicates the amount of time to wait until the next SPF calculation occurs. Each wait interval after that calculation is twice as long as the previous one until the wait interval reaches the maximum wait time specified.

The SPF timing can be better explained using an example. In this example the start interval is set at 5 milliseconds (ms), the wait interval at 1000 milliseconds, and the maximum wait time is set at 90,000 milliseconds.

```
timers throttle spf 5 1000 90000
```

[Figure 55](#) shows the intervals at which the SPF calculations occur so long as at least one topology change event is received in a given wait interval.

**Figure 55** *SPF Calculation Intervals Set by the timers throttle spf Command*

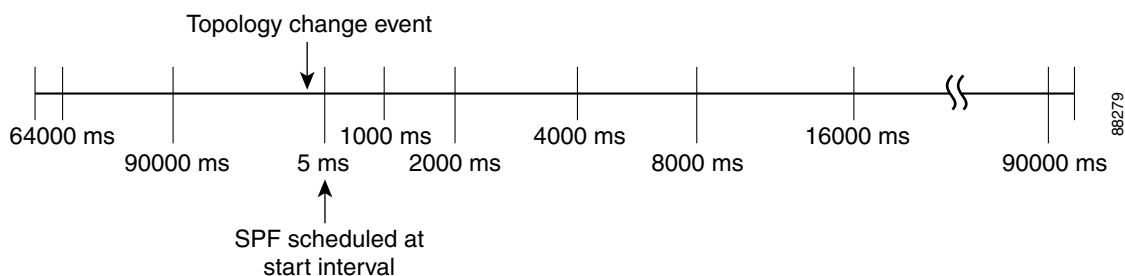


Notice that the wait interval between SPF calculations doubles when at least one topology change event is received during the previous wait interval. Once the maximum wait time is reached, the wait interval remains the same until the topology stabilizes and no event is received in that interval.

If the first topology change event is received after the current wait interval, the SPF calculation is delayed by the amount of time specified as the start interval. The subsequent wait intervals continue to follow the dynamic pattern.

If the first topology change event occurs after the maximum wait interval begins, the SPF calculation is again scheduled at the start interval and subsequent wait intervals are reset according to the parameters specified in the **timers throttle spf** command. Notice in [Figure 56](#) that a topology change event was received after the start of the maximum wait time interval and that the SPF intervals have been reset.

**Figure 56** *Timer Intervals Reset after Topology Change Event*



# How to Configure OSPF SPF Throttling

Perform the following tasks to configure OSPF SPF throttling:

- [Configuring OSPF SPF Throttling, page 679](#) (required)
- [Verifying SPF Throttle Values, page 680](#) (optional)

## Configuring OSPF SPF Throttling

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **ip address** *ip-address mask [secondary]*
5. **exit**
6. **router ospf** *process-id*
7. **network** *network-number [mask | prefix-length]*
8. **timers throttle spf** *spf-start spf-hold spf-max-wait*
9. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                      | Purpose                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                 | Enables higher privilege levels, such as privileged EXEC mode.<br><br>Enter your password if prompted. |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                         | Enters global configuration mode.                                                                      |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/1/1                              | Enters interface configuration mode for the interface specified.                                       |
| Step 4 | <b>ip address</b> <i>ip-address mask [secondary]</i><br><br><b>Example:</b><br>Router(config-if)# ip address 192.168.0.2 255.255.255.0 | Sets a primary or secondary IP address for an interface.                                               |

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                         |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>router# exit                                                                                                   | Exits interface configuration mode.                                                                                             |
| Step 6 | <b>router ospf process-id</b><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                | Configures an OSPF routing process.                                                                                             |
| Step 7 | <b>network network-number [mask   prefix-length]</b><br><br><b>Example:</b><br>Router(config-router)# network 192.168.0.0<br>0.0.255.255 area 0      | Configures the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP Server. |
| Step 8 | <b>timers throttle spf spf-start spf-hold<br/>spf-max-wait</b><br><br><b>Example:</b><br>Router(config-router)# timers throttle spf 10<br>4800 90000 | Sets OSPF throttling timers.                                                                                                    |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                      | Exits configuration mode.                                                                                                       |

## Verifying SPF Throttle Values

To verify SPF throttle timer values, use the **show ip ospf** command. The values are displayed in the lines that begin, “Initial SPF schedule delay...,” “Minimum hold time between two consecutive SPF’s...,” and “Maximum wait time between two consecutive SPF’s....”

```
Router# show ip ospf

Routing Process "ospf 1" with ID 10.10.10.2 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
Initial SPF schedule delay 5 msec
Minimum hold time between two consecutive SPF's 1000 msec
Maximum wait time between two consecutive SPF's 90000 msec
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 4. Checksum Sum 0x17445
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
```

```

Number of interfaces in this area is 2
Area has no authentication
SPF algorithm last executed 19:11:15.140 ago
SPF algorithm executed 28 times
Area ranges are
Number of LSA 4. Checksum Sum 0x2C1D4
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

```

Table 20 describes the **show ip ospf** display fields and their descriptions.

**Table 20** *show ip ospf Field Descriptions*

| Field                                             | Description                                                                                                   |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Routing process “ospf 201” with ID 192.42.110.200 | Process ID and OSPF router ID.                                                                                |
| Supports ...                                      | Number of types of service supported (Type 0 only).                                                           |
| It is ...                                         | Possible types are internal, area border, or autonomous system boundary.                                      |
| Summary Link update interval                      | Specifies summary update interval in hours:minutes:seconds, and time until next update.                       |
| External Link update interval                     | Specifies external update interval in hours:minutes:seconds, and time until next update.                      |
| Redistributing External Routes from               | Lists of redistributed routes, by protocol.                                                                   |
| SPF calculations                                  | Lists start, hold, and maximum wait interval values in milliseconds.                                          |
| Number of areas                                   | Number of areas in router, area addresses, and so on.                                                         |
| SPF algorithm last executed                       | Shows the last time an SPF calculation was performed in response to topology change event records.            |
| Link State Update Interval                        | Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update. |
| Link State Age Interval                           | Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.  |

## Configuration Examples for OSPF SPF Throttling

This section contains the following examples:

- [Throttle Timers Example, page 681](#)

### Throttle Timers Example

This example shows a router configured with the start, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1,000, and 90,000 milliseconds, respectively.

```
router ospf 1
```

```

router-id 10.10.10.2
log-adjacency-changes
timers throttle spf 5 1000 90000
redistribute static subnets
network 21.21.21.0 0.0.0.255 area 0
network 22.22.22.0 0.0.0.255 area 00

```

## Additional References

For additional information related to OSPF, refer to the following references:

- [Related Documents, page 682](#)
- [Standards, page 682](#)
- [MIBs, page 682](#)
- [RFCs, page 683](#)
- [Technical Assistance, page 683](#)

## Related Documents

| Related Topic            | Document Title                                                                                                        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------|
| OSPF commands            | “OSPF Commands” chapter in the <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.2 |
| OSPF configuration tasks | “Configuring OSPF ” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.2                             |

## Standards

| Standards                                                                                                                   | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. |       |

## MIBs

| MIBs                                                     | MIBs Link                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• None</li> </ul> | <p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p> |



## RFCs

| RFCs                                                                                                                                  | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. |       |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- timers throttle spf





# OSPF Support for Fast Hello Packets

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration would result in faster convergence in an Open Shortest Path First (OSPF) network.

## Feature Specifications for OSPF Support for Fast Hello Packets

### Feature History

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(23)S | This feature was introduced.                                  |
| 12.2(15)T | This feature was integrated into Cisco IOS Release 12.2(15)T. |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Supported Platforms

Refer to Feature Navigator as referenced below.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Support for Fast Hello Packets, page 686](#)
- [Information About OSPF Support for Fast Hello Packets, page 686](#)
- [How to Configure OSPF Fast Hello Packets, page 687](#)
- [Configuration Examples for OSPF Support of Fast Hello Packets, page 688](#)
- [Additional References, page 689](#)
- [Command Reference, page 690](#)

# Prerequisites for OSPF Support for Fast Hello Packets

OSPF must be configured in the network already or configured at the same time as the OSPF Support for Fast Hello Packets feature.

## Information About OSPF Support for Fast Hello Packets

The following sections describe concepts related to OSPF support for fast hello packets:

- [OSPF Hello Interval and Dead Interval, page 686](#)
- [OSPF Fast Hello Packets, page 686](#)
- [Benefits of OSPF Fast Hello Packets, page 687](#)

## OSPF Hello Interval and Dead Interval

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a nonbroadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the *dead interval*. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

## OSPF Fast Hello Packets

OSPF fast hello packets refer to hello packets being sent at intervals of less than 1 second. To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See the section [“OSPF Hello Interval and Dead Interval”](#).

OSPF fast hello packets are achieved by using the **ip ospf dead-interval** command. The dead interval is set to 1 second, and the hello-multiplier value is set to the number of hello packets you want sent during that 1 second, thus providing subsecond or “fast” hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

## Benefits of OSPF Fast Hello Packets

The benefit of the OSPF Fast Hello Packets feature is that your OSPF network will experience faster convergence time than it would without fast hello packets. This feature allows you to detect lost neighbors within 1 second. It is especially useful in LAN segments, where neighbor loss might not be detected by the Open System Interconnection (OSI) physical layer and data-link layer.

## How to Configure OSPF Fast Hello Packets

The following section describes how to enable OSPF fast hello packets:

- [Configure OSPF Fast Hello Packets, page 687](#)

## Configure OSPF Fast Hello Packets

This section describes how to configure OSPF fast hello packets.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf dead-interval minimal hello-multiplier** *multiplier*
5. **end**
6. **show ip ospf interface** [*interface-type interface-number*]

### DETAILED STEPS

|        | Command or Action                                       | Purpose                                                               |
|--------|---------------------------------------------------------|-----------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                           | Enables higher privilege levels, such as privileged EXEC mode.        |
|        | <b>Example:</b><br>Router> enable                       | Enter your password if prompted.                                      |
| Step 2 | <b>configure terminal</b>                               | Enters global configuration mode.                                     |
|        | <b>Example:</b><br>Router# configure terminal           |                                                                       |
| Step 3 | <b>interface</b> <i>type number</i>                     | Configures an interface type and enters interface configuration mode. |
|        | <b>Example:</b><br>Router(config)# interface ethernet 0 |                                                                       |

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>ip ospf dead-interval minimal hello-multiplier multiplier</b><br><br><b>Example:</b><br>Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5 | Sets the interval during which at least one hello packet must be received, or else the neighbor is considered down. <ul style="list-style-type: none"> <li>In the example, OSPF Support for Fast Hello Packets is enabled by specifying the <b>minimal</b> keyword and the <b>hello-multiplier</b> keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                    | (Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode. <ul style="list-style-type: none"> <li>Use this command when you are ready to exit configuration mode and save the configuration to the running configuration file.</li> </ul>                                                                                           |
| Step 6 | <b>show ip ospf interface [interface-type interface-number]</b><br><br><b>Example:</b><br>Router# show ip ospf interface ethernet 1/3                          | (Optional) Displays OSPF-related interface information. <ul style="list-style-type: none"> <li>The relevant fields that verify OSPF fast hello packets are indicated in the sample output following this table.</li> </ul>                                                                                                                                                                                         |

The following example output verifies that OSPF Support for Fast Hello Packets is configured. In the line that begins with “Timer intervals configured,” the hello interval is 200 milliseconds, the dead interval is 1 second, and the next hello packet is due in 76 milliseconds.

```
Router# show ip ospf interface ethernet 1/3
```

```
Ethernet1/3 is up, line protocol is up
 Internet Address 172.16.1.2/24, Area 0
 Process ID 1, Router ID 176.17.0.2, Network Type BROADCAST, Cost:1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 176.17.0.2, Interface address 172.16.1.2
 Backup Designated router (ID) 172.16.0.1, Interface address 172.16.1.1
 Timer intervals configured, Hello 200 msec, Dead 1, Wait 1, Retransmit 5
   Hello due in 76 msec
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 3
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.0.1 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

## Configuration Examples for OSPF Support of Fast Hello Packets

The following section provides a configuration example:

- [OSPF Fast Hello Packets Example, page 689](#)

## OSPF Fast Hello Packets Example

The following example configures OSPF fast hello packets; the dead interval is 1 second and five hello packets are sent every second:

```
interface ethernet 1
 ip ospf dead-interval minimal hello-multiplier 5
```

## Additional References

For additional information related to OSPF Support for Fast Hello Packets, refer to the following references:

- [Standards, page 689](#)
- [Standards, page 689](#)
- [MIBs, page 689](#)
- [RFCs, page 690](#)

## Related Documents

| Related Topic                                                                                                   | Document Title                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| OSPF configuration tasks                                                                                        | “Configuring OSPF” chapter in the part, “IP Routing Protocols” in the <i>Cisco IOS Release 12.0 Network Protocols Configuration Guide, Part 1</i> |
| OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | “OSPF Commands” chapter in the part “IP Routing Protocols” in the <i>Cisco IOS Release 12.0 Network Protocols Command Reference, Part 1</i>       |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                         | Link                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **ip ospf dead-interval**





## OSPF Incremental SPF

The Open Shortest Path First (OSPF) protocol can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event.

### Feature History for the OSPF Incremental SPF Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(24)S | This feature was introduced.                                  |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Incremental SPF, page 691](#)
- [Information About OSPF Incremental SPF, page 692](#)
- [How to Enable OSPF Incremental SPF, page 692](#)
- [Configuration Examples for OSPF Incremental SPF, page 693](#)
- [Additional References, page 694](#)
- [Command Reference, page 695](#)

## Prerequisites for OSPF Incremental SPF

It is presumed that you have OSPF configured in your network.

# Information About OSPF Incremental SPF

Before you enable OSPF Incremental SPF, you should understand the concept described in this section.

- [Benefits of OSPF Incremental SPF, page 692](#)

## Benefits of OSPF Incremental SPF

OSPF uses Dijkstra's SPF algorithm to compute the shortest path tree (SPT). During the computation of the SPT, the shortest path to each node is discovered. The topology tree is used to populate the routing table with routes to IP networks. When changes to a Type-1 or Type-2 link-state advertisement (LSA) occur in an area, the entire SPT is recomputed. In many cases, the entire SPT need not be recomputed because most of the tree remains unchanged. Incremental SPF allows the system to recompute only the affected part of the tree. Recomputing only a portion of the tree rather than the entire tree results in faster OSPF convergence and saves CPU resources. Note that if the change to a Type-1 or Type-2 LSA occurs in the calculating router itself, then the full SPT is performed.

Incremental SPF is scheduled in the same way as the full SPF. Routers enabled with incremental SPF and routers not enabled with incremental SPF can function in the same internetwork.

## How to Enable OSPF Incremental SPF

This section contains the following procedure:

- [Enabling Incremental SPF, page 692](#)

## Enabling Incremental SPF

This section describes how to enable incremental SPF.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **ispf**
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                     | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal        | Enters global configuration mode.                                                                                |
| Step 3 | <b>router ospf process-id</b><br><br><b>Example:</b><br>Router(config)# router ospf 1 | Configures an OSPF routing process.                                                                              |
| Step 4 | <b>ispf</b><br><br><b>Example:</b><br>Router(config-router)# ispf                     | Enables incremental SPF.                                                                                         |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                       | Exits router configuration mode.                                                                                 |

# Configuration Examples for OSPF Incremental SPF

This section contains an example of configuring OSPF incremental SPF:

- [Incremental SPF: Example, page 693](#)

## Incremental SPF: Example

This example enables incremental SPF:

```
router ospf 1
 ispf
```

# Additional References

The following sections provide references related to OSPF Incremental SPF.

## Related Documents

| Related Topic            | Document Title                                                                                         |
|--------------------------|--------------------------------------------------------------------------------------------------------|
| OSPF commands            | “OSPF Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0       |
| OSPF configuration tasks | “Configuring OSPF ” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br><br><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **ispf**





## OSPF Limit on Number of Redistributed Routes

Open Shortest Path First (OSPF) supports a user-defined maximum number of prefixes (routes) that are allowed to be redistributed into OSPF from other protocols or other OSPF processes. Such a limit could help prevent the router from being flooded by too many redistributed routes.

### Feature History for the OSPF Limit on Number of Redistributed Routes Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(25)S | This feature was introduced.                                  |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Limit on Number of Redistributed Routes, page 697](#)
- [Information About OSPF Limit on Number of Redistributed Routes, page 698](#)
- [How to Limit OSPF Redistributed Routes or Receive Warning About Number of OSPF Redistributed Routes, page 698](#)
- [Configuration Examples for OSPF Limit on Number of Redistributed Routes, page 701](#)
- [Additional References, page 702](#)
- [Command Reference, page 703](#)

## Prerequisites for OSPF Limit on Number of Redistributed Routes

It is presumed that you have OSPF configured in your network, along with another protocol or another OSPF process you are redistributing.

# Information About OSPF Limit on Number of Redistributed Routes

Before you limit the number of OSPF redistributed routes, you should understand the concept described in this section:

- [Benefits of OSPF Limit on Number of Redistributed Routes, page 698](#)

## Benefits of OSPF Limit on Number of Redistributed Routes

If someone mistakenly injects a large number of IP routes into OSPF, perhaps by redistributing BGP into OSPF, the network can be severely flooded. Limiting the number of redistributed routes prevents this potential problem.

## How to Limit OSPF Redistributed Routes or Receive Warning About Number of OSPF Redistributed Routes

This section contains the following procedures, which are mutually exclusive. That is, you cannot both limit redistributed prefixes and also choose to be warned only.

- [Limiting the Number of OSPF Redistributed Routes, page 698](#)
- [Requesting a Warning About the Number of Routes Redistributed into OSPF, page 700](#)

## Limiting the Number of OSPF Redistributed Routes

This task describes how to limit the number of OSPF redistributed routes. If the number of redistributed routes reaches the maximum value configured, no more routes will be redistributed.


The redistribution limit applies to all IP redistributed prefixes, including summarized ones. The redistribution limit does not apply to default routes or prefixes that are generated as a result of Type-7 to Type-5 translation.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf *process-id***
4. **redistribute *protocol* [*process-id*] [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]**
5. **redistribute maximum-prefix *maximum* [*threshold*]**
6. **end**
7. **show ip ospf [*process-id*]**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>router ospf process-id</b><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                                                                                                                                  | Configures an OSPF routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <b>redistribute protocol [process-id] [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b><br><br><b>Example:</b><br>Router(config-router)# redistribute eigrp 10 | Redistributes routes from one routing domain into another routing domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 5 | <b>redistribute maximum-prefix maximum [threshold]</b><br><br><b>Example:</b><br>Router(config-router)# redistribute maximum-prefix 100 80                                                                                                                             | Sets a maximum number of IP prefixes that are allowed to be redistributed into OSPF. <ul style="list-style-type: none"> <li>There is no default value for the <i>maximum</i> argument.</li> <li>The <i>threshold</i> value defaults to 75 percent.</li> </ul> <div>  <b>Note</b> If the <b>warning-only</b> keyword had been configured in this command, no limit would be enforced; a warning message is simply logged.         </div> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                                                                                                        | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 7 | <b>show ip ospf [process-id]</b><br><br><b>Example:</b><br>Router# show ip ospf 1                                                                                                                                                                                      | (Optional) Displays general information about OSPF routing processes. <ul style="list-style-type: none"> <li>If a redistribution limit was configured, the output will include the maximum limit of redistributed prefixes and the threshold for warning messages.</li> </ul>                                                                                                                                                                                                                                              |

## Requesting a Warning About the Number of Routes Redistributed into OSPF

This task describes how to cause the system to generate a warning message when the number of redistributed prefixes reaches a maximum value. However, additional redistribution is not prevented.

The redistribution count applies to external IP prefixes, including summarized routes. Default routes and prefixes that are generated as a result of Type-7 to Type-5 translation are not considered.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id*] [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistribute maximum-prefix** *maximum* [*threshold*] **warning-only**
6. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                       | Purpose                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                  | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                                                                          | Enters global configuration mode.                                                                                   |
| Step 3 | <b>router ospf</b> <i>process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                                                                                                                                                                                                                                                            | Configures an OSPF routing process.                                                                                 |
| Step 4 | <b>redistribute</b> <i>protocol</i> [ <i>process-id</i> ] [ <i>as-number</i> ] [ <b>metric</b> <i>metric-value</i> ] [ <b>metric-type</b> <i>type-value</i> ] [ <b>match</b> { <b>internal</b>   <b>external 1</b>   <b>external 2</b> }] [ <b>tag</b> <i>tag-value</i> ] [ <b>route-map</b> <i>map-tag</i> ] [ <b>subnets</b> ]<br><br><b>Example:</b><br>Router(config-router)# redistribute eigrp 10 | Redistributes routes from one routing domain into another routing domain.                                           |

|        | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>redistribute maximum-prefix</b> <i>maximum</i> [ <i>threshold</i> ]<br><b>warning-only</b><br><br><b>Example:</b><br><pre>Router(config-router)# redistribute maximum-prefix 1000 80 warning-only</pre> | <p>Causes a warning message to be logged when the maximum number of IP prefixes has been redistributed into OSPF.</p> <ul style="list-style-type: none"> <li>Because the <b>warning-only</b> keyword is included, no limit is imposed on the number of redistributed prefixes into OSPF.</li> <li>There is no default value for the <i>maximum</i> argument.</li> <li>The <i>threshold</i> value defaults to 75 percent.</li> <li>This example causes two warnings: one at 80 percent of 1000 (800 routes redistributed) and another at 1000 routes redistributed.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br><pre>Router(config-router)# end</pre>                                                                                                                                 | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Configuration Examples for OSPF Limit on Number of Redistributed Routes

This section contains the following examples:

- [OSPF Limit on Number of Redistributed Routes: Example, page 701](#)
- [Requesting a Warning About the Number of Redistributed Routes: Example, page 702](#)

### OSPF Limit on Number of Redistributed Routes: Example

This example sets a maximum of 1200 prefixes that can be redistributed into OSPF process 1. Prior to reaching the limit, when the number of prefixes redistributed reaches 80 percent of 1200 (960 prefixes), a warning message is logged. Another warning is logged when the limit is reached and no more routes are redistributed.

```
router ospf 1
router-id 10.0.0.1
domain-id 5.6.7.8
log-adjacency-changes
timers lsa-interval 2
network 10.0.0.1 0.0.0.0 area 0
network 10.1.5.1 0.0.0.0 area 0
network 10.2.2.1 0.0.0.0 area 0
redistribute static subnets
redistribute maximum-prefix 1200 80
```

## Requesting a Warning About the Number of Redistributed Routes: Example

This example allows two warning messages to be logged, the first if the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second if the number of redistributed routes reaches 600. However, the number of redistributed routes is not limited.

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 600 85 warning-only
```

## Additional References

The following sections provide references related to OSPF Limit on Number of Redistributed Routes.

## Related Documents

| Related Topic                      | Document Title                                                                                                                            |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Redistribution commands            | “IP Routing Protocol-Independent Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0               |
| Redistribution configuration tasks | “Configuring IP Routing Protocol-Independent Features” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0 |
| OSPF commands                      | “OSPF Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0                                          |
| OSPF configuration tasks           | “Configuring OSPF” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0                                     |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Command

- **redistribute maximum-prefix**

### Modified Commands

- **show ip ospf**
- **show ip ospf database**





# OSPF Link-State Advertisement (LSA) Throttling

The OSPF Link-State Advertisement (LSA) Throttling feature provides a dynamic mechanism to slow down link-state advertisement (LSA) updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds.

## Feature History for the OSPF LSA Throttling Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(25)S | This feature was introduced.                                  |
| 12.3(2)T  | This feature was integrated into Cisco IOS Release 12.3(2)T.  |
| 12.2(18)S | This feature was integrated into Cisco IOS Release 12.2(18)S. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF LSA Throttling, page 705](#)
- [Information About OSPF LSA Throttling, page 706](#)
- [How to Customize OSPF LSA Throttling, page 706](#)
- [Configuration Examples for OSPF LSA Throttling, page 709](#)
- [Additional References, page 709](#)
- [Command Reference, page 710](#)

## Prerequisites for OSPF LSA Throttling

It is presumed that you have OSPF configured in your network.

# Information About OSPF LSA Throttling

Before you enable OSPF LSA Throttling, you should understand the following concepts:

- [Benefits of OSPF LSA Throttling, page 706](#)
- [How OSPF LSA Throttling Works, page 706](#)

## Benefits of OSPF LSA Throttling

Prior to the OSPF LSA Throttling feature, LSA generation was rate-limited for 5 seconds. That meant that changes in an LSA could not be propagated in milliseconds, so the OSPF network could not achieve millisecond convergence.

The OSPF LSA Throttling feature is enabled by default and allows faster OSPF convergence (in milliseconds). This feature can be customized. One command controls the generation (sending) of LSAs and another command controls the receiving interval. This feature also provides a dynamic mechanism to slow down the frequency of LSA updates in OSPF during times of network instability.

## How OSPF LSA Throttling Works

The **timers throttle lsa all** command controls the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID.

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the **timers throttle lsa all** command.

## How to Customize OSPF LSA Throttling

This section contains the following optional procedure:

- [Customizing OSPF LSA Throttling, page 706](#) (optional)

## Customizing OSPF LSA Throttling

This task describes how to customize OSPF LSA throttling if you prefer to set values other than the defaults.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers throttle lsa all** *start-interval hold-interval max-interval*



5. **timers lsa arrival** *milliseconds*
6. **end**
7. **show ip ospf timers rate-limit**
8. **show ip ospf**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                |
| Step 3 | <b>router ospf</b> <i>process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                             | Configures an OSPF routing process.                                                                                                                                                                                                                                                                                                                                                              |
| Step 4 | <b>timers throttle lsa all</b> <i>start-interval hold-interval max-interval</i><br><br><b>Example:</b><br>Router(config-router)# timers throttle lsa all 100 10000 45000 | (Optional) Sets the rate-limiting values (in milliseconds) for LSA generation. <ul style="list-style-type: none"> <li>The default values are as follows: <ul style="list-style-type: none"> <li><i>start-interval</i> is 0 milliseconds</li> <li><i>hold-interval</i> is 5000 milliseconds</li> <li><i>max-interval</i> is 5000 milliseconds</li> </ul> </li> </ul>                              |
| Step 5 | <b>timers lsa arrival</b> <i>milliseconds</i><br><br><b>Example:</b><br>Router(config-router)# timers lsa arrival 2000                                                   | (Optional) Sets the minimum interval (in milliseconds) between instances of receiving the same LSA. <ul style="list-style-type: none"> <li>The default value is 1000 milliseconds.</li> <li>We suggest you keep the <i>milliseconds</i> value of the LSA arrival timer less than or equal to the neighbors' <i>hold-interval</i> value of the <b>timers throttle lsa all</b> command.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                          | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                 |

| Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 7</b>    <b>show ip ospf timers rate-limit</b></p> <p><b>Example:</b><br/>Router# show ip ospf timers rate-limit</p> <pre> LSAID: 10.1.1.1      Type: 1    Adv Rtr: 172.16.2.2 Due in: 00:00:00.028  LSAID: 192.168.4.1   Type: 3    Adv Rtr: 172.17.2.2 Due in: 00:00:00.028 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>(Optional) Displays a list of the LSAs in the rate limit queue (about to be generated).</p> <ul style="list-style-type: none"> <li>The example shows two LSAs in the queue. Each LSA is identified by LSA ID number, Type (of LSA), Advertising router ID, and the time in hours:minutes:seconds (to the milliseconds) when the LSA is due to be generated.</li> </ul> |
| <p><b>Step 8</b>    <b>show ip ospf</b></p> <p><b>Example:</b><br/>Router# <b>show ip ospf</b></p> <pre> Routing Process "ospf 4" with ID 10.10.24.4   Supports only single TOS(TOS0) routes   Supports opaque LSA   Supports Link-local Signaling (LLS)   Initial SPF schedule delay 5000 msec   Minimum hold time between two consecutive SPF 10000 msec   Maximum wait time between two consecutive SPF 10000 msec   Incremental-SPF disabled   <b>Initial LSA throttle delay 100 msec</b>   <b>Minimum hold time for LSA throttle 10000 msec</b>   <b>Maximum wait time for LSA throttle 45000 msec</b>   Minimum LSA arrival 1000 msec   LSA group pacing timer 240 secs   Interface flood pacing timer 33 msec   Retransmission pacing timer 66 msec   Number of external LSA 0. Checksum Sum 0x0   Number of opaque AS LSA 0. Checksum Sum 0x0   Number of DCbitless external and opaque AS LSA 0   Number of DoNotAge external and opaque AS LSA 0   Number of areas in this router is 1. 1 normal 0 stub   0 nssa   External flood list length 0     Area 24       Number of interfaces in this area is 2       Area has no authentication       SPF algorithm last executed 04:28:18.396 ago       SPF algorithm executed 8 times       Area ranges are         Number of LSA 4. Checksum Sum 0x23EB9       Number of opaque link LSA 0. Checksum Sum 0x0       Number of DCbitless LSA 0       Number of indication LSA 0       Number of DoNotAge LSA 0       Flood list length 0 </pre> | <p>(Optional) Displays information about OSPF.</p> <ul style="list-style-type: none"> <li>The output lines shown in bold in the example indicate the LSA throttling values.</li> </ul>                                                                                                                                                                                    |

# Configuration Examples for OSPF LSA Throttling

This section contains an example of customizing OSPF LSA throttling:

- [OSPF LSA Throttling: Example, page 709](#)

## OSPF LSA Throttling: Example

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

## Additional References

The following sections provide references related to OSPF LSA Throttling.

## Related Documents

| Related Topic            | Document Title                                                                                         |
|--------------------------|--------------------------------------------------------------------------------------------------------|
| OSPF commands            | “OSPF Commands” chapter in the <i>Network Protocols Command Reference, Part 1</i> , Release 12.0       |
| OSPF configuration tasks | “Configuring OSPF ” chapter in the <i>Network Protocols Configuration Guide, Part 1</i> , Release 12.0 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new and modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

### New Commands

- **debug ip ospf database-timer rate-limit**
- **show ip ospf timers rate-limit**
- **timers lsa arrival**
- **timers throttle lsa all**

### Modified Command

- **show ip ospf**



# OSPF Support for Unlimited Software VRFs per Provider Edge Router

In a Multiprotocol Label Switching—Virtual Private Network (MPLS-VPN) deployment, each VPN routing and forwarding instance (VRF) needs a separate Open Shortest Path First (OSPF) process when configured to run OSPF. The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature addresses the scalability issue for OSPF VPNs by eliminating the OSPF VPN limit of 32 processes.

## Feature History for OSPF Support for Unlimited Software VRFs per Provider Edge Router

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.3(4)T    | This feature was introduced.                                    |
| 12.0(27)S   | This feature was integrated into Cisco IOS Release 12.0(27)S.   |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Support for Unlimited Software VRFs per Provider Edge Router, page 712](#)
- [Restrictions for OSPF Support for Unlimited Software VRFs per Provider Edge Router, page 712](#)
- [Information About OSPF Support for Unlimited Software VRFs per Provider Edge Router, page 712](#)
- [How to Configure the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature, page 713](#)

- [Configuration Examples for the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature, page 714](#)
- [Additional References, page 715](#)
- [Command Reference, page 716](#)
- [Glossary, page 717](#)

## Prerequisites for OSPF Support for Unlimited Software VRFs per Provider Edge Router

You must have OSPF configured in your network.

## Restrictions for OSPF Support for Unlimited Software VRFs per Provider Edge Router

Only 32 processes per VRF can be supported. For different VRF processes, there is no limit.

## Information About OSPF Support for Unlimited Software VRFs per Provider Edge Router

Before you configure the OSPF Support for Unlimited Software VRFs per Provider Edge Router feature, you should understand the following concept:

- [Benefits of Having Unlimited Software VRFs per PE Router, page 712](#)

## Benefits of Having Unlimited Software VRFs per PE Router

Before Cisco IOS Releases 12.3(4)T and 12.0(27)S, a separate OSPF process was necessary for each VRF that receives VPN routes via OSPF. When VPNs are deployed, an MPLS Provider Edge (PE) router will be running both multiprotocol Border Gateway Protocol (BGP) for VPN distribution, and Interior Gateway Protocol (IGP) for PE-P connectivity. It is a common scenario when OSPF is used as the IGP between a customer edge (CE) router and a PE router. OSPF was not scalable in VPN deployment because of the limit of 32 processes. By default one process is used for connected routes and another process is used for static routes, therefore only 28 processes can be created for VRFs.

The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature allows for an approximate range of 300 to 10,000 VRFs, depending on the particular platform and on the applications, processes, and protocols that are currently running on the platform.

# How to Configure the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature

This section contains the following procedure:

- [Configuring and Verifying Unlimited Software VRFs per Provider Edge Router, page 713](#) (optional)

## Configuring and Verifying Unlimited Software VRFs per Provider Edge Router

This task describes how to configure and verify unlimited software VRFs for OSPF routing.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **exit**
5. **show ip ospf** [*process-id*]

### DETAILED STEPS

|        | Command or Action                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                      |
| Step 3 | <b>router ospf</b> <i>process-id</i> [ <b>vrf</b> <i>vpn-name</i> ]<br><br><b>Example:</b><br>Router(config)# router ospf 1 vrf crf-1 | Enables OSPF routing.<br><ul style="list-style-type: none"><li>• The <i>process-id</i> argument identifies the OSPF process.</li><li>• Use the <b>vrf</b> keyword and <i>vpn-name</i> argument to identify a VPN.</li></ul><br><b>Note</b> You now can configure as many OSPF VRF processes as needed. |

|        | Command or Action                                                                  | Purpose                                                    |
|--------|------------------------------------------------------------------------------------|------------------------------------------------------------|
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# end                          | Returns to privileged EXEC mode.                           |
| Step 5 | <b>show ip ospf</b> [process-id]<br><br><b>Example:</b><br>Router# show ip ospf 10 | Displays general information about OSPF routing processes. |

## Configuration Examples for the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature

This section contains the following configuration examples:

- [Configuring the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature: Example, page 714](#)
- [Verifying the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature: Example, page 714](#)

### Configuring the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature: Example

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```

### Verifying the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature: Example

This example illustrates the output display from the **show ip ospf** command to verify that the OSPF VRF process 12 has been created for the VRF named first. The output that relates to the VRF first appears in bold.

```
Router# show ip ospf 12

main ID type 0x0005, value 0.0.0.100
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Connected to MPLS VPN Superbackbone, VRF first
It is an area border router
```



```

Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 sec
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 sec
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    Area has no authentication
    SPF algorithm last executed 00:00:15.204 ago
    SPF algorithm executed 2 times
    Area ranges are
    Number of LSA 1. Checksum Sum 0xD9F3
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

## Additional References

The following sections provide references related to the OSPF Support for Unlimited Software VRFs per Provider Edge Router feature.

## Related Documents

| Related Topic    | Document Title                                                                                                                                                                             |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring OSPF | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Routing Configuration Guide</a></li> <li><a href="#">Cisco IOS IP Routing Command Reference, Release 12.3 T</a></li> </ul> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

This feature uses no new or modified commands. To see the command pages for the commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

# Glossary

**multiprotocol BGP**—Border Gateway Protocol (BGP) can be used as an interdomain routing protocol in networks that use Connectionless Network Service (CLNS) as the network-layer protocol.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---





## OSPF Area Transit Capability

The OSPF Area Transit Capability feature provides an OSPF Area Border Router (ABR) the ability to discover shorter paths through the transit area for forwarding traffic that would normally need to travel through the virtual-link path. This functionality allows Cisco IOS software to be compliant with RFC 2328.

### Feature History for OSPF Area Transit Capability

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(27)S | This feature was introduced.                                  |
| 12.3(7)T  | This feature was integrated into Cisco IOS Release 12.3(7)T.  |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S. |



#### Note

Software images for Cisco 12000 series Internet routers have been deferred to Cisco IOS Release 12.0(27)S1.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About OSPF Area Transit Capability, page 720](#)
- [How to Disable OSPF Area Transit Capability, page 720](#)
- [Additional References, page 721](#)
- [Command Reference, page 722](#)

# Information About OSPF Area Transit Capability

To use the OSPF Area Transit Capability feature, you should understand the concept in the following section:

- [How the OSPF Area Transit Capability Feature Works, page 720](#)

## How the OSPF Area Transit Capability Feature Works

The OSPF Area Transit Capability feature is enabled by default. RFC 2328 defines OSPF area transit capability as the ability of the area to carry data traffic that neither originates nor terminates in the area itself. This capability enables the OSPF ABR to discover shorter paths through the transit area and forward traffic along those paths rather than using the virtual link or path, which are not as optimal.

For a detailed description of OSPF area transit capability, refer to RFC 2328, *OSPF Version 2* at the following URL:

<http://www.faqs.org/rfcs/rfc2328.html>

## How to Disable OSPF Area Transit Capability

This section contains the following procedure:

- [Disabling OSPF Area Transit Capability on an Area Border Router, page 720](#) (required)

## Disabling OSPF Area Transit Capability on an Area Border Router

This task describes how to disable the OSPF Area Transit Capability feature on an OSPF ABR.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** [*process-id*]
4. **no capability transit**

## DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                                                                        |
| Step 3 | <b>router ospf</b> [ <i>process-id</i> ]<br><br><b>Example:</b><br>Router(config)# router ospf 100  | Enables OSPF routing and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>process-id</i> argument identifies the OSPF process.</li> </ul> |
| Step 4 | <b>no capability transit</b><br><br><b>Example:</b><br>Router(config-router)# no capability transit | Disables OSPF area capability transit on all areas for a router process.                                                                                                 |

## Additional References

The following sections provide references related to the OSPF Area Transit Capability feature.

## Related Documents

| Related Topic    | Document Title                                                                                                                                                                                           |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring OSPF | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Routing Configuration Guide</a>, Release 12.3</li> <li><a href="#">Cisco IOS IP Routing Command Reference</a>, Release 12.0 S</li> </ul> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title                 |
|----------|-----------------------|
| RFC 2328 | <i>OSPF Version 2</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **capability transit**





## OSPF Link-Local Signaling Per-Interface Basis

The OSPF per-Interface Link-Local Signaling feature allows you to selectively enable or disable Link-Local Signaling (LLS) for a specific interface regardless of the global (router level) setting that you previously have configured.

### Feature History for OSPF per-Interface Link-Local Signaling

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(27)S   | This feature was introduced.                                    |
| 12.3(7)T    | This feature was integrated into Cisco IOS Release 12.3(7)T.    |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About OSPF per-Interface Link-Local Signaling, page 724](#)
- [How to Configure the OSPF per-Interface Link-Local Signaling Feature, page 724](#)
- [Configuration Examples for the OSPF per-Interface Link-Local Signaling Feature, page 726](#)
- [Additional References, page 727](#)
- [Command Reference, page 728](#)

# Information About OSPF per-Interface Link-Local Signaling

Before configuring the feature, you should understand the concept in the following section:

- [Benefits of the OSPF Per-Interface Link-Local Signaling Feature, page 724](#)

## Benefits of the OSPF Per-Interface Link-Local Signaling Feature

When LLS is enabled at the router level, it is automatically enabled for all interfaces. The OSPF per-Interface Link-Local Signaling feature allows you to selectively enable or disable the LLS feature for a specific interface. Disabling LLS on an interface that is connected to a non-Cisco device that may be noncompliant with RFC 2328 can prevent problems with the forming of Open Shortest Path First (OSPF) neighbors in the network.

## How to Configure the OSPF per-Interface Link-Local Signaling Feature

This section contains the following procedure:

- [Turning Off LLS on a per-Interface Basis, page 724](#) (optional)

### Turning Off LLS on a per-Interface Basis

This task disables LLS on a specific interface.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **ip address** *ip-address mask* [**secondary**]
5. **no ip directed-broadcast** [*access-list-number* | *extended access-list-number*]
6. **ip ospf message-digest-key** *key-id md5 encryption-type key*
7. **{no | default} ip ospf lls [disable]**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 1/0                                                                  | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                   |
| Step 4 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.2.145.20 255.255.255.0                          | Sets a primary or secondary IP address for an interface.                                                                                                                                                                                                |
| Step 5 | <b>no ip directed-broadcast</b> [ <i>access-list-number</i>   <i>extended access-list-number</i> ]<br><br><b>Example:</b><br>Router(config-if)# no ip directed broadcast | Drops directed broadcasts destined for the subnet to which that interface is attached, rather than broadcasting them. <ul style="list-style-type: none"> <li>The forwarding of IP directed broadcasts on Ethernet interface 1/0 is disabled.</li> </ul> |
| Step 6 | <b>ip ospf message-digest-key</b> <i>key-id md5 encryption-type key</i><br><br><b>Example:</b><br>Router(config-if)# ip ospf message-digest-key 1 md5 testing            | Enables OSPF Message Digest 5 (MD5) algorithm authentication.                                                                                                                                                                                           |
| Step 7 | <b>{no   default} ip ospf llsl</b> [ <b>disable</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip ospf llsl disable                                                  | Disables LLS on an interface, regardless of the global (router level) setting.                                                                                                                                                                          |

## What to Do Next

To verify that LLS has been enabled or disabled for a specific interface, use the **show ip ospf interface** command. See the [“Configuring and Verifying the OSPF per-Interface Link-Local Signaling Feature: Example”](#) section on page 726 for an example of the information displayed.

# Configuration Examples for the OSPF per-Interface Link-Local Signaling Feature

This section contains the following configuration example:

- [Configuring and Verifying the OSPF per-Interface Link-Local Signaling Feature: Example, page 726](#)

## Configuring and Verifying the OSPF per-Interface Link-Local Signaling Feature: Example

In the following example, LLS has been enabled on Ethernet interface 1/0 and disabled on Ethernet interface 2/0:

```
interface Ethernet1/0
ip address 10.2.145.2 255.255.255.0
no ip directed-broadcast
ip ospf message-digest-key 1 md5 testing
ip ospf lls
!
interface Ethernet2/0
ip address 10.1.145.2 255.255.0.0
no ip directed-broadcast
ip ospf message-digest-key 1 md5 testing
!
ip ospf lls disable
interface Ethernet3/0
ip address 10.3.145.2 255.255.255.0
no ip directed-broadcast
!
router ospf 1
log-adjacency-changes detail
area 0 authentication message-digest
redistribute connected subnets
network 10.0.0.0 0.255.255.255 area 1
network 10.2.3.0 0.0.0.255 area 1
```

In the following example, the **show ip ospf interface** command has been entered to verify that LLS has been enabled for Ethernet interface 1/0 and disabled for interface Ethernet 2/0:

Router# **show ip ospf interface**

```
Ethernet1/0 is up, line protocol is up
Internet Address 10.2.145.2/24, Area 1
Process ID 1, Router ID 2.22.222.2, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 10.2.2.3, Interface address 10.2.145.1
Backup Designated router (ID) 10.22.222.2, Interface address 10.2.145.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:00
! Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 2, maximum is 8
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.2.2.3 (Designated Router)
```

```

Suppress hello for 0 neighbor(s)
Ethernet2/0 is up, line protocol is up
  Internet Address 10.1.145.2/16, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.1.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.1.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
! Does not support Link-local Signaling (LLS)
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 45.2.2.3 (Designated Router)
    Suppress hello for 0 neighbor(s)
Ethernet3/0 is up, line protocol is up
  Internet Address 10.3.145.2/24, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.3.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.3.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
! Supports Link-local Signaling (LLS)
Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.3 (Designated Router)
    Suppress hello for 0 neighbor(s)

```

## Additional References

The following sections provide references related to the OSPF per-Interface Link-Local Signaling feature.

## Related Documents

| Related Topic    | Document Title                                                                           |
|------------------|------------------------------------------------------------------------------------------|
| Configuring OSPF | <a href="#">Cisco IOS IP Configuration Guide</a> , Release 12.3                          |
| OSPF commands    | <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> , Release 12.3 T |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs     | Title          |
|----------|----------------|
| RFC 2328 | OSPF Version 2 |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **ip ospf lls**



# OSPF Link-State Database Overload Protection

The OSPF Link-State Database Overload Protection feature allows you to limit the number of nonself-generated link-state advertisements (LSAs) for a given Open Shortest Path First (OSPF) process. Excessive LSAs generated by other routers in the OSPF domain can substantially drain the CPU and memory resources of the router.

## Feature History for OSPF Link-State Database Overload Protection

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(27)S   | This feature was introduced.                                    |
| 12.3(7)T    | This feature was integrated into Cisco IOS Release 12.3(7)T.    |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S.   |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for OSPF Link-State Database Overload Protection, page 730](#)
- [Information About OSPF Link-State Database Overload Protection, page 730](#)
- [How to Configure the OSPF Link-State Database Overload Protection Feature, page 730](#)
- [Configuration Examples for the OSPF Link-State Database Overload Protection Feature, page 733](#)
- [Additional References, page 734](#)
- [Command Reference, page 735](#)
- [Glossary, page 736](#)

# Prerequisites for OSPF Link-State Database Overload Protection

It is presumed you have OSPF running on your network.

## Information About OSPF Link-State Database Overload Protection

Before you configure the OSPF Link-State Database Overload Protection feature, you should understand the concepts described in the following sections:

- [Benefits of Using OSPF Link-State Database Overload Protection, page 730](#)
- [How OSPF Link-State Database Overload Protection Works, page 730](#)

## Benefits of Using OSPF Link-State Database Overload Protection

The OSPF Link-State Database Overload Protection feature provides a mechanism at the OSPF level to limit the number of nonself-generated LSAs for a given OSPF process. When other routers in the network have been misconfigured, they may generate a high volume of LSAs, for instance, to redistribute large numbers of prefixes. This protection mechanism prevents routers from receiving a large number of LSAs and therefore experiencing CPU and memory shortages.

## How OSPF Link-State Database Overload Protection Works

When the OSPF Link-State Database Overload Protection feature is enabled, the router keeps a count of the number of received (nonself-generated) LSAs it has received. When the configured threshold number of LSAs is reached, an error message is logged. When the configured maximum number of LSAs is exceeded, the router will send a notification. If the count of received LSAs is still higher than the configured maximum after one minute, the OSPF process takes down all adjacencies and clears the OSPF database. In this ignore state, all OSPF packets received on any interface that belongs to this OSPF process are ignored and no OSPF packets are generated on any of these interfaces. The OSPF process remains in the ignore state for the time configured by the **ignore-time** keyword of the **max-lsa** command. Each time the OSPF process gets into an ignore state a counter is incremented. If this counter exceeds the number of minutes configured by the **ignore-count** keyword, the OSPF process stays permanently in the same ignore state and manual intervention is required to get the OSPF process out of the ignore state. The ignore state counter is reset to 0 when the OSPF process remains in the normal state of operation for the amount of time that was specified by the **reset-time** keyword.

If the **warning-only** keyword of the **max-lsa** command has been configured, the OSPF process will send only a warning that the LSA maximum has been exceeded.

## How to Configure the OSPF Link-State Database Overload Protection Feature

This section contains the following procedure:

- [Limiting the Number of Self-Generating LSAs for an OSPF Process, page 731](#) (required)



# Limiting the Number of Self-Generating LSAs for an OSPF Process

This task describes how to configure and verify a limit on the number of nonself-generating LSAs for an OSPF process.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **router-id** *ip-address*
5. **log-adjacency-changes** [**detail**]
6. **max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*]
7. **network** *ip-address wildcard-mask area* *area-id*

## DETAILED STEPS

|        | Command or Action                                                                                                     | Purpose                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                        | Enters global configuration mode.                                                                                                     |
| Step 3 | <b>router ospf</b> <i>process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 1                          | Enables OSPF routing.<br><ul style="list-style-type: none"><li>The <i>process-id</i> argument identifies the OSPF process.</li></ul>  |
| Step 4 | <b>router-id</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config)# router-id 10.0.0.1                       | Specifies a fixed router ID for an OSPF process.<br><ul style="list-style-type: none"><li>Enters router configuration mode.</li></ul> |
| Step 5 | <b>log-adjacency-changes</b> [ <b>detail</b> ]<br><br><b>Example:</b><br>Router(config-router)# log-adjacency-changes | Configures the router to send a syslog message when an OSPF neighbor goes up or down.                                                 |

|        | Command or Action                                                                                                                                                                                                                                                                        | Purpose                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>max-lsa</b> <i>maximum-number</i> [ <i>threshold-percentage</i> ]<br>[ <b>warning-only</b> ] [ <b>ignore-time</b> <i>minutes</i> ] [ <b>ignore-count</b><br><i>count-number</i> ] [ <b>reset-time</b> <i>minutes</i> ]<br><br><b>Example:</b><br>Router(config-router)# max-lsa 12000 | Limits the number of nonself-generated LSAs an OSPF routing process can keep in the OSPF link-state database (LSDB). |
| Step 7 | <b>network</b> <i>ip-address wildcard-mask area</i> <i>area-id</i><br><br><b>Example:</b><br>Router(config-router)# network 209.165.201.1<br>255.255.255.255 area 0                                                                                                                      | Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.                              |

## Verifying the Number of Nonself-Generated LSAs on a Router

The **show ip ospf** command is entered with the **database-summary** keyword to verify the actual number of nonself-generated LSAs on a router. This command can be used at any given point in time to display lists of information related to the OSPF database for a specific router.

```
Router# show ip ospf 2000 database database-summary
```

```
OSPF Router with ID (192.168.1.3) (Process ID 2000)
```

```
Area 0 database summary
```

| LSA Type                         | Count | Delete | Maxage |
|----------------------------------|-------|--------|--------|
| Router                           | 5     | 0      | 0      |
| Network                          | 2     | 0      | 0      |
| Summary Net                      | 8     | 2      | 2      |
| Summary ASBR                     | 0     | 0      | 0      |
| Type-7 Ext                       | 0     | 0      | 0      |
| Prefixes redistributed in Type-7 | 0     |        |        |
| Opaque Link                      | 0     | 0      | 0      |
| Opaque Area                      | 0     | 0      | 0      |
| Subtotal                         | 15    | 2      | 2      |

```
Process 2000 database summary
```

| LSA Type                         | Count | Delete | Maxage |
|----------------------------------|-------|--------|--------|
| Router                           | 5     | 0      | 0      |
| Network                          | 2     | 0      | 0      |
| Summary Net                      | 8     | 2      | 2      |
| Summary ASBR                     | 0     | 0      | 0      |
| Type-7 Ext                       | 0     | 0      | 0      |
| Opaque Link                      | 0     | 0      | 0      |
| Opaque Area                      | 0     | 0      | 0      |
| Type-5 Ext                       | 4     | 0      | 0      |
| Prefixes redistributed in Type-5 | 0     |        |        |
| Opaque AS                        | 0     | 0      | 0      |
| Non-self                         | 16    |        |        |
| Total                            | 19    | 2      | 2      |

# Configuration Examples for the OSPF Link-State Database Overload Protection Feature

This section contains the following example:

- [Setting a Limit for LSA Generation: Example, page 733](#)

## Setting a Limit for LSA Generation: Example

In the following example, the router is configured to not accept any more nonself-generated LSAs once a maximum of 14,000 has been exceeded:

```
Router(config)# router ospf 1
Router(config-router)# router-id 192.68.0.1
Router(config-router)# log-adjacency-changes
Router(config-router)# max-lsa 14000
Router(config-router)# area 33 nssa
Router(config-router)# network 192.68.0.1 0.0.0.0 area 1
Router(config-router)# network 192.68.5.1 0.0.0.0 area 1
Router(config-router)# network 192.68.2.1 0.0.0.0 area 0
```

In the following example, the **show ip ospf** command has been entered to confirm the configuration:

```
Router# show ip ospf 1

Routing Process "ospf 1" with ID 192.68.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
  Threshold for warning message 75%
  Ignore-time 5 minutes, reset-time 10 minutes
  Ignore-count allowed 5, current ignore-count 0
It is an area border and autonomous system boundary router
```

In the following example, the following output appears when the **show ip ospf** command has been entered during the time when the router is in the ignore state:

```
Router# show ip ospf 1

Routing Process "ospf 1" with ID 192.68.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
  Threshold for warning message 75%
  Ignore-time 5 minutes, reset-time 10 minutes
  Ignore-count allowed 5, current ignore-count 1
  Ignoring all neighbors due to max-lsa limit, time remaining: 00:04:52
It is an area border and autonomous system boundary router
```

The following output appears when the **show ip ospf** command has been entered after the router left the ignore state:

```
Router# show ip ospf 1

Routing Process "ospf 1" with ID 192.68.0.1
Supports only single TOS(TOS0) routes
```

```

Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
  Threshold for warning message 75%
  Ignore-time 5 minutes, reset-time 10 minutes
  Ignore-count allowed 5, current ignore-count 1 - time remaining: 00:09:51
It is an area border and autonomous system boundary router

```

The following output appears when the **show ip ospf** command has been entered for a router that is permanently in the ignore state:

```

Router# show ip ospf 1

Routing Process "ospf 1" with ID 192.68.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
  Threshold for warning message 75%
  Ignore-time 5 minutes, reset-time 10 minutes
  Ignore-count allowed 5, current ignore-count 6
  Permanently ignoring all neighbors due to max-lsa limit
It is an area border and autonomous system boundary router

```

## Additional References

The following sections provide references related to OSPF Link-State Database Overload Protection.

## Related Documents

| Related Topic    | Document Title                                                                                                                                                                                                       |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring OSPF | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Routing Configuration Guide</a></li> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</a>, Release 12.3 T</li> </ul> |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **max-lsa**

# Glossary

**LSDB**—link-state database.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---



## **Part 6: Protocol-Independent Routing**









# Configuring IP Routing Protocol-Independent Features

---

This chapter describes how to configure IP routing protocol-independent features. For a complete description of the IP routing protocol-independent commands in this chapter, refer to the “IP Routing Protocol-Independent Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication. To locate documentation of other commands in this chapter, use the command reference master index, or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

## Protocol-Independent Feature Task List

Previous chapters addressed configurations of specific routing protocols. To configure optional protocol-independent features, perform any of the tasks described in the following sections:

- [Using Variable-Length Subnet Masks](#) (Optional)
- [Configuring Static Routes](#) (Optional)
- [Specifying Default Routes](#) (Optional)
- [Changing the Maximum Number of Paths](#) (Optional)
- [Configuring Multi-Interface Load Splitting](#) (Optional)
- [Redistributing Routing Information](#) (Optional)
- [Filtering Routing Information](#) (Optional)
- [Enabling Policy Routing](#) (Optional)
- [Managing Authentication Keys](#) (Optional)
- [Monitoring and Maintaining the IP Network](#) (Optional)

See the section “[IP Routing Protocol-Independent Configuration Examples](#)” at the end of this chapter for configuration examples.

# Using Variable-Length Subnet Masks

Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF), Routing Information Protocol (RIP) Version 2, and static routes support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space. However, using VLSMs also presents address assignment challenges for the network administrator and ongoing administrative challenges.

Refer to [RFC 1219](#) for detailed information about VLSMs and how to correctly assign addresses.



**Note**

Consider your decision to use VLSMs carefully. You can easily make mistakes in address assignments and you will generally find it more difficult to monitor your network using VLSMs.



**Note**

The best way to implement VLSMs is to keep your existing addressing plan in place and gradually migrate some networks to VLSMs to recover address space. See the “[Variable-Length Subnet Mask Example](#)” section at the end of this chapter for an example of using VLSMs.

# Configuring Static Routes

Static routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination. They are also useful for specifying a gateway of last resort to which all unroutable packets will be sent.

To configure a static route, use the following command in global configuration mode:

| Command                                                                                                                                                               | Purpose                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Router(config)# <b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent   track number] [tag tag]</i> | Establishes a static route. |

See the “[Overriding Static Routes with Dynamic Protocols Example](#)” section at the end of this chapter for an example of configuring static routes.

Static routes remains in the router configuration until you remove them (using the **no** form of the **ip route** global configuration command). However, you can override static routes with dynamic routing information through prudent assignment of administrative distance values. Each dynamic routing protocol has a default administrative distance, as listed in [Table 21](#). If you would like a static route to be overridden by information from a dynamic routing protocol, simply ensure that the administrative distance of the static route is higher than that of the dynamic protocol.

**Table 21**      *Dynamic Routing Protocol Default Administrative Distances*

| Route Source        | Default Distance |
|---------------------|------------------|
| Connected interface | 0                |
| Static route        | 1                |

**Table 21**      *Dynamic Routing Protocol Default Administrative Distances (continued)*

| Route Source        | Default Distance |
|---------------------|------------------|
| EIGRP summary route | 5                |
| External BGP        | 20               |
| Internal EIGRP      | 90               |
| IGRP                | 100              |
| OSPF                | 110              |
| IS-IS               | 115              |
| RIP                 | 120              |
| EGP                 | 140              |
| ODR                 | 160              |
| External EIGRP      | 170              |
| Internal BGP        | 200              |
| Unknown             | 255              |

Static routes that point to an interface will be advertised via RIP, EIGRP, and other dynamic routing protocols, regardless of whether **redistribute static** router configuration commands were specified for those routing protocols. These static routes are advertised because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. However, if you define a static route to an interface that is not one of the networks defined in a **network** command, no dynamic routing protocols will advertise the route unless a **redistribute static** command is specified for these protocols.

When an interface goes down, all static routes through that interface are removed from the IP routing table. Also, when the software can no longer find a valid next hop for the address specified as the address of the forwarding router in a static route, the static route is removed from the IP routing table.

## Specifying Default Routes

A router might not be able to determine the routes to all other networks. To provide complete routing capability, the common practice is to use some routers as *smart routers* and give the remaining routers default routes to the smart router. (Smart routers have routing table information for the entire internetwork.) These default routes can be passed along dynamically, or can be configured into the individual routers.

Most dynamic interior routing protocols include a mechanism for causing a smart router to generate dynamic default information that is then passed along to other routers.

## Specifying a Default Network

If a router has a directly connected interface onto the specified default network, the dynamic routing protocols running on that device will generate or source a default route. In the case of RIP, the router will advertise the pseudonetwork 0.0.0.0. In the case of EIGRP, the network itself is advertised and flagged as an external route.

A router that is generating the default for a network also may need a default of its own. One way a router can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.

To define a static route to a network as the static default route, use the following command in global configuration mode:

| Command                                                         | Purpose                      |
|-----------------------------------------------------------------|------------------------------|
| Router(config)# <b>ip default-network</b> <i>network-number</i> | Specifies a default network. |

## Understanding Gateway of Last Resort

When default information is being passed along through a dynamic routing protocol, no further configuration is required. The system periodically scans its routing table to choose the optimal default network as its default route. In the case of RIP, there is only one choice, network 0.0.0.0. In the case of EIGRP, there might be several networks that can be candidates for the system default. Cisco IOS software uses both administrative distance and metric information to determine the default route (gateway of last resort). The selected default route appears in the gateway of last resort display of the **show ip route EXEC** command.

If dynamic default information is not being passed to the software, candidates for the default route are specified with the **ip default-network** global configuration command. In this usage, the **ip default-network** command takes an unconnected network as an argument. If this network appears in the routing table from any source (dynamic or static), it is flagged as a candidate default route and is a possible choice as the default route.

If the router has no interface on the default network, but does have a route to it, it considers this network as a candidate default path. The route candidates are examined and the best one is chosen, based on administrative distance and metric. The gateway to the best default path becomes the gateway of last resort.

## Changing the Maximum Number of Paths

By default, most IP routing protocols install a maximum of four parallel routes in a routing table. Static routes always install six routes. The exception is BGP, which by default allows only one path (best path) to a destination. However, BGP can be configured to use equal and unequal cost multipath load sharing. See the [BGP configuration guide](#) for more information.

The number of parallel routes that you can configured to be installed in the routing table is dependent on the installed version of Cisco IOS software. To change the maximum number of parallel paths allowed, use one of the following command in router configuration mode:

| Command                                                                                                                  | Purpose                                                                     |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Router(config-router)# <b>maximum-paths</b> <i>number</i> [ <b>import</b> <i>number</i> ]<br><b>import</b> <i>number</i> | Configures the maximum number of parallel paths allowed in a routing table. |

## Configuring Multi-Interface Load Splitting

Multi-interface load splitting allows you to efficiently control traffic that travels across multiple interfaces to the same destination. The **traffic-share min** router configuration command specifies that if multiple paths are available to the same destination, only paths with the minimum metric will be installed in the routing table. The number of paths allowed is never more than six. For dynamic routing protocols, the number of paths is controlled by the **maximum-paths** router configuration command. The static route source can always install six paths. If more paths are available, the extra paths are discarded. If some installed paths are removed from the routing table, pending routes are added automatically.

When the **traffic-share min** command is used with the **across-interfaces** keyword, an attempt is made to use as many different interfaces as possible to forward traffic to the same destination. When the maximum path limit has been reached and a new path is installed, the router compares the installed paths. For example, if path X references the same interface as path Y and the new path uses a different interface, path X is removed and the new path is installed.

To configure traffic that is distributed among multiple routes of unequal cost for equal cost paths across multiple interfaces, use the following command in router configuration mode:

| Command                                                                          | Purpose                                                                                      |
|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Router(config-router) # <b>traffic-share min</b><br>{ <b>across-interfaces</b> } | Configures multi-interface load splitting across different interfaces with equal cost paths. |

## Redistributing Routing Information

In addition to running multiple routing protocols simultaneously, Cisco IOS software can be configured to redistribute information from one routing protocol to another. For example, you can configure a router to readvertise EIGRP-derived routes using RIP, or to readvertise static routes using the EIGRP protocol. Redistribution from one routing protocol to another can be configured in all of the IP-based routing protocols.

You also can conditionally control the redistribution of routes between routing domains by configuring *route maps* between the two domains. A route map is a route/ packet filter that is configured with permit and deny statements, match and set clauses, and sequence numbers.

The following four tables list tasks associated with route redistribution. Although redistribution is a protocol-independent feature, some of the **match** and **set** commands are specific to a particular protocol.

To define a route map for redistribution, use the following command in global configuration mode:

| Command                                                                                        | Purpose                                                                  |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Router(config) # <b>route-map</b> map-tag [ <b>permit</b>   <b>deny</b> ]<br>[sequence-number] | Defines conditions for redistributing one routing protocol into another. |

One or more **match** commands and one or more **set** commands are configured in route-map configuration mode. If there are no **match** commands, then everything matches. If there are no **set** commands, then no set action is performed.

## ■ Redistributing Routing Information

To define conditions for redistributing routes from one routing protocol into another, use at least one of the following commands in route-map configuration mode, as needed:

| Command                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-route-map)# <b>match as-path</b> <i>path-list-number</i>                                                                                                                                                                                                                                          | Matches a BGP autonomous system path access list.                                                                                                                                                 |
| Router(config-route-map)# <b>match community</b> { <i>standard-list-number</i>   <i>expanded-list-number</i>   <i>community-list-name</i> [ <b>exact</b> ]}                                                                                                                                                     | Matches a BGP community.                                                                                                                                                                          |
| Router(config-route-map)# <b>match ip address</b> { <i>access-list-number</i> [ <i>access-list-number</i> ...   <i>access-list-name</i> ...]   <i>access-list-name</i> [ <i>access-list-number</i> ...   <i>access-list-name</i> ]   <b>prefix-list</b> <i>prefix-list-name</i> [ <i>prefix-list-name</i> ...]} | Matches any routes that have a destination network number address that is permitted by a standard access list, an extended access list, or a prefix list, or to perform policy routing on packets |
| Router(config-route-map)# <b>match metric</b> <i>metric-value</i>                                                                                                                                                                                                                                               | Matches routes with the specified metric.                                                                                                                                                         |
| Router(config-route-map)# <b>match ip next-hop</b> { <i>access-list-number</i>   <i>access-list-name</i> } [ <i>access-list-number</i>   <i>access-list-name</i> ]                                                                                                                                              | Matches a next-hop router address passed by one of the access lists specified.                                                                                                                    |
| Router(config-route-map)# <b>match tag</b> <i>tag-value</i> [ <i>tag-value</i> ]                                                                                                                                                                                                                                | Matches the specified tag value.                                                                                                                                                                  |
| Router(config-route-map)# <b>match interface</b> <i>interface-type</i> <i>interface-number</i> [ <i>interface-type</i> <i>interface-number</i> ]                                                                                                                                                                | Matches the specified next hop route out one of the interfaces specified.                                                                                                                         |
| Router(config-route-map)# <b>match ip route-source</b> { <i>access-list-number</i>   <i>access-list-name</i> } [ <i>access-list-number</i>   <i>access-list-name</i> ]                                                                                                                                          | Matches the address specified by the specified advertised access lists.                                                                                                                           |
| Router(config-route-map)# <b>match route-type</b> { <b>local</b>   <b>internal</b>   <b>external</b> [ <b>type-1</b>   <b>type-2</b> ]   <b>level-1</b>   <b>level-2</b> }                                                                                                                                      | Matches the specified route type.                                                                                                                                                                 |

To define conditions for redistributing routes from one routing protocol into another, use at least one of the following **set** commands in route-map configuration mode as needed:

| Command                                                                                                                                | Purpose                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Router(config-route-map)# <b>set community</b> { <i>community-number</i> [ <b>additive</b> ]}   <b>none</b>                            | Sets the BGP communities attribute.                                             |
| Router(config-route-map)# <b>set dampening</b> <i>halflife</i> <i>reuse</i> <i>suppress</i> <i>max-suppress-time</i>                   | Sets BGP route dampening parameters.                                            |
| Router(config-route-map)# <b>set local-preference</b> <i>number-value</i>                                                              | Assigns a BGP local-preference value to a path.                                 |
| Router(config-route-map)# <b>set weight</b> <i>weight</i>                                                                              | Specifies the BGP weight for the routing table.                                 |
| Router(config-route-map)# <b>set origin</b> { <b>igp</b>   <b>egp</b> <i>as-number</i>   <b>incomplete</b> }                           | Sets the route origin code.                                                     |
| Router(config-route-map)# <b>set as-path</b> { <b>tag</b>   <b>prepend</b> <i>as-path-string</i> }                                     | Modifies the BGP autonomous system path.                                        |
| Router(config-route-map)# <b>set next-hop</b> <i>next-hop</i>                                                                          | Specifies the address of the next hop.                                          |
| Router(config-route-map)# <b>set automatic-tag</b>                                                                                     | Enables automatic computation of the tag table.                                 |
| Router(config-route-map)# <b>set level</b> { <b>level-1</b>   <b>level-2</b>   <b>level-1-2</b>   <b>stub-area</b>   <b>backbone</b> } | Specifies the areas in which to import routes.                                  |
| Router(config-route-map)# <b>set metric</b> <i>metric-value</i>                                                                        | Sets the metric value for redistributed routes (for any protocol except EIGRP). |

| Command                                                                                                                | Purpose                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-route-map)# <b>set metric</b> <i>bandwidth delay reliability load mtu</i>                                | Sets the metric value to give the redistributed routes (for EIGRP only).                                                                                           |
| Router(config-route-map)# <b>set metric-type</b> { <b>internal</b>   <b>external</b>   <b>type-1</b>   <b>type-2</b> } | Sets the metric type assigned to redistributed routes.                                                                                                             |
| Router(config-route-map)# <b>set metric-type internal</b>                                                              | Sets the Multi Exit Discriminator (MED) value on prefixes advertised to Exterior BGP neighbor to match the Interior Gateway Protocol (IGP) metric of the next hop. |
| Router(config-route-map)# <b>set tag</b> <i>tag-value</i>                                                              | Sets a tag value to apply to redistributed routes.                                                                                                                 |

See the “BGP Route Map Examples” section in the “Configuring BGP” chapter for examples of BGP route maps. See the “BGP Community with Route Maps Examples” section in the “Configuring BGP” chapter for examples of BGP communities and route maps.

To distribute routes from one routing domain into another and to control route redistribution, use the following commands in router configuration mode:

|               | Command                                                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                         |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config-router)# <b>redistribute</b> <i>protocol</i> [ <i>process-id</i> ] { <b>level-1</b>   <b>level-1-2</b>   <b>level-2</b> } [ <b>metric</b> <i>metric-value</i> ] [ <b>metric-type</b> <i>type-value</i> ] [ <b>match</b> <b>internal</b>   <b>external</b> <i>type-value</i> ] [ <b>tag</b> <i>tag-value</i> ] [ <b>route-map</b> <i>map-tag</i> ] [ <b>subnets</b> ] | Redistributes routes from one routing protocol to another routing protocol.                                     |
| <b>Step 2</b> | Router(config-router)# <b>default-metric</b> <i>number</i>                                                                                                                                                                                                                                                                                                                         | Causes the current routing protocol to use the same metric value for all redistributed routes (BGP, OSPF, RIP). |
| <b>Step 3</b> | Router(config-router)# <b>default-metric</b> <i>bandwidth delay reliability loading mtu</i>                                                                                                                                                                                                                                                                                        | Causes the EIGRP routing protocol to use the same metric value for all non-EIGRP redistributed routes.          |
| <b>Step 4</b> | Router(config-router)# <b>no default-information</b> { <b>in</b>   <b>out</b> }                                                                                                                                                                                                                                                                                                    | Disables the redistribution of default information between EIGRP processes, which is enabled by default.        |

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count and the EIGRP metric is a combination of five metric values. In such situations, a dynamic metric is assigned to the redistributed route. Redistribution in these cases should be applied consistently and carefully in conjunction with inbound filtering to avoid routing loops.

## Understanding Supported Metric Translations

This section describes supported automatic metric translations between the routing protocols. The following descriptions assume that you have not defined a default redistribution metric that replaces metric conversions:

- RIP can automatically redistribute static routes. It assigns static routes a metric of 1 (directly connected).
- BGP does not normally send metrics in its routing updates.

- EIGRP can automatically redistribute static routes from other EIGRP-routed autonomous systems as long as the static route and any associated interfaces are covered by an EIGRP network statement. EIGRP assigns static routes a metric that identifies them as directly connected. EIGRP does not change the metrics of routes derived from EIGRP updates from other autonomous systems.
- Note that any protocol can redistribute routes from other routing protocols as long as a default metric is configured.

# Filtering Routing Information

To filter routing protocol information performing the tasks in the following sections. The tasks in the first section are required; the remaining sections are optional:

- [Preventing Routing Updates Through an Interface](#) (Required)
- [Controlling the Advertising of Routes in Routing Updates](#) (Optional)
- [Controlling the Processing of Routing Updates](#) (Optional)
- [Filtering Sources of Routing Information](#) (Optional)



Note

When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

## Preventing Routing Updates Through an Interface

To prevent other routers on a local network from learning about routes dynamically, you can keep routing update messages from being sent through a router interface. Keeping routing update messages from being sent through a router interface prevents other systems on the interface from learning about routes dynamically. This feature applies to all IP-based routing protocols except BGP.

OSPF and IS-IS behave somewhat differently. In OSPF, the interface address you specify as passive appears as a stub network in the OSPF domain. OSPF routing information is neither sent nor received through the specified router interface. In IS-IS, the specified IP addresses are advertised without actually running IS-IS on those interfaces.

To prevent routing updates through a specified interface, use the following command in router configuration mode:

| Command                                                                                   | Purpose                                                                    |
|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Router(config-router)# <b>passive-interface</b><br><i>interface-type interface-number</i> | Suppresses the sending of routing updates through the specified interface. |

See the “[Passive Interface Examples](#)” section at the end of this chapter for examples of configuring passive interfaces.



## Configuring Default Passive Interfaces

In Internet service provider (ISP) and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the introduction of the Default Passive Interface feature, there were two possibilities for obtaining routing information from these interfaces:

- Configure a routing protocol such as OSPF on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive.

Network operators may not always be able to summarize type 5 link-state advertisements (LSAs) at the router level where redistribution occurs, as in the first possibility. Thus, a large number of type 5 LSAs can be flooded over the domain.

In the second possibility, large type 1 LSAs might be flooded into the area. The Area Border Router (ABR) creates type 3 LSAs, one for each type 1 LSA, and floods them to the backbone. It is possible, however, to have unique summarization at the ABR level, which will inject only one summary route into the backbone, thereby reducing processing overhead.

The prior solution to this problem was to configure the routing protocol on all interfaces and manually set the **passive-interface** router configuration command on the interfaces where adjacency was not desired. But in some networks, this solution meant coding 200 or more passive interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single **passive-interface default** command, then configuring individual interfaces where adjacencies are desired using the **no passive-interface** command.

Thus, the Default Passive Interface feature simplifies the configuration of distribution routers and allows the network manager to obtain routing information from the interfaces in large ISP and enterprise networks.

To set all interfaces as passive by default and then activate only those interfaces that need to have adjacencies set, use the following commands beginning in global configuration mode:

|               | Command                                                                         | Purpose                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router</b> <i>protocol</i>                                   | Configures the routing protocol on the network.                                                                                                                             |
| <b>Step 2</b> | Router(config-router)# <b>passive-interface default</b>                         | Sets all interfaces as passive by default.                                                                                                                                  |
| <b>Step 3</b> | Router(config-router)# <b>no passive-interface</b> <i>interface-type</i>        | Activates only those interfaces that need to have adjacencies set.                                                                                                          |
| <b>Step 4</b> | Router(config-router)# <b>network</b> <i>network-address</i> [ <i>options</i> ] | Specifies the list of networks for the routing process. The <i>network-address</i> argument is an IP address written in dotted decimal notation—172.24.101.14, for example. |

See the section “[Default Passive Interface Example](#)” at the end of this chapter for an example of a default passive interface.

To verify that interfaces on your network have been set to passive, you could enter a network monitoring command such as the **show ip ospf interface** EXEC command, or you could verify the interfaces you enabled as active using a command such as the **show ip interface** EXEC command.

## Controlling the Advertising of Routes in Routing Updates

To prevent other routers from learning one or more routes, you can suppress routes from being advertised in routing updates. Suppressing routes in route updates prevents other routers from learning the interpretation of a particular device of one or more routes. You cannot specify an interface name in OSPF. When used for OSPF, this feature applies only to external routes.

To suppress routes from being advertised in routing updates, use the following command in router configuration mode:

| Command                                                                                                                                                                                | Purpose                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Router(config-router)# <b>distribute-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>out</b> [ <i>interface-name</i>   <i>routing-process</i>   <i>as-number</i> ] | Permits or denies routes from being advertised in routing updates depending upon the action listed in the access list. |

## Controlling the Processing of Routing Updates

You might want to avoid processing certain routes listed in incoming updates. This feature does not apply to OSPF or IS-IS. To suppress routes in incoming updates, use the following command in router configuration mode:

| Command                                                                                                                                                           | Purpose                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Router(config-router)# <b>distribute-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>in</b> [ <i>interface-type</i> <i>interface-number</i> ] | Suppresses routes listed in updates from being processed. |

## Filtering Sources of Routing Information

Filtering sources of routing information prioritizes routing information from different sources because some pieces of routing information may be more accurate than others. An *administrative distance* is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. In a large network, some routing protocols and some routers can be more reliable than others as sources of routing information. Also, when multiple routing processes are running in the same router for IP, it is possible for the same route to be advertised by more than one routing process. By specifying administrative distance values, you enable the router to intelligently discriminate between sources of routing information. The router will always pick the route whose routing protocol has the lowest administrative distance.

To filter sources of routing information, use the following command in router configuration mode:

| Command                                                                                                                                 | Purpose                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| Router(config-router)# <b>distance</b> { <i>ip-address</i> { <i>wildcard-mask</i> }} [ <i>ip-standard-list</i> ] [ <i>ip-extended</i> ] | Filters on routing information sources. |

There are no general guidelines for assigning administrative distances because each network has its own requirements. You must determine a reasonable matrix of administrative distances for the network as a whole. [Table 21](#) shows the default administrative distance for various routing information sources.

For example, consider a router using EIGRP and RIP. Suppose you trust the EIGRP-derived routing information more than the RIP-derived routing information. In this example, because the default EIGRP administrative distance is lower than the default RIP administrative distance, the router uses the EIGRP-derived information and ignores the RIP-derived information. However, if you lose the source of the EIGRP-derived information (because of a power shutdown at the source network, for example), the router uses the RIP-derived information until the EIGRP-derived information reappears. <<>>

For an example of filtering on sources of routing information, see the section “[Administrative Distance Examples](#)” later in this chapter.



**Note**

You also can use administrative distance to rate the routing information from routers running the same routing protocol. This application is generally discouraged if you are unfamiliar with this particular use of administrative distance, because it can result in inconsistent routing information, including forwarding loops.



**Note**

The weight of a route can no longer be set with the **distance** command. To set the weight for a route, use a route-map.

## Enabling Policy Routing

Policy routing is a more flexible mechanism for routing packets than destination routing. It is a process whereby the router puts packets through a route map before routing them. The route map determines which packets are routed to which router next. You might enable policy routing if you want certain packets to be routed some way other than the obvious shortest path. Possible applications for policy routing are to provide equal access, protocol-sensitive routing, source-sensitive routing, routing based on interactive versus batch traffic, and routing based on dedicated links.

To enable policy routing, you must identify which route map to use for policy routing and create the route map. The route map itself specifies the match criteria and the resulting action if all of the match clauses are met. These steps are described in the following task tables.

To enable policy routing on an interface, indicate which route map the router should use by using the following command in interface configuration mode. A packet arriving on the specified interface will be subject to policy routing except when its destination IP address is the same as the IP address of the router’s interface. This command disables fast switching of all packets arriving on this interface.

| Command                                                      | Purpose                                             |
|--------------------------------------------------------------|-----------------------------------------------------|
| Router(config-if)# <b>ip policy route-map</b> <i>map-tag</i> | Identifies the route map to use for policy routing. |

To define the route map to be used for policy routing, use the following command in global configuration mode:

| Command                                                                                                       | Purpose                                                  |
|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Router(config)# <b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ]<br>[ <i>sequence-number</i> ] | Defines a route map to control where packets are output. |

To define the criteria by which packets are examined to learn if they will be policy-routed, use either one or both of the following commands in route-map configuration mode. No match clause in the route map indicates all packets.

| Command                                                                                                                                                              | Purpose                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Router(config-route-map)# <b>match length</b> <i>minimum-length</i> <i>maximum-length</i>                                                                            | Matches the Layer 3 length of the packet.                                                              |
| Router(config-route-map)# <b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i> }<br>[ <i>access-list-number</i>   <i>access-list-name</i> ] | Matches the destination IP address that is permitted by one or more standard or extended access lists. |

To set the precedence and specify where the packets that pass the match criteria are output, use the following commands in route-map configuration mode:

|               | Command                                                                                                                                                   | Purpose                                                                                                                                                                                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config-route-map)# <b>set ip precedence</b> <i>number</i>   <i>name</i>                                                                            | Sets the precedence value in the IP header.                                                                                                                                                                                                      |
| <b>Step 2</b> | Router(config-route-map)# <b>set ip next-hop</b> <i>ip-address</i> [ <i>ip-address</i> ]                                                                  | Specifies the next hop to which to route the packet.<br><b>Note</b> It must be an adjacent router.                                                                                                                                               |
| <b>Step 3</b> | Router(config-route-map)# <b>set interface</b> <i>interface-type</i> <i>interface-number</i> [... <i>interface-type</i> <i>interface-number</i> ]         | Specifies the output interface for the packet.                                                                                                                                                                                                   |
| <b>Step 4</b> | Router(config-route-map)# <b>set ip default next-hop</b> <i>ip-address</i> [ <i>ip-address</i> ]                                                          | Specifies the next hop to which to route the packet, if there is no explicit route for this destination.<br><b>Note</b> Like the <b>set ip next-hop</b> command, the <b>set ip default next-hop</b> command needs to specify an adjacent router. |
| <b>Step 5</b> | Router(config-route-map)# <b>set default interface</b> <i>interface-type</i> <i>interface-number</i> [... <i>interface-type</i> <i>interface-number</i> ] | Specifies the output interface for the packet if there is no explicit route for the destination.                                                                                                                                                 |



**Note**

The **set ip next-hop** and **set ip default next-hop** are similar commands but have a different order of operations. Configuring the **set ip next-hop** command causes the system to use policy routing first and then use the routing table. Configuring the **set ip default next-hop** causes the system to use the routing table first and then policy route the specified next hop.

The precedence setting in the IP header determines whether, during times of high traffic, the packets will be treated with more or less precedence than other packets. By default, the Cisco IOS software leaves this value untouched; the header remains with the precedence value it had.

The precedence bits in the IP header can be set in the router when policy routing is enabled. When the packets containing those headers arrive at another router, the packets are ordered for transmission according to the precedence set, if the queueing feature is enabled. The router does not honor the precedence bits if queueing is not enabled; the packets are sent in FIFO order.

You can change the precedence setting, using either a number or name. The names came from [RFC 791](#), but are evolving. You can enable other features that use the values in the **set ip precedence** route-map configuration command to determine precedence. [Table 22](#) lists the possible numbers and their corresponding name, from least important to most important.

**Table 22** *IP Precedence Values*

| Number | Name           |
|--------|----------------|
| 0      | routine        |
| 1      | priority       |
| 2      | immediate      |
| 3      | flash          |
| 4      | flash-override |
| 5      | critical       |
| 6      | internet       |
| 7      | network        |

The **set** commands can be used with each other. They are evaluated in the order shown in the previous task table. A usable next hop implies an interface. Once the local router finds a next hop and a usable interface, it routes the packet.

To display the cache entries in the policy route cache, use the **show ip cache policy EXEC** command.

If you want policy routing to be fast switched, see the following section “[Enabling Fast-Switched Policy Routing](#).”

See the “[Policy Routing Example](#)” section at the end of this chapter for an example of policy routing.

## Enabling Fast-Switched Policy Routing

IP policy routing can also be fast switched. Prior to fast-switched policy routing, policy routing could only be process switched, which meant that on most platforms, the switching rate was approximately 1000 to 10,000 packets per second. Such rates were not fast enough for many applications. Users that need policy routing to occur at faster speeds can now implement policy routing without slowing down the router.

Fast-switched policy routing supports all of the **match** commands and most of the **set** commands, except for the following restrictions:

- The **set ip default** command is not supported.
- The **set interface** command is supported only over point-to-point links, unless a route cache entry exists using the same interface specified in the **set interface** command in the route map. Also, at the process level, the routing table is consulted to determine if the interface is on a reasonable path to the destination. During fast switching, the software does not make this check. Instead, if the packet matches, the software blindly forwards the packet to the specified interface.

Policy routing must be configured before you configure fast-switched policy routing. Fast switching of policy routing is disabled by default. To have policy routing be fast switched, use the following command in interface configuration mode:

| Command                                         | Purpose                                   |
|-------------------------------------------------|-------------------------------------------|
| Router(config-if)# <b>ip route-cache policy</b> | Enables fast switching of policy routing. |

## Enabling Local Policy Routing

Packets that are generated by the router are not normally policy routed. To enable local policy routing for such packets, indicate which route map the router should use by using the following command in global configuration mode. All packets originating on the router will then be subject to local policy routing.

| Command                                                         | Purpose                                                   |
|-----------------------------------------------------------------|-----------------------------------------------------------|
| Router(config)# <b>ip local policy route-map</b> <i>map-tag</i> | Identifies the route map to use for local policy routing. |

Use the **show ip local policy EXEC** command to display the route map used for local policy routing, if one exists.

## Enabling NetFlow Policy Routing

NetFlow policy routing (NPR) integrates policy routing, which enables traffic engineering and traffic classification, with NetFlow services, which provide billing, capacity planning, and monitoring information on real-time traffic flows. IP policy routing now works with Cisco Express Forwarding (CEF), distributed CEF (dCEF), and NetFlow.

As quality of service (QoS) and traffic engineering become more popular, so does interest in the ability of policy routing to selectively set IP Precedence and type of service (ToS) bits (based on access lists and packet size), thereby routing packets based on predefined policy. It is important that policy routing work well in large, dynamic routing environments. Hence, distributed support allows customers to leverage their investment in distributed architecture.

NetFlow policy routing leverages the following technologies:

- CEF, which looks at a Forwarding Information Base (FIB) instead of a routing table when switching packets, to address maintenance problems of a demand caching scheme.
- dCEF, which addresses the scalability and maintenance problems of a demand caching scheme.
- NetFlow, which provides accounting, capacity planning, and traffic monitoring capabilities.

Following are NPR benefits:

- NPR takes advantage of the new switching services. CEF, dCEF, and NetFlow can now use policy routing.
- Now that policy routing is integrated into CEF, policy routing can be deployed on a wide scale and on high-speed interfaces.

Following are NPR restrictions:

- NPR is only available on Cisco IOS platforms that support CEF.
- Distributed FIB-based policy routing is only available on platforms that support dCEF.
- The **set ip next-hop verify-availability** route-map configuration command of route-map is not supported in dCEF because dCEF does not support the Cisco Discovery Protocol (CDP) database.

In order for NetFlow policy routing to work, the following features must already be configured:

- CEF, dCEF, or NetFlow
- Policy routing

To configure CEF, dCEF, or NetFlow, refer to the appropriate chapter of the *Cisco IOS Switching Services Configuration Guide*.

NPR is the default policy routing mode. No additional configuration tasks are required to enable policy routing in conjunction with CEF, dCEF, or NetFlow. As soon as one of these features is turned on, packets are automatically subject to policy routing in the appropriate switching path.

There is one new, optional configuration command (**set ip next-hop verify-availability**). This command has the following restrictions:

- It can cause some performance degradation due to CDP database lookup overhead per packet.
- CDP must be enabled on the interface.
- The directly connected next hop must be a Cisco device with CDP enabled.
- The command will not work with dCEF configurations, due to the dependency of the CDP neighbor database.

It is assumed that policy routing itself is already configured.

If the router is policy routing packets to the next hop and the next hop happens to be down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior can continue indefinitely.

To prevent this situation from occurring, you can configure the router to first verify that the next hop, using a route map, are CDP neighbors of the router before routing to that next hop.

This task is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending the router traffic.

To configure the router to verify that the next hop is a CDP neighbor before the router tries to policy route to it, use the following command in route-map configuration mode:

| Command                                                               | Purpose                                                                                           |
|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Router(config-route-map) # <b>set ip next-hop verify-availability</b> | Causes the router to confirm that the next hops of the route map are CDP neighbors of the router. |

If the command shown is set and the next hop is not a CDP neighbor, the router looks to the subsequent next hop, if there is one. If there is none, the packets simply are not policy routed.

If the command shown is not set, the packets are either policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route-map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and use the **set ip next-hop verify-availability** configuration command selectively.

Typically, you would use existing policy routing and NetFlow **show EXCEC** commands to monitor these features. For more information on these **show** commands, refer to the “IP Routing Protocol-Independent Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication for policy routing commands and the appropriate chapter of the *Cisco IOS Switching Services Command Reference* publication for NetFlow commands.

To display the route map Inter Processor Communication (IPC) message statistics in the Route Processor (RP) or Versatile Interface Processor (VIP), use the following command in EXEC mode:

| Command                           | Purpose                                                         |
|-----------------------------------|-----------------------------------------------------------------|
| Router# <b>show route-map ipc</b> | Displays the route map IPC message statistics in the RP or VIP. |

# Managing Authentication Keys

Key management is a method of controlling authentication keys used by routing protocols. Not all protocols can use key management. Authentication keys are available for Director Response Protocol (DRP) Agent, EIGRP, and RIP Version 2.

Before you manage authentication keys, authentication must be enabled. See the appropriate protocol chapter to learn how to enable authentication for that protocol.

To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid. Each key has its own key identifier (specified with the **key** key-chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use.

You can configure multiple keys with lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. The lifetimes allow for overlap during key changes. Note that the router must know the time. Refer to the Network Time Protocol (NTP) and calendar commands in the “Performing Basic System Management” chapter of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

To manage authentication keys, use the following commands beginning in global configuration mode:

|        | Command                                                                                                                                      | Purpose                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| Step 1 | Router(config)# <b>key chain</b> <i>name-of-chain</i>                                                                                        | Identifies a key chain.                                         |
| Step 2 | Router(config-keychain)# <b>key</b> <i>number</i>                                                                                            | Identifies the key number in key chain configuration mode.      |
| Step 3 | Router(config-keychain-key)# <b>key-string</b> <i>text</i>                                                                                   | Identifies the key string in key chain configuration mode.      |
| Step 4 | Router(config-keychain-key)# <b>accept-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> } | Specifies the time period during which the key can be received. |
| Step 5 | Router(config-keychain-key)# <b>send-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> }   | Specifies the time period during which the key can be sent.     |

Use the **show key chain** EXEC command to display key chain information. For examples of key management, see the “[Key Management Examples](#)” section at the end of this chapter.



# Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You also can display specific statistics. The following sections describe each of these tasks.

## Clearing Routes from the IP Routing Table

You can remove all contents of a particular table. Clearing a table can become necessary when the contents of the particular structure have become, or are suspected to be, invalid.

To clear one or more routes from the IP routing table, use the following command in EXEC mode:

| Command                                                             | Purpose                                              |
|---------------------------------------------------------------------|------------------------------------------------------|
| Router# <b>clear ip route</b> { <i>network</i> [ <i>mask</i> ]   *} | Clears one or more routes from the IP routing table. |

## Displaying System and Network Statistics

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path packets leaving your device are taking through the network.

To display various routing statistics, use the following commands in EXEC mode, as needed:

| Command                                                                                                                                                                                                                                                      | Purpose                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Router# <b>show ip cache policy</b>                                                                                                                                                                                                                          | Displays the cache entries in the policy route cache.                             |
| Router# <b>show ip local policy</b>                                                                                                                                                                                                                          | Displays the local policy route map if one exists.                                |
| Router# <b>show ip policy</b>                                                                                                                                                                                                                                | Displays policy route maps.                                                       |
| Router# <b>show ip protocols</b>                                                                                                                                                                                                                             | Displays the parameters and current state of the active routing protocol process. |
| Router# <b>show ip route</b> [[ <i>ip-address</i> [ <i>mask</i> ]<br>[ <b>longer-prefixes</b> ]]   [ <i>protocol</i> [ <i>process-id</i> ]]   [ <b>list</b><br><i>access-list-number</i>   <i>access-list-name</i> ]   [ <b>static</b><br><b>download</b> ]] | Displays the current state of the routing table.                                  |
| Router# <b>show ip route summary</b>                                                                                                                                                                                                                         | Displays the current state of the routing table in summary form.                  |
| Router# <b>show ip route supernets-only</b>                                                                                                                                                                                                                  | Displays supernets.                                                               |
| Router# <b>show key chain</b> [ <i>name-of-chain</i> ]                                                                                                                                                                                                       | Displays authentication key information.                                          |
| Router# <b>show route-map</b> [ <i>map-name</i> ]                                                                                                                                                                                                            | Displays all route maps configured or only the one specified.                     |

# IP Routing Protocol-Independent Configuration Examples

The following sections provide routing protocol-independent configuration examples:

- [Variable-Length Subnet Mask Example](#)
- [Overriding Static Routes with Dynamic Protocols Example](#)
- [Administrative Distance Examples](#)
- [Static Routing Redistribution Example](#)
- [EIGRP Redistribution Examples](#)
- [RIP and EIGRP Redistribution Examples](#)
- [OSPF Routing and Route Redistribution Examples](#)
- [Default Metric Values Redistribution Example](#)
- [Route Map Examples](#)
- [Passive Interface Examples](#)
- [Policy Routing Example](#)
- [Policy Routing with CEF Example](#)
- [Key Management Examples](#)

## Variable-Length Subnet Mask Example

In the following example, a /25 subnet mask is configured, leaving seven bits of address space (126 hosts) for hosts that are reachable through Ethernet interface 0/0. A /30 subnet mask is configured, leaving two bits of address space (2 hosts) reserved for serial line host addresses, allowing two host endpoints to be configured on a point-to-point serial link. Both subnets are covered by the OSPF network statement.

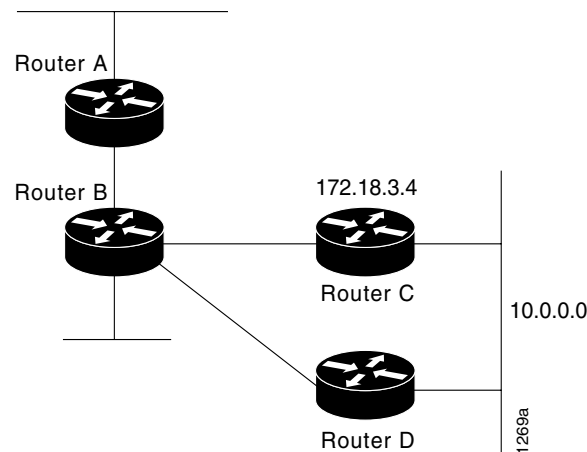
```
Router(config)# interface Ethernet 0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# ! 7 bits of host address space reserved for Ethernet interfaces
Router(config-if)# exit
Router(config)# interface Serial 0/0
Router(config-if)# ip address 192.168.1.130 255.255.255.252
Router(config-if)# ! 2 bits of address space reserved for Serial interface
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.0.0 0.0.255.255 area 10
Router(config-router)# ! Specifies the network directly connected to the router
```

## Overriding Static Routes with Dynamic Protocols Example

In the following example, packets for network 10.0.0.0 from Router B (where the static route is installed) will be routed through 172.18.3.4 if a route with an administrative distance less than 110 is not available. Figure 57 illustrates this example. The route learned by a protocol with an administrative distance of less than 110 might cause Router B to send traffic destined for network 10.0.0.0 via the alternate path—through Router D.

```
Router(config)# ip route 10.0.0.0 255.0.0.0 172.18.3.4 110
```

**Figure 57** Overriding Static Routes



## Administrative Distance Examples

In the following example, the **router eigrp** global configuration command configures EIGRP routing in autonomous system 1. The **network** command configuration specifies EIGRP routing on networks 192.168.7.0 and 172.16.0.0. The first **distance** router configuration command sets the default administrative distance to 255, which instructs the router to ignore all routing updates from routers for which an explicit distance has not been set. The second **distance** command sets the administrative distance to 80 for internal EIGRP routes and to 100 for external EIGRP routes. The third **distance** command sets the administrative distance to 120 for the router with the address 172.16.1.3.

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.7.0
Router(config-router)# network 172.16.0.0
Router(config-router)# distance 255
Router(config-router)# distance eigrp 80 100
Router(config-router)# distance 120 172.16.1.3 0.0.0.0
```



**Note**

The **distance eigrp** command must be used to set the administrative distance for EIGRP-derived routes.

The following example assigns the router with the address 192.168.7.18 an administrative distance of 100 and all other routers on subnet 192.168.7.0 an administrative distance of 200:

```
Router(config-router)# distance 100 192.168.7.18 0.0.0.0
Router(config-router)# distance 200 192.168.7.0 0.0.0.255
```

However, if you reverse the order of these two commands, all routers on subnet 192.168.7.0 are assigned an administrative distance of 200, including the router at address 192.168.7.18:

```
Router(config-router)# distance 200 192.168.7.0 0.0.0.255
Router(config-router)# distance 100 192.168.7.18 0.0.0.0
```

**Note**

Assigning administrative distances can be used to solve unique problems. However, administrative distances should be applied carefully and consistently to avoid the creation of routing loops or other network failures.

In the following example, the distance value for IP routes learned is 90. Preference is given to these IP routes rather than routes with the default administrative distance value of 110.

```
Router(config)# router isis
Router(config-router)# distance 90 ip
```

## Static Routing Redistribution Example

In the example that follows, three static routes are specified, two of which are to be advertised. The static routes are created by specifying the **redistribute static** router configuration command and then specifying an access list that allows only those two networks to be passed to the EIGRP process. Any redistributed static routes should be sourced by a single router to minimize the likelihood of creating a routing loop.

```
Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.7.65
Router(config)# ip route 192.168.5.0 255.255.255.0 192.168.7.65
Router(config)# ip route 10.10.10.0 255.255.255.0 10.20.1.2
Router(config)# !
Router(config)# access-list 3 permit 192.168.2.0 0.0.255.255
Router(config)# access-list 3 permit 192.168.5.0 0.0.255.255
Router(config)# access-list 3 permit 10.10.10.0 0.0.0.255
Router(config)# !
Router(config)# router eigrp 1
Router(config-router)# network 192.168.0.0
Router(config-router)# network 10.10.10.0
Router(config-router)# redistribute static metric 10000 100 255 1 1500
Router(config-router)# distribute-list 3 out static
```

## EIGRP Redistribution Examples

Each EIGRP routing process provides routing information to only one autonomous system. The Cisco IOS software must run a separate EIGRP process and maintain a separate routing database for each autonomous system that it services. However, you can transfer routing information between these routing databases.

In the following configuration, network 10.0.0.0 is configured under EIGRP autonomous system 1 and network 192.168.7.0 is configured under EIGRP autonomous system 101:

```
Router(config)# router eigrp 1
Router(config-router)# network 10.0.0.0
Router(config-router)# exit
Router(config)# router eigrp 101
Router(config-router)# network 192.168.7.0
```

In the following example, routes from the 192.168.7.0 network are redistributed into autonomous system 1 (without passing any other routing information from autonomous system 101):

```
Router(config)# access-list 3 permit 192.168.7.0
```

```
Router(config)# !
Router(config)# route-map 101-to-1 permit 10
Router(config-route-map)# match ip address 3
Router(config-route-map)# set metric 10000 100 1 255 1500
Router(config-route-map)# exit
Router(config)# router eigrp 1
Router(config-router)# redistribute eigrp 101 route-map 101-to-1
Router(config-router)# !
```

The following example is an alternative way to redistribute routes from the 192.168.7.0 network into autonomous system 1. Unlike the previous configuration, this method does not allow you to set the metric for redistributed routes.

```
Router(config)# access-list 3 permit 192.168.7.0
Router(config)# !
Router(config)# router eigrp 1
Router(config-router)# redistribute eigrp 101
Router(config-router)# distribute-list 3 out eigrp 101
Router(config-router)# !
```

## RIP and EIGRP Redistribution Examples

This section provides a simple RIP redistribution example and a complex redistribution example between EIGRP and BGP.

### Simple Redistribution Example

Consider a WAN at a university that uses RIP as an interior routing protocol. Assume that the university wants to connect its WAN to a regional network, 172.16.0.0, which uses EIGRP as the routing protocol. The goal in this case is to advertise the networks in the university network to the routers on the regional network.

In the following example, EIGRP to RIP redistribution is configured:

```
Router(config)# access-list 10 permit 172.16.0.0
Router(config)# !
Router(config)# router eigrp 1
Router(config-router)# network 172.16.0.0
Router(config-router)# redistribute rip metric 10000 100 255 1 1500
Router(config-router)# distribute-list 10 out rip
Router(config-router)# exit
Router(config)# router rip
Router(config-router)# redistribute eigrp 1
Router(config-router)# !
```

In this example, the **router** global configuration command starts an EIGRP routing process. The **network** router configuration command specifies that network 172.16.0.0 (the regional network) is to send and receive EIGRP routing information. The **redistribute** router configuration command specifies that RIP-derived routing information be advertised in the routing updates. The **default-metric** router configuration command assigns an EIGRP metric to all RIP-derived routes. The **distribute-list** router configuration command instructs the Cisco IOS software to use access list 10 (not defined in this example) to limit the entries in each outgoing update. The access list prevents unauthorized advertising of university routes to the regional network.

### Complex Redistribution Example

In the following example, *mutual* redistribution is configured between EIGRP and BGP.

Routes from BGP autonomous system 50000 are injected into EIGRP routing process 101. A filter is configured to ensure that the correct routes are advertised.

```
Router(config)# ! All networks that should be advertised from R1 are controlled with ACLs:
Router(config)# access-list 1 permit 172.18.0.0 0.0.255.255
Router(config)# access-list 1 permit 172.16.0.0 0.0.255.255
Router(config)# access-list 1 permit 172.25.0.0 0.0.255.255
Router(config)# ! Configuration for router R1:
Router(config)# router bgp 50000
Router(config-router)# network 172.18.0.0
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 192.168.10.1 remote-as 2
Router(config-router)# neighbor 192.168.10.15 remote-as 1
Router(config-router)# neighbor 192.168.10.24 remote-as 3
Router(config-router)# redistribute eigrp 101
Router(config-router)# distribute-list 1 out eigrp 101
Router(config-router)# exit
Router(config)# router eigrp 101
Router(config-router)# network 172.25.0.0
Router(config-router)# redistribute bgp 50000
Router(config-router)# distribute-list 1 out bgp 50000
Router(config-router)# !
```



#### Caution

BGP should be redistributed into an IGP when there are no other suitable options. Redistribution from BGP into any IGP should be applied with proper filtering using distribute-lists, IP prefix-list, and route-map statements to limit the number of prefixes. BGP routing tables can be very large. Redistributing all BGP prefixes into an IGP can have a detrimental effect on IGP network operations.

## OSPF Routing and Route Redistribution Examples

OSPF typically requires coordination among many internal routers, ABRs, and Autonomous System Boundary Routers (ASBRs). At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three types of examples follow:

- The first examples are simple configurations illustrating basic OSPF commands.
- The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
- The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

### Basic OSPF Configuration Examples

The following example illustrates a simple OSPF configuration that enables OSPF routing process 1, attaches Ethernet interface 0 to area 0.0.0.0, and redistributes RIP into OSPF and OSPF into RIP:

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip ospf cost 1
Router(config-if)# exit
Router(config)# interface Ethernet 1
Router(config-if)# ip address 172.17.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 172.18.0.0 0.0.255.255 area 0.0.0.0
```

```

Router(config-router)# redistribute rip metric 1 subnets
Router(config-router)# exit
Router(config)# router rip
Router(config-router)# network 172.17.0.0
Router(config-router)# redistribute ospf 1
Router(config-router)# default-metric 1
Router(config-router)# !

```

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 1 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, whereas area 0 enables OSPF for *all other* networks.

```

Router(config)# router ospf 1
Router(config-router)# network 172.18.20.0 0.0.0.255 area 10.9.50.0
Router(config-router)# network 172.18.0.0 0.0.255.255 area 2
Router(config-router)# network 172.19.10.0 0.0.0.255 area 3
Router(config-router)# network 0.0.0.0 255.255.255.255 area 0
Router(config-router)# exit
Router(config)# ! Ethernet interface 0 is in area 10.9.50.0:
Router(config)# interface Ethernet 0
Router(config-if)# ip address 172.18.20.5 255.255.255.0
Router(config-if)# exit
Router(config)# ! Ethernet interface 1 is in area 2:
Router(config)# interface Ethernet 1
Router(config-if)# ip address 172.18.1.5 255.255.255.0
Router(config-if)# exit
Router(config)# ! Ethernet interface 2 is in area 2:
Router(config)# interface Ethernet 2
Router(config-if)# ip address 172.18.2.5 255.255.255.0
Router(config-if)# exit
Router(config)# ! Ethernet interface 3 is in area 3:
Router(config)# interface Ethernet 3
Router(config-if)# ip address 172.19.10.5 255.255.255.0
Router(config-if)# exit
Router(config)# ! Ethernet interface 4 is in area 0:
Router(config)# interface Ethernet 4
Router(config-if)# ip address 172.19.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# ! Ethernet interface 5 is in area 0:
Router(config)# interface Ethernet 5
Router(config-if)# ip address 10.1.0.1 255.255.0.0
Router(config-if)# !

```

Each **network** router configuration command is evaluated sequentially, so the specific order of these commands in the configuration is important. The Cisco IOS software sequentially evaluates the address/wildcard-mask pair for each interface. See the “IP Routing Protocols Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* publication for more information.

Consider the first **network** command. Area ID 10.9.50.0 is configured for the interface on which subnet 172.18.20.0 is located. Assume that a match is determined for Ethernet interface 0. Ethernet interface 0 is attached to Area 10.9.50.0 only.

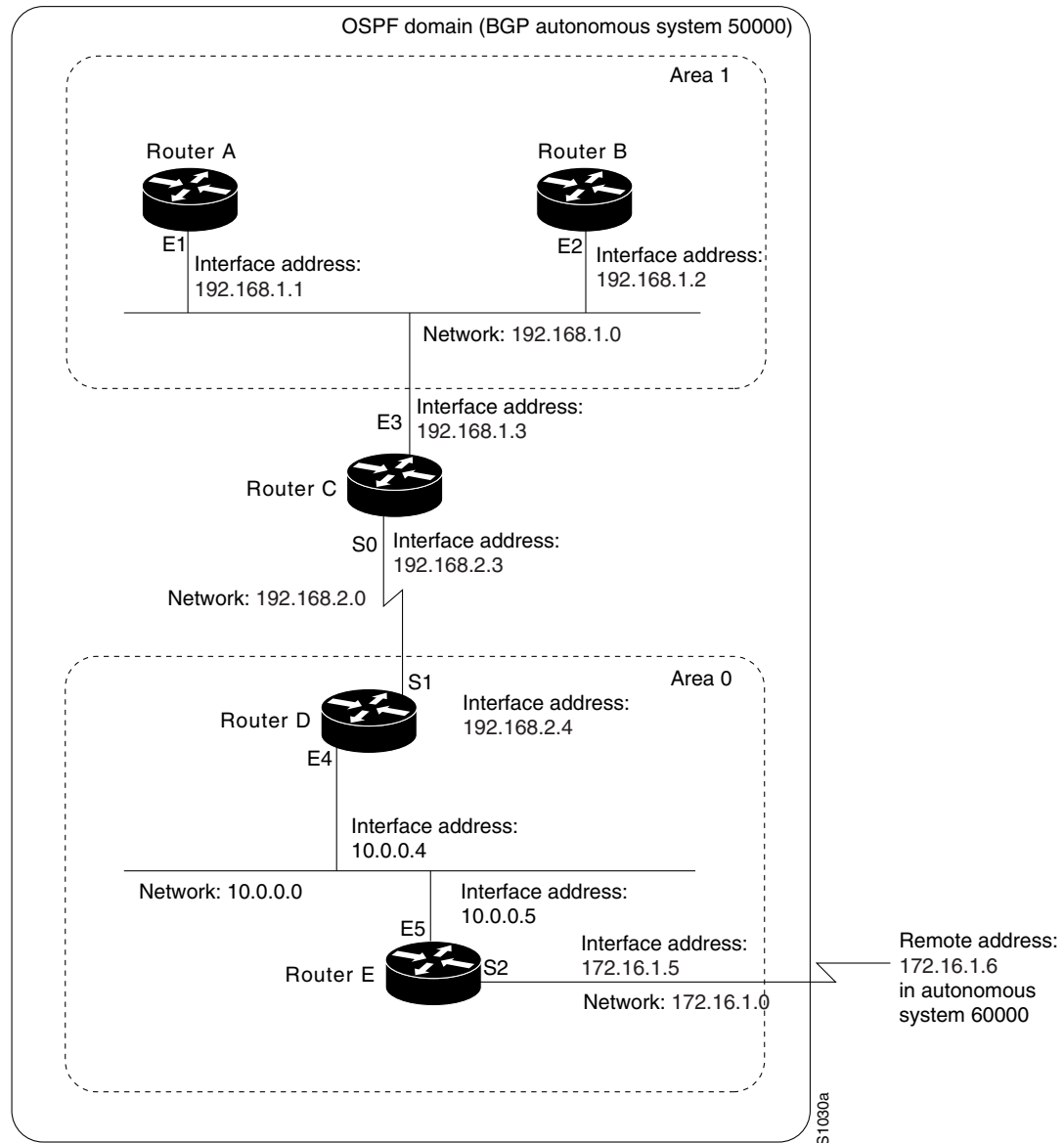
The second **network** command is evaluated next. For Area 2, the same process is then applied to all interfaces (except Ethernet interface 0). Assume that a match is determined for Ethernet interface 1. OSPF is then enabled for that interface and Ethernet 1 is attached to Area 2.

This process of attaching interfaces to OSPF areas continues for all **network** commands. Note that the last **network** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to Area 0.

## Internal Router, ABR, and ASBRs Configuration Example

Figure 58 provides a general network map that illustrates a sample configuration for several routers within a single OSPF autonomous system.

**Figure 58** Example OSPF Autonomous System Network Map



In this configuration, five routers are configured in OSPF autonomous system 1:

- Router A and Router B are both internal routers within area 1.
- Router C is an OSPF ABR. Note that for Router C, area 1 is assigned to E3 and Area 0 is assigned to S0.
- Router D is an internal router in area 0 (backbone area). In this case, both **network** router configuration commands specify the same area (area 0, or the backbone area).



- Router E is an OSPF ASBR. Note that BGP routes are redistributed into OSPF and that these routes are advertised by OSPF.

**Note**

It is not necessary to include definitions of all areas in an OSPF autonomous system in the configuration of all routers in the autonomous system. You must define only the *directly* connected areas. In the example that follows, routes in Area 0 are learned by the routers in area 1 (Router A and Router B) when the ABR (Router C) injects summary LSAs into area 1.

Autonomous system 60000 is connected to the outside world via the BGP link to the external peer at IP address 172.16.1.6.

Following is the example configuration for the general network map shown in [Figure 58](#).

**Router A Configuration—Internal Router**

```
Router(config)# interface Ethernet 1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 1
Router(config-router)# exit
```

**Router B Configuration—Internal Router**

```
Router(config)# interface Ethernet 2
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 1
Router(config-router)# exit
```

**Router C Configuration—ABR**

```
Router(config)# interface Ethernet 3
Router(config-if)# ip address 192.168.1.3 255.255.255.0
Router(config-if)# exit
Router(config)# interface Serial 0
Router(config-if)# ip address 192.168.2.3 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 1
Router(config-router)# network 192.168.2.0 0.0.0.255 area 0
Router(config-router)# exit
```

**Router D Configuration—Internal Router**

```
Router(config)# interface Ethernet 4
Router(config-if)# ip address 10.0.0.4 255.0.0.0
Router(config-if)# exit
Router(config)# interface Serial 1
Router(config-if)# ip address 192.168.2.4 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.2.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# exit
```

**Router E Configuration—ASBR**

```
Router(config)# interface Ethernet 5
Router(config-if)# ip address 10.0.0.5 255.0.0.0
Router(config-if)# exit
```

```

Router(config)# interface Serial 2
Router(config-if)# ip address 172.16.1.5 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-router)# redistribute bgp 50000 metric 1 metric-type 1
Router(config-router)# exit
Router(config)# router bgp 50000
Router(config-router)# network 192.168.0.0
Router(config-router)# network 10.0.0.0
Router(config-router)# neighbor 172.16.1.6 remote-as 60000

```

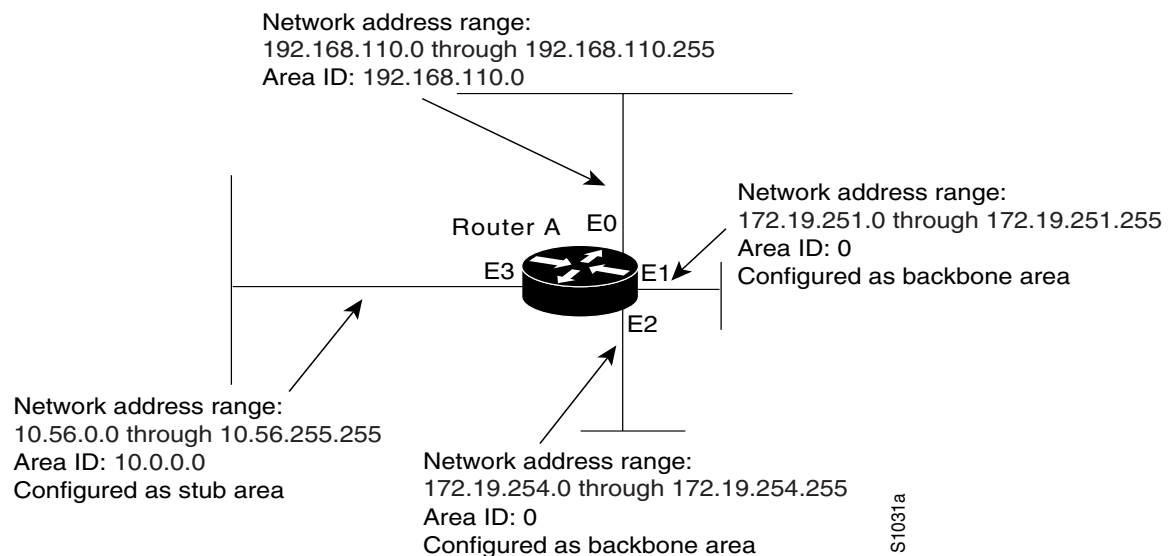
## Complex OSPF Configuration Example

The following example configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

- Basic OSPF configuration
- Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. [Figure 59](#) illustrates the network address ranges and area assignments for the interfaces.

**Figure 59** Interface and Area Specifications for OSPF Configuration Example



The basic configuration tasks in this example are as follows:

- Configure address ranges for Ethernet interface 0 through Ethernet interface 3.
- Enable OSPF on each interface.
- Set up an OSPF authentication password for each area and network.
- Assign link-state metrics and other OSPF interface configuration options.
- Create a *stub area* with area ID 10.0.0.0. (Note that the **authentication** and **stub** options of the **area** router configuration command are specified with separate **area** command entries, but they can be merged into a single **area** command.)
- Specify the backbone area (area 0).

Configuration tasks associated with redistribution are as follows:

- Redistribute EIGRP and RIP into OSPF with various options set (including **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 192.168.110.201 255.255.255.0
Router(config-if)# ip ospf authentication-key abcdefgh
Router(config-if)# ip ospf cost 10
Router(config-if)# exit
Router(config)# interface Ethernet 1
Router(config-if)# ip address 172.19.251.201 255.255.255.0
Router(config-if)# ip ospf authentication-key ijklmnop
Router(config-if)# ip ospf cost 20
Router(config-if)# ip ospf retransmit-interval 10
Router(config-if)# ip ospf transmit-delay 2
Router(config-if)# ip ospf priority 4
Router(config-if)# exit
Router(config)# interface Ethernet 2
Router(config-if)# ip address 172.19.254.201 255.255.255.0
Router(config-if)# ip ospf authentication-key abcdefgh
Router(config-if)# ip ospf cost 10
Router(config-if)# exit
Router(config)# interface Ethernet 3
Router(config-if)# ip address 10.56.0.201 255.255.0.0
Router(config-if)# ip ospf authentication-key ijklmnop
Router(config-if)# ip ospf cost 20
Router(config-if)# ip ospf dead-interval 80
Router(config-if)# exit
```

In the following configuration, OSPF is on network 172.19.0.0:

```
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 10.0.0.0
Router(config-router)# network 192.168.110.0 0.0.0.255 area 192.68.110.0
Router(config-router)# network 172.19.0.0 0.0.255.255 area 0
Router(config-router)# area 0 authentication
Router(config-router)# area 10.0.0.0 stub
Router(config-router)# area 10.0.0.0 authentication
Router(config-router)# area 10.0.0.0 default-cost 20
Router(config-router)# area 192.168.110.0 authentication
Router(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
Router(config-router)# area 192.168.110.0 range 192.168.110.0 255.255.255.0
Router(config-router)# area 0 range 172.19.251.0 255.255.255.0
Router(config-router)# area 0 range 172.19.254.0 255.255.255.0
Router(config-router)# redistribute eigrp 200 metric-type 2 metric 1 tag 200 subnets
Router(config-router)# redistribute rip metric-type 2 metric 1 tag 200
Router(config-router)# exit
```

In the following configuration, IGRP autonomous system 1 is on 172.19.0.0:

```
Router(config)# router eigrp 1
Router(config-router)# network 172.19.0.0
Router(config-router)# exit
Router(config)# ! RIP for 192.168.110.0:
Router(config)# router rip
Router(config-router)# network 192.168.110.0
Router(config-router)# redistribute eigrp 1 metric 1
Router(config-router)# redistribute ospf 201 metric 1
Router(config-router)# exit
```

## Default Metric Values Redistribution Example

The following example shows a router in autonomous system 1 that is configured to run both RIP and EIGRP. The example advertises EIGRP-derived routes using RIP and assigns the EIGRP-derived routes a RIP metric of 10.

```
Router(config)# router rip
Router(config-router)# default-metric 10
Router(config-router)# redistribute eigrp 1
Router(config-router)# exit
```

## Route Map Examples

The examples in this section illustrate the use of redistribution, with and without route maps. Examples from both the IP and Connectionless Network Service (CLNS) routing protocols are given. The following example redistributes all OSPF routes into EIGRP:

```
Router(config)# router eigrp 1
Router(config-router)# redistribute ospf 101
Router(config-router)# exit
```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a metric of 5, metric type of type 1, and a tag equal to 1.

```
Router(config)# router ospf 1
Router(config-router)# redistribute rip route-map rip-to-ospf
Router(config-router)# exit
Router(config)# route-map rip-to-ospf permit
Router(config-route-map)# match metric 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type 1
Router(config-route-map)# set tag 1
Router(config-route-map)# exit
```

The following example redistributes OSPF learned routes with tag 7 as a RIP metric of 15:

```
Router(config)# router rip
Router(config-router)# redistribute ospf 1 route-map 5
Router(config-router)# exit
Router(config)# route-map 5 permit
Router(config-route-map)# match tag 7
Router(config-route-map)# set metric 15
```

The following example redistributes OSPF intra-area and interarea routes with next hop routers on serial interface 0 into BGP with an INTER\_AS metric of 5:

```
Router(config)# router bgp 50000
Router(config-router)# redistribute ospf 1 route-map 10
Router(config-router)# exit
Router(config)# route-map 10 permit
Router(config-route-map)# match route-type internal
Router(config-route-map)# match interface serial 0
Router(config-route-map)# set metric 5
```

The following example redistributes two types of routes into the integrated IS-IS routing table (supporting both IP and CLNS). The first type is OSPF external IP routes with tag 5; these routes are inserted into Level 2 IS-IS link-state packets (LSPs) with a metric of 5. The second type is ISO-IGRP derived CLNS prefix routes that match CLNS access list 2000; these routes will be redistributed into IS-IS as Level 2 LSPs with a metric of 30.

```

Router(config)# router isis
Router(config-router)# redistribute ospf 1 route-map 2
Router(config-router)# redistribute iso-igrp nsfnet route-map 3
Router(config-router)# exit
Router(config)# route-map 2 permit
Router(config-route-map)# match route-type external
Router(config-route-map)# match tag 5
Router(config-route-map)# set metric 5
Router(config-route-map)# set level level-2
Router(config-route-map)# exit
Router(config)# route-map 3 permit
Router(config-route-map)# match address 2000
Router(config-route-map)# set metric 30
Router(config-route-map)# exit

```

With the following configuration, OSPF external routes with tags 1, 2, 3, and 5 are redistributed into RIP with metrics of 1, 1, 5, and 5, respectively. The OSPF routes with a tag of 4 are not redistributed.

```

Router(config)# router rip
Router(config-router)# redistribute ospf 101 route-map 1
Router(config-router)# exit
Router(config)# route-map 1 permit
Router(config-route-map)# match tag 1 2
Router(config-route-map)# set metric 1
Router(config-route-map)# exit
Router(config)# route-map 1 permit
Router(config-route-map)# match tag 3
Router(config-route-map)# set metric 5
Router(config-route-map)# exit
Router(config)# route-map 1 deny
Router(config-route-map)# match tag 4
Router(config-route-map)# exit
Router(config)# route-map 1 permit
Router(config-route-map)# match tag 5
Router(config-route-map)# set metric 5
Router(config-route-map)# exit

```

Given the following configuration, a RIP learned route for network 172.18.0.0 and an ISO-IGRP learned route with prefix 49.0001.0002 will be redistributed into an IS-IS Level 2 LSP with a metric of 5:

```

Router(config)# router isis
Router(config-router)# redistribute rip route-map 1
Router(config-router)# redistribute iso-igrp remote route-map 1
Router(config-router)# exit
Router(config)# route-map 1 permit
Router(config-route-map)# match ip address 1
Router(config-route-map)# match clns address 2
Router(config-route-map)# set metric 5
Router(config-route-map)# set level level-2
Router(config-route-map)# exit
Router(config)# access-list 1 permit 172.18.0.0 0.0.255.255
Router(config)# clns filter-set 2 permit 49.0001.0002...

```

The following configuration example illustrates how a route map is referenced by the **default-information** router configuration command. This type of reference is called *conditional default origination*. OSPF will originate the default route (network 0.0.0.0) with a type 2 metric of 5 if 172.20.0.0 is in the routing table.

```

Router(config)# route-map ospf-default permit
Router(config-route-map)# match ip address 1
Router(config-route-map)# set metric 5
Router(config-route-map)# set metric-type type-2
Router(config-route-map)# exit
Router(config)# access-list 1 172.20.0.0 0.0.255.255

```

```
Router(config)# !
Router(config)# router ospf 101
Router(config-router)# default-information originate route-map ospf-default
```

See more route map examples in the “BGP Route Map Examples” and “BGP Community with Route Maps Examples” sections of the “Configuring BGP” chapter.

## Passive Interface Examples

In OSPF, hello packets are not sent on an interface that is specified as passive. Hence, the router will not be able to discover any neighbors, and none of the OSPF neighbors will be able to see the router on that network. In effect, this interface will appear as a stub network to the OSPF domain. This configuration is useful if you want to import routes associated with a connected network into the OSPF domain without any OSPF activity on that interface.

The **passive-interface** router configuration command is typically used when the wildcard specification on the **network** router configuration command configures more interfaces than is desirable. The following configuration causes OSPF to run on all subnets of 172.18.0.0:

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 172.18.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# interface Ethernet 1
Router(config-if)# ip address 172.18.2.1 255.255.255.0
Router(config-if)# exit
Router(config)# interface Ethernet 2
Router(config-if)# ip address 172.18.3.1 255.255.255.0
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 172.18.0.0 0.0.255.255 area 0
Router(config-router)# exit
```

If you do not want OSPF to run on 172.18.3.0, enter the following commands:

```
Router(config)# router ospf 1
Router(config-router)# network 172.18.0.0 0.0.255.255 area 0
Router(config-router)# passive-interface Ethernet 2
Router(config-router)# exit
```

## Default Passive Interface Example

The following example configures the network interfaces, sets all interfaces that are running OSPF as passive, and then enables serial interface 0:

```
Router(config)# interface Ethernet 0
Router(config-if)# ip address 172.19.64.38 255.255.255.0 secondary
Router(config-if)# ip address 172.19.232.70 255.255.255.240
Router(config-if)# no ip directed-broadcast
Router(config-if)# exit
Router(config)# interface Serial 0
Router(config-if)# ip address 172.24.101.14 255.255.255.252
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip mroute-cache
Router(config-if)# exit
Router(config)# interface TokenRing 0
Router(config-if)# ip address 172.20.10.4 255.255.255.0
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip mroute-cache
Router(config-if)# ring-speed 16
Router(config-if)# exit
```

```
Router(config)# router ospf 1
Router(config-router)# passive-interface default
Router(config-router)# no passive-interface Serial 0
Router(config-router)# network 172.16.10.0 0.0.0.255 area 0
Router(config-router)# network 172.19.232.0 0.0.0.255 area 4
Router(config-router)# network 172.24.101.0 0.0.0.255 area 4
Router(config-router)# exit
```

## Policy Routing Example

The following example provides two sources with equal access to two different service providers. Packets that arrive on asynchronous interface 1 from the source 10.1.1.1 are sent to the router at 172.16.6.6 if the router has no explicit route for the destination of the packet. Packets that arrive from the source 172.17.2.2 are sent to the router at 192.168.7.7 if the router has no explicit route for the destination of the packet. All other packets for which the router has no explicit route to the destination are discarded.

```
Router(config)# access-list 1 permit ip 10.1.1.1
Router(config)# access-list 2 permit ip 172.17.2.2
Router(config)# !
Router(config)# interface async 1
Router(config-if)# ip policy route-map equal-access
Router(config-if)# exit
Router(config)# route-map equal-access permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip default next-hop 172.16.6.6
Router(config-route-map)# exit
Router(config)# route-map equal-access permit 20
Router(config-route-map)# match ip address 2
Router(config-route-map)# set ip default next-hop 192.168.7.7
Router(config-route-map)# exit
Router(config)# route-map equal-access permit 30
Router(config-route-map)# set default interface null 0
Router(config-route-map)# exit
```

## Policy Routing with CEF Example

The following example configures policy routing with CEF. The route is configured to verify that next hop 10.0.0.8 of the route map named test1 is a CDP neighbor before the router tries to policy-route to it.

```
Router(config)# ip cef
Router(config)# interface Ethernet 0/0/1
Router(config-if)# ip route-cache flow
Router(config-if)# ip policy route-map test
Router(config-if)# exit
Router(config)# route-map test permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set ip precedence priority
Router(config-route-map)# set ip next-hop 10.0.0.8
Router(config-route-map)# set ip next-hop verify-availability
Router(config-route-map)# exit
Router(config)# route-map test permit 20
Router(config-route-map)# match ip address 101
Router(config-route-map)# set interface Ethernet 0/0/3
Router(config-route-map)# set ip tos max-throughput
Router(config-route-map)# exit
```

## Key Management Examples

The following example configures a key chain named trees. In this example, the software will always accept and send willow as a valid key. The key chestnut will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The overlap allows for migration of keys or discrepancy in the set time of the router. Likewise, the key birch immediately follows chestnut, and there is a 30-minute leeway on each side to handle time-of-day differences.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip rip authentication key-chain trees
Router(config-if)# ip rip authentication mode md5
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# network 172.19.0.0
Router(config-router)# version 2
Router(config-router)# exit
Router(config)# key chain trees
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string willow
Router(config-keychain-key)# key 2
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2005 duration 7200
Router(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2005 duration 3600
Router(config-keychain-key)# key 3
Router(config-keychain-key)# key-string birch
Router(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2005 duration 7200
Router(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2005 duration 3600
Router(config-keychain-key)# exit
```

The following example configures a key chain named trees:

```
Router(config)# key chain trees
Router(config-keychain)# key 1
Router(config-keychain-key)# key-string willow
Router(config-keychain-key)# key 2
Router(config-keychain-key)# key-string chestnut
Router(config-keychain-key)# accept-lifetime 00:00:00 Dec 5 2004 23:59:59 Dec 5 2005
Router(config-keychain-key)# send-lifetime 06:00:00 Dec 5 2004 18:00:00 Dec 5 2005
Router(config-keychain-key)# exit
Router(config-keychain)# exit
Router(config)# interface Ethernet 0
Router(config-if)# ip address 172.19.104.75 255.255.255.0 secondary 172.19.232.147
255.255.255.240
Router(config-if)# ip rip authentication key-chain trees
Router(config-if)# media-type 10BaseT
Router(config-if)# exit
Router(config)# interface Ethernet 1
Router(config-if)# no ip address
Router(config-if)# shutdown
Router(config-if)# media-type 10BaseT
Router(config-if)# exit
Router(config)# interface Fddi 0
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no keepalive
Router(config-if)# exit
Router(config)# interface Fddi 1
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip rip send version 1
Router(config-if)# ip rip receive version 1
Router(config-if)# no keepalive
Router(config-if)# exit
Router(config)# router rip
Router(config-router)# version 2
```



```
Router(config-router)# network 172.19.0.0  
Router(config-router)# network 10.0.0.0  
Router(config-router)# network 172.16.0.0
```





# IP Event Dampening

---

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

## Feature History for the IP Event Dampening feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(22)S   | This feature was introduced.                                    |
| 12.2(14)S   | This feature was integrated into Cisco IOS Release 12.2(14)S.   |
| 12.2(13)T   | This feature was integrated into Cisco IOS Release 12.2(13)T.   |
| 12.2(18)SXD | This feature was integrated into Cisco IOS Release 12.2(18)SXD. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Restrictions for IP Event Dampening, page 774](#)
- [Information About IP Event Dampening, page 774](#)
- [How to Configure IP Event Dampening, page 778](#)
- [Configuration Examples for IP Event Dampening, page 780](#)
- [Additional References, page 781](#)
- [Command Reference, page 782](#)
- [Glossary, page 783](#)

# Restrictions for IP Event Dampening

## Subinterface Restrictions

Only primary interfaces can be configured with this feature. Primary interface configuration is applied to all subinterfaces by default. IP Event Dampening does not track the flapping of individual subinterfaces on an interface.

## Virtual Templates Not Supported

Copying a dampening configuration from virtual templates to virtual access interfaces is not supported because dampening has limited usefulness to existing applications that use virtual templates. Virtual access interfaces are released when an interface flaps, and new connections and virtual access interfaces are acquired when the interface comes up and is made available to the network. Since dampening states are attached to the interface, the dampening states would not survive an interface flap.

## IPX Routing Protocols Not Supported

IPX protocols are not supported by the IP Event Dampening feature. However, IPX variants of these protocols will still receive up and down state event information when this feature is enabled. This should not create any problems or routing issues.

# Information About IP Event Dampening

- [IP Event Dampening Overview, page 774](#)
- [Interface State Change Events, page 775](#)
- [Affected Components, page 776](#)
- [Network Deployments, page 777](#)
- [Benefits of IP Event Dampening, page 778](#)

## IP Event Dampening Overview

Interface state changes occur when interfaces are administratively brought up or down or if an interface changes state. When an interface changes state or flaps, routing protocols are notified of the status of the routes that are affected by the change in state. Every interface state change requires all affected devices in the network to recalculate best paths, install or remove routes from the routing tables, and then advertise valid routes to peer routers. An unstable interface that flaps excessively can cause other devices in the network to consume substantial amounts of system processing resources and cause routing protocols to lose synchronization with the state of the flapping interface.

The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping. Dampening an interface removes the interface from the network until the interface stops flapping and becomes stable. Configuring the IP Event Dampening feature improves convergence times and stability throughout the network by isolating failures so that disturbances are not propagated, which reduces the utilization of system processing resources by other devices in the network and improves overall network stability.

## Interface State Change Events

This section describes the interface state change events of the IP Event Dampening features. This feature employs a configurable exponential decay mechanism that is used to suppress the effects of excessive interface flapping or state changes. When the IP Event Dampening feature is enabled, flapping interfaces are dampened from the perspective of the routing protocol by filtering excessive route updates. Flapping interfaces are identified, assigned penalties, suppressed if the necessary, and made available to the network when the interface stabilizes. [Figure 60](#) is a chart that displays interface state events as they are perceived by routing protocols.

### Suppress Threshold

The suppress threshold is the value of the accumulated penalty that triggers the router to dampen a flapping interface. The flapping interface is identified by the router and assigned a penalty for each up and down state change, but the interface is not automatically dampened. The router tracks the penalties that a flapping interface accumulates. When the accumulated penalty reaches the default or preconfigured suppress threshold, the interface is placed in a dampened state.

### Half-Life Period

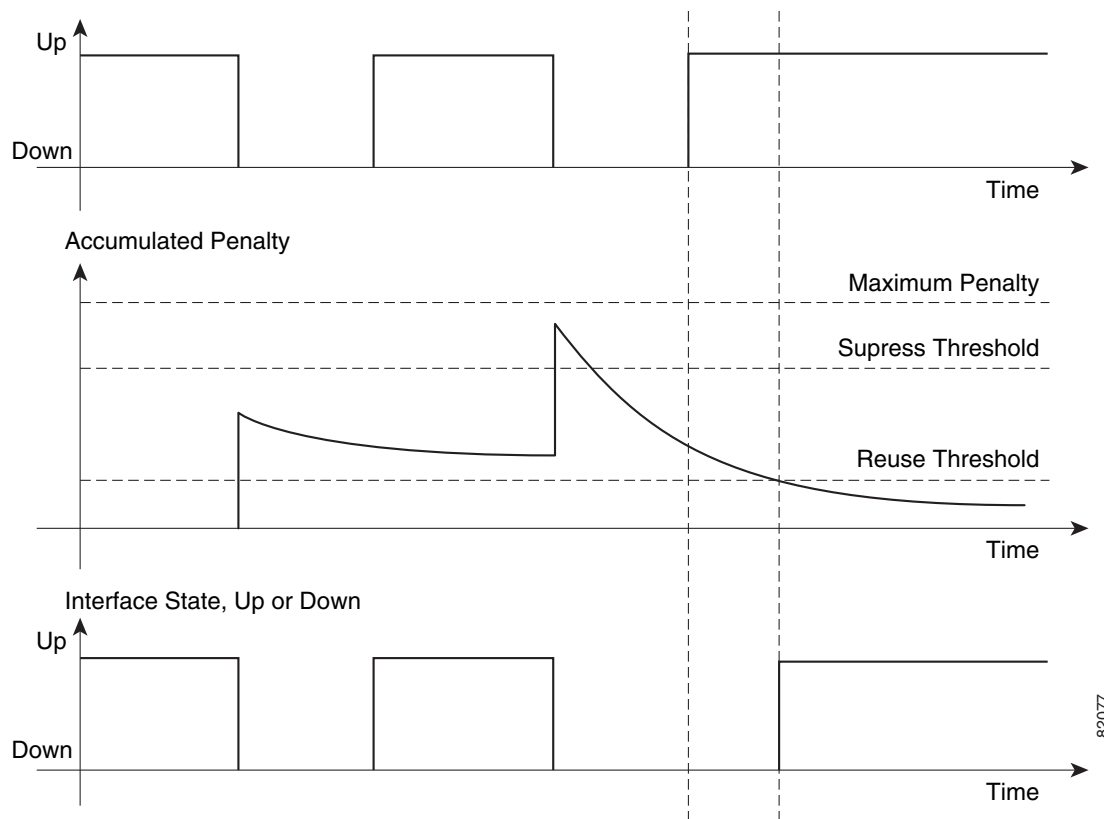
The half-life period determines how fast the accumulated penalty can decay exponentially. When an interface is placed in a dampened state, the router monitors the interface for additional up and down state changes. If the interface continues to accumulate penalties and the interface remains in the suppress threshold range, the interface will remain dampened. If the interface stabilizes and stops flapping, the penalty is reduced by half after each half-life period expires. The accumulated penalty will be reduced until the penalty drops to the reuse threshold. The configurable range of the half-life period timer is from 1 to 30 seconds. The default half-life period timer is 5 seconds.

### Reuse Threshold

When the accumulated penalty decreases until the penalty drops to the reuse threshold, the route is unsuppressed and made available to the other devices on the network. The range of the reuse value is from 1 to 20000 penalties. The default value is 1000 penalties.

### Maximum Suppress Time

The maximum suppress time represents the maximum amount of time an interface can remain dampened when a penalty is assigned to an interface. The maximum suppress time can be configured from 1 to 20000 seconds. The default of the maximum penalty timer is 20 seconds or four times the default half-life period (5 seconds). The maximum value of the accumulated penalty is calculated, based on the maximum suppress time, reuse threshold, and half-life period.

**Figure 60** *Interface State Change Events Perceived by the Routing Protocols*

## Affected Components

When an interface is not configured with dampening, or when an interface is configured with dampening but is not suppressed, the routing protocol behavior as a result of interface state transitions is not changed by the IP Event Dampening feature. However, if an interface is suppressed, the routing protocols and routing tables are immune to any further state transitions of the interface until it is unsuppressed.

## Route Types

The following interfaces are affected by the configuration of this feature:

- Connected routes:
  - The connected routes of dampened interfaces are not installed into the routing table.
  - When a dampened interface is unsuppressed, the connected routes will be installed into the routing table if the interface is up.
- Static routes:
  - Static routes assigned to a dampened interface are not installed into the routing table.
  - When a dampened interface is unsuppressed, the static route will be installed to the routing table if the interface is up.

**Note**

Only the primary interface can be configured with this feature, and all the subinterfaces are subject to the same dampening configuration as the primary interface. IP Event Dampening does not track the flapping of individual subinterfaces on an interface.

## Supported Protocols

The IP Event Dampening feature supports Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP), Connectionless Network Services (CLNS), and Hot Standby Routing Protocol (HSRP). The following list provides some general information about the operation of this feature with these protocols.

- RIP, OSPF, EIGRP, IS-IS, and BGP:
  - When an interface is dampened, the interface is considered to be down by the routing protocol. The routing protocol will not hold any adjacencies with this peer router over the dampened interface or generate advertisements of any routes related to this interface to other peer routers.
  - When the interface is unsuppressed and made available to the network, the interface will be considered by the routing protocols to be up. The routing protocols will be notified that the interface is in an up state and routing conditions will return to normal.
- HSRP:
  - When an interface is dampened, it is considered to be down by HSRP. HSRP will not generate HSRP messages out of the dampened interface or respond to any message received by the dampened interface. When the interface is unsuppressed and made available to the network, HSRP will be notified of the up state and will return to normal operations.
- CLNS:
  - When an interface is dampened, the interface is dampened to both IP and CLNS routing equally. The interface is dampened to both IP and CLNS because integrated routing protocols like IS-IS, IP, and CLNS routing are closely interconnected, so it is impossible to apply dampening separately.

**Note**

The IP Event Dampening feature has no effect on any routing protocols if it is not enabled or an interface is not dampened.

## Network Deployments

In real network deployments, some routers would not be configured with interface dampening, and not all of the routers would even support this feature. No major routing issues are expected, even if the router at the other end of a point-to-point interface or if routers of the same multicast LAN do not have interface dampening turned on or do not have this feature implemented at all. On the router where the interface is dampened, any routes associated with this interface will not be used. No packets will be sent out of this interface, and no routing protocol activity will be initiated with the routers on the other side of the interface. However, those other routers could still install some routes in their routing tables that are associated with this subnet because those routers recognize that their own interfaces are up and could start forwarding packets to the dampened interface. In this situation, the router with the dampened interface will start forwarding these packets, depending on the routes in its routing table.

The IP Event Dampening feature does not introduce new information into the network. In fact, the effect of dampening is to subtract a subset of all such routing information from the network. Therefore, looping should not occur as a result of dampening.

## Benefits of IP Event Dampening

### Reduced Processing Load

The IP Event Dampening Feature employs a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on the routing protocols. Excessive interface up and down state changes that are received in a short period of time are not processed and do not consume system resources. Other routers in the network need not waste system resources because of a flapping route.

### Faster Convergence

The IP Event Dampening feature improves convergence times and stability throughout the network by isolating failures so that disturbances are not propagated. Routers that are not experiencing link flap reach convergence sooner, because routing tables are not rebuilt each time the offending router leaves and enters service.

### Improved Network Stability

The IP Event Dampening feature provides increased network stability. A router with a flapping interface removes the flapping interface from the network until the interface stabilizes, so other routers simply redirect traffic around the affected router until the interface becomes stable, which ensures that the router loses no data packets.

## How to Configure IP Event Dampening

This section contains the following tasks:

- [Enabling IP Event Dampening, page 778](#)
- [Verifying IP Event Dampening, page 779](#)

## Enabling IP Event Dampening

The **dampening** command is entered in interface configuration mode to enable the IP Event Dampening feature. If this command is applied to an interface that already has dampening configured, all dampening states are reset and the accumulated penalty will be set to 0. If the interface has been dampened, the accumulated penalty will fall into the reuse threshold range, and the dampened interface will be made available to the network. The flap counts, however, are retained.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **dampening**[*half-life-period reuse-threshold*] [*suppress-threshold max-suppress*] [*restart-penalty*]
5. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>interface type number</b><br><br><b>Example:</b><br>Router(config)# <b>interface type number</b>                                                                   | Enters interface configuration mode and configures the specified interface.                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>dampening [half-life-period reuse-threshold] [suppress-threshold max-suppress [restart-penalty]]</b><br><br><b>Example:</b><br>Router(config-if)# <b>dampening</b> | Enables interface dampening. <ul style="list-style-type: none"> <li>Entering the <b>dampening</b> command without any keywords or arguments enables interface dampening with the default configuration parameters.</li> <li>When manually configuring the timer for the <i>restart-penalty</i> argument, the values must be manually entered for all arguments.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# <b>end</b>                                                                                                    | Exits interface configuration mode and enters Privileged EXEC mode.                                                                                                                                                                                                                                                                                                        |

## Verifying IP Event Dampening

Use the **show dampening interface** or **show interface dampening** EXEC commands to verify the configuration of the IP Event Dampening feature.

The **clear counters** Privileged EXEC command be used to clear the flap count and reset it to zero. All other parameters and status, including dampening states and accumulated penalties, are not affected by this command.

## SUMMARY STEPS

1. **enable**
2. **show dampening interface**
3. **show interface dampening**

## DETAILED STEPS

|        | Command or Action                                                                                             | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show dampening interface</b><br><br><b>Example:</b><br>Router# configure terminal                          | Enters global configuration mode.                                                                                |
| Step 3 | <b>show interface dampening</b><br><br><b>Example:</b><br>Router(config)# <b>interface</b> <i>type number</i> | Enters interface configuration mode for the specified interface.                                                 |

## Configuration Examples for IP Event Dampening

The following examples show how to configure this feature:

- [Configuring IP Event Dampening: Example, page 780](#)
- [Verifying IP Event Dampening: Example, page 781](#)

### Configuring IP Event Dampening: Example

The following example configures interface dampening on Ethernet interface 0/0 and sets the half life to 30 seconds, the reuse threshold to 1500, the suppress threshold to 10000; and the maximum suppress time to 120 seconds:

```
interface Ethernet 0/0
 dampening 30 1500 10000 120
```

The following example configures interface dampening on ATM interface 6/0 and uses the default interface dampening values:

```
interface atm 6/0
 dampening
```

The following example configures the router to apply a penalty of 500 on Ethernet interface 0/0 when the interface comes up for the first time after the router is reloaded:

```
interface Ethernet 0/0
 dampening 5 500 1000 20 500
```

## Verifying IP Event Dampening: Example

The output of the **show dampening interface** command displays a summary of interface dampening. The following is sample output from the **show dampening interface** command:

```
Router# show dampening interface

3 interfaces are configured with dampening.
No interface is being suppressed.
Features that are using interface dampening:
  IP Routing
  CLNS Routing
```

The output of the **show interface dampening** command displays the a summary of the dampening parameters and status. The following is sample output from the **show interface dampening** command.

```
Router# show interface dampening

FastEthernet0/0
  Flaps Penalty    Supp ReuseTm   HalfL ReuseV   SuppV MaxSTm   MaxP Restart
    0      0    FALSE      0      5    1000    2000    20   16000      0
ATM2/0
  Flaps Penalty    Supp ReuseTm   HalfL ReuseV   SuppV MaxSTm   MaxP Restart
    0      0    FALSE      0      5    1000    2000    20   16000      0
POS6/0
  Flaps Penalty    Supp ReuseTm   HalfL ReuseV   SuppV MaxSTm   MaxP Restart
    0      0    FALSE      0      5    1000    2000    20   16000      0
```

## Additional References

The following sections provide references related to IP Event Dampening feature.

### Related Documents

| Related Topic                        | Document Title                                                                                                                                    |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Protocol Commands            | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3T</a></li> </ul> |
| Routing Protocol Configuration Tasks | <ul style="list-style-type: none"> <li><a href="#">Cisco IOS IP Configuration Guide, Release 12.3</a></li> </ul>                                  |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                             | Title |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following new commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **dampening**
- **debug dampening**
- **show dampening interface**
- **show interface dampening**

# Glossary

**event dampening**—The process in which a router dampens a flapping interface from the perspective of the routing tables and routing protocols of IP and CLNS by filtering the excessive route adjust message because of the interface state change.

**Flap**—Rapid interface state changes from up to down and down to up within a short period of time.

**half life**—The rate of the exponential decay of the accumulated penalty is determined by this value.

**maximum penalty**—The maximum value beyond which the penalty assigned does not increase. It is derived from the maximum suppress time.

**maximum suppress time**—The maximum amount of time the interface can stay suppressed at the time a penalty is assigned.

**penalty**—A value assigned to an interface when it flaps. This value increases with each flap and decreases over time. The rate at which it decreases depends on the half life.

**reuse threshold**—The threshold value after which the interface will be unsuppressed and can be used again.

**suppress threshold**—Value of the accumulated penalty that triggers the router to dampen a flapping interface. When the accumulated penalty exceeds this value, the interface state is considered to be down from the perspective of the routing protocol.

**suppressed**—Suppressing an interface removes an interface from the network from the perspective of the routing protocol. An interface enters the suppressed state when it has flapped frequently enough for the penalty assigned to it to cross a threshold limit.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---





## PBR Support for Multiple Tracking Options

The PBR Support for Multiple Tracking Options feature extends the capabilities of object tracking using Cisco Discovery Protocol (CDP) to allow the policy-based routing (PBR) process to verify object availability by using additional methods. The verification method can be an Internet Control Message Protocol (ICMP) ping, User Datagram Protocol (UDP) ping, or an HTTP GET request.

### Feature History for PBR Support for Multiple Tracking Options

| Release   | Modification                                                                                                                                                          |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.3(4)T  | This feature was introduced.                                                                                                                                          |
| 12.2(25)S | This feature was integrated into Cisco IOS Release 12.2(25)S.                                                                                                         |
| 12.4      | The SAA (rtr) feature was replaced by the IP SLAs feature. See <a href="http://www.cisco.com/go/ipsla/">http://www.cisco.com/go/ipsla/</a> for updated documentation. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information About PBR Support for Multiple Tracking Options, page 786](#)
- [How to Configure PBR Support for Multiple Tracking Options, page 786](#)
- [Configuration Examples for PBR Support for Multiple Tracking Options, page 789](#)
- [Additional References, page 790](#)
- [Command Reference, page 791](#)

# Information About PBR Support for Multiple Tracking Options

To configure the PBR Support for Multiple Tracking Options feature, you should understand the following concepts:

- [Object Tracking, page 786](#)
- [PBR Support for Multiple Tracking Options Feature Design, page 786](#)

## Object Tracking

Object tracking is an independent process that monitors objects such as the following:

- State of the line protocol of an interface
- Existence of an entry in the routing table
- Results of an IP SLA monitoring operation, such as a ping

Clients such as Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), Gateway Load Balancing Protocol (GLBP), and (with this feature) PBR can register their interest in specific, tracked objects and then take action when the state of the objects changes.

## PBR Support for Multiple Tracking Options Feature Design

The PBR Support for Multiple Tracking Options feature gives PBR access to all the objects that are available through the tracking process. The tracking process provides the ability to track individual objects such as ICMP ping reachability, routing adjacency, an application running on a remote device, a route in the Routing Information Base (RIB), or to track the state of an interface line protocol.

Object tracking functions in the following manner. PBR will inform the tracking process that a certain object should be tracked. The tracking process will in turn notify PBR when the state of that object changes.

## How to Configure PBR Support for Multiple Tracking Options

This section contains the following procedure:

- [Configuring PBR Support for Multiple Tracking Options, page 786](#) (required)

## Configuring PBR Support for Multiple Tracking Options

This task configures PBR support for multiple tracking options.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **rtr operation-number**
4. **type echo protocol protocol-type target [source-ipaddr ip-address]**



5. **exit**
6. **rtr schedule** *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh:mm[:ss]* [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss*}] [**ageout** *seconds*]
7. **track** *object-number* **rtr** *entry-number* [**reachability**]
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask* [**secondary**]
11. **ip policy route-map** *map-tag*
12. **exit**
13. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
14. **set ip next-hop verify-availability** [*next-hop-address sequence track object*]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                       |
| Step 3 | <b>rtr</b> <i>operation-number</i><br><br><b>Example:</b><br>Router(config)# rtr 1<br>OR<br>Router(config)# ip sla monitor 1                                                      | Enters SAA RTR configuration mode and configures an SAA operation.<br><br><b>Note</b> This command is replaced by the ‘ip sla monitor <i>operation-number</i> ’ command in Release 12.3(14)T and later. |
| Step 4 | <b>type echo protocol</b> <i>protocol-type target</i> [ <i>source-ipaddr ip-address</i> ]<br><br><b>Example:</b><br>Router (config-rtr)# type echo protocol ipicmp echo 10.1.1.10 | Configures an SAA end-to-end echo response time probe operation.                                                                                                                                        |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-rtr)# exit                                                                                                                    | Exits SAA RTR configuration mode and returns the router to global configuration mode.                                                                                                                   |

|         | Command or Action                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                          |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre><b>rtr schedule</b> operation-number [<b>life</b> {<b>forever</b>   <b>seconds</b>}] [<b>start-time</b> {hh:mm:ss} [month day   day month]   <b>pending</b>   <b>now</b>   <b>after</b> hh:mm:ss}] [<b>ageout</b> seconds]</pre> <p><b>Example:</b><br/>Router(config)# rtr schedule 1 life forever start-time now</p> | <p>Configures the time parameters for the SAA operation.</p> <p><b>Note</b> This command is replaced by the <b>ip sla monitor schedule</b> command in Release 12.3(14)T and later.</p>                                                                                           |
| Step 7  | <pre><b>track</b> object-number <b>rtr</b> entry-number [<b>reachability</b>]</pre> <p><b>Example:</b><br/>Router(config)# track 123 rtr 1 reachability</p>                                                                                                                                                                 | Tracks the reachability of an Response Time Reporter (RTR) object and enters tracking configuration mode.                                                                                                                                                                        |
| Step 8  | <pre><b>exit</b></pre> <p><b>Example:</b><br/>Router(config-track)# exit</p>                                                                                                                                                                                                                                                | Exits tracking configuration mode, and returns the router to global configuration mode.                                                                                                                                                                                          |
| Step 9  | <pre><b>interface</b> type number</pre> <p><b>Example:</b><br/>Router(config)# interface ethernet 0</p>                                                                                                                                                                                                                     | Specifies an interface type and number, and enters interface configuration mode.                                                                                                                                                                                                 |
| Step 10 | <pre><b>ip address</b> ip-address mask [<b>secondary</b>]</pre> <p><b>Example:</b><br/>Router(config-if)# ip address 10.1.1.11 255.0.0.0</p>                                                                                                                                                                                | <p>Specifies a primary or secondary IP address for an interface.</p> <ul style="list-style-type: none"> <li>Refer to the “Configuring IP Addressing” chapter of the Release 12.3 <i>Cisco IOS IP Configuration Guide</i> for information on configuring IP addresses.</li> </ul> |
| Step 11 | <pre><b>ip policy route-map</b> map-tag</pre> <p><b>Example:</b><br/>Router(config-if)# ip policy route-map alpha</p>                                                                                                                                                                                                       | Enables policy routing and identifies a route map to be used for policy routing.                                                                                                                                                                                                 |
| Step 12 | <pre><b>exit</b></pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                                                                                                                                                                                   | Exits interface configuration mode and returns the router to global configuration mode.                                                                                                                                                                                          |
| Step 13 | <pre><b>route-map</b> map-tag [<b>permit</b>   <b>deny</b>] [<b>sequence-number</b>]</pre> <p><b>Example:</b><br/>Router(config)# route-map alpha</p>                                                                                                                                                                       | Specifies a route map and enters route-map configuration mode.                                                                                                                                                                                                                   |
| Step 14 | <pre><b>set ip next-hop verify-availability</b> [<b>next-hop-address</b> <b>sequence</b> <b>track</b> object]</pre> <p><b>Example:</b><br/>Router(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123</p>                                                                                          | Configures the route map to verify the reachability of the tracked object.                                                                                                                                                                                                       |

# Configuration Examples for PBR Support for Multiple Tracking Options

This section provides the following configuration example:

- [PBR Support for Multiple Tracking Options: Example, page 789](#)

## PBR Support for Multiple Tracking Options: Example

In the following example, object tracking is configured for PBR.

The policy is that packets received on Ethernet 0, should be forwarded to 10.1.1.1 only if that device is reachable (responding to pings). If 10.1.1.1 is not up, then the packets should be forwarded to 10.2.2.2. If 10.2.2.2 is also not reachable, then the policy routing fails and the packets are routed according to the routing table.

Two SAA Echo operations are configured to ping the remote devices. The SAA operations are then tracked. Policy routing will monitor the state of the tracked operations and make forwarding decisions based on their state.

```
! define and start the SAA operations
rtr 1
  type echo protocol ipicmpecho 10.1.1.1
  rtr schedule 1 start-time now life forever
!
rtr 2
  type echo protocol ipicmpecho 10.2.2.2
  rtr schedule 2 start-time now life forever
!
!track the SAA operations
track 123 rtr 1 reachability
track 124 rtr 2 reachability
!
! enable policy routing on the incoming interface
interface ethernet 0
  ip address 10.4.4.4 255.255.255.0
  ip policy route-map alpha
!
! 10.1.1.1 is via this interface
interface ethernet 1
  ip address 10.1.1.254 255.255.255.0
!
! 10.2.2.2 is via this interface
interface ethernet 2
  ip address 10.2.2.254 255.255.255.0
!
! define a route-map to set the next-hop depending on the state of the tracked rtrs
route-map alpha
  set ip next-hop verify-availability 10.1.1.1 10 track 123
  set ip next-hop verify-availability 10.2.2.2 20 track 124
```

# Additional References

The following sections provide references related to the PBR Support for Multiple Tracking Options feature.

## Related Documents

| Related Topic                             | Document Title                                                                                    |
|-------------------------------------------|---------------------------------------------------------------------------------------------------|
| Object tracking within Cisco IOS software | <i>Enhanced Object Tracking</i> feature document, Cisco IOS Release 12.2(15)T                     |
| Configuring IP addresses                  | “Configuring IP Addressing” chapter in the <i>Cisco IOS IP Configuration Guide</i> , Release 12.3 |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified command is pertinent to this feature. To see the command pages for this command and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **set ip next-hop verify-availability**





## PBR Recursive Next Hop

---

The PBR Recursive Next Hop feature enhances route maps to enable configuration of a recursive next-hop IP address that is used by policy-based routing (PBR). The recursive next-hop IP address is installed in the routing table and can be a subnet that is not directly connected. If the recursive next-hop IP address is not available, packets are routed using a default route.

Because Cisco Express Forwarding (CEF) or process switching provides the infrastructure, the benefit of this feature is the CEF load sharing.

### Feature History for the PBR Recursive Next Hop Feature

| Release   | Modification                                                  |
|-----------|---------------------------------------------------------------|
| 12.0(28)S | This feature was introduced.                                  |
| 12.3(14)T | This feature was integrated into Cisco IOS Release 12.3(14)T. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [How to Configure PBR Recursive Next Hop, page 794](#)
- [Configuration Examples for PBR Recursive Next Hop, page 796](#)
- [Additional References, page 797](#)
- [Command Reference, page 797](#)

# How to Configure PBR Recursive Next Hop

This section contains the following procedures:

- [Setting the Recursive Next-Hop IP Address, page 794](#) (required)
- [Verifying the Recursive Next-Hop Configuration, page 796](#) (optional)

## Setting the Recursive Next-Hop IP Address

The infrastructure provided by CEF or process switching performs the recursion to the next-hop IP address. The configuration sequence, which affects routing, is as follows:

1. Next-hop
2. Next-hop recursive
3. Interface
4. Default next-hop
5. Default interface

If both a next-hop and a recursive next-hop IP address are present in the same route-map entry, the next-hop is used. If the next-hop is not available, the recursive next-hop is used. If the recursive next-hop is not available and no other IP address is present, the packet is routed using the default routing table; it is not dropped. If the packet is supposed to be dropped, use the **set next-hop recursive** command followed by a **set interface null0** configuration.

Perform this task to set the IP address for the recursive next-hop router.

## Prerequisites

If load sharing is required, CEF load sharing should be configured for per-packet or per-destination load sharing. Load balancing should be done over all equal-cost routes to the subnet that have been configured by the **set next-hop recursive** command.

This functionality should be available in centralized and distributed systems.

## Restrictions

Only one recursive next-hop IP address is supported per route-map entry.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list permit** *source*
4. **route-map** *map-tag*
5. **set ip next-hop** *ip-address*
6. **set ip next-hop recursive** *ip-address*
7. **match ip address** *access-list-number*
8. **exit**



## DETAILED STEPS

|        | Command or Action                                                                                                                   | Purpose                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                      | Enters global configuration mode.                                                                                                                                                                                       |
| Step 3 | <b>access-list permit source</b><br><br><b>Example:</b><br>Router(config)# access-list permit 10.60.0.0 0.0.255.255                 | Configures an access list. The example configuration permits any source IP address that falls within the 10.60.0.0. 0.0.255.255 subnet.                                                                                 |
| Step 4 | <b>route-map map-tag</b><br><br><b>Example:</b><br>Router(config)# route-map abccomp                                                | Enables policy routing and enters route-map configuration mode.                                                                                                                                                         |
| Step 5 | <b>set ip next-hop ip-address</b><br><br><b>Example:</b><br>Router(config-route-map)# set ip next-hop 10.10.1.1                     | Sets a next-hop router IP address.<br><br><b>Note</b> Set this IP address separately from the next-hop recursive router configuration.                                                                                  |
| Step 6 | <b>set ip next-hop recursive ip-address</b><br><br><b>Example:</b><br>Router(config-route-map)# set ip next-hop recursive 10.20.3.3 | Sets a recursive next-hop IP address.<br><br><b>Note</b> This configuration does not ensure that packets get routed using the recursive IP address if an intermediate IP address is a shorter route to the destination. |
| Step 7 | <b>match ip address access-list-number</b><br><br><b>Example:</b><br>Router(config-route-map)# match ip address 101                 | Sets an access list to be matched.                                                                                                                                                                                      |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-route-map)# exit                                                                | Exits global configuration mode.                                                                                                                                                                                        |

## Verifying the Recursive Next-Hop Configuration

To verify the recursive next-hop configuration, perform the following steps.

### SUMMARY STEPS

1. **show running-config | beg abccomp**
2. **show route-map abccomp**

### DETAILED STEPS

#### Step 1 **show running-config | beg abccomp**

Use this command to verify the IP addresses for a next-hop and recursive next-hop IP address, for example:

```
Router# show running-config | beg abccomp

route-map abccomp permit 10
  match ip address 101 ! Defines the match criteria for an access list.
  set ip next-hop recursive 10.3.3.3 ! If the match criteria is met, the recursive IP
address is set.
  set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
```

#### Step 2 **show route-map abccomp**

Use this command to display the route-maps, for example:

```
Router# show route-map abccomp

route-map abccomp, permit, sequence 10
Match clauses:
  ip address (access-lists): 101
Set clauses:
  ip next-hop recursive 10.3.3.3
  ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
Policy routing matches: 0 packets, 0 bytes
```

## Configuration Examples for PBR Recursive Next Hop

This section provides the following configuration example:

- [Recursive Next-Hop IP Address: Example, page 796](#)

### Recursive Next-Hop IP Address: Example

The following example shows the configuration of IP address 10.3.3.3 as the recursive next-hop router:

```
route-map abccomp
  set ip next-hop 10.1.1.1
  set ip next-hop 10.2.2.2
  set ip next-hop recursive 10.3.3.3
  set ip next-hop 10.4.4.4
```

# Additional References

The following sections provide references related to the PBR Recursive Next Hop feature.

## Related Documents

| Related Topic                                                                                                          | Document Title                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| IP routing commandss: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> , Release 12.3T                                                             |
| Policy-based routing overview and configuration                                                                        | “ <a href="#">onfiguring Policy-Based Routing</a> ” chapter in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.2 |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                              | Link                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a> |

## Command Reference

The following modified commands are pertinent to this feature. To see the command pages for these commands and other commands used with this feature, go to the *Cisco IOS Master Commands List*, Release 12.4, at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124index.htm>.

- **set ip next-hop**
- **show route-map**





## **Part 7: RIP**







# Configuring Routing Information Protocol

---

This chapter describes how to configure Routing Information Protocol (RIP). For a complete description of the RIP commands that appear in this chapter, refer to the “RIP Commands” chapter of the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

RIP is a relatively old but still commonly used interior gateway protocol created for use in small, homogeneous networks. It is a classical distance-vector routing protocol. RIP is documented in RFC 1058.

RIP uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. Cisco IOS software sends routing information updates every 30 seconds, which is termed *advertising*. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by the nonupdating router as being unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the nonupdating router.

The metric that RIP uses to rate the value of different routes is *hop count*. The hop count is the number of routers that can be traversed in a route. A directly connected network has a metric of zero; an unreachable network has a metric of 16. This small range of metrics makes RIP an unsuitable routing protocol for large networks.

A router that is running RIP can receive a default network via an update from another router that is running RIP, or the router can source (generate) the default network itself with RIP. In both cases, the default network is advertised through RIP to other RIP neighbors.

Cisco IOS software will source the default network with RIP if one of the following conditions is met:

- The **ip default-network** command is configured.
- The **default-information originate** command is configured.
- The default route is learned via another routing protocol or static route and then redistributed into RIP.

RIP sends updates to the interfaces in the specified networks. If the network of an interface network is not specified, it will not be advertised in any RIP update.

The Cisco implementation of RIP Version 2 supports plain text and Message Digest 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs).

For protocol-independent features, which also apply to RIP, see the chapter “Configuring IP Routing Protocol-Independent Features” in this book.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the “[Using Cisco IOS Software for Release 12.4](#)” chapter in this book.

# RIP Configuration Task List

To configure RIP, perform the tasks described in the following sections. The tasks in the first two sections are required; the tasks in the remaining sections are optional.

- [Enabling RIP](#) (Required)
- [Allowing Unicast Updates for RIP](#) (Required)
- [Applying Offsets to Routing Metrics](#) (Optional)
- [Adjusting Timers](#) (Optional)
- [Specifying a RIP Version](#) (Optional)
- [Enabling RIP Authentication](#) (Optional)
- [Configuring Route Summarization on an Interface](#) (Optional)
- [Verifying IP Route Summarization](#) (Optional)
- [Disabling Automatic Route Summarization](#) (Optional)
- [Disabling the Validation of Source IP Addresses](#) (Optional)
- [Enabling or Disabling Split Horizon](#) (Optional)
- [Configuring Interpacket Delay](#) (Optional)
- [Connecting RIP to a WAN](#) (Optional)

For information about the following topics, see the “Configuring IP Routing Protocol-Independent Features” chapter:

- Filtering RIP information
- Key management (available in RIP Version 2)
- VLSM

## Enabling RIP

To enable RIP, use the following commands beginning in global configuration mode:

|        | Command                                                 | Purpose                                                                       |
|--------|---------------------------------------------------------|-------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>router rip</b>                       | Enables a RIP routing process, which places you in router configuration mode. |
| Step 2 | Router(config-router)# <b>network</b> <i>ip-address</i> | Associates a network with a RIP routing process.                              |



## Allowing Unicast Updates for RIP

Because RIP is normally a broadcast protocol, in order for RIP routing updates to reach nonbroadcast networks, you must configure the Cisco IOS software to permit this exchange of routing information. To do so, use the following command in router configuration mode:

| Command                                                  | Purpose                                                                  |
|----------------------------------------------------------|--------------------------------------------------------------------------|
| Router(config-router)# <b>neighbor</b> <i>ip-address</i> | Defines a neighboring router with which to exchange routing information. |

To control the set of interfaces with which you want to exchange routing updates, you can disable the sending of routing updates on specified interfaces by configuring the **passive-interface** router configuration command. See the discussion on filtering in the “Filter Routing Information” section in the “Configuring IP Routing Protocol-Independent Features” chapter.

## Applying Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Optionally, you can limit the offset list with either an access list or an interface. To increase the value of routing metrics, use the following command in router configuration mode:

| Command                                                                                                                                                                                      | Purpose                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| Router(config-router)# <b>offset-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ] { <b>in</b>   <b>out</b> } <i>offset</i> [ <i>interface-type</i> <i>interface-number</i> ] | Applies an offset to routing metrics. |

## Adjusting Timers

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internetwork needs. You can make the following timer adjustments:

- The rate (time in seconds between updates) at which routing updates are sent
- The interval of time (in seconds) after which a route is declared invalid
- The interval (in seconds) during which routing information regarding better paths is suppressed
- The amount of time (in seconds) that must pass before a route is removed from the routing table
- The amount of time for which routing updates will be postponed

It also is possible to tune the IP routing support in the software to enable faster convergence of the various IP routing algorithms, and, hence, quicker fallback to redundant routers. The total effect is to minimize disruptions to end users of the network in situations where quick recovery is essential

In addition, an address family can have explicitly specified timers that apply to that address-family (or VRF) only. The **timers basic** command must be specified for an address family or the system defaults for the **timers basic** command are used regardless of what is configured for RIP routing. The VRF does not inherit the timer values from the base RIP configuration. The VRF will always use the system default timers unless explicitly changed using the **timers basic** command.

To adjust the timers, use the following command in router configuration mode:

| Command                                                                                      | Purpose                          |
|----------------------------------------------------------------------------------------------|----------------------------------|
| Router(config-router)# <b>timers basic</b> <i>update invalid holddown flush [sleep-time]</i> | Adjusts routing protocol timers. |

See the “[Address Family Timers Example](#)” section at the end of this chapter for examples of adjusting timers for an address family (VRF).

## Specifying a RIP Version

The Cisco implementation of RIP Version 2 supports authentication, key management, route summarization, CIDR, and VLSMs. Key management and VLSM are described in the chapter “Configuring IP Routing Protocol-Independent Features.”

By default, the software receives RIP Version 1 and Version 2 packets, but sends only Version 1 packets. You can configure the software to receive and send only Version 1 packets. Alternatively, you can configure the software to receive and send only Version 2 packets. To configure the software to send and receive packets from only one version, use the following command in router configuration mode:

| Command                                       | Purpose                                                                                       |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------|
| Router(config-router)# <b>version</b> {1   2} | Configures the software to receive and send only RIP Version 1 or only RIP Version 2 packets. |

The preceding task controls the default behavior of RIP. You can override that behavior by configuring a particular interface to behave differently. To control which RIP version an interface sends, use the following commands in interface configuration mode, as needed:

| Command                                           | Purpose                                                              |
|---------------------------------------------------|----------------------------------------------------------------------|
| Router(config-if)# <b>ip rip send version 1</b>   | Configures an interface to send only RIP Version 1 packets.          |
| Router(config-if)# <b>ip rip send version 2</b>   | Configures an interface to send only RIP Version 2 packets.          |
| Router(config-if)# <b>ip rip send version 1 2</b> | Configures an interface to send RIP Version 1 and Version 2 packets. |

Similarly, to control how packets received from an interface are processed, use the following commands in interface configuration mode, as needed:

| Command                                              | Purpose                                                              |
|------------------------------------------------------|----------------------------------------------------------------------|
| Router(config-if)# <b>ip rip receive version 1</b>   | Configures an interface to accept only RIP Version 1 packets.        |
| Router(config-if)# <b>ip rip receive version 2</b>   | Configures an interface to accept only RIP Version 2 packets.        |
| Router(config-if)# <b>ip rip receive version 1 2</b> | Configures an interface to accept either RIP Version 1 or 2 packets. |

## Enabling RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface.

The key chain determines the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed on that interface, not even the default authentication. Therefore, you must also perform the tasks in the section “Managing Authentication Keys” in the “Configuring IP Routing Protocol-Independent Features” chapter.

We support two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.



### Note

Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet. Use plain text authentication when security is not an issue, for example, to ensure that misconfigured hosts do not participate in routing.

To configure RIP authentication, use the following commands in interface configuration mode:

|        | Command                                                                           | Purpose                                                                                                     |
|--------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config-if)# <b>ip rip authentication key-chain</b><br><i>name-of-chain</i> | Enables RIP authentication.                                                                                 |
| Step 2 | Router(config-if)# <b>ip rip authentication mode {text   md5}</b>                 | Configures the interface to use MD5 digest authentication (or let it default to plain text authentication). |

See the “Key Management Examples” section of the “Configuring IP Routing Protocol-Independent Features” chapter for key management information and examples.

## RIP Route Summarization

Summarizing routes in RIP Version 2 improves scalability and efficiency in large networks.

Summarizing IP addresses means that there is no entry for child routes (routes that are created for any combination of the individual IP addresses contained within a summary address) in the RIP routing table, reducing the size of the table and allowing the router to handle more routes.

Summary IP address functions more efficiently than multiple individually advertised IP routes for the following reasons:

- The summarized routes in the RIP database are processed first.
- Any associated child routes that are included in a summarized route are skipped as RIP looks through the routing database, reducing the processing time required.

Cisco routers can summarize routes in two ways:

- Automatically, by summarizing subprefixes to the classful network boundary when crossing classful network boundaries (automatic summary).



### Note

You need not configure anything for automatic summary to be enabled. To disable automatic summary, use the Router (config-router)# **no auto-summary** router configuration command.

- As specifically configured, advertising a summarized local IP address pool on the specified interface (on a network access server) so that the address pool can be provided to dialup clients.

Automatic summary addressing always summarizes to the classful address boundary, while the **ip summary-address** router configuration command summarizes addresses on a specified interface. If automatic summary addressing is enabled, automatic summarization is the default behavior for interfaces on the router not associated with dial-in clients (the “backbone”), with *or* without the **ip summary-address rip** interface command present.

For example, if a local IP address pool of 10.1.1.1 to 10.1.1.254 is configured on the network access server, you could configure the **ip summary-address rip 10.1.1.0 255.255.255.0** command on the network access server port that provides addresses to dialup clients to cause the router to advertise 10.1.1.0/24 routes to dialup clients. Because a summary route is advertised, advertisement of the /32 host routes (installed when the dialup client connects) is suppressed so that the router does not advertise these routes to the network access server interface.

Automatic summary will override the configured summary address feature on a given interface except when *both* of the following conditions are true:

- The configured interface summary address and the IP address of the configured interface share the same major network (the classful, nonsubnetted portion of the IP address).
- Split horizon is not enabled on the interface.



#### Note

If split horizon is enabled, neither an automatic summary address nor the interface summary address is advertised.

In the following example configuration, the major network is 10.0.0.0. The 10 in the address defines a Class A address space, allowing space for 0.x.x.x unique hosts where *x* defines unique bit positions in the addresses for these hosts. The summary of the major net defines the prefix as implied by the class (A, B, or C) of the address, without any network mask. The summary address 10.2.0.0 overrides the automatic summary address of 10.0.0.0, 10.2.0.0 is advertised out interface E1, and 10.0.0.0 is not advertised.

```
Router(config)# interface Ethernet1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)# no ip split-horizon
Router(config-if)# exit
Router(config)# router rip
Router(config)# network 10.0.0.0
```

When RIP determines that a summary address is required in the RIP database, a summary entry is created in the RIP routing database. As long as there are child routes for a summary address, the address remains in the routing database. When the last child route is removed, the summary entry also is removed from the database. This method of handling database entries reduces the number of entries in the database because each child route is not listed in an entry, and the aggregate entry itself is removed when there are no longer any valid child routes for it.

RIP Version 2 route summarization requires that the lowest metric of the “best route” of an aggregated entry, or the lowest metric of all current child routes, be advertised. The best metric for aggregated summarized routes is calculated at route initialization or when there are metric modifications of specific routes at advertisement time, and not at the time the aggregated routes are advertised.

## Restrictions to RIP Route Summarization

Supernet advertisement (advertising any network prefix less than its classful major network) is not allowed in RIP route summarization, other than advertising a supernet learned in the routing tables. Supernets learned on any interface that is subject to configuration are still learned.

For example, the following summarization is invalid: (invalid supernet summarization)

```
Router(config)# interface Ethernet 1
Router(config-if)# ip summary-address rip 10.0.0.0 252.0.0.0
.
.
.
```

Each route summarization on an interface must have a unique major net, even if the subnet mask is unique. For example, the following is not permitted:

```
Router(config)# interface Ethernet 1
Router(config)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```



### Note

The **ip summary-address eigrp** router configuration command uses other options that are not applicable to RIP. Do not confuse EIGRP summary address with the new RIP command, **ip summary-address rip**.

## Configuring Route Summarization on an Interface

The **ip summary-address rip** router configuration command causes the router to summarize a given set of routes learned via RIP Version 2 or redistributed into RIP Version 2. Host routes are especially applicable for summarization. To configure IP summary addressing, use the following commands beginning in global configuration mode:

|        | Command                                                                         | Purpose                                                                              |
|--------|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>type number</i>                             | Enters interface configuration mode.                                                 |
| Step 2 | Router(config-if)# <b>ip summary-address rip</b> <i>ip-address network-mask</i> | Specifies the IP address and network mask that identify the routes to be summarized. |

See the “[Route Summarization Examples](#)” section at the end of this chapter for examples of using split horizon.

## Verifying IP Route Summarization

You can verify which routes are summarized for an interface using the **show ip protocols EXEC** command. The following example shows potential summarizations and the associated interface summary address and network mask for Ethernet interface 2:

```
Router# show ip protocols

Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 8 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
```

```

Redistributing: rip
Default version control: send version 2, receive version 2
  Interface      Send  Recv  Triggered RIP  Key-chain
  Ethernet2      2     2
  Ethernet3      2     2
  Ethernet4      2     2
  Ethernet5      2     2
Automatic network summarization is not in effect
Address Summarization:
  10.11.0.0/16 for Ethernet2

```

You can check summary address entries in the RIP database. These entries will appear in the database only if relevant child routes are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table. The following example shows a summary address entry for route 10.11.0.0/16, with three child routes active:

```

router# show ip rip database
10.0.0.0/8      auto-summary
10.11.11.0/24   directly connected, Ethernet2
10.1.0.0/8      auto-summary
10.11.0.0/16    int-summary
^^^^^^^^^^^^^^
10.11.10.0/24   directly connected, Ethernet3
10.11.11.0/24   directly connected, Ethernet4
10.11.12.0/24   directly connected, Ethernet5

```

Disabling Automatic Route Summarization

RIP Version 2 supports automatic route summarization by default. The software summarizes subprefixes to the classful network boundary when crossing classful network boundaries.

If you have disconnected subnets, disable automatic route summarization to advertise the subnets. When route summarization is disabled, the software sends subnet and host routing information across classful network boundaries. To disable automatic summarization, use the following command in router configuration mode:

| Command                                       | Purpose                           |
|-----------------------------------------------|-----------------------------------|
| Router(config-router)# <b>no auto-summary</b> | Disables automatic summarization. |

Disabling the Validation of Source IP Addresses

By default, the software validates the source IP address of incoming RIP routing updates. If that source address is not valid, the software discards the routing update. You might want to disable this feature if you have a router that is “off network” and you want to receive its updates. However, disabling this feature is not recommended under normal circumstances.

To disable the default function that validates the source IP addresses of incoming routing updates, use the following command in router configuration mode:

| Command                                                 | Purpose                                                                           |
|---------------------------------------------------------|-----------------------------------------------------------------------------------|
| Router(config-router)# <b>no validate-update-source</b> | Disables the validation of the source IP address of incoming RIP routing updates. |

## Enabling or Disabling Split Horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the *split horizon* mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with nonbroadcast networks (such as Frame Relay and Switched Multimegabit Digital System [SMDS]), situations can arise for which this behavior is less than ideal. For these situations, you may want to disable split horizon with RIP.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by the secondary address. One routing update is sourced per network number unless split horizon is disabled.

To enable or disable split horizon, use the following commands in interface configuration mode, as needed:

| Command                                       | Purposes                |
|-----------------------------------------------|-------------------------|
| Router(config-if)# <b>ip split-horizon</b>    | Enables split horizon.  |
| Router(config-if)# <b>no ip split-horizon</b> | Disables split horizon. |

Split horizon for Frame Relay and SMDS encapsulation is disabled by default. Split horizon is not disabled by default for interfaces using any of the X.25 encapsulations. For all other encapsulations, split horizon is enabled by default.

See the “[Split Horizon Examples](#)” section at the end of this chapter for examples of using split horizon.



### Note

In general, changing the state of the default is not recommended unless you are certain that your application requires making a change in order to advertise routes properly. Remember that if split horizon is disabled on a serial interface (and that interface is attached to a packet-switched network), you *must* disable split horizon for all routers in any relevant multicast groups on that network.

## Configuring Interpacket Delay

By default, the software adds no delay between packets in a multiple-packet RIP update being sent. If you have a high-end router sending to a low-speed router, you might want to add such interpacket delay to RIP updates, in the range of 8 to 50 milliseconds. To do so, use the following command in router configuration mode:

| Command                                                        | Purpose                                                |
|----------------------------------------------------------------|--------------------------------------------------------|
| Router(config-router)# <b>output-delay</b> <i>milliseconds</i> | Configures interpacket delay for outbound RIP updates. |

## Connecting RIP to a WAN

Routers are used on connection-oriented networks to allow potential connectivity to many remote destinations. Circuits on the WAN are established on demand and are relinquished when the traffic subsides. Depending on the application, the connection between any two sites for user data could be short and relatively infrequent.

There are two problems using RIP to connect to a WAN:

- Periodic broadcasting by RIP generally prevents WAN circuits from being closed.
- Even on fixed, point-to-point links, the overhead of periodic RIP transmissions could seriously interrupt normal data transfer because of the quantity of information that passes through the line every 30 seconds.

To overcome these limitations, triggered extensions to RIP cause RIP to send information on the WAN only when there has been an update to the routing database. Periodic update packets are suppressed over the interface on which this feature is enabled. RIP routing traffic is reduced on point-to-point, serial interfaces. Therefore, you can save money on an on-demand circuit for which you are charged for usage. Triggered extensions to RIP partially support [RFC 2091](#), *Triggered Extensions to RIP to Support Demand Circuits*.

To enable triggered extensions to RIP, use the following commands in global configuration mode:

|               | Command                                                          | Purpose                              |
|---------------|------------------------------------------------------------------|--------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface serial</b> <i>controller-number</i> | Configures a serial interface.       |
| <b>Step 2</b> | Router(config-if)# <b>ip rip triggered</b>                       | Enables triggered extensions to RIP. |



To display the contents of the RIP private database, use the following command in EXEC mode:

| Command                                                    | Purpose                                            |
|------------------------------------------------------------|----------------------------------------------------|
| Router# <b>show ip rip database</b> [ <i>prefix mask</i> ] | Displays the contents of the RIP private database. |

## RIP Configuration Examples

The following section provides RIP configuration examples:

- [Route Summarization Examples, page 811s](#)
- [Split Horizon Examples, page 812](#)
- [Address Family Timers Example, page 814](#)

## Route Summarization Examples

A correct and an incorrect configuration example of route summarization are provided.

### Example 1: Correct Configuration

The following example shows how the **ip summary-address rip** router configuration command works with automatic summary addressing in RIP, starting in global configuration mode. In the example, the major network is 10.0.0.0. The summary address 10.2.0.0 overrides the automatic summary address of 10.0.0.0, so that 10.2.0.0 is advertised out Ethernet interface 1 and 10.0.0.0 is not advertised.



#### Note

If split horizon is enabled, neither automatic summary nor interface summary addresses (those configured with the **ip summary-address rip** router configuration command) are advertised.

```
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# exit
Router(config)# interface ethernet1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Router(config-if)# no ip split-horizon
Router(config-if)# exit
```

## Example 2: Incorrect Configuration

The following example shows an illegal use of the **ip summary-address rip** router configuration command, because both addresses to be summarized have the same major network. Each route summarization on an interface must have a unique major network, whether or not the addresses have unique address masks.

```
Router(config)# interface Ethernet 1
Router(config-if)# ip summary-address rip 10.1.0.0 255.255.0.0
Router(config-if)# ip summary-address rip 10.2.2.0 255.255.255.0
.
.
.
```

## Split Horizon Examples

Two examples of configuring split horizon are provided.

### Example 1

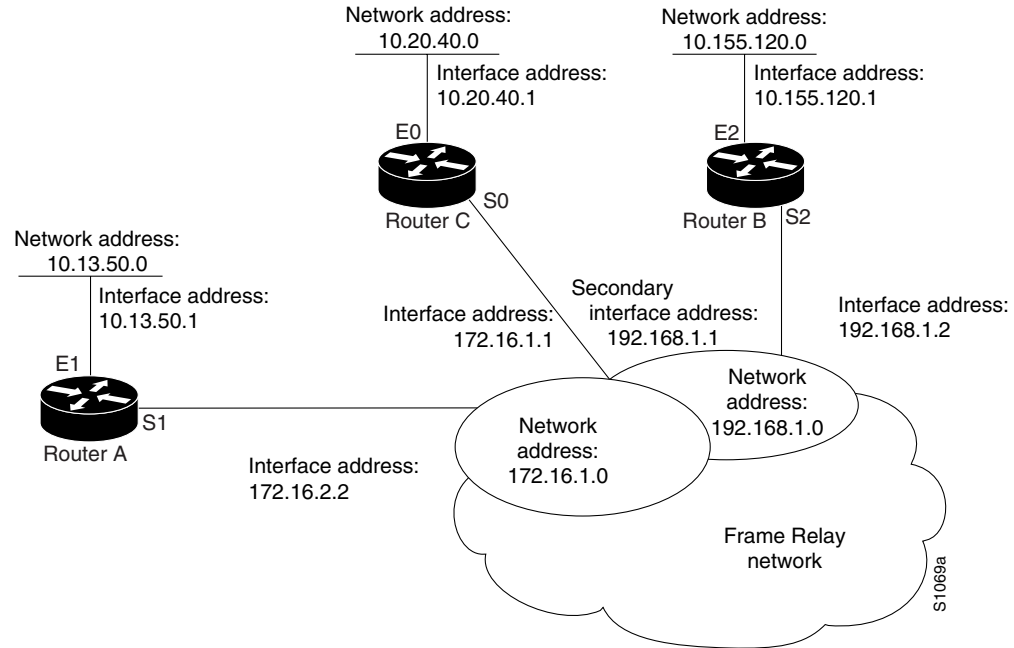
The following configuration shows a simple example of disabling split horizon on a serial link. In this example, the serial link is connected to an X.25 network.

```
Router(config)# interface Serial 0
Router(config-if)# encapsulation x25
Router(config-if)# no ip split-horizon
```

### Example 2

In the next example, [Figure 61](#) illustrates a typical situation in which the **no ip split-horizon** interface configuration command would be useful. This figure depicts two IP subnets that are both accessible via a serial interface on Router C (connected to Frame Relay network). In this example, the serial interface on Router C accommodates one of the subnets via the assignment of a secondary IP address.

The Ethernet interfaces for Router A, Router B, and Router C (connected to IP networks 10.13.50.0, 10.20.40.0, and 10.155.120.0, respectively, all have split horizon *enabled* by default, while the serial interfaces connected to networks 172.16.1.0 and 192.168.1.0 all have split horizon *disabled* with the **no ip split-horizon** command. [Figure 61](#) shows the topology and interfaces.

**Figure 61 Disabled Split Horizon Example for Frame Relay Network**

In this example, split horizon is disabled on all serial interfaces. The split horizon must be disabled on Router C in order for network 172.16.0.0 to be advertised into network 192.168.0.0 and vice versa. These subnets overlap at Router C, interface S0. If split horizon were enabled on serial interface S0, it would not advertise a route back into the Frame Relay network for either of these networks.

#### Configuration for Router A

```
interface ethernet 1
 ip address 10.13.50.0
!
interface serial 1
 ip address 172.16.2.2
 encapsulation frame-relay
 no ip split-horizon
```

#### Configuration for Router B

```
interface ethernet 2
 ip address 10.155.120.0
!
interface serial 2
 ip address 192.168.1.2
 encapsulation frame-relay
 no ip split-horizon
```

#### Configuration for Router C

```
interface ethernet 0
 ip address 10.20.40.1
!
interface serial 0
 ip address 172.16.1.1
 ip address 192.168.1.1 secondary
 encapsulation frame-relay
 no ip split-horizon
```

## Address Family Timers Example

The following example shows how to adjust individual address family timers.

Note that the address family “notusingtimers” will use the system defaults of 30, 180, 180, and 240 even though timer values of 5, 10, 15, and 20 are used under the general RIP configuration. Address family timers are not inherited from the general RIP configuration.

```
Router(config)#router rip
Router(config-router)# version 2
Router(config-router)# timers basic 5 10 15 20
Router(config-router)# redistribute connected
Router(config-router)# network 5.0.0.0
Router(config-router)# default-metric 10
Router(config-router)# no auto-summary
Router(config-router)#!
Router(config-router)# address-family ipv4 vrf foo
Router(config-router-af)# timers basic 10 20 20 20
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 10.0.0.0
Router(config-router-af)# default-metric 5
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)# !
Router(config-router)# address-family ipv4 vrf bar
Router(config-router-af)# timers basic 20 40 60 80
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#!
Router(config-router)# address-family ipv4 vrf notusingtimers
Router(config-router-af)# redistribute connected
Router(config-router-af)# network 20.0.0.0
Router(config-router-af)# default-metric 2
Router(config-router-af)# no auto-summary
Router(config-router-af)# version 2
Router(config-router-af)# exit-address-family
Router(config-router)#!
```