IP Routing: EIGRP Configuration Guide, Cisco IOS XE Fuji 16.9.x

Americas 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: 408 527-0883

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.

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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1 Read Me First 1

CHAPTER 2 EIGRP 3

Finding Feature Information 3

Information About Configuring EIGRP 3

EIGRP Features 3

EIGRP Autonomous System Configuration 4

EIGRP Named Configuration 4

EIGRP Neighbor Relationship Maintenance 4

Neighbor Authentication 5

DUAL Finite State Machine 5

Protocol-Dependent Modules 5

Goodbye Message 5

EIGRP Metric Weights 6

Mismatched K Values 6

Routing Metric Offset Lists 7

EIGRP Cost Metrics 7

Route Summarization 9

Summary Aggregate Addresses 9

Floating Summary Routes 9

Hello Packets and the Hold-Time Intervals 11

Split Horizon 12

EIGRP Dual DMVPN Domain Enhancement 12

Link Bandwidth Percentage 12

EIGRP vNETs 13

EIGRP vNET Interface and Command Inheritance 13

How to Configure EIGRP 14

Enabling EIGRP Autonomous System Configuration 14

Enabling the EIGRP Named Configuration 15

Configuring Optional EIGRP Parameters in an Autonomous System Configuration 16

Configuring Optional EIGRP Parameters in a Named Configuration 18

Configuring the EIGRP Redistribution Autonomous System Configuration 20

Configuring the EIGRP Route Summarization Autonomous System Configuration 22

Configuring the EIGRP Route Summarization Named Configuration 23

Configuring the EIGRP Event Logging Autonomous System Configuration 25

Configuring the EIGRP Event Logging Named Configuration 26

Configuring Equal and Unequal Cost Load Balancing Autonomous System Configuration 28

Configuring Equal and Unequal Cost Load Balancing Named Configuration 29

Adjusting the Interval Between Hello Packets and the Hold Time in an Autonomous System Configuration 31

Adjusting the Interval Between Hello Packets and the Hold Time in a Named Configuration 33

Disabling the Split Horizon Autonomous System Configuration 34

Disabling the Split Horizon and Next-Hop-Self Named Configuration 35

Monitoring and Maintaining the EIGRP Autonomous System Configuration 37

Monitoring and Maintaining the EIGRP Named Configuration 38

Configuration Examples for EIGRP 41

Example: Enabling EIGRP—Autonomous System Configuration 41

Example: Enabling EIGRP—Named Configuration 41

Example: EIGRP Parameters—Autonomous System Configuration 41

Example: EIGRP Parameters—Named Configuration 41

Example: EIGRP Redistribution—Autonomous System Configuration 42

Example: EIGRP Route Summarization—Autonomous System Configuration 42

Example: EIGRP Route Summarization—Named Configuration 42

Example: EIGRP Event Logging—Autonomous System Configuration 43

Example: EIGRP Event Logging—Named Configuration 43

Example: Equal and Unequal Cost Load Balancing—Autonomous System Configuration 43

Example: Equal and Unequal Cost Load Balancing—Named Configuration 44

Example: Adjusting the Interval Between Hello Packets and the Hold Time— Autonomous System Configuration 44

Example: Adjusting the Interval Between Hello Packets and the Hold Time—Named Configuration 44

Example: Disabling the Split Horizon—Autonomous System Configuration 44
Example: Disabling the Split Horizon and Next-Hop-Self—Named Configuration 45
Example: Command Inheritance and Virtual Network Interface Mode Override in an EIGRP Environment 45
Example: Monitoring and Maintaining the EIGRP Autonomous System Configuration 48
Example: Monitoring and Maintaining the EIGRP Named Configuration 50
Additional References for EIGRP 52
Feature Information for EIGRP 54

CHAPTER 3 IPv6 Routing: EIGRP Support 57
Finding Feature Information 57
Restrictions for IPv6 Routing EIGRP Support 57
Information About IPv6 Routing EIGRP Support 58
Cisco EIGRP for IPv6 Implementation 58
How to Configure IPv6 Routing EIGRP Support 59
Enabling EIGRP for IPv6 on an Interface 59
Configuring the Percentage of Link Bandwidth Used by EIGRP 61
Configuring Summary Addresses 62
Configuring EIGRP Route Authentication 63
Overriding the Next Hop in EIGRP 65
Adjusting the Interval Between Hello Packets in EIGRP for IPv6 66
Adjusting the Hold Time in EIGRP for IPv6 67
Disabling Split Horizon in EIGRP for IPv6 68
Configuring EIGRP Stub Routing for Greater Network Stability 69
Configuring a Device for EIGRP Stub Routing 69
Verifying EIGRP Stub Routing 70
Customizing an EIGRP for IPv6 Routing Process 70
Logging EIGRP Neighbor Adjacency Changes 70
Configuring Intervals Between Neighbor Warnings 71
Adjusting EIGRP for IPv6 Metric Weights 72
Deleting Entries from EIGRP for IPv6 Routing Tables 73
Configuration Examples for IPv6 Routing EIGRP Support 74
Example: Configuring EIGRP to Establish Adjacencies on an Interface 74
Additional References 74

Feature Information for IPv6 Routing: EIGRP Support 75

CHAPTER 4 EIGRP MIB 79

Finding Feature Information 79

Prerequisites for EIGRP MIB 79

Restrictions for EIGRP MIB 80

Information About EIGRP MIB 80

EIGRP MIB Overview 80

EIGRP Interface Table 80

EIGRP Neighbor Table 81

EIGRP Topology Table 82

EIGRP Traffic Statistics Table 83

EIGRP VPN Table 85

EIGRP Notifications 85

How to Enable EIGRP MIB 86

Enabling EIGRP MIB Notifications 86

Configuration Examples for EIGRP MIB 87

Example: Enabling EIGRP MIB Notifications 87

Additional References for EIGRP MIB 88

Feature Information for EIGRP MIB 89

CHAPTER 5 EIGRP MPLS VPN PE-CE Site of Origin 91

Finding Feature Information 91

Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin 91

Restrictions for EIGRP MPLS VPN PE-CE Site of Origin 92

Information About EIGRP MPLS VPN PE-CE Site of Origin 92

EIGRP MPLS VPN PE-CE Site of Origin Support Overview 92

Site of Origin Support for Backdoor Links 92

Router Interoperation with the Site of Origin Extended Community 93

Redistribution of BGP VPN Routes That Carry the Site of Origin into EIGRP 93

BGP Cost Community Support for EIGRP MPLS VPN PE-CE Network Topologies 94

Benefits of the EIGRP MPLS VPN PE-CE Site of Origin Support Feature 94

How to Configure EIGRP MPLS VPN PE-CE Site of Origin Support 94

Configuring the Site of Origin Extended Community 94

What to Do Next 96
Verifying the Configuration of the SoO Extended Community 97
Configuration Examples for EIGRP MPLS VPN PE-CE SoO 97
Example Configuring the Site of Origin Extended Community 97
Example Verifying the Site of Origin Extended Community 98
Additional References 98
Feature Information for EIGRP MPLS VPN PE-CE Site of Origin 99
Glossary 100

CHAPTER 6 EIGRP Nonstop Forwarding Awareness 101
Finding Feature Information 101
Prerequisites for EIGRP Nonstop Forwarding Awareness 101
Restrictions for EIGRP Nonstop Forwarding Awareness 102
Information About EIGRP Nonstop Forwarding Awareness 102
Cisco NSF Routing and Forwarding Operation 102
Cisco Express Forwarding 102
EIGRP Nonstop Forwarding Awareness 103
EIGRP NSF-Capable and NSF-Aware Interoperation 103
Non-NSF Aware EIGRP Neighbors 104
EIGRP NSF Timers 104
How to Configure EIGRP Nonstop Forwarding Awareness 105
Enabling EIGRP Nonstop Forwarding Awareness 105
Modifying EIGRP Nonstop Forwarding Awareness Timers 106
Troubleshooting Tips 107
Monitoring EIGRP NSF Debug Events and Notifications 107
Verifying the Local Configuration of EIGRP NSF Awareness 108
Configuration Examples for EIGRP Nonstop Forwarding Awareness 109
Example: EIGRP Graceful-Restart Purge-Time Timer Configuration 109
Example: Monitoring EIGRP NSF Debug Events and Notifications Configuration 109
Example: Verifying Local Configuration of EIGRP NSF Awareness 109
Additional References for EIGRP Nonstop Forwarding Awareness 110
Feature Information for EIGRP Nonstop Forwarding Awareness 110

CHAPTER 7 EIGRP Nonstop Forwarding 113

Finding Feature Information 113
Prerequisites for EIGRP Nonstop Forwarding 113
Restrictions for EIGRP Nonstop Forwarding 114
Information About EIGRP Nonstop Forwarding 114
Nonstop Forwarding 114
EIGRP NSF Operations 115
How to Configure EIGRP Nonstop Forwarding 116
Configuring and Verifying EIGRP NSF 116
Troubleshooting EIGRP Nonstop Forwarding 117
Configuration Examples for EIGRP Nonstop Forwarding 119
Example: EIGRP NSF 119
Additional References 119
Feature Information for EIGRP Nonstop Forwarding 121

CHAPTER 8 EIGRP IPv6 NSF/GR 123
Finding Feature Information 123
Prerequisites for EIGRP IPv6 NSF/GR 123
Restrictions for EIGRP IPv6 NSF/GR 124
Information About EIGRP IPv6 NSF/GR 124
EIGRP IPv6 NSF/GR 124
EIGRP IPv6 NSF Timers 124
How to Configure EIGRP IPv6 NSF/GR 125
Enabling EIGRP IPv6 NSF/GR 125
Modifying EIGRP IPv6 NSF Timers 126
Verifying the EIGRP IPv6 NSF/GR Configuration 127
Monitoring EIGRP IPv6 NSF/GR Events 128
Configuration Examples for EIGRP IPv6 NSF/GR 128
Example: Configuring an EIGRP NSF Converge Timer 128
Example: Verifying the Configuration of EIGRP IPv6 NSF/GR on an NSF-Aware Device 129
Additional References for EIGRP IPv6 NSF/GR 129
Feature Information for EIGRP IPv6 NSF/GR 130

CHAPTER 9 EIGRP Prefix Limit Support 133
Finding Feature Information 133

Prerequisites for EIGRP Prefix Limit Support 133

Restrictions for EIGRP Prefix Limit Support 134

Information About EIGRP Prefix Limit Support 134

Misconfigured VPN Peers 134

EIGRP Prefix Limit Support Overview 134

External Peer Router Protection 134

Redistributed Prefix Number Limiting 134

EIGRP Process Level Router Protection 135

EIGRP Prefix Limiting Warning-Only Mode 135

EIGRP Prefix Limiting Restart Reset and Dampening Timers and Counters 135

Restart Timer 135

Restart Counter 135

Reset Timer 135

Dampening Mechanism 136

How to Configure the Maximum-Prefix Limit 136

Configuring the Maximum Number of Prefixes Accepted from Peering Sessions Autonomous System Configuration 136

Troubleshooting Tips 138

Configuring the Maximum Number of Prefixes Accepted from Peering Sessions Named Configuration 138

Troubleshooting Tips 140

Configuring the Maximum Number of Prefixes Learned Through Redistribution Autonomous System Configuration 140

Troubleshooting Tips 142

Configuring the Maximum Number of Prefixes Learned Through Redistribution Named Configuration 142

Troubleshooting Tips 144

Configuring the Maximum-Prefix Limit for an EIGRP Process Autonomous System Configuration 144

Troubleshooting Tips 145

Configuring the Maximum-Prefix Limit for an EIGRP Process Named Configuration 146

Troubleshooting Tips 148

Configuration Examples for Configuring the Maximum-Prefix Limit 148

Example Configuring the Maximum-Prefix Limit for a Single Peer--Autonomous System Configuration 148

Example Configuring the Maximum-Prefix Limit for a Single Peer--Named Configuration 148
Example Configuring the Maximum-Prefix Limit for All Peers--Autonomous System Configuration 148
Example Configuring the Maximum-Prefix Limit for All Peers--Named Configuration 149
Example Configuring the Maximum-Prefix Limit for Redistributed Routes--Autonomous System Configuration 149
Example Configuring the Maximum-Prefix Limit for Redistributed Routes--Named Configuration 149
Example Configuring the Maximum-Prefix Limit for an EIGRP Process--Autonomous System Configuration 150
Example Configuring the Maximum-Prefix Limit for an EIGRP Process--Named Configuration 150
Additional References 150
Feature Information for EIGRP Prefix Limit Support 152

CHAPTER 10 **EIGRP Support for Route Map Filtering** 153
Finding Feature Information 153
Information About EIGRP Support for Route Map Filtering 153
EIGRP Route Map Support 153
How to Configure EIGRP Support for Route Map Filtering 154
Setting EIGRP Tags Using a Route Map for Autonomous System Configurations 154
Setting EIGRP Tags Using a Route Map for Named Configurations 156
Configuring EIGRP Route-map for Distribute-list in IPv6 160
Configuration Examples for EIGRP Support for Route Map Filtering 164
Example Setting EIGRP Tags Using a Route Map--Autonomous System Configuration Examples 164
Example Setting EIGRP Tags Using a Route Map--Named Configuration Examples 164
Example Configuring EIGRP Route-map for Distribute-list in IPv6 165
Additional References 165
Feature Information for EIGRP Support for Route Map Filtering 166

CHAPTER 11 **EIGRP Route Tag Enhancements** 169
Finding Feature Information 169
Restrictions for EIGRP Route Tag Enhancements 169
Information About EIGRP Route Tag Enhancements 170

EIGRP Route Tag Enhancements Overview 170

How to Configure EIGRP Route Tag Enhancements 170

Enabling Dotted-Decimal Notation for Route Tags 170

Setting a Route Tag in a Route Map 171

Matching a Route Tag in a Route Map 172

Creating a Route Tag List 173

Matching a Route Tag List 174

Setting a Default Route Tag for EIGRP Internal Routes 175

Configuration Examples for EIGRP Route Tag Enhancements 177

Example: Enabling Dotted-Decimal Notation for Route Tags 177

Example: Setting a Route Tag 177

Example: Matching a Route Tag 178

Example: Configuring a Route Tag List 178

Example: Matching a Route Tag List 178

Example: Setting a Default Route Tag 179

Additional References 179

Feature Information for EIGRP Route Tag Enhancements 179

CHAPTER 12 **BFD Support for EIGRP IPv6** 181

Finding Feature Information 181

Prerequisites for BFD Support for EIGRP IPv6 181

Restrictions for BFD Support for EIGRP IPv6 182

Information About BFD Support for EIGRP IPv6 182

BFD for EIGRP IPv6 182

How to Configure BFD Support for EIGRP IPv6 182

Configuring BFD Support on All Interfaces 182

Configuring BFD Support on an Interface 184

Configuration Examples for BFD Support for EIGRP IPv6 186

Example: Configuring BFD Support on All Interfaces 186

Example: Configuring BFD Support on an Interface 187

Additional References 187

Feature Information for BFD Support for EIGRP IPv6 188

CHAPTER 13 **EIGRP Loop-Free Alternate Fast Reroute** 189

Finding Feature Information 189
Restrictions for EIGRP Loop-Free Alternate Fast Reroute 189
Information About EIGRP Loop-Free Alternate Fast Reroute 190
Repair Paths Overview 190
LFA Computation 190
LFA Tie-Breaking Rules 191
How to Configure EIGRP Loop-Free Alternate Fast Reroute 191
Configuring LFA FRRs per Prefix 191
Disabling Load Sharing Among Prefixes 192
Enabling Tie-Breaking Rules for EIGRP LFAs 194
Configuration Examples for EIGRP Loop-Free Alternate Fast Reroute 195
Example: Configuring LFA FRRs Per Prefix 195
Example: Disabling Load Sharing Among Prefixes 195
Example: Enabling Tie-Breaking Rules 196
Additional References 196
Feature Information for EIGRP Loop-Free Alternate Fast Reroute 197

CHAPTER 14 **Add Path Support in EIGRP** 199
Finding Feature Information 199
Prerequisites for Add Path Support in EIGRP 199
Restrictions for Add Path Support in EIGRP 200
Information About Add Path Support in EIGRP 200
EIGRP Add Path Support Overview 200
How Add Path Support in EIGRP Works 200
How to Configure Add Path Support in EIGRP 202
Configuring IPv4 Add Path Support on a Hub 202
Configuring IPv6 Add Path Support on a Hub 203
Configuration Examples for Add Path Support in EIGRP 205
Example: Configuring IPv4 Add Path Support on a Hub 205
Example: Configuring IPv6 Add Path Support on a Hub 205
Additional References for Add Path Support in EIGRP 205
Feature Information for Add Path Support in EIGRP 206

CHAPTER 15 **EIGRP Wide Metrics** 207

Information About EIGRP Wide Metrics 207

EIGRP Composite Cost Metrics 207

EIGRP Wide Metrics 208

EIGRP Metric Weights 209

Mismatched K Values 210

Additional References 211

Feature Information for EIGRP Wide Metrics 211

CHAPTER 16 **EIGRP/SAF HMAC-SHA-256 Authentication** 213

Finding Feature Information 213

Information About EIGRP/SAF HMAC-SHA-256 Authentication 213

EIGRP Neighbor Relationship Maintenance 213

HMAC-SHA-256 Authentication 214

How to Configure EIGRP/SAF HMAC-SHA-256 Authentication 215

Configuring HMAC-SHA-256 Authentication 215

Configuration Examples for EIGRP/SAF HMAC-SHA-256 Authentication 217

Example: Configuring HMAC-SHA-256 Authentication 217

Additional References 217

Feature Information for EIGRP/SAF HMAC-SHA-256 Authentication 218

CHAPTER 17 **IP EIGRP Route Authentication** 219

Finding Feature Information 219

Information About IP EIGRP Route Authentication 219

EIGRP Route Authentication 219

How to Configure IP EIGRP Route Authentication 220

Defining an Autonomous System for EIGRP Route Authentication 220

Defining a Named Configuration for EIGRP Route Authentication 222

Configuration Examples for IP EIGRP Route Authentication 225

Example: EIGRP Route Authentication—Autonomous System Definition 225

Example: EIGRP Route Authentication—Named Configuration 226

Additional References 227

Feature Information for IP EIGRP Route Authentication 228

CHAPTER 18 **EIGRP IPv6 VRF-Lite** 229

Finding Feature Information 229
Information About EIGRP IPv6 VRF-Lite 229
VRF-Lite for EIGRP IPv6 229
EIGRP Named Configuration 230
How to Configure EIGRP IPv6 VRF-Lite 230
Enabling the EIGRP IPv6 VRF-Lite Named Configuration 230
Configuration Examples for EIGRP IPv6 VRF-Lite 231
Example: Enabling EIGRP IPv6 VRF-Lite—Named Configuration 231
Additional References 232
Feature Information for EIGRP IPv6 VRF-Lite 232

CHAPTER 19 EIGRP Stub Routing 235
Finding Feature Information 235
Information About EIGRP Stub Routing 235
EIGRP Stub Routing 235
Dual-Homed Remote Topology 237
How to Configure EIGRP Stub Routing 239
Configuring the EIGRP Stub Routing Autonomous System Configuration 239
Configuring the EIGRP Stub Routing Named Configuration 240
Configuration Examples for EIGRP Stub Routing 242
Example: EIGRP Stub Routing—Autonomous System Configuration 242
Example: eigrp stub Command 242
Example: eigrp stub connected static Command 243
Example: eigrp stub leak-map Command 243
Example: eigrp stub receive-only Command 243
Example: eigrp stub redistributed Command 243
Example: EIGRP Stub Routing—Named Configuration 243
Example: eigrp stub Command 244
Example: eigrp stub connected static Command 244
Example: eigrp stub leak-map Command 244
Example: eigrp stub receive-only Command 244
Example: eigrp stub redistributed Command 245
Additional References 245
Feature Information for EIGRP Stub Routing 246

CHAPTER 20 **EIGRP Support for 6PE/6VPE** 247

Finding Feature Information 247

Information About EIGRP Support for 6PE/6VPE 247

BGP Extended Communities 247

Preserving Route Metrics 248

EIGRP 6PE/6VPE SoO 248

Backdoor Devices 249

Additional References for EIGRP Support for 6PE/6VPE 250

Feature Information For EIGRP Support for 6PE/6VPE 250

CHAPTER 21 **EIGRP Over the Top** 253

Finding Feature Information 253

Information About EIGRP Over the Top 253

EIGRP Over the Top Overview 253

How EIGRP Over the Top Works 254

Security Groups and SGTs 254

EIGRP OTP Support to Propagate SGT 255

How to Configure EIGRP Over the Top 255

Configuring EIGRP Over the Top on a CE Device 255

Configuring EIGRP Route Reflectors 256

Configuring EIGRP OTP Support to Propagate SGT 258

Configuration Examples for EIGRP Over the Top 259

Example: Configuring EIGRP Over the Top on a CE Device 259

Example: Configuring EIGRP Route Reflectors 259

Example: Configuring EIGRP OTP Support to Propagate SGT 260

Feature Information for EIGRP Over the Top 260

CHAPTER 22 **EIGRP OTP VRF Support** 261

Prerequisites for EIGRP OTP VRF Support 261

Restrictions for EIGRP OTP VRF Support 261

Information About EIGRP OTP VRF Support 261

Overview of EIGRP OTP VRF Support 261

How EIGRP OTP VRF Support Works 262

Data Encapsulation 262

Interfaces and Topology Command 262

Differences between EIGRP OTP Feature and EIGRP OTP VRF Support Feature 263

How to Configure EIGRP OTP VRF Support 263

Configuring EIGRP OTP VRF Support on a CE Device 263

Configuring EIGRP OTP VRF Support on EIGRP Route Reflectors 266

Configuration Examples for EIGRP OTP VRF Support 267

Example: Configuring EIGRP OTP VRF Support on a CE Device 267

Example: Configuring EIGRP OTP VRF Support on EIGRP Route Reflectors 267

Additional References for EIGRP OTP VRF Support 268

Feature Information for Configuring EIGRP OTP VRF Support 268

CHAPTER 23 **EIGRP Classic to Named Mode Conversion** 269

Finding Feature Information 269

Restrictions for EIGRP Classic to Named Mode Conversions 269

Information About EIGRP Classic to Named Mode Conversion 270

EIGRP Classic to Named Mode Conversion - Overview 270

Additional References for EIGRP Classic to Named Mode 271

Feature Information for EIGRP Classic to Named Mode Conversion 271

CHAPTER 24 **EIGRP Scale for DMVPN** 273

Finding Feature Information 273

Information About EIGRP Scale for DMVPN 273

EIGRP Scale for DMVPN Overview 273

Additional References for EIGRP Scale for DMVPN 274

Feature Information for EIGRP Scale for DMVPN 274

CHAPTER 25 **EIGRP IWAN Simplification** 275

Finding Feature Information 275

Information About EIGRP IWAN Simplification 275

Stub Site ID Configuration 275

How to Configure EIGRP IWAN Simplification 276

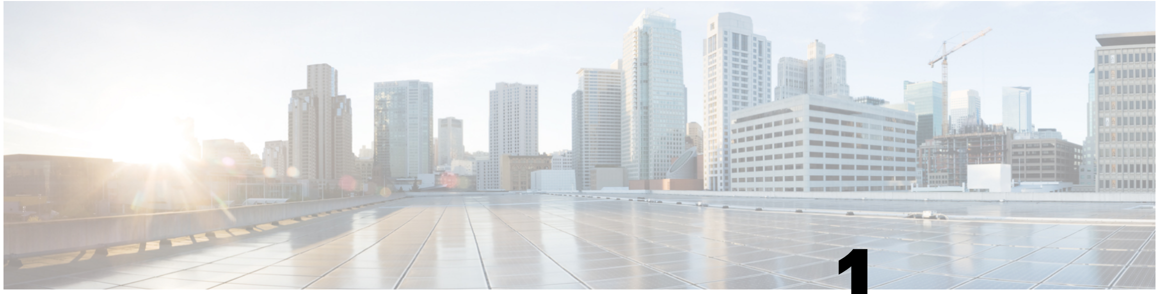
Configuring the Stub Site ID 276

Configuration Examples for EIGRP IWAN Simplification 278

  Example: Configuring the Stub Site ID 278

Additional References for EIGRP IWAN Simplification 278

Feature Information for EIGRP IWAN Simplification 279



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

CHAPTER 2

EIGRP

The Enhanced Interior Gateway Routing Protocol (EIGRP) is an enhanced version of the Interior Gateway Routing Protocol (IGRP) developed by Cisco. The convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP, and IGRP is now obsolete.

The convergence technology of EIGRP is based on an algorithm called the Diffusing Update Algorithm (DUAL). The algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize. Devices that are not affected by topology changes are not involved in recomputations.

- Finding Feature Information, on page 3
- Information About Configuring EIGRP, on page 3
- How to Configure EIGRP, on page 14
- Configuration Examples for EIGRP, on page 41
- Additional References for EIGRP, on page 52
- Feature Information for EIGRP, on page 54

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Configuring EIGRP

EIGRP Features

- 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 EIGRP metric is large enough to support thousands of hops.

- 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.
- Neighbor discovery mechanism--This simple protocol-independent hello mechanism is used to learn about neighboring devices.
- Scaling--EIGRP scales to large networks.

EIGRP Autonomous System Configuration

Configuring the **router eigrp** command with the *autonomous-system-number* argument creates an EIGRP configuration called the EIGRP autonomous system configuration, or EIGRP classic mode. The EIGRP autonomous system configuration creates an EIGRP routing instance that can be used for exchanging routing information.

In EIGRP autonomous system configurations, EIGRP VPNs can be configured only under IPv4 address family configuration mode. A virtual routing and forwarding (VRF) instance and a route distinguisher must be defined before the address family session can be created.

When the address family is configured, we recommend that you configure an autonomous system number either by using the *autonomous-system-number* argument with the **address-family** command or by using the **autonomous-system** command.

EIGRP Named Configuration

Configuring the **router eigrp** command with the *virtual-instance-name* argument creates an EIGRP configuration referred to as the EIGRP named configuration or EIGRP named mode. An EIGRP named configuration does not create an EIGRP routing instance by itself; it is a base configuration that is required to define address-family configurations that are used for routing.

In EIGRP named configurations, EIGRP VPNs can be configured in IPv4 and IPv6 named configurations. A VRF instance and a route distinguisher must be defined before the address family session can be created.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited only by the available system resources on the device, which is determined by the number running processes and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

EIGRP Neighbor Relationship Maintenance

Neighbor relationship maintenance is the process that devices use to dynamically learn of other devices on their directly attached networks. Devices must also discover when their neighbors become unreachable or inoperative. Neighbor relationship maintenance is achieved with low overhead by devices when they periodically send small hello packets to each other. As long as hello packets are received, the Cisco software can determine whether a neighbor is alive and functioning. After the status of the neighbor is determined, neighboring devices can exchange routing information.

The reliable transport protocol is responsible for the guaranteed, ordered delivery of Enhanced Interior Gateway Routing Protocol (EIGRP) packets to all neighbors. The reliable transport protocol supports intermixed transmission of multicast and unicast packets. Some EIGRP packets (such as updates) must be sent reliably; this means that the packets require acknowledgment from the destination. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities, hello packets need not be sent reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello packet with an indication in the packet informing receivers that the packet need not be acknowledged. The reliable transport protocol can send multicast packets quickly when unacknowledged packets are pending, thereby ensuring that the convergence time remains low in the presence of varying speed links.

Some EIGRP remote unicast-listen (any neighbor that uses unicast to communicate) and remote multicast-group neighbors may peer with any device that sends a valid hello packet, thus causing security concerns. By authenticating the packets that are exchanged between neighbors, you can ensure that a device accepts packets only from devices that know the preshared authentication key.

Neighbor Authentication

The authentication of packets being sent between neighbors ensures that a device accepts packets only from devices that have the same preshared key. If this authentication is not configured, you can intentionally or accidentally add another device to the network or send packets with different or conflicting route information onto the network, resulting in topology corruption and denial of service (DoS).

Enhanced Interior Gateway Routing Protocol (EIGRP) authentication is configurable on a per-interface basis; packets exchanged between neighbors connected through an interface are authenticated. EIGRP supports message digest algorithm 5 (MD5) authentication to prevent the introduction of unauthorized information from unapproved sources. MD5 authentication is defined in RFC 1321.

DUAL Finite State Machine

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 the 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 device (used for packet forwarding) that has the least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors but only neighbors advertising the destination, a recomputation must occur to determine a new successor. The time required to recompute the route affects the convergence time. Recomputation is processor-intensive, and unnecessary recomputation must be avoided. When a topology change occurs, DUAL will test for feasible successors. If there are feasible successors, DUAL will use any feasible successors it finds to avoid unnecessary recomputation.

Protocol-Dependent Modules

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 the IP. The EIGRP module is also responsible for parsing EIGRP packets and informing DUAL about 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 from other IP routing protocols.

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 shut down to inform adjacent peers about an 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 following message is displayed by devices 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 device 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 error 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 terminates the session when the hold timer expires. The sending and receiving devices reconverge normally after the sender reloads.

EIGRP Metric Weights

You can use the **metric weights** command to adjust the default behavior of Enhanced Interior Gateway Routing Protocol (EIGRP) routing and metric computations. EIGRP metric defaults (K values) 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 K values without guidance from an experienced network designer.

By default, the EIGRP composite cost metric is a 32-bit quantity that is the sum of segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. The formula used to scale and invert the bandwidth value is 10^7/minimum bandwidth in kilobits per second. However, with the EIGRP Wide Metrics feature, the EIGRP composite cost metric is scaled to include 64-bit metric calculations for EIGRP named mode configurations.

For a network of homogeneous media, this metric reduces to a hop count. For a network of mixed media (FDDI, Gigabit Ethernet (GE), 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

EIGRP K values are the metrics that EIGRP uses to calculate routes. Mismatched K values can prevent neighbor relationships from being established and can negatively impact network convergence. The example given below explains this behavior between two EIGRP peers (Device-A and Device-B).

The following configuration is applied to Device-A. The K values are changed using the **metric weights** command. A value of 2 is entered for the *k1* argument to adjust the bandwidth calculation. A value of 1 is entered for the *k3* argument to adjust the delay calculation.

```
Device(config)# hostname Device-A
Device-A(config)# interface serial 0
Device-A(config-if)# ip address 10.1.1.1 255.255.255.0
Device-A(config-if)# exit
Device-A(config)# router eigrp name1
Device-A(config-router)# address-family ipv4 autonomous-system 4533
Device-A(config-router-af)# network 10.1.1.0 0.0.0.255
Device-A(config-router-af)# metric weights 0 2 0 1 0 0 1
```

The following configuration is applied to Device-B, and the default K values are used. The default K values are 1, 0, 1, 0, 0, and 0.

```
Device(config)# hostname Device-B
Device-B(config)# interface serial 0
Device-B(config-if)# ip address 10.1.1.2 255.255.255.0
Device-B(config-if)# exit
Device-B(config)# router eigrp name1
Device-B(config-router)# address-family ipv4 autonomous-system 4533
Device-B(config-router-af)# network 10.1.1.0 0.0.0.255
Device-B(config-router-af)# metric weights 0 1 0 1 0 0 0
```

The bandwidth calculation is set to 2 on Device-A and set to 1 (by default) on Device-B. This configuration prevents these peers from forming a neighbor relationship.

The following error message is displayed on the console of Device-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
```

The following are two scenarios where the above error message can be displayed:

- Two devices are connected on the same link and configured to establish a neighbor relationship. However, each device is configured with different K values.
- One of two peers has transmitted a "peer-termination" message (a message that is broadcast when an EIGRP routing process is shut down), and the receiving device does not support this message. The receiving device will interpret this message as a K-value mismatch.

Routing Metric Offset Lists

An offset list is a mechanism for increasing incoming and outgoing metrics to routes learned via EIGRP. Optionally, you can limit the offset list with either an access list or an interface.

Note Offset lists are available only in IPv4 configurations. IPv6 configurations do not support offset lists.

EIGRP Cost Metrics

When EIGRP receives dynamic raw radio link characteristics, it computes a composite EIGRP cost metric based on a proprietary formula. To avoid churn in the network as a result of a change in the link characteristics, a tunable dampening mechanism is used.

EIGRP uses metric weights along with a set of vector metrics to compute the composite metric for local RIB installation and route selections. The EIGRP composite cost metric is calculated using the formula:

EIGRP composite cost metric = 256*((K1*Bw) + (K2*Bw)/(256 – Load) + (K3*Delay)*(K5/(Reliability + K4)))

EIGRP uses one or more vector metrics to calculate the composite cost metric. The table below lists EIGRP vector metrics and their descriptions.

Table 1: EIGRP Vector Metrics

Vector Metric	Description
bandwidth	The minimum bandwidth of the route, in kilobits per second. It can be 0 or any positive integer. The bandwidth for the formula is scaled and inverted by the following formula: (10^7/minimum bandwidth (Bw) in kilobits per second)
delay	Route delay, in tens of microseconds.
delay reliability	The likelihood of successful packet transmission, expressed as a number between 0 and 255, where 255 means 100 percent reliability and 0 means no reliability.
load	The effective load of the route, expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	The minimum maximum transmission unit (MTU) size of the route, in bytes. It can be 0 or any positive integer.

EIGRP monitors metric weights on an interface to allow the tuning of EIGRP metric calculations and indicate the type of service (ToS). The table below lists the K values and their defaults.

Table 2: EIGRP K-Value Defaults

Setting	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

Most configurations use the delay and bandwidth metrics, with bandwidth taking precedence. The default formula of 256*(Bw + Delay) is the EIGRP metric. The bandwidth for the formula is scaled and inverted by the following formula:

(10^7/minimum Bw in kilobits per second)

Note You can change the weights, but these weights must be the same on all devices.

For example, look at a link whose bandwidth to a particular destination is 128 k and the delay is 84,000 microseconds.

By using a cut-down formula, you can simplify the EIGRP metric calculation to 256*(Bw + Delay), thus resulting in the following value:

Metric = 256*(10^7/128 + 84000/10) = 256*86525 = 22150400

To calculate route delay, divide the delay value by 10 to get the true value in tens of microseconds.

When EIGRP calculates the delay for Mobile Ad Hoc Networks (MANET) and the delay is obtained from a device interface, the delay is always calculated in tens of microseconds. In most cases, when using MANET, you will not use the interface delay, but rather the delay that is advertised by the radio. The delay you will receive from the radio is in microseconds, so you must adjust the cut-down formula as follows:

Metric = (256*(10^7/128) + (84000*256)/10) = 20000000 + 2150400 = 22150400

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 been configured with subnets of 192.168.7.0. Automatic summarization is performed when two or more **network** router configuration or address family configuration commands are configured for an EIGRP process. This feature is enabled by default.

Route summarization works in conjunction with the **ip summary-address eigrp** command available in interface configuration mode for autonomous system configurations and with the **summary-address** (EIGRP) command for named configurations. You can use these commands to perform additional summarization. If automatic summarization is in effect, there usually is no need to configure network-level summaries using the **ip summary-address eigrp** command.

Summary Aggregate Addresses

You can configure a summary aggregate address for a specified interface. If there are specific routes in the routing table, EIGRP will advertise the summary address of the interface with a metric equal to the minimum metric of the specific routes.

Floating Summary Routes

A floating summary route is created by applying a default route and an administrative distance at the interface level or address family interface level. You can use a floating summary route when configuring the **ip summary-address eigrp** command for autonomous system configurations or the **summary-address** command for named configurations. The following scenarios illustrate the behavior of floating summary routes.

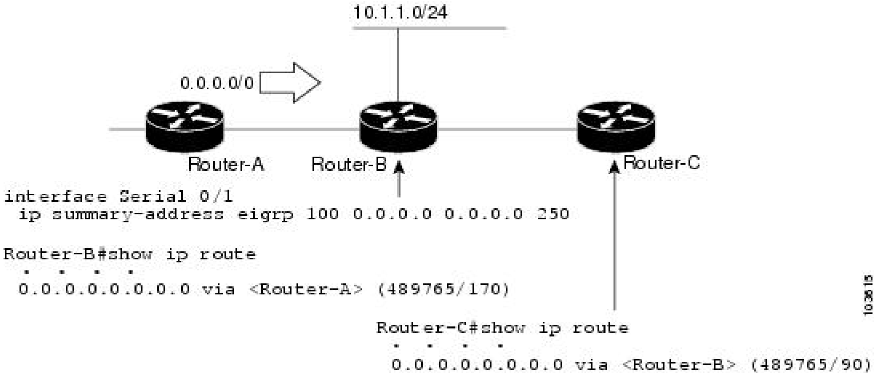
The figure below shows a network with three devices, Device-A, Device-B, and Device-C. Device-A learns a default route from elsewhere in the network and then advertises this route to Device-B. Device-B is configured so that only a default summary route is advertised to Device-C. The default summary route is applied to serial interface 0/1 on Device-B with the following autonomous system configuration:

```
Device-B(config)# interface Serial 0/1
Device-B(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
```

The default summary route is applied to serial interface 0/1 on Device-B with the following named configuration:

```
Device-B(config)# Router eigrp virtual-name1
Device-B(config-router)# address-family ipv4 unicast vrf vrf1 autonomous-system 1
Device-B(config-router-af)# interface serial 0/1
Device-B(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0 95
```

Figure 1: Floating Summary Route Applied to Device-B



```
interface Serial 0/1
 ip summary-address eigrp 100 0.0.0.0 0.0.0.0 250

Router-B#show ip route
  .   .   .   .
 0.0.0.0.0.0.0.0 via <Router-A> (489765/170)
```

```
Router-C#show ip route
  .   .   .   .
 0.0.0.0.0.0.0.0 via <Router-B> (489765/90)
```

The configuration of the default summary route on Device-B sends a 0.0.0.0/0 summary route to Device-C and blocks all other routes, including the 10.1.1.0/24 route, from being advertised to Device-C. However, this configuration also generates a local discard route—a route for 0.0.0.0/0 on the null 0 interface with an administrative distance of 5—on Device-B. When this route is created, it overrides the EIGRP-learned default route. Device-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 Device-B that connects to Device-C. The floating summary route is applied by configuring an administrative distance for the default summary route on the interface of Device-B with the following statement for an autonomous system configuration:

```
Device-B(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0 250
```

The floating summary route is applied by configuring an administrative distance for the default summary route on the interface of Device-B with the following statement for a named configuration:

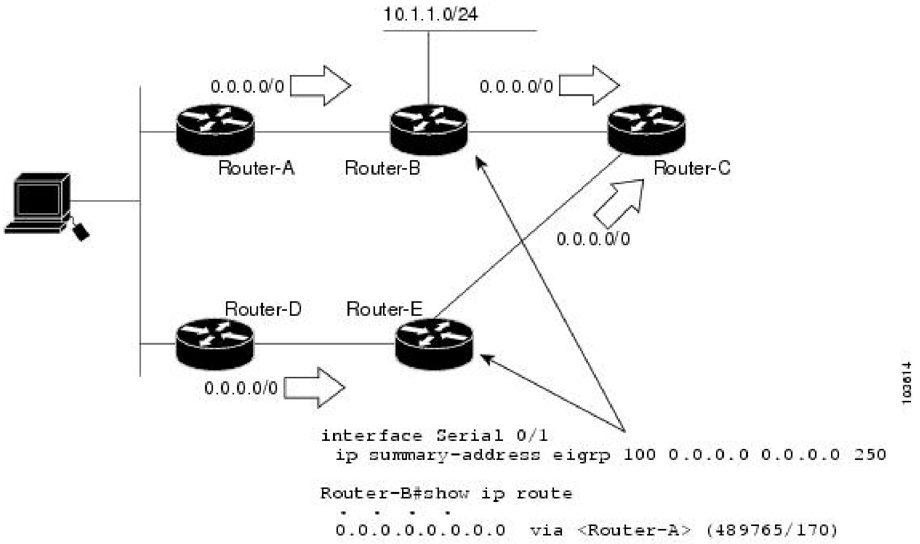
```
Device-B(config)# router eigrp virtual-name1
Device-B(config-router)# address-family ipv4 unicast vrf vrf1 autonomous-system 1
Device-B(config-router-af)# af-interface serial0/1
Device-B(config-router-af-interface)# summary-address eigrp 100 0.0.0.0 0.0.0.0 250
```

The administrative distance of 250, applied in the **summary-address** command, is now assigned to the discard route generated on Device-B. The 0.0.0.0/0, from Device-A, is learned through EIGRP and installed in the local routing table. Routing to Device-C is restored.

If Device-A loses the connection to Device-B, Device-B will continue to advertise a default route to Device-C, which allows traffic to continue to reach destinations attached to Device-B. However, traffic destined to networks connected to Device-A or behind Device-A will be dropped when the traffic reaches Device-B.

The figure below shows a network with two connections from the core, Device-A and Device-D. Both Device-B and Device-E have floating summary routes configured on the interfaces connected to Device-C. If the connection between Device-E and Device-C fails, the network will continue to operate normally. All traffic will flow from Device-C through Device-B to hosts attached to Device-A and Device-D.

Figure 2: Floating Summary Route Applied for Dual-Homed Remotes



```
interface Serial 0/1
 ip summary-address eigrp 100 0.0.0.0 0.0.0.0 250

Router-B#show ip route
 .  .  .  .
 0.0.0.0.0.0.0.0  via <Router-A> (489765/170)
```

However, if the link between Device-A and Device-B fails, the network may incorrectly direct traffic because Device-B will continue to advertise the default route (0.0.0.0/0) to Device-C. In this scenario, Device-C still forwards traffic to Device-B, but Device-B drops the traffic. To avoid this problem, you should configure the summary address with an administrative distance only on single-homed remote devices or areas that have only one exit point between two 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 result in the formation of a black hole route (a route that has quick packet dropping capabilities).

Hello Packets and the Hold-Time Intervals

You can adjust the interval between hello packets and the hold time. Hello packets and hold-time intervals are protocol-independent parameters that work for IP and Internetwork Packet Exchange (IPX).

Routing devices periodically send hello packets to each other to dynamically learn of other devices 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 only if the interface has not been configured to use physical multicasting.

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.

On very congested and large networks, the default hold time might not be sufficient for all devices to receive hello packets from their neighbors. In such cases, you may want to increase the hold time.

Note Do not adjust the hold time without informing your technical support personnel.

Split Horizon

Split horizon controls the sending of EIGRP update and query packets. Split horizon is a protocol-independent parameter that works for IP and IPX. When split horizon is enabled on an interface, update and query packets are not sent to 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 device 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. In such situations and in networks that have EIGRP configured, you may want to disable split horizon.

EIGRP Dual DMVPN Domain Enhancement

The EIGRP Dual DMVPN Domain Enhancement feature supports the **no next-hop self** command on dual Dynamic Multipoint VPN (DMVPN) domains in both IPv4 and IPv6 configurations.

EIGRP, by default, sets the local outbound interface as the next-hop value while advertising a network to a peer, even when advertising routes out of the interface on which the routes were learned. This default setting can be disabled by using the **no ip next-hop-self** command in autonomous system configurations or the **no next-hop-self** command in named configurations. When the **next-hop self** command is disabled, EIGRP does not advertise the local outbound interface as the next hop if the route has been learned from the same interface. Instead, the received next-hop value is used to advertise learned routes. However, this functionality only evaluates the first entry in the EIGRP table. If the first entry shows that the route being advertised is learned on the same interface, then the received next hop is used to advertise the route. The **no next-hop-self** configuration ignores subsequent entries in the table, which may result in the **no-next-hop-self** configuration being dishonored on other interfaces.

The EIGRP Dual DMVPN Domain Enhancement feature introduces the **no-ecmp-mode** keyword, which is an enhancement to the **no next-hop-self** and **no ip next-hop-self** commands. When this keyword is used, all routes to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface. If a route advertised by an interface was learned on the same interface, the **no next-hop-self** configuration is honored and the received next hop is used to advertise this route.

Link Bandwidth Percentage

By default, EIGRP packets consume a maximum of 50 percent of the link bandwidth when configured with the **bandwidth** interface configuration command for autonomous system configurations and with the **bandwidth-percent** command for named configurations. You might want to change the bandwidth value if a different level of link utilization is required or if the configured bandwidth does not match the actual link bandwidth (which may have been configured to influence route metric calculations). This is a protocol-independent parameter that works for IP and IPX.

EIGRP vNETs

The EIGRP vNET feature uses Layer 3 routing techniques to provide limited fate sharing (the term fate sharing refers to the failure of interconnected systems; that is, different elements of a network are interconnected in such a way that they either fail together or not at all), traffic isolation, and access control with simple configurations. EIGRP virtual network (vNET) configurations are supported in both autonomous-system configurations and named configurations.

The vNET feature allows you to have multiple virtual networks by utilizing a single set of routers and links provided by the physical topology. Routers and links can be broken down into separate virtual networks using separate routing tables and routing processes by using vNETs and VRF configuration commands. The virtual networks facilitate traffic isolation and limited fate sharing. EIGRP's primary role in vNETs is to populate routing tables used by each vNET so that appropriate forwarding can take place. In the vNET model, each vNET effectively has its own complete set of EIGRP processes and resources, thus minimizing the possibility of actions within one vNET affecting another vNET.

The vNET feature supports command inheritance that allows commands entered in interface configuration mode to be inherited by every vNET configured on that interface. These inherited commands, including EIGRP interface commands, can be overridden by vNET-specific configurations in vNET submodes under the interface.

The following are some of the limitations of EIGRP vNETs:

- EIGRP does not support Internetwork Packet Exchange (IPX) within a vNET.
- vNET and VRF configurations are mutually exclusive on an interface. Both VRFs and vNETs can be configured on the router, but they cannot both be defined on the same interface. A VRF cannot be configured within a vNET and a vNET cannot be configured within a VRF.
- Each vNET has its own routing table, and routes cannot be redistributed directly from one vNET into another. EIGRP uses the route replication functionality to meet the requirements of shared services and to copy routes from one vNET Routing Information Base (RIB) to other vNET RIBs.
- Bidirectional Forwarding Detection (BFD) is not supported with EIGRP mode vNET.

EIGRP vNET Interface and Command Inheritance

A vNET router supports two types of interfaces: Edge interface and core (shared) interface.

An edge interface is an ingress point for vNET-unaware networks and is restricted to a single VRF. Use the **vrf forwarding** command to associate the edge interface with a VRF. The **vrf forwarding** command also allows entry into VRF submodes used to define interface settings on a per-VRF basis.

A vNET core interface is used to connect vNET-aware systems and can be shared by multiple vNETs. Use the **vnet trunk** command to enable a core interface.

When the **vnet trunk** command exists on an interface, with or without a VRF list, any EIGRP interface commands on that interface will be applied to the EIGRP instance for every vNET on that interface, including the instance running on the base or the global RIB. If the **vnet trunk** command is deleted from the interface, EIGRP interface commands will remain on and apply to only the global EIGRP instance. If an EIGRP interface command is removed from the main interface, the command will also be removed from every vNET on that interface.

End systems or routing protocol peers reached through an edge interface are unaware of vNETs and do not perform the vNET tagging done in the core of the vNET network.

EIGRP also supports the capability of setting per-vNET interface configurations, which allow you to define interface attributes that influence EIGRP behavior for a single vNET. In the configuration hierarchy, a specific vNET interface setting has precedence over settings applied to the entire interface and inherited by each vNET configured on that interface.

EIGRP provides interface commands to modify the EIGRP-specific attributes of an interface, and these interface commands can be entered directly on the interface for EIGRP autonomous system configurations, or in address family interface configuration mode for the EIGRP named mode configurations.

How to Configure EIGRP

Enabling EIGRP Autonomous System Configuration

Perform this task to enable EIGRP and create an EIGRP routing process. EIGRP sends updates to interfaces in specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

Configuring the **router eigrp** *autonomous-system-number* command creates an EIGRP autonomous system configuration that creates an EIGRP routing instance, which can be used for tagging routing information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system-number*
4. **network** *network-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system-number* **Example:** `Device(config)# router eigrp 1`	Configures an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.

	Command or Action	Purpose
Step 4	**network** *network-number* **Example:** `Device(config-router)# network 172.16.0.0`	Associates a network with an EIGRP routing process.

Step 5	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Enabling the EIGRP Named Configuration

Perform this task to enable EIGRP and to create an EIGRP routing process. EIGRP sends updates to interfaces in specified networks. If you do not specify the network of an interface, the interface will not be advertised in any EIGRP update.

Configuring the **router eigrp** *virtual-instance-name* command creates an EIGRP named configuration. The EIGRP named configuration does not create an EIGRP routing instance by itself. The EIGRP named configuration is the base configuration, which is required to define address family configurations used for routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Configures the EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Specifies a network for the EIGRP routing process.

Step 6	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Configuring Optional EIGRP Parameters in an Autonomous System Configuration

Perform this task to configure optional EIGRP parameters, which include applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization in an EIGRP autonomous system configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system*
4. **network** *ip-address* [*wildcard-mask*]
5. **passive-interface** [**default**] [*interface-type interface-number*]
6. **offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*]
7. **metric weights** *tos k1 k2 k3 k4 k5*
8. **no auto-summary**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system* **Example:** `Device(config)# router eigrp 1`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router)# network 172.16.0.0`	Associates networks with an EIGRP routing process.
Step 5	**passive-interface** [**default**] [*interface-type interface-number*] **Example:** `Device(config-router)# passive-interface`	(Optional) Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.
Step 6	**offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*] **Example:** `Device(config-router)# offset-list 21 in 10 gigabitethernet 0/0/1`	(Optional) Applies an offset to routing metrics.
Step 7	**metric weights** *tos k1 k2 k3 k4 k5* **Example:** `Device(config-router)# metric weights 0 2 0 2 0 0`	(Optional) Adjusts the EIGRP metric or K value. • EIGRP uses the following formula to determine the total metric to the network: EIGRP Metric = 256*((K1*Bw) + (K2*Bw)/(256-Load) + (K3*Delay)*(K5/(Reliability + K4))) **Note** If K5 is 0, then (K5/ (Reliability + K4)) is defined as 1.
Step 8	**no auto-summary** **Example:**	(Optional) Disables automatic summarization. **Note** Automatic summarization is enabled by default.

	Command or Action	Purpose
	`Device(config-router)# no auto-summary`	

Step 9	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuring Optional EIGRP Parameters in a Named Configuration

Perform this task to configure optional EIGRP named configuration parameters, which includes applying offsets to routing metrics, adjusting EIGRP metrics, setting the RIB-scaling factor, and disabling automatic summarization.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**unicast**] [**vrf** *vrf-name*] [**multicast**] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **metric weights** *tos k1 k2 k3 k4 k5 k6*
7. **af-interface** *interface-type interface-number*}
8. **passive-interface**
9. **bandwidth-percent** *maximum-bandwidth-percentage*
10. **exit-af-interface**
11. **topology** {**base** | *topology-name* **tid** *number*}
12. **offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*]
13. **no auto-summary**
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**unicast**] [**vrf** *vrf-name*] [**multicast**] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Specifies a network for the EIGRP routing process.
Step 6	**metric weights** *tos k1 k2 k3 k4 k5 k6* **Example:** `Device(config-router-af)# metric weights 0 2 0 2 0 0 0`	(Optional) Adjusts the EIGRP metric or K value. • EIGRP uses the following formula to determine the total 32-bit metric to the network: EIGRP Metric = 256*((K1*Bw) + (K2*Bw)/(256-Load) + (K3*Delay)*(K5/(Reliability + K4))) • EIGRP uses the following formula to determine the total 64-bit metric to the network: EIGRP Metric = 256*((K1*Throughput) + (K2*Throughput)/(256-Load) + (K3*Latency)+ (K6*Extended Attributes))*(K5/(Reliability + K4))) **Note** If K5 is 0, then (K5/ (Reliability + K4)) is defined as 1.

Step 7	**af-interface** *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface gigabitethernet 0/0/1`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 8	**passive-interface** **Example:** `Device(config-router-af-interface)# passive-interface`	Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.

	Command or Action	Purpose
Step 9	**bandwidth-percent** *maximum-bandwidth-percentage* **Example:** `Device(config-router-af-interface)# bandwidth-percent 75`	Configures the percentage of bandwidth that may be used by an EIGRP address family on an interface.
Step 10	**exit-af-interface** **Example:** `Device(config-router-af-interface)# exit-af-interface`	Exits address family interface configuration mode.

Step 11	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Device(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 12	**offset-list** [*access-list-number* | *access-list-name*] {**in** | **out**} *offset* [*interface-type interface-number*] **Example:** `Device(config-router-af-topology)# offset-list 21 in 10 gigabitethernet 6/2`	(Optional) Applies an offset to routing metrics.
Step 13	**no auto-summary** **Example:** `Device(config-router-af-topology)# no auto-summary`	(Optional) Disables automatic summarization. **Note** Automatic summarization is enabled by default.

Step 14	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Returns to privileged EXEC mode.

Configuring the EIGRP Redistribution Autonomous System Configuration

Perform this task to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and to configure the EIGRP administrative distance in an EIGRP autonomous system configuration.

You must use a default metric to redistribute a protocol into EIGRP, unless you use the **redistribute** command.

Note Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values.

Default metrics are supported only when you are redistributing from EIGRP or static routes.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system*
4. **network** *ip-address* [*wildcard-mask*]
5. **redistribute** *protocol*
6. **distance eigrp** *internal-distance external-distance*
7. **default-metric** *bandwidth delay reliability loading mtu*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system* **Example:** `Device(config)# router eigrp 1`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router)# network 172.16.0.0`	Associates networks with an EIGRP routing process.
Step 5	**redistribute** *protocol* **Example:** `Device(config-router)# redistribute rip`	Redistributes routes from one routing domain into another routing domain.
Step 6	**distance eigrp** *internal-distance external-distance* **Example:** `Device(config-router)# distance eigrp 80 130`	Allows the use of two administrative distances—internal and external.
Step 7	**default-metric** *bandwidth delay reliability loading mtu* **Example:**	Sets metrics for EIGRP.

	Command or Action	Purpose
	`Device(config-router)# default-metric 1000 100 250 100 1500`	

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuring the EIGRP Route Summarization Autonomous System Configuration

Perform this task to configure EIGRP to perform automatic summarization of subnet routes into network-level routes in an EIGRP autonomous system configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system*
4. **no auto-summary**
5. **exit**
6. **interface** *type number*
7. **no switchport**
8. **bandwidth** *kpbs*
9. **ip summary-address eigrp** *as-number ip-address mask* [*admin-distance*] [**leak-map** *name*]
10. **ip bandwidth-percent eigrp** *as-number percent*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system* **Example:** `Device(config)# router eigrp 101`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.

	Command or Action	Purpose
Step 4	**no auto-summary** **Example:** `Device(config-router)# no auto-summary`	Disables automatic summarization of subnet routes into network-level routes
Step 5	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0/3`	Enters interface configuration mode.
Step 7	**no switchport** **Example:** `Device(config-if)# no switchport`	Puts an interface into Layer 3 mode
Step 8	**bandwidth** *kpbs* **Example:** `bandwidth 56`	Sets the inherited and received bandwidth values for an interface
Step 9	**ip summary-address eigrp** *as-number ip-address mask* [*admin-distance*] [**leak-map** *name*] **Example:** `Device(config-if)# ip summary-address eigrp 100 10.0.0.0 0.0.0.0`	(Optional) Configures a summary aggregate address.
Step 10	**ip bandwidth-percent eigrp** *as-number percent* **Example:** `Device(config-if)# ip bandwidth-percent eigrp 209 75`	(Optional) Configures the percentage of bandwidth that may be used by EIGRP on an interface.

Step 11	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring the EIGRP Route Summarization Named Configuration

Perform this task to configure EIGRP to perform automatic summarization of subnet routes into network-level routes in an EIGRP named configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **af-interface** {**default** | *interface-type interface-number*}
6. **summary-address** *ip-address mask* [*administrative-distance* [**leak-map** *leak-map-name*]]
7. **exit-af-interface**
8. **topology** {**base** | *topology-name* **tid** *number*}
9. **summary-metric** *network-address subnet-mask bandwidth delay reliability load mtu*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose

Step 5	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface gigabitethernet 0/0/1`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 6	**summary-address** *ip-address mask* [*administrative-distance* [**leak-map** *leak-map-name*]] **Example:** `Device(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0`	Configures a summary address for EIGRP.
Step 7	**exit-af-interface** **Example:** `Device(config-router-af-interface)# exit-af-interface`	Exits address family interface configuration mode.

Step 8	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Device(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 9	**summary-metric** *network-address subnet-mask bandwidth delay reliability load mtu* **Example:** `Device(config-router-af-topology)# summary-metric 192.168.0.0/16 10000 10 255 1 1500`	(Optional) Configures a fixed metric for an EIGRP summary aggregate address.

Step 10	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits address family topology configuration mode and returns to privileged EXEC mode.

Configuring the EIGRP Event Logging Autonomous System Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system*
4. **eigrp event-log-size** *size*
5. **eigrp log-neighbor-changes**
6. **eigrp log-neighbor-warnings** [*seconds*]

7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system* **Example:** `Device(config)# router eigrp 101`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**eigrp event-log-size** *size* **Example:** `Device(config-router)# eigrp event-log-size 5000010`	(Optional) Sets the size of the EIGRP event log.
Step 5	**eigrp log-neighbor-changes** **Example:** `Device(config-router)# eigrp log-neighbor-changes`	(Optional) Enables logging of EIGRP neighbor adjacency changes. • By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.
Step 6	**eigrp log-neighbor-warnings** [*seconds*] **Example:** `Device(config-router)# eigrp log-neighbor-warnings 300`	(Optional) Enables the logging of EIGRP neighbor warning messages.

Step 7	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuring the EIGRP Event Logging Named Configuration

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **eigrp log-neighbor-warnings** [*seconds*]
6. **eigrp log-neighbor-changes**
7. **topology** {**base** | *topology-name* **tid** *number*}
8. **eigrp event-log-size** *size*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**eigrp log-neighbor-warnings** [*seconds*] **Example:**	(Optional) Enables the logging of EIGRP neighbor warning messages.

	Command or Action	Purpose
	`Device(config-router-af)# eigrp log-neighbor-warnings 300`	
Step 6	**eigrp log-neighbor-changes** **Example:** `Device(config-router-af)# eigrp log-neighbor-changes`	(Optional) Enables logging of EIGRP neighbor adjacency changes. • By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.

Step 7	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Device(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 8	**eigrp event-log-size** *size* **Example:** `Device(config-router-af-topology)# eigrp event-log-size 10000`	(Optional) Sets the size of the EIGRP event log.

Step 9	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits address family topology configuration mode and returns to privileged EXEC mode.

Configuring Equal and Unequal Cost Load Balancing Autonomous System Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system*
4. **traffic-share balanced**
5. **maximum-paths** *number-of-paths*
6. **variance** *multiplier*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system* **Example:** `Device(config)# router eigrp 101`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**traffic-share balanced** **Example:** `Device(config-router)# traffic-share balanced`	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.
Step 5	**maximum-paths** *number-of-paths* **Example:** `Device(config-router)# maximum-paths 5`	Controls the maximum number of parallel routes that an IP routing protocol can support.
Step 6	**variance** *multiplier* **Example:** `Device(config-router)# variance 1`	Controls load balancing in an internetwork based on EIGRP.

Step 7	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Configuring Equal and Unequal Cost Load Balancing Named Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **topology** {**base** | *topology-name* **tid** *number*}

6. **traffic-share balanced**
7. **maximum-paths** *number-of-paths*
8. **variance** *multiplier*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Device(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 6	**traffic-share balanced** **Example:** `Device(config-router-af-topology)# traffic-share balanced`	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.

	Command or Action	Purpose
Step 7	**maximum-paths** *number-of-paths* **Example:** `Device(config-router-af-topology)# maximum-paths 5`	Controls the maximum number of parallel routes that an IP routing protocol can support.
Step 8	**variance** *multiplier* **Example:** `Device(config-router-af-topology)# variance 1`	Controls load balancing in an internetwork based on EIGRP.

Step 9	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits address family topology configuration mode and returns to privileged EXEC mode.

Adjusting the Interval Between Hello Packets and the Hold Time in an Autonomous System Configuration

Note Cisco recommends not to adjust the hold time.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system-number*
4. **exit**
5. **interface** *type number*
6. **no switchport**
7. **ip hello-interval eigrp** *autonomous-system-number seconds*
8. **ip hold-time eigrp** *autonomous-system-number seconds*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system-number* **Example:** `Device(config)# router eigrp 101`	Enables an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**exit** **Example:** `Device(config-router)# exit`	Exits to global configuration mode.
Step 5	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0/9`	Enters interface configuration mode.
Step 6	**no switchport** **Example:** `Device(config-if)# no switchport`	Puts an interface into Layer 3 mode
Step 7	**ip hello-interval eigrp** *autonomous-system-number seconds* **Example:** `Device(config-if)# ip hello-interval eigrp 109 10`	Configures the hello interval for an EIGRP routing process.
Step 8	**ip hold-time eigrp** *autonomous-system-number seconds* **Example:** `Device(config-if)# ip hold-time eigrp 109 40`	Configures the hold time for an EIGRP routing process. **Note** Do not adjust the hold time without consulting your technical support personnel.

Step 9	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Adjusting the Interval Between Hello Packets and the Hold Time in a Named Configuration

Note Do not adjust the hold time without consulting your technical support personnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **af-interface** {**default** | *interface-type interface-number*}
6. **hello-interval** *seconds*
7. **hold-time** *seconds*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.
Step 4	Enter one of the following: • **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* • **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose

	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`	

Step 5	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface gigabitethernet 0/0/1`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 6	**hello-interval** *seconds* **Example:** `Device(config-router-af-interface)# hello-interval 10`	Configures the hello interval for an EIGRP address family named configuration.
Step 7	**hold-time** *seconds* **Example:** `Device(config-router-af-interface)# hold-time 50`	Configures the hold time for an EIGRP address family named configuration.

Step 8	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address family interface configuration mode and returns to privileged EXEC mode.

Disabling the Split Horizon Autonomous System Configuration

Split horizon controls the sending of EIGRP updates and query packets. When split horizon is enabled on an interface, updates and query packets are not sent for destinations for which this interface is the next hop. Controlling updates and query packets in this manner reduces the possibility of routing loops.

By default, split horizon is enabled on all interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip split-horizon eigrp** *autonomous-system-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/1`	Configures an interface and enters interface configuration mode.
Step 4	**no ip split-horizon eigrp** *autonomous-system-number* **Example:** `Device(config-if)# no ip split-horizon eigrp 101`	Disables split horizon.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Disabling the Split Horizon and Next-Hop-Self Named Configuration

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back from the same interface from where they were learned. Perform this task to change this default setting and configure EIGRP to use the received next-hop value when advertising these routes. Disabling next-hop-self is primarily useful in DMVPN spoke-to-spoke topologies.

By default, split horizon is enabled on all interfaces.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
    - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
    - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **af-interface** {**default** | *interface-type interface-number*}

6. **no split-horizon**
7. **no next-hop-self** [**no-ecmp-mode**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface gigabitethernet 0/0/1`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 6	**no split-horizon** **Example:** `Device(config-router-af-interface)# no split-horizon`	Disables EIGRP split horizon.

	Command or Action	Purpose
Step 7	**no next-hop-self [no-ecmp-mode]** **Example:** `Device(config-router-af-interface)# no next-hop-self no-ecmp-mode`	(Optional) Instructs an EIGRP router to use the received next hop rather than the local outbound interface address as the next hop. • The **no-ecmp-mode** keyword is an enhancement to the **no next-hop-self** command. When this optional keyword is enabled, all paths to a network in the EIGRP table are evaluated to check whether routes advertised from an interface were learned on the same interface.

Step 8	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address family interface configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining the EIGRP Autonomous System Configuration

This task is optional. Use the commands in any order desired to monitor and maintain EIGRP autonomous system configuration.

SUMMARY STEPS

1. **enable**
2. **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **accounting**
3. **show ip eigrp events** [*starting-event-number ending-event-number*] [**type**]
4. **show ip eigrp interfaces** [**vrf** {*vrf-name*| *****}] [*autonomous-system-number*] [*type number*] [**detail**]
5. **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **topology** [*ip-address* [*mask*]] | [**name**] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]
6. **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **topology** [*ip-address* [*mask*]] | [**name**] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]
7. **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **traffic**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device# enable
```

Step 2 **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **accounting**

Displays prefix accounting information for EIGRP processes.

Example:

```
Device# show ip eigrp vrf VRF1 accounting
```

Step 3 **show ip eigrp events** [*starting-event-number ending-event-number*] [**type**]

Displays information about interfaces that are configured for EIGRP.

Example:

```
Device# show ip eigrp events
```

Step 4 **show ip eigrp interfaces** [**vrf** {*vrf-name*| *****}] [*autonomous-system-number*] [*type number*] [**detail**]

Displays neighbors discovered by EIGRP.

Example:

```
Device# show ip eigrp interfaces
```

Step 5 **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **topology** [*ip-address* [*mask*]] | [**name**] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]

Displays neighbors discovered by EIGRP

Example:

```
Device# show ip eigrp neighbors
```

Step 6 **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **topology** [*ip-address* [*mask*]] | [**name**] [**active** | **all-links** | **detail-links** | **pending** | **summary** | **zero-successors**]

Displays entries in the EIGRP topology table.

Example:

```
Device# show ip eigrp topology
```

Step 7 **show ip eigrp** [**vrf** {*vrf-name* | *****}] [*autonomous-system-number*] **traffic**

Displays the number of EIGRP packets sent and received.

Example:

```
Device# show ip eigrp traffic
```

Monitoring and Maintaining the EIGRP Named Configuration

This task is optional. Use the commands in any order desired to monitor and maintain the EIGRP named configuration.

SUMMARY STEPS

1. **enable**
2. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **accounting**
3. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **events** [*starting-event-number ending-event-number*] [**errmsg** [*starting-event-number ending-event-number*]] [**sia** [*starting-event-number ending-event-number*]] [**type**]

4. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **interfaces** [**detail**] [*interface-type interface-number*]
5. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **neighbors** [**static**] [**detail**] [*interface-type interface-number*]
6. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **timers**
7. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **topology** [*topology-name*] [*ip-address*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**route-type** {**connected** | **external** | **internal** | **local** | **redistributed** | **summary** | **vpn**}]
8. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **traffic**
9. **show eigrp plugins** [*plugin-name*] [**detailed**]
10. **show eigrp protocols** [**vrf** *vrf-name*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Device# enable
```

Step 2 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **accounting**

Displays prefix accounting information for EIGRP processes.

Example:

```
Device# show eigrp address-family ipv4 22 accounting
```

Step 3 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **events** [*starting-event-number ending-event-number*] [**errmsg** [*starting-event-number ending-event-number*]] [**sia** [*starting-event-number ending-event-number*]] [**type**]

Displays information about EIGRP address-family events.

Example:

```
Device# show eigrp address-family ipv4 3 events
```

Step 4 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **interfaces** [**detail**] [*interface-type interface-number*]

Displays information about interfaces that are configured for EIGRP.

Example:

```
Device# show eigrp address-family ipv4 4453 interfaces
```

Step 5 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **neighbors** [**static**] [**detail**] [*interface-type interface-number*]

Displays the neighbors that are discovered by EIGRP.

Example:

```
Device# show eigrp address-family ipv4 4453 neighbors
```

Step 6 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **timers**

Displays information about EIGRP timers and expiration times.

Example:

```
Device# show eigrp address-family ipv4 4453 timers
```

Step 7 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **topology** [*topology-name*] [*ip-address*] [**active**] [**all-links**] [**detail-links**] [**pending**] [**summary**] [**zero-successors**] [**route-type** {**connected** | **external** | **internal** | **local** | **redistributed** | **summary** | **vpn**}]

Displays entries in the EIGRP topology table.

Example:

```
Device# show eigrp address-family ipv4 4453 topology
```

Step 8 **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **traffic**

Displays the number of EIGRP packets that are sent and received.

Example:

```
Device# show eigrp address-family ipv4 4453 traffic
```

Step 9 **show eigrp plugins** [*plugin-name*] [**detailed**]

Displays general information, including the versions of the EIGRP protocol features that are currently running on the device.

Example:

```
Device# show eigrp plugins
```

Step 10 **show eigrp protocols** [**vrf** *vrf-name*]

Displays further information about EIGRP protocols that are currently running on a device.

Example:

```
Device# show eigrp protocols
```

Configuration Examples for EIGRP

Example: Enabling EIGRP—Autonomous System Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# network 172.16.0.0
```

Example: Enabling EIGRP—Named Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
```

Example: EIGRP Parameters—Autonomous System Configuration

The following example shows how to configure optional EIGRP autonomous system configuration parameters, including applying offsets to routing metrics, adjusting EIGRP metrics, and disabling automatic summarization:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# network 172.16.0.0
Device(config-router)# passive-interface
Device(config-router)# offset-list 21 in 10 ethernet 0
Device(config-router)# metric weights 0 2 0 2 0 0
Device(config-router)# no auto-summary
Device(config-router)# exit
```

Example: EIGRP Parameters—Named Configuration

The following example shows how to configure optional EIGRP named configuration parameters, including applying offsets to routing metrics, adjusting EIGRP metrics, setting RIB-scaling factor, and disabling automatic summarization.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# metric weights 0 2 0 2 0 0 0
Device(config-router-af)# metric rib-scale 100
Device(config-router-af)# af-interface gigabitethernet 0/0/1
Device(config-router-af-interface)# passive-interface
Device(config-router-af-interface)# bandwidth-percent 75
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af-interface)# topology base
Device(config-router-af-topology)# offset-list 21 in 10 gigabitethernet 0/0/1
Device(config-router-af-topology)# no auto-summary
Device(config-router-af-topology)# exit-af-topology
```

Example: EIGRP Redistribution—Autonomous System Configuration

The following example shows how to configure redistribution of non-EIGRP protocol metrics into EIGRP metrics and configure the EIGRP administrative distance in an EIGRP autonomous system configuration:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# network 172.16.0.0
Device(config-router)# redistribute rip
Device(config-router)# distance eigrp 80 130
Device(config-router)# default-metric 1000 100 250 100 1500
```

Example: EIGRP Route Summarization—Autonomous System Configuration

The following example shows how to configure route summarization on an interface and configure the automatic summary feature for an EIGRP autonomous system configuration. The following configuration causes EIGRP to summarize the network from Ethernet interface 0/0.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 101
Device(config-router)# no auto-summary
Device(config-router)# exit
Device(config)# interface Gigabitethernet 1/0/1
Device(config-if)# no switchport
bandwidth 56
Device(config-if)# ip summary-address eigrp 100 0.0.0.0 0.0.0.0
Device(config-if)# ip bandwidth-percent eigrp 209 75
```

Note You should not use the **ip summary-address eigrp** summarization command to generate the default route (0.0.0.0) from an interface because this creates 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 through 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, traffic will be sent to the null 0 interface, where it is dropped. The recommended way to send only the default route out of a given interface is to use the **distribute-list** command. You can configure this command to filter all outbound route advertisements sent out from the interface with the exception of the default (0.0.0.0).

Example: EIGRP Route Summarization—Named Configuration

The following example shows how to configure route summarization on an interface and configure the automatic summary feature for an EIGRP named configuration. This configuration causes EIGRP to summarize network 192.168.0.0 only from Ethernet interface 0/0.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)# topology base
Device(config-router-af-topology)# summary-metric 192.168.0.0/16 10000 10 255 1 1500
```

Example: EIGRP Event Logging—Autonomous System Configuration

The following example shows how to configure EIGRP event logging parameters, including setting the size of the EIGRP event log for an EIGRP autonomous system configuration:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# eigrp event-log-size 5000
Device(config-router)# eigrp log-neighbor-changes
Device(config-router)# eigrp log-neighbor-warnings 300
```

Example: EIGRP Event Logging—Named Configuration

The following example shows how to configure EIGRP event logging parameters, including setting the size of the EIGRP event log for an EIGRP named configuration:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# eigrp log-neighbor-warnings 300
Device(config-router-af)# eigrp log-neighbor-changes
Device(config-router-af)# topology base
Device(config-router-af-topology)# eigrp event-log-size 10000
```

Example: Equal and Unequal Cost Load Balancing—Autonomous System Configuration

The following example shows how to configure traffic distribution among routes, the maximum number of parallel routes, and load balancing in an EIGRP named configuration network:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# traffic-share balanced
Device(config-router)# maximum-paths 5
Device(config-router)# variance 1
```

Example: Equal and Unequal Cost Load Balancing—Named Configuration

The following example shows how to configure traffic distribution among routes, the maximum number of parallel routes, and load balancing in an EIGRP named configuration network:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# topology base
Device(config-router-af-topology)# traffic-share balanced
Device(config-router-af-topology)# maximum-paths 5
Device(config-router-af-topology)# variance 1
```

Example: Adjusting the Interval Between Hello Packets and the Hold Time—Autonomous System Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Gibabitethernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# ip hello-interval eigrp 109 10
Device(config-if)# ip hold-time eigrp 109 40
```

Example: Adjusting the Interval Between Hello Packets and the Hold Time—Named Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# hello-interval 10
Device(config-router-af-interface)# hold-time 50
```

Example: Disabling the Split Horizon—Autonomous System Configuration

Split horizon is enabled on all interfaces by default. The following example shows how to disable split horizon for an EIGRP autonomous system configuration:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Ethernet 0/1
Device(config-if)# no ip split-horizon eigrp 101
```

Example: Disabling the Split Horizon and Next-Hop-Self—Named Configuration

Split horizon is enabled on all interfaces by default. The following example shows how to disable split horizon in an EIGRP named configuration.

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it advertises, even when advertising those routes back out of the same interface from where they were learned. The following example shows how to change this default to instruct EIGRP to use the received next-hop value when advertising these routes in an EIGRP named configuration. Disabling the **next-hop-self** command is primarily useful in DMVPN spoke-to-spoke topologies.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# no split-horizon
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
```

Example: Command Inheritance and Virtual Network Interface Mode Override in an EIGRP Environment

Suppose a GigabitEthernet interface is configured with the following EIGRP commands:

```
interface gigabitethernet 0/0/0
 vnet trunk
 ip address 192.0.2.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 x
 ip bandwidth-percent eigrp 1 3
 ip dampening-change eigrp 1 30
 ip hello-interval eigrp 1 6
 ip hold-time eigrp 1 18
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 end
```

Because a trunk is configured, a VRF subinterface is automatically created and the commands on the main interface are inherited by the VRF subinterface (g0/0/0.3, where the number 3 is the tag number from vnet tag 3.)

Use the **show derived-config** command to display the hidden subinterface. The following sample output shows that all the commands entered on GigabitEthernet 0/0/0 have been inherited by GigabitEthernet 0/0/0.3:

```
Device# show derived-config interface gigabitethernet 0/0/0.3

Building configuration...
Derived configuration : 478 bytes
!
interface GigabitEthernet0/0/0.3
 description Subinterface for VNET vrf1
 vrf forwarding vrf1
 encapsulation dot1Q 3
 ip address 192.0.2.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 x
 ip bandwidth-percent eigrp 1 3
 ip dampening-change eigrp 1 30
 ip hello-interval eigrp 1 6
 ip hold-time eigrp 1 18
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
 end
```

Use the virtual network interface mode to override the commands entered in interface configuration mode. For example:

```
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vnet name vrf1
Device(config-if-vnet)# no ip authentication mode eigrp 1 md5
! disable authen for e0/0.3 only
Device(config-if-vnet)# ip authentication key-chain eigrp 1 y
! different key-chain
Device(config-if-vnet)# ip band eigrp 1 99
! higher bandwidth-percent
Device(config-if-vnet)# no ip dampening-change eigrp 1
! disable dampening-change
Device(config-if-vnet)# ip hello eigrp 1 7
Device(config-if-vnet)# ip hold eigrp 1 21
Device(config-if-vnet)# ip next-hop-self eigrp 1
! enable next-hop-self for e0/0.3
Device(config-if-vnet)# ip split-horizon eigrp 1
! enable split-horizon


Device(config-if-vnet)# do show running-config interface gigabitethernet 0/0/0

Building configuration...
Current configuration : 731 bytes
!
interface GigabitEthernet0/0/0
 vnet trunk
 ip address 192.0.2.1 255.255.255.0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 x
 ip bandwidth-percent eigrp 1 3
 ip dampening-change eigrp 1 30
 ip hello-interval eigrp 1 6
 ip hold-time eigrp 1 18
 no ip next-hop-self eigrp 1
 no ip split-horizon eigrp 1
  vnet name vrf1
  ip split-horizon eigrp 1
  no ip authentication mode eigrp 1 md5
  ip authentication key-chain eigrp 1 y
  ip bandwidth-percent eigrp 1 99
  no ip dampening-change eigrp 1
  ip hello-interval eigrp 1 7
  ip hold-time eigrp 1 21
  !
end
```

Notice that g/0/0.3 is now using the override settings:

```
Device(config-if-vnet)# do show derived-config interface gigabitethernet 0/0.3

Building configuration...
Derived configuration : 479 bytes
!
interface GigabitEthernet0/0/0.3
```

```
 description Subinterface for VNET vrf1
 vrf forwarding vrf1
 encapsulation dot1Q 3
 ip address 192.0.2.1 255.255.255.0
 no ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 y
 ip bandwidth-percent eigrp 1 99
 no ip dampening-change eigrp 1
 ip hello-interval eigrp 1 7
 ip hold-time eigrp 1 21
 ip next-hop-self eigrp 1
 ip split-horizon eigrp 1
 end
```

Commands entered in virtual network interface mode are sticky. That is, when you enter a command in this mode, the command will override the default value configured in interface configuration mode.

The following example shows how to change the default hello interval value in vrf 1. The example also shows sample outputs of the current and derived configurations.

```
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# ip address 192.0.2.1 255.255.255.0
Device(config-if)# vnet trunk
Device(config-if)# ip hello eigrp 1 7
Device(config-if)# do show run interface gigabitethernet 0/0/2

Building configuration...
Current configuration : 134 bytes
!
interface GigabitEthernet0/0/0
 vnet trunk
 ip address 192.0.2.1 255.255.255.0
 ip hello-interval eigrp 1 7
 ipv6 enable
 vnet global
 !
 end

Device(config-if)# do show derived interface gigabitethernet 0/0/0.3

Building configuration...

Derived configuration : 177 bytes
!
interface Ethernet0/0.3
 description Subinterface for VNET vrf1
 encapsulation dot1Q 3
 vrf forwarding vrf1
 ip address 192.0.2.1 255.255.255.0
 ip hello-interval eigrp 1 7
end

Device(config-if)# vnet name vrf1
Device(config-if-vnet)# ip hello-interval eigrp 1 10
Device(config-if-vnet)# do show run interface gigabitethernet 0/0/0

Building configuration...
Current configuration : 183 bytes
!
interface GigabitEthernet0/0/0
 vnet trunk
 ip address 192.0.2.1 255.255.255.0
 ip hello-interval eigrp 1 7
 ipv6 enable
 vnet name vrf1
  ip hello-interval eigrp 1 10
 !
 vnet global
 !
end

Device(config-if-vnet)# do show derived interface gigabitethernet 0/0/0.3

Building configuration...

Derived configuration : 178 bytes
!
interface GigabitEthernet0/0/0.3
 description Subinterface for VNET vrf1
 encapsulation dot1Q 3
 vrf forwarding vrf1
 ip address 192.0.2.1 255.255.255.0
 ip hello-interval eigrp 1 10
end
```

Because of this sticky factor, to remove a configuration entry in virtual network interface mode, use the default form of that command. Some commands can also be removed using the **no** form.

```
R1(config-if-vnet)# default ip authentication mode eigrp 1 md5
R1(config-if-vnet)# no ip bandwidth-percent eigrp 1
R1(config-if-vnet)# no ip hello eigrp 1

R1(config-if-vnet)# do show running-config interface gigabitethernet 0/0/0

Building configuration...
Current configuration : 138 bytes
!
interface GigabitEthernet0/0/0
 vnet trunk
 no ip address
 vnet name vrf1
 !
end
```

Example: Monitoring and Maintaining the EIGRP Autonomous System Configuration

The **show ip eigrp** command displays prefix accounting information for EIGRP processes. The following is sample output from this command:

```
Device# show ip eigrp vrf VRF1 accounting

EIGRP-IPv4 Accounting for AS(100)/ID(10.0.2.1) VRF(VRF1)
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          Gi0/0              2          0         84
 P    10.0.2.4          Se2/0              0          2        114
 D    10.0.1.3          Gi0/0              0          3          0
```

The **show ip eigrp events** command displays the EIGRP event log. The following is sample output from this command:

```
Device# show ip eigrp events

1    02:37:58.171 NSF stale rt scan, peer: 10.0.0.0
2    02:37:58.167 Metric set: 10.0.0.1/24 284700416
3    02:37:58.167 FC sat rdbmet/succmet: 284700416 0
4    02:37:58.167 FC sat nh/ndbmet: 10.0.0.2 284700416
5    02:37:58.167 Find FS: 10.0.0.0/24 284700416
6    02:37:58.167 Rcv update met/succmet: 284956416 284700416
7    02:37:58.167 Rcv update dest/nh: 10.0.0.0/24 10.0.0.1
8    02:37:58.167 Peer nsf restarted: 10.0.0.1 Tunnel0
9    02:36:38.383 Metric set: 10.0.0.0/24 284700416
10   02:36:38.383 RDB delete: 10.0.0.0/24 10.0.0.1
11   02:36:38.383 FC sat rdbmet/succmet: 284700416 0
12   02:36:38.383 FC sat nh/ndbmet: 0.0.0.0 284700416
```

The **show ip eigrp interfaces** command displays information about interfaces that are configured for EIGRP. The following is sample output from this command:

```
Device# show ip eigrp interfaces

EIGRP-IPv4 Interfaces for AS(60)
                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
Gi0           0         0/0          0      11/434          0          0
Gi0           1         0/0        337       0/10           0          0
SE0:1.16      1         0/0         10       1/63         103          0
Tu0           1         0/0        330       0/16           0          0
```

The **show ip eigrp neighbors** command displays neighbors discovered by EIGRP. The following is sample output from this command:

```
Device# show ip eigrp neighbors

H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   10.1.1.2                 Gi0/0           13 00:00:03  1996   5000  0  5
2   10.1.1.9                 Gi0/0           14 00:02:24   206   5000  0  5
1   10.1.2.3                 Gi0/1           11 00:20:39  2202   5000  0  5
```

The **show ip eigrp topology** command displays entries in the EIGRP topology table. The following is sample output from this command:

```
Device# show ip eigrp topology

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia status
P 10.0.0.0/8, 1 successors, FD is 409600
        via 10.0.0.1 (409600/128256), GigabirEthernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600
        via 10.0.0.1 (409600/128256), GigabitEthernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600
        via Summary (281600/0), Null0
P 10.0.1.0/24, 1 successors, FD is 281600
        via Connected, GigabitEthernet0/0
```

The **show ip eigrp traffic** command displays the number of EIGRP packets sent and received. The following is sample output from this command:

```
Device# show ip eigrp traffic

EIGRP-IPv4 Traffic Statistics for AS(60)
Hellos sent/received: 21429/2809
Updates sent/received: 22/17
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 16/13
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 204
PDM Process ID: 203
Socket Queue: 0/2000/2/0 (current/max/highest/drops)
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

Example: Monitoring and Maintaining the EIGRP Named Configuration

In this example, the **show eigrp address-family** command displays prefix accounting information for EIGRP processes:

```
Device# show eigrp address-family ipv4 22 accounting

EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)
Total Prefix Count: 3  States: A-Adjacency, P-Pending, D-Down
State Address/Source    Interface       Prefix   Restart  Restart/
                                        Count     Count   Reset(s)
 A    10.0.0.2          Gi0/0              2         0        0
 P    10.0.2.4          Se2/0              0         2        114
 D    10.0.1.3          Gi0/0              0         3        0
```

In this example, the **show eigrp address-family** command displays information about EIGRP address-family events:

```
Device# show eigrp address-family ipv4 3 events

Event information for AS 3:
1 15:37:47.015 Change queue emptied, entries: 1
2 15:37:47.015 Metric set: 10.0.0.0/24 307200
3 15:37:47.015 Update reason, delay: new if 4294967295
4 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
5 15:37:47.015 Update reason, delay: metric chg 4294967295
6 15:37:47.015 Update sent, RD: 10.0.0.0/24 4294967295
7 15:37:47.015 Route installed: 10.0.0.0/24 10.0.1.2
8 15:37:47.015 Route installing: 10.0.0.0/24 10.0.1.2
```

In this example, the **show eigrp address-family** command displays information about interfaces that are configured for EIGRP:

```
Device# show eigrp address-family ipv4 4453 interfaces

EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
     Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface     Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Services
Se0           1          0/0        28      0/15          127           0
Se1           1          0/0        44      0/15          211           0
```

In this example, the **show eigrp address-family** command displays information about the neighbors that are discovered by EIGRP:

```
Device# show eigrp address-family ipv4 4453 neighbors
```

```
EIGRP-IPv4 VR(Virtual-name) Address-family Neighbors for AS(4453)
Address       Interface     Hold Uptime  SRTT  RTO    Q     Seq
                                 (sec)         (ms)  (ms)   Cnt   Num
172.16.81.28           GigabitEthernet1/1/1     13   0:00:41  0      11   4     20
172.16.80.28           GigabitEthernet0/0/1     14   0:02:01  0      10   12    24
172.16.80.31           GigabitEthernet0/1/1     12   0:02:02  0      4    5
```

In this example, the **show eigrp address-family** command displays information about EIGRP timers and expiration times:

```
Device# show eigrp address-family ipv4 4453 timers

EIGRP-IPv4 VR(Virtual-name) Address-family Timers for AS(4453)
Hello Process
Expiration Type
| 1.022 (parent)
| 1.022 Hello (Et0/0)
Update Process
Expiration Type
| 14.984 (parent)
| 14.984 (parent)
| 14.984 Peer holding
SIA Process
Expiration Type for Topo(base)
| 0.000 (parent)
```

In this example, the **show eigrp address-family** command displays entries in the EIGRP topology table:

```
Device# show eigrp address-family ipv4 4453 topology

EIGRP-IPv4 VR(Virtual-name) Topology Table for AS(4453)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status, s - sia Status
P  10.17.17.0/24, 1 successors, FD is 409600
         via 10.10.10.2 (409600/128256), GigabitEthernet3/0/1
P  172.16.19.0/24, 1 successors, FD is 409600
         via 10.10.10.2 (409600/128256), GigabitEthernet3/0/1
P  192.168.10.0/24, 1 successors, FD is 281600
         via Connected, GigabitEthernet3/0/1
P  10.10.10.0/24, 1 successors, FD is 281600
         via Redistributed (281600/0)
```

In this example, the **show eigrp address-family** command displays information about the number of EIGRP packets that are sent and received:

```
Device# show eigrp address-family ipv4 4453 traffic

EIGRP-IPv4 VR(virtual-name) Address-family Traffic Statistics for AS(4453)
  Hellos sent/received: 122/122
  Updates sent/received: 3/1
  Queries sent/received: 0/0
  Replies sent/received: 0/0
  Acks sent/received: 0/3
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 128
  PDM Process ID: 191
  Socket Queue: 0/2000/1/0 (current/max/highest/drops)
  Input Queue: 0/2000/1/0 (current/max/highest/drops
```

In this example, the **show eigrp plugins** command displays general information, including the versions of the EIGRP protocol features that are currently running on the device:

```
Device# show eigrp plugins

EIGRP feature plugins:::
    eigrp-release      :   5.00.00 : Portable EIGRP Release
                       :  19.00.00 : Source Component Release(rel5)
    igrp2              :   3.00.00 : Reliable Transport/Dual Database
    bfd                :   1.01.00 : BFD Platform Support
    mtr                :   1.00.01 : Multi-Topology Routing(MTR)
    eigrp-pfr          :   1.00.01 : Performance Routing Support
    ipv4-af            :   2.01.01 : Routing Protocol Support
    ipv4-sf            :   1.01.00 : Service Distribution Support
    external-client    :   1.02.00 : Service Distribution Client Support
    ipv6-af            :   2.01.01 : Routing Protocol Support
    ipv6-sf            :   1.01.00 : Service Distribution Support
    snmp-agent         :   1.01.01 : SNMP/SNMPv2 Agent Support
```

In this example, the **show eigrp protocols** command displays general information about EIGRP protocols that are currently running on a device:

```
Device# show eigrp protocols

EIGRP-IPv4 Protocol for AS(10)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 10.0.1.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
EIGRP-IPv4 Protocol for AS(5) VRF(VRF1)
Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
NSF-aware route hold timer is 240
Router-ID: 10.1.2.1
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170
Maximum path: 4
Maximum hopcount 100
Maximum metric variance 1
Total Prefix Count: 0
Total Redist Count: 0
```

Additional References for EIGRP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
EIGRP commands	IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions

Related Topic	Document Title
EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks feature	“Mobile Ad Hoc Networks for Router-to-Radio Communications” module of *the IP Mobility Configuration Guide*
EIGRP Technology Support	Enhanced Interior Gateway Routing Protocol
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol
IPv6 Routing EIGRP Support	*IPv6 Routing: EIGRP Support*
Protocol-independent features that work with EIGRP	*IP Routing: Protocol-Independent Configuration Guide*
Service Advertisement Framework	*Service Advertisement Framework Configuration Guide*
Service Advertisement Framework commands	Service Advertisement Framework Command Reference

Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	*SECURE HASH STANDARD (SHS)*
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for EIGRP Features

Feature Name	Releases	Feature Information
EIGRP		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, and IGRP is obsolete. The following commands were introduced or modified: **auto-summary (EIGRP) ,clear ip eigrp neighbors**, **default-information**, **default-metric (EIGRP)**, **distance (EIGRP)**, **eigrp log-neighbor-changes**, **eigrp log-neighbor-warnings**, **eigrp router-id**, **ip bandwidth-percent eigrp**, **ip hello-interval eigrp**, **ip hold-time eigrp**, **ip next-hop-self eigrp**, **ip split-horizon eigrp**, **ip summary-address eigrp**, **metric maximum-hops**, **metric weights (EIGRP)**, **neighbor (EIGRP)**, **network (EIGRP)**, **offset-list (EIGRP)**, **router eigrp**, **set metric (EIGRP)**, **show ip eigrp accounting**, **show ip eigrp interfaces**, **show ip eigrp neighbors**, **show ip eigrp topology**, **show ip eigrp traffic**, **show ip eigrp vrf accounting**, **show ip eigrp vrf interfaces**, **show ip eigrp vrf neighbors**, **show ip eigrp vrf topology**, **show ip eigrp vrf traffic**, **summary-metric, timers active-time**, **traffic-share balanced**, **variance (EIGRP)**.

Feature Name	Releases	Feature Information
EIGRP Dual DMVPN Domain Enhancement		The EIGRP Dual DMVPN Domain Enhancement feature supports the no next-hop-self functionality on dual DMVPN domains in both IPv4 and IPv6 configurations. The following commands were introduced or modified by this feature: **ip next-hop-self eigrp**, **ipv6 next-hop self eigrp**, **next-hop-self**, **show ip eigrp interfaces**, **show ipv6 eigrp interfaces**, **show ip eigrp topology**, **show ipv6 eigrp topology**.
Named mode for EIGRP vNETs IPv4	Cisco IOS Release 15.2(1)SY.	The EIGRP vNET feature allows the creation of multiple virtual networks by utilizing a single set of routers and links provided by the physical topology. EIGRP vNET configurations are supported in both classic and named modes. In Cisco IOS Release 15.1(1)SG, EIGRP vNET configurations are supported only in the classic mode. The following command was modified: **vnet**.

CHAPTER 3

IPv6 Routing: EIGRP Support

Customers can configure Enhanced Interior Gateway Routing Protocol (EIGRP) to route IPv6 prefixes. EIGRP IPv4 runs over an IPv4 transport, communicates only with IPv4 peers, and advertises only IPv4 routes, and EIGRP for IPv6 follows the same model. EIGRP for IPv4 and EIGRP for IPv6 are configured and managed separately. However, the configuration of EIGRP for IPv4 and IPv6 is similar and provides operational familiarity and continuity.

- Finding Feature Information, on page 57
- Restrictions for IPv6 Routing EIGRP Support, on page 57
- Information About IPv6 Routing EIGRP Support, on page 58
- How to Configure IPv6 Routing EIGRP Support, on page 59
- Configuration Examples for IPv6 Routing EIGRP Support, on page 74
- Additional References, on page 74
- Feature Information for IPv6 Routing: EIGRP Support, on page 75

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 Routing EIGRP Support

This section lists ways in which EIGRP for IPv6 differs from EIGRP IPv4 and lists EIGRP for IPv6 restrictions:

- EIGRP for IPv6 is directly configured on the interfaces over which it runs. This feature allows EIGRP for IPv6 to be configured without the use of a global IPv6 address. There is no network statement in EIGRP for IPv6.

In per-interface configuration at system startup, if EIGRP has been configured on an interface, then the EIGRP protocol may start running before any EIGRP router mode commands have been executed.

- An EIGRP for IPv6 protocol instance requires a router ID before it can start running.

- EIGRP for IPv6 has a shutdown feature. The routing process should be in "no shut" mode in order to start running.
- EIGRP for IPv6 provides route filtering using the **distribute-list prefix-list** command. Use of the **route-map** command is not supported for route filtering with a distribute list.

Information About IPv6 Routing EIGRP Support

Cisco EIGRP for IPv6 Implementation

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 called 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. Devices 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.

EIGRP provides the following features:

- Increased network width--With Routing Information Protocol (RIP), the largest possible width of your network is 15 hops. When EIGRP is enabled, the largest possible width is 224 hops. Because the EIGRP metric is large enough to support thousands of hops, the only barrier to expanding the network is the transport layer hop counter. Cisco works around this limitation by incrementing the transport control field only when an IPv4 or an IPv6 packet has traversed 15 devices and the next hop to the destination was learned by way of EIGRP. When a RIP route is being used as the next hop to the destination, the transport control field is incremented as usual.
- Fast convergence--The DUAL algorithm allows routing information to converge as quickly as any other 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.
- Neighbor discovery mechanism--This is a simple hello mechanism used to learn about neighboring devices. It is protocol-independent.
- Arbitrary route summarization.
- Scaling--EIGRP scales to large networks.
- Route filtering--EIGRP for IPv6 provides route filtering using the **distribute-list prefix-list**command. Use of the **route-map** command is not supported for route filtering with a distribute list.

EIGRP has the following four basic components:

- Neighbor discovery--Neighbor discovery is the process that devices use to dynamically learn of other devices on their directly attached networks. Devices must also discover when their neighbors become unreachable or inoperative. EIGRP neighbor discovery is achieved with low overhead by periodically sending small hello packets. EIGRP neighbors can also discover a neighbor that has recovered after an outage because the recovered neighbor will send out a hello packet. As long as hello packets are received, the Cisco software can determine that a neighbor is alive and functioning. Once this status is determined, the neighboring devices can exchange routing information.

- Reliable transport protocol--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, 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.
- DUAL finite state machine--The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses several metrics including distance and cost information to select efficient, loop-free paths. When multiple routes to a neighbor exist, DUAL determines which route has the lowest metric (named the feasible distance), and enters this route into the routing table. Other possible routes to this neighbor with larger metrics are received, and DUAL determines the reported distance to this network. The reported distance is defined as the total metric advertised by an upstream neighbor for a path to a destination. DUAL compares the reported distance with the feasible distance, and if the reported distance is less than the feasible distance, DUAL considers the route to be a feasible successor and enters the route into the topology table. The feasible successor route that is reported with the lowest metric becomes the successor route to the current route if the current route fails. To avoid routing loops, DUAL ensures that the reported distance is always less than the feasible distance for a neighbor device to reach the destination network; otherwise, the route to the neighbor may loop back through the local device.
- Protocol-dependent modules--When there are no feasible successors to a route that has failed, but there are neighbors advertising the route, a recomputation must occur. This is the process in which DUAL determines a new successor. 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, DUAL will use them in order to avoid unnecessary recomputation.

The protocol-dependent modules are responsible for network layer protocol-specific tasks. For example, the EIGRP module is responsible for sending and receiving EIGRP packets that are encapsulated in IPv4 or IPv6. 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 IPv4 or IPv6 routing table. Also, EIGRP is responsible for redistributing routes learned by other IPv4 or IPv6 routing protocols.

How to Configure IPv6 Routing EIGRP Support

Enabling EIGRP for IPv6 on an Interface

EIGRP for IPv6 is directly configured on the interfaces over which it runs, which allows EIGRP for IPv6 to be configured without the use of a global IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **no shut**
6. **ipv6 enable**
7. **ipv6 eigrp** *as-number*
8. **ipv6 router eigrp** *as-number*
9. **eigrp router-id** *router-id*
10. **exit**
11. **show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [*as-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is to be configured.
Step 5	**no shut** **Example:** `Device(config-if)# no shut`	Enables no shut mode so the routing process can start running.
Step 6	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

	Command or Action	Purpose
Step 7	**ipv6 eigrp** *as-number* **Example:** `Device(config-if)# ipv6 eigrp 1`	Enables EIGRP for IPv6 on a specified interface.
Step 8	**ipv6 router eigrp** *as-number* **Example:** `Device(config-if)# ipv6 router eigrp 1`	Enters router configuration mode and creates an EIGRP IPv6 routing process.
Step 9	**eigrp router-id** *router-id* **Example:** `Device(config-router)# eigrp router-id 10.1.1.1`	Enables the use of a fixed router ID. Use this command only if an IPv4 address is not defined on the router eligible for router ID.
Step 10	**exit** **Example:** `Device(config-router) exit`	Enter three times to return to privileged EXEC mode.
Step 11	**show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [*as-number*] **Example:** `Device# show ipv6 eigrp interfaces`	Displays information about interfaces configured for EIGRP for IPv6.

Configuring the Percentage of Link Bandwidth Used by EIGRP

By default, EIGRP packets consume a maximum of 50 percent of the link bandwidth, as configured with the **bandwidth interface** 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).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **ipv6 bandwidth-percent eigrp** *as-number percent*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**ipv6 bandwidth-percent eigrp** *as-number percent* **Example:** `Device(config-if)# ipv6 bandwidth-percent eigrp 1 75`	Configures the percentage of bandwidth that may be used by EIGRP for IPv6 on an interface

Configuring Summary Addresses

If any more specific routes are in the routing table, EIGRP for IPv6 will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **ipv6 summary-address eigrp** *as-number ipv6-address* [*admin-distance*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**ipv6 summary-address eigrp** *as-number ipv6-address* [*admin-distance*] **Example:** `Device(config-if)# ipv6 summary-address eigrp 1 2001:DB8:0:1::/64`	Configures a summary aggregate address for a specified interface.

Configuring EIGRP Route Authentication

EIGRP route authentication provides message digest algorithm 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.

Each key has its own key identifier, 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **ipv6 authentication mode eigrp** *as-number* **md5**
6. **ipv6 authentication key-chain eigrp** *as-number key-chain*
7. **exit**
8. **key chain** *name-of-chain*
9. **key** *key-id*

10. **key-string** *text*
11. **accept-lifetime** *start-time* **infinite** | *end-time*| **duration** *seconds*
12. **send-lifetime** *start-time* **infinite** | *end-time* | **duration** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**ipv6 authentication mode eigrp** *as-number* **md5** **Example:** `Device(config-if)# ipv6 authentication mode eigrp 1 md5`	Specifies the type of authentication used in EIGRP for IPv6 packets.
Step 6	**ipv6 authentication key-chain eigrp** *as-number key-chain* **Example:** `Device(config-if)# ipv6 authentication key-chain eigrp 1 chain1`	Enables authentication of EIGRP for IPv6 packets.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits to global configuration mode.
Step 8	**key chain** *name-of-chain* **Example:** `Device(config)# key chain chain1`	Identifies a group of authentication keys. • Use the name specified in Step 5.

	Command or Action	Purpose
Step 9	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies an authentication key on a key chain.
Step 10	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string chain 1`	Specifies the authentication string for a key.
Step 11	**accept-lifetime** *start-time* **infinite** | *end-time*| **duration** *seconds* **Example:** `Device(config-keychain-key)# accept-lifetime 14:30:00 Jan 10 2006 duration 7200`	Sets the time period during which the authentication key on a key chain is received as valid.
Step 12	**send-lifetime** *start-time* **infinite** | *end-time* | **duration** *seconds* **Example:** `Device(config-keychain-key)# send-lifetime 15:00:00 Jan 10 2006 duration 3600`	Sets the time period during which an authentication key on a key chain is valid to be sent.

Overriding the Next Hop in EIGRP

EIGRP will, by default, set the IPv6 next-hop value to be itself for routes that it is advertising, even when advertising those routes back out the same interface where it learned them. Perform this task to change this default and instruct EIGRP to use the received next-hop value when advertising these routes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **no ipv6 next-hop-self eigrp** *as-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**no ipv6 next-hop-self eigrp** *as-number* **Example:** `Device(config-if)# no ipv6 next-hop-self eigrp 1`	Changes the default IPv6 next-hop value and instructs EIGRP to use the received next-hop value.

Adjusting the Interval Between Hello Packets in EIGRP for IPv6

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 hello-interval eigrp** *as-number seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.
Step 4	**ipv6 hello-interval eigrp** *as-number seconds* **Example:** `Device(config)# ipv6 hello-interval eigrp 1 10`	Configures the hello interval for the EIGRP for IPv6 routing process designated by an autonomous system number.

Adjusting the Hold Time in EIGRP for IPv6

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.

Perform this task to 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 nonbroadcast multi-access (NBMA) networks, the default hold time is 180 seconds. The hold time should be changed if the hello-interval value is changed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **ipv6 hold-time eigrp** *as-number seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies the interface on which EIGRP is configured.

	Command or Action	Purpose
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**ipv6 hold-time eigrp** *as-number seconds* **Example:** `Device(config)# ipv6 hold-time eigrp 1 40`	Configures the hold time for a particular EIGRP for IPv6 routing process designated by the autonomous system number.

Disabling Split Horizon in EIGRP for IPv6

By default, split horizon is enabled on all interfaces. 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.

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 multipoint GRE), situations can arise for which this behavior is not ideal. For these situations, including networks in which you have EIGRP configured, you may want to disable split horizon.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no shut**
5. **no ipv6 split-horizon eigrp** *as-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:**	Specifies the interface on which EIGRP is configured.

	Command or Action	Purpose
	`Device(config)# interface GigabitEthernet 0/0/0`	
Step 4	**no shut** **Example:** `Device(config)# no shut`	Enables no shut mode so the routing process can start running.
Step 5	**no ipv6 split-horizon eigrp** *as-number* **Example:** `Device(config-if)# no ipv6 split-horizon eigrp 101`	Disables EIGRP for IPv6 split horizon on the specified interface.

Configuring EIGRP Stub Routing for Greater Network Stability

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 devices. Instead, distribution devices to which the stub device is connected answer the query on behalf of the stub device. 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 devices to prevent those remote devices from appearing as transit paths to the hub devices.

Caution EIGRP stub routing should be used only on stub devices. A stub device is defined as a device connected to the network core or distribution layer through which core transit traffic should not flow. A stub device should not have any EIGRP neighbors other than distribution devices.

Configuring a Device for EIGRP Stub Routing

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eigrp stub receive-only | leak-map | connected | static | summary | redistributed**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router eigrp** *as-number* **Example:** `Device(config)# ipv6 router eigrp 1`	Specifies the EIGRP for IPv6 routing process to be configured.
Step 4	**eigrp stub receive-only | leak-map | connected | static | summary | redistributed** **Example:** `Device(config-router)# eigrp stub`	Configures a device as a stub using EIGRP.

Verifying EIGRP Stub Routing

SUMMARY STEPS

1. **enable**
2. **show ipv6 eigrp neighbors detail** *interface-type* | *as-number* | **static**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 eigrp neighbors detail** *interface-type* | *as-number* | **static** **Example:** `Device# show ipv6 eigrp neighbors detail`	Displays the neighbors discovered by EIGRP for IPv6. This command is performed on the distribution layer device to view the status of the remote device.

Customizing an EIGRP for IPv6 Routing Process

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 logged.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eigrp log-neighbor-changes**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router eigrp** *as-number* **Example:** `Device(config)# ipv6 router eigrp 1`	Specifies the EIGRP for IPv6 routing process to be configured.
Step 4	**eigrp log-neighbor-changes** **Example:** `Device(config-router)# eigrp log-neighbor-changes`	Enables the logging of changes in EIGRP for IPv6 neighbor adjacencies.

Configuring Intervals Between Neighbor Warnings

When neighbor warning messages occur, they are logged by default.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **eigrp log-neighbor-warnings** [*seconds*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router eigrp** *as-number* **Example:** `Device(config)# ipv6 router eigrp 1`	Specifies the EIGRP for IPv6 routing process to be configured.
Step 4	**eigrp log-neighbor-warnings** [*seconds*] **Example:** `Device(config-router)# eigrp log-neighbor-warnings 300`	Configures the logging intervals of EIGRP neighbor warning messages.

Adjusting EIGRP for IPv6 Metric Weights

EIGRP for IPv6 uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. You can use the **metric weights** command to adjust the default behavior of EIGRP for IPv6 routing and metric computations. EIGRP for IPv6 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.

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 (e.g., GigabitEthernet, FastEthernet, Ethernet), the route with the lowest metric reflects the most desirable path to a destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router eigrp** *as-number*
4. **metric weights** *tos k1 k2 k3 k4 k5*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 router eigrp** *as-number* **Example:** `Device(config)# ipv6 router eigrp 1`	Specifies the EIGRP for IPv6 routing process to be configured.
Step 4	**metric weights** *tos k1 k2 k3 k4 k5* **Example:** `Device(config-router)# metric weights 0 2 0 2 0 0`	Tunes EIGRP metric calculations.

Deleting Entries from EIGRP for IPv6 Routing Tables

SUMMARY STEPS

1. **enable**
2. **clear ipv6 eigrp** [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 eigrp** [*as-number*] [**neighbor** [*ipv6-address* | *interface-type interface-number*]] **Example:** `Device# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32`	Deletes entries from EIGRP for IPv6 routing tables. The routes that are cleared are the routes that were learned by the specified device.

Configuration Examples for IPv6 Routing EIGRP Support

Example: Configuring EIGRP to Establish Adjacencies on an Interface

EIGRP for IPv6 is configured directly on the interfaces over which it runs. This example shows the minimal configuration required for EIGRP for IPv6 to send hello packets in order to establish adjacencies on GigabitEthernet 0/0/0:

```
ipv6 unicast-routing
interface gigabitethernet0/0/0
no shut
  ipv6 enable
  ipv6 eigrp 1
!
ipv6 router eigrp 1
  eigrp router-id 10.1.1.1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CEF commands	*Cisco IOS IP Switching Command Reference*
EIGRP commands	*Cisco IOS IP Routing: EIGRP Command Reference*
NSF with SSO deployment	Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 4724	*Graceful Restart Mechanism for BGP*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Routing: EIGRP Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for IPv6 Routing: EIGRP Support

Feature Name	Releases	Feature Information
IPv6 Routing: EIGRP Support		Customers can configure EIGRP to route IPv6 prefixes. There is no linkage between EIGRP for IPv4 and EIGRP for IPv6; they are configured and managed separately. However, the configuration of EIGRP for IPv4 and IPv6 is similar and provides operational familiarity and continuity. The following commands were introduced or modified: **accept-lifetime**, **clear ipv6 eigrp**, **eigrp log-neighbor-changes**, **eigrp log-neighbor-warnings**, **eigrp router-id**, **eigrp stub**, **ipv6 authentication key-chain eigrp**, **ipv6 authentication mode eigrp**, **ipv6 eigrp**, **ipv6 hello-interval eigrp**, **ipv6 hold-time eigrp**, **ipv6 next-hop-self eigrp**, **ipv6 router eigrp**, **ipv6 split-horizon eigrp**, **ipv6 summary-address eigrp**, **ipv6 unicast-routing**, **key**, **key chain**, **key-string**, **metric weights**, **send-lifetime**, **show ipv6 eigrp**, **show ipv6 eigrp neighbors**.

Feature Name	Releases	Feature Information
EIGRP IPv6 VRF Lite		The EIGRP IPv6 VRF Lite feature provides EIGRP IPv6 support for multiple VRFs. EIGRP for IPv6 can operate in the context of a VRF. The EIGRP IPv6 VRF Lite feature provides separation between routing and forwarding, providing an additional level of security because no communication between devices belonging to different VRFs is allowed unless it is explicitly configured. The EIGRP IPv6 VRF Lite feature simplifies the management and troubleshooting of traffic belonging to a specific VRF. The EIGRP IPv6 VRF Lite feature is available only in EIGRP named configurations. There are no new or modified commands for this feature.

CHAPTER 4

EIGRP MIB

The EIGRP MIB feature provides complete Enhanced Interior Gateway Routing Protocol (EIGRP) support for GET requests and limited notification (also known as trap) support for neighbor authentication failure, neighbor down, and stuck-in-active (SIA) events. This MIB is accessed through remote Simple Network Management Protocol (SNMP) software clients. The EIGRP IPv6 MIB feature enables IPv6 support for the EIGRP MIB.

- Finding Feature Information, on page 79
- Prerequisites for EIGRP MIB, on page 79
- Restrictions for EIGRP MIB, on page 80
- Information About EIGRP MIB, on page 80
- How to Enable EIGRP MIB, on page 86
- Configuration Examples for EIGRP MIB, on page 87
- Additional References for EIGRP MIB, on page 88
- Feature Information for EIGRP MIB, on page 89

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP MIB

- An Enhanced Interior Gateway Routing Protocol (EIGRP) routing process must be enabled and a Simple Network Management Protocol (SNMP) community string must be configured on at least one device for EIGRP MIB table objects to be visible via SNMP.
- Support for EIGRP notifications (traps) is not activated until a trap destination is configured.

Restrictions for EIGRP MIB

EIGRP MIB support was not implemented for the EIGRP Prefix Limit Support feature.

Information About EIGRP MIB

EIGRP MIB Overview

The EIGRP MIB feature provides MIB support in Cisco software for Enhanced Interior Gateway Routing Protocol (EIGRP) routing processes that run over IPv4 and IPv6. The EIGRP MIB is accessed through remote Simple Network Management Protocol (SNMP) software clients. MIB table objects are accessed as read-only through GETBULK, GETINFO, GETMANY, GETONE, and GETNEXT requests. Counters for MIB table objects are cleared when the EIGRP routing process is reset or when the routing table is refreshed when you enter the **clear ip route** or **clear ip eigrp** command. Managed objects for all EIGRP routing processes are implemented as five table objects—EIGRP Interface, EIGRP Neighbor, EIGRP Topology, EIGRP Traffic Statistics, and EIGRP VPN—on a per-autonomous-system or per-VPN basis.

EIGRP Interface Table

The EIGRP Interface table contains information and statistics for all interfaces on which the Enhanced Interior Gateway Routing Protocol (EIGRP) has been configured. The objects in this table are populated on a per-interface basis. The table below describes EIGRP Interface table objects and the values populated for each object.

Table 5: EIGRP Interface Table Object Descriptions

EIGRP Interface Table Object	Description
cEigrpAcksSuppressed	Total number of individual acknowledgment packets that have been suppressed and combined in an already enqueued outbound reliable packet on an interface.
cEigrpAuthKeyChain	The name of the authentication key chain that is configured on the interface. The key chain is a reference to the set of secret keys that need to be accessed to determine the key string that needs to be used.
cEigrpAuthMode	The authentication mode that is configured for traffic that uses the interface. A value of 0 is displayed when no authentication is enabled. A value of 1 is displayed when message digest algorithm 5 (MD5) authentication is enabled.
cEigrpCRpkts	Total number conditional receive (CR) packets sent from the interface.
cEigrpHelloInterval	The configured time interval (in seconds) between hello packet transmissions on the interface.
cEigrpPacingReliable	The configured time interval (in milliseconds) between EIGRP packet transmissions on the interface when the reliable transport is used.

EIGRP Interface Table Object	Description
cEigrpPacingUnreliable	The configured time interval (in milliseconds) between EIGRP packet transmissions on the interface when the unreliable transport is used.
cEigrpPeerCount	Total number of neighbor adjacencies formed through the interface.
cEigrpPendingRoutes	Total number of routing updates that are queued for transmission on the interface.
cEigrpMcastExcept	Total number of EIGRP multicast exception transmissions that have occurred on the interface.
cEigrpMeanSrtt	The computed smooth round-trip time (SRTT) for packets that were transmitted to and received from all neighbors on the interface.
cEigrpMFlowTimer	The configured multicast flow control timer value (in milliseconds) for the interface.
cEigrpOOSrcvd	Total number of out-of-sequence packets received on the interface.
cEigrpRetranSent	Total number of packet retransmissions sent from the interface.
cEigrpRMcasts	Total number of reliable (acknowledgment required) multicast packets that were transmitted on the interface.
cEigrpRUcasts	Total number of reliable (acknowledgment required) unicast packets that were transmitted on the interface.
cEigrpUMcasts	Total number of unreliable (no acknowledgment required) multicast packets that were transmitted on the interface.
cEigrpUUcasts	Total number of unreliable (no acknowledgment required) unicast packets that were transmitted on the interface.
cEigrpXmitNextSerial	The serial number of the next packet that is queued for transmission on the interface.
cEigrpXmitReliableQ	Total number of packets waiting in the reliable transport transmission queue (acknowledgment required).
cEigrpXmitUnreliableQ	Total number of packets waiting in the unreliable transport transmission queue (no acknowledgment required).

EIGRP Neighbor Table

The EIGRP Neighbor table contains information about Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors with 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. The table below describes EIGRP Neighbor table objects and the values populated for each object.

Table 6: EIGRP Neighbor Table Object Descriptions

EIGRP Neighbor Table Object	Description
cEigrpHoldTime	The hold timer value for an adjacency with a neighbor. If this timer expires, the neighbor is declared down and removed from the neighbor table.
cEigrpLastSeq	The number of the last sequence of a packet transmitted to a neighbor. This table object value increases as the sequence number increases.
cEigrpPeerAddr	The source IP address of a neighbor that was used to establish an EIGRP adjacency with the local device. The source IP address can be an IPv4 or IPv6 address.
cEigrpPeerAddrType	The protocol type of the remote source IP address that was used by a neighbor to establish an EIGRP adjacency with the local device. The protocol type can be IPv4 or IPv6.
cEigrpPeerIfIndex	The index of the local interface through which a neighbor can be reached.
cEigrpPeerInterface	The name of the local interface through which a neighbor can be reached.
cEigrpPktsEnqueued	Total number of EIGRP packets (all types) currently queued for transmission to a neighbor.
cEigrpRetrans	Cumulative number of packets retransmitted to a neighbor while the neighbor is in an up state.
cEigrpRetries	Total number of times an unacknowledged packet is sent to a neighbor.
cEigrpRto	The computed retransmission timeout (RTO) for a neighbor. The value for this table object is computed as an aggregate average of the time required for packet delivery.
cEigrpSrtt	The computed smooth round-trip time (SRTT) for packets that are transmitted to and received from a neighbor.
cEigrpUpTime	The period for which the EIGRP adjacency to a neighbor has been in an up state. The time period is displayed in hours:minutes:seconds.
cEigrpVersion	EIGRP version information reported by a remote neighbor.

EIGRP Topology Table

The EIGRP Topology table contains information about Enhanced Interior Gateway Routing Protocol (EIGRP) routes that are received in updates and routes that are locally originated. EIGRP sends routing updates to and receives routing updates from adjacent routers with which adjacencies have been formed. The objects in this table are populated on a per-topology table entry (route) basis. The table below describes EIGRP Topology table objects and the values populated for each object.

Table 7: EIGRP Topology Table Object Descriptions

EIGRP Topology Table Object	Description
cEigrpActive	Status of 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 is in active state. A value of 2 is displayed when a route is in passive state (normal).
cEigrpDestSuccessors	Total number of successors (a successor is 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 value increases each time a successor is added.
cEigrpDistance	The computed distance to the destination network entry from the local router.
cEigrpFdistance	The feasible (best) distance to a destination network. This value is used to calculate a feasible successor for a topology table entry.
cEigrpNextHopAddress	The next-hop IP address for a route in a topology table entry. The next hop can be an IPv4 or IPv6 address.
cEigrpNextHopAddressType	The protocol type of the next-hop IP address for a route in a topology table entry. The protocol type can be IPv4 or IPv6.
cEigrpNextHopInterface	The interface through which the next-hop IP address is reached to forward traffic to the destination.
cEigrpReportDistance	The computed distance to the destination network in the topology entry as reported by the originator of the route.
cEigrpRouteOriginAddr	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. The route origin address can be an IPv4 or IPv6 address.
cEigrpRouteOriginType	The protocol type of the IP address defined as the origin of the topology route entry. The protocol type can be IPv4 or IPv6.
cEigrpStuckInActive	Stuck-in-active (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 is in SIA state (that is, no reply has been received for queries about alternate paths). SIA queries are transmitted when a route is placed in this state.

EIGRP Traffic Statistics Table

The EIGRP Traffic Statistics table contains counters and statistics for specific types of Enhanced Interior Gateway Routing Protocol (EIGRP) packets that are sent and the related, collective information that is generated. Objects in this table are populated on a per-autonomous-system basis. Objects in this table are populated for adjacencies formed on interfaces that have IP addresses configured under EIGRP network statements. The table below describes EIGRP Traffic Statistics table objects and the values populated for each object.

Table 8: EIGRP Traffic Statistics Table Object Descriptions

EIGRP Traffic Statistics Table Object	Description
cEigrpAcksRcvd	Total number of acknowledgment packets that are received in response to the transmitted update packets. This table object value increases as packets are received.
cEigrpAcksSent	Total number of acknowledgment packets that are transmitted in response to received update packets. This table object value increases as packets are transmitted.
cEigrpAsRouterId	The configured or automatically selected router ID in 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.
cEigrpAsRouterIdType	The type of IP address that is used as the router ID. The value for this table object is an IPv4 address.
cEigrpInputQDrops	Total number of packets that are dropped from the input queue because the input queue was full. This table object value increases each time a packet is dropped.
cEigrpInputQHighMark	The highest number of packets that have been in the input queue. This table object value increases only when the previous highest number is exceeded.
cEigrpHeadSerial	Internal sequencing number (serial) that is 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.
cEigrpHellosRcvd	Total number of received hello packets. This table object value increases as packets are received.
cEigrpHellosSent	Total number of hello packets transmitted. This table object value increases as packets are transmitted.
cEigrpNbrCount	Total number of live neighbors. This table object value increases or decreases as peering sessions are established or expired.
cEigrpNextSerial	Serial number that is applied to the next route in the sequence.
cEigrpQueriesSent	Total number of alternate route query packets that are transmitted. This table object value increases as packets are transmitted.
cEigrpQueriesRcvd	Total number of alternate route query packets that are received. This table object value increases as packets are received.
cEigrpRepliesSent	Total number of reply packets that are transmitted in response to the received query packets. This table object value increases as packets are transmitted.
cEigrpRepliesRcvd	Total number of reply packets that are received in response to transmitted query packets. This table object value increases as packets are received.

EIGRP Traffic Statistics Table Object	Description
cEigrpSiaQueriesSent	Total number of query packets that are sent in response to a destination that is in a stuck-in-active (SIA) state for a down peer. This table object value increases each time an SIA query packet is sent.
cEigrpSiaQueriesRcvd	Total number of SIA query packets that are received from neighbors searching for an alternate path to a destination. This table object value increases each time an SIA query packet is received.
cEigrpTopoRoutes	Total number of EIGRP-derived routes in the topology table. This table object value increases if a route is added.
cEigrpUpdatesRcvd	Total number of routing update packets that are received. This table object value increases as packets are received.
cEigrpUpdatesSent	Total number of routing update packets that are transmitted. This table object value increases as packets are transmitted.
cEigrpXmitDummies	Total number of temporary entries in the topology table. Dummies are internal entries and not transmitted in routing updates.
cEigrpXmitPendReplies	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.

EIGRP VPN Table

The EIGRP VPN table contains information about VPNs that are configured to run an Enhanced Interior Gateway Routing Protocol (EIGRP) process. Devices index VPN routes by using the VPN name and the EIGRP autonomous system number. The table below describes the EIGRP VPN table object and the value populated for that object.

Table 9: EIGRP VPN Table Object Description

EIGRP VPN Table Object	Description
cEigrpVpnName	The VPN routing and forwarding (VRF) name. Only VRFs that are configured to run an EIGRP routing process are populated.

EIGRP Notifications

The EIGRP MIB provides limited notification (trap) support for neighbor authentication failure, neighbor down, and stuck-in-active (SIA) events. Use the **snmp-server enable traps eigrp** command to enable Enhanced Interior Gateway Routing Protocol (EIGRP) notifications or traps on a Cisco device. To activate support for trap events, you must configure a trap destination by using the **snmp-server host** command and define a community string by using the **snmp-server community** command. EIGRP notifications are described in the table below.

Table 10: EIGRP Notifications

EIGRP Notifications	Description
cEigrpAuthFailureEvent	When EIGRP message digest algorithm 5 (MD5) authentication is enabled on any interface and neighbor adjacencies are formed, a notification is sent if any adjacency goes down because of an authentication failure. This notification will be sent once per down event. This notification includes the source IP address of the neighbor from which the authentication failure occurred.
cEigrpNbrDownEvent	This notification is sent when a neighbor goes down for any reason, such as hold time expiry, neighbor shutdown, interface shutdown, SIA events, or authentication failure. If a neighbor is down because of an authentication failure, both cEigrpAuthFailureEvent and cEigrpNbrDownEvent notifications are sent.
cEigrpRouteStuckInActive	During the query phase for a new route to a destination network, the route is placed in active state (during which an alternate path is actively sought) and a query packet is broadcast to the network. If no replies are received for the query, SIA query packets are broadcast. If no replies are received for the SIA queries, the neighbor adjacency is dropped, the route is declared to be in an SIA state, and this notification is sent.

How to Enable EIGRP MIB

Enabling EIGRP MIB Notifications

Perform this task to specify a Simple Network Management Protocol (SNMP) server host, configure an SNMP community access string, and enable Enhanced Interior Gateway Routing Protocol (EIGRP) MIB notifications.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. **snmp-server community** *string*
5. **snmp-server enable traps** [*notification-type*]
6. **end**
7. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs** | **version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Device(config)# snmp-server host 10.0.0.1 traps version 2c NETMANAGER`	Specifies the destination server host or destination address for SNMP notifications.
Step 4	**snmp-server community** *string* **Example:** `Device(config)# snmp-server community EIGRP1NET1A`	Configures a community access string to permit SNMP access to the local router by the remote SNMP software client. **Note** Cisco software supports both IPv4 and IPv6.
Step 5	**snmp-server enable traps** [*notification-type*] **Example:** `Device(config)# snmp-server enable traps eigrp`	Enables SNMP support for EIGRP notifications. • Notifications can be configured for only neighbor authentication failure, neighbor down, and stuck-in-active (SIA) events.

Step 6	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to privileged EXEC mode.

Step 7	**show running-config** **Example:** `Device# show running-config | include snmp`	Displays contents of the current running configuration file. • Use the output modifier "|" to display and verify the SNMP configuration.

Configuration Examples for EIGRP MIB

Example: Enabling EIGRP MIB Notifications

The following example shows how to specify a Simple Network Management Protocol (SNMP) server host, configure an SNMP community string, and enable support for Enhanced Interior Gateway Routing Protocol (EIGRP) notifications:

```
Device(config)# snmp-server host 10.0.0.2 traps version 2c NETMANAGER eigrp
Device(config)# snmp-server community EIGRP1NET1A
Device(config)# snmp-server enable traps eigrp
```

The following sample output from the **show running-config** command displays the EIGRP MIB configuration:

```
Device# show running-config | include snmp

snmp-server community EIGRP1NET1A
snmp-server enable traps eigrp
snmp-server host 10.0.0.2 version 2c NETMANAGER eigrp
```

Additional References for EIGRP MIB

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	EIGRP Command Reference
Basic EIGRP configuration tasks	“Configuring EIGRP” module in the *EIGRP Configuration Guide*
SNMP commands	SNMP Support Command Reference
SNMP configuration tasks	“Configuring SNMP Support” module in the *SNMP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internet: MIB-II

MIBs

MIB	MIBs Link
CISCO-EIGRP-MIB.my	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for EIGRP MIB

Feature Name	Releases	Feature Information
EIGRP IPv6 MIB	15.2(4)S 15.3(1)T	The EIGRP IPv6 MIB feature enables IPv6 support for the EIGRP MIB. No commands were introduced or modified by this feature.
EIGRP MIB		The EIGRP MIB feature provides complete Enhanced Interior Gateway Routing Protocol (EIGRP) support for GET requests and limited notification (trap) support for neighbor authentication failure, neighbor down, and stuck-in-active (SIA) events. This MIB is accessed through remote Simple Network Management Protocol (SNMP) software clients. The following commands were introduced or modified by this feature: **snmp-server enable traps eigrp** and **snmp-server host**.

CHAPTER 5

EIGRP MPLS VPN PE-CE Site of Origin

The EIGRP MPLS VPN PE-CE Site of Origin 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. Site of Origin (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 backdoor links is provided by this feature when installed on PE routers that support EIGRP MPLS VPNs.

- Finding Feature Information, on page 91
- Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin, on page 91
- Restrictions for EIGRP MPLS VPN PE-CE Site of Origin, on page 92
- Information About EIGRP MPLS VPN PE-CE Site of Origin, on page 92
- How to Configure EIGRP MPLS VPN PE-CE Site of Origin Support, on page 94
- Configuration Examples for EIGRP MPLS VPN PE-CE SoO, on page 97
- Additional References, on page 98
- Feature Information for EIGRP MPLS VPN PE-CE Site of Origin, on page 99
- Glossary, on page 100

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP MPLS VPN PE-CE Site of Origin

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 XE Release 2.1 or a later release, which provides support for the SoO extended community.

Restrictions for EIGRP MPLS VPN PE-CE Site of Origin

- If a VPN site is partitioned and the SoO extended community attribute is configured on a backdoor router interface, the backdoor link cannot be used as an alternate path to reach prefixes originated in other partitions of the same site.
- A unique SoO value must be configured for each individual VPN site. The same value must be configured on all provider edge and customer edge 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

EIGRP MPLS VPN PE-CE Site of Origin Support Overview

The EIGRP MPLS VPN PE-CE Site of Origin 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 readvertisement 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 backdoor 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. 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 Support for Backdoor Links

The EIGRP MPLS VPN PE-CE Site of Origin (SoO) feature introduces support for backdoor links. A backdoor 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. Backdoor 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 backdoor link so that the route though the backdoor router is not selected unless there is a VPN link failure.

The SoO extended community is defined on the interface of the backdoor 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 backdoor router receives an EIGRP update (or reply) from a neighbor across the backdoor link, the router checks the update for an SoO value. If the SoO value in the EIGRP update matches the SoO value on the local backdoor interface, the route is rejected and not added to the EIGRP topology table. This scenario 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 backdoor link by the backdoor router in the other VPN site. SoO filtering on the backdoor 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 backdoor router interface, the backdoor link cannot be used as an alternate path to reach prefixes originated in other partitions of the same site.

If this feature is enabled on the PE routers and the backdoor routers in the customer sites, and SoO values are defined on both the PE and backdoor routers, both the PE and backdoor 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 Diffusing Update Algorithm (DUAL) computations.

Router Interoperation with the Site of Origin Extended Community

The configuration of an SoO extended community allows routers that support EIGRP MPLS VPN PE-CE Site of Origin 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 an 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 because it was learned from another PE router or from a backdoor link. This behavior is designed to prevent routing loops.

- A received route from a CE router is configured with an 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 added to 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 an 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.

Redistribution of BGP VPN Routes That Carry the Site of Origin into EIGRP

When an EIGRP routing process on a PE router redistributes BGP VPN routes into an 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 adding 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 nontransitive 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 BGP cost community support for EIGRP MPLS VPN PE-CE network topologies was introduced, BGP preferred locally sourced routes over routes learned from BGP peers. Backdoor links in an EIGRP MPLS VPN topology were preferred by BGP when the backdoor link was learned first. (A backdoor 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 “prebest path” 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 “prebest 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 XE Release 2.1 or later is installed on the PE routers or the CE and backdoor router at the customer sites.

For more information about the BGP Cost Community feature, see to the BGP Cost Community module in the *Cisco IOS XE IP Routing: BGP Configuration Guide, Release 2*.

Benefits of the EIGRP MPLS VPN PE-CE Site of Origin Support Feature

The configuration of the EIGRP MPLS VPN PE-CE Site of Origin Support feature introduces per-site VPN filtering, which improves support for complex topologies, such as MPLS VPNs with backdoor links, CE routers that are dual-homed to different 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 Support

Configuring the Site of Origin 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. 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.

Before you begin

- Border Gateway Protocol (BGP) is configured in the network core (or the service provider backbone).
- Configure an EIGRP MPLS VPN before configuring this feature.

- 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** *type number*
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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-name* {**permit** | **deny**} [*sequence-number*] **Example:** `Router(config)# route-map Site-of-Origin permit 10`	Enters route-map configuration mode and creates a route map. • The route map is created in this step so that SoO extended community can be applied.

Step 4	**set extcommunity** {**rt** *extended-community-value* [**additive**] | **soo** *extended-community-value*}
	Example:
	`Router(config-route-map)# set extcommunity soo 100:1`
		Sets BGP extended community attributes.
		• The **rt** keyword specifies the route target extended community attribute.
		• The **soo** keyword specifies the site of origin extended community attribute.
		• The *extended-community-value*argument specifies the value to be set. The value can be one of the following formats:

	Command or Action	Purpose
		• autonomous-system-number: network-number • ip-address: network-number The colon is used to separate the autonomous system number and network number or IP address and network number. • The **additive** keyword adds a route target to the existing route target list without replacing any existing route targets.
Step 5	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/0`	Enters interface configuration mode to configure the specified interface.
Step 7	**ip vrf forwarding** *vrf-name* **Example:** `Router(config-if)# ip vrf forwarding VRF1`	Associates the VRF with an interface or subinterface. • 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.
Step 8	**ip vrf sitemap** *route-map-name* **Example:** `Router(config-if)# ip vrf sitemap Site-of-Origin`	Associates the VRF with an interface or subinterface. • The route map name configured in this step should match the route map name created to apply the SoO extended community in Step 3.
Step 9	**ip address** *ip-address subnet-mask* **Example:** `Router(config-if)# ip address 10.0.0.1 255.255.255.255`	Configures the IP address for the interface. • The IP address needs to be reconfigured after enabling VRF forwarding.

Step 10	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and enters privileged EXEC mode.

What to Do Next

- For mixed EIGRP MPLS VPN network topologies that contain backdoor routes, the next task is to configure the “prebest path” cost community for backdoor 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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 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**] **Example:** `Router# show ip bgp vpnv4 all 10.0.0.1`	Displays VPN address information from the BGP table. • Use the **show ip bgp vpnv4** command with the **all** keyword to verify that the specified route has been configured with the SoO extended community attribute.

Configuration Examples for EIGRP MPLS VPN PE-CE SoO

Example Configuring the Site of Origin Extended Community

The following example, beginning in global configuration mode, configures SoO extended community 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
```

Example Verifying the Site of Origin Extended Community

The following 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
```

The following example shows how to display EIGRP metrics for specified internal services and external services:

```
Router# show eigrp address-family ipv4 4453 topology 10.10.10.0/24
EIGRP-IPv4 VR(virtual-name) Topology Entry for AS(4453)/ID(10.0.0.1) for 10.10.10.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 128256
  Descriptor Blocks:
  0.0.0.0 (Null0), from Connected, Send flag is 0x0
      Composite metric is (128256/0), service is Internal
      Vector metric:
        Minimum bandwidth is 10000000 Kbit
        Total delay is 5000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1514
        Hop count is 0
        Originating router is 10.0.0.1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
BGP Cost Community feature and the “pre-bestpath” point of insertion	BGP Cost Community module of the *Cisco IOS IP Routing: BGP Configuration Guide*
CEF commands	*Cisco IOS IP Switching Command Reference*
CEF configuration tasks	Cisco Express Forwarding Overview module of the *Cisco IOS IP Switching Configuration Guide*
EIGRP commands	*Cisco IOS IP Routing: EIGRP Command Reference*

Related Topic	Document Title
EIGRP configuration tasks	Configuring EIGRP
MPLS VPNs	MPLS Layer 3 VPNs module of the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP MPLS VPN PE-CE Site of Origin

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for EIGRP MPLS VPN PE-CE Site of Origin (SoO)

Feature Name	Releases	Feature Information
EIGRP MPLS VPN PE-CE Site of Origin (SoO)	Cisco IOS XE Release 2.1	The EIGRP MPLS VPN PE-CE SoO feature introduces the capability to filter MPLS VPN traffic on a per-site basis for EIGRP networks. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following command was introduced or modified by this feature: **ip vrf sitemap**.

Glossary

AFI --Address Family Identifier. Carries the identity of the network layer protocol that is associated with the network address.

Backdoor link --A link connecting two backdoor routers.

Backdoor router --A router that connects two or more sites, that are also connected to each other through an MPLS VPN EIGRP PE to CE links.

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). BGP 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 best path calculation.

customer edge (CE) router --A router that belongs to a customer network, that 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.

CHAPTER 6

EIGRP Nonstop Forwarding 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.

- Finding Feature Information, on page 101
- Prerequisites for EIGRP Nonstop Forwarding Awareness, on page 101
- Restrictions for EIGRP Nonstop Forwarding Awareness, on page 102
- Information About EIGRP Nonstop Forwarding Awareness, on page 102
- How to Configure EIGRP Nonstop Forwarding Awareness, on page 105
- Configuration Examples for EIGRP Nonstop Forwarding Awareness, on page 109
- Additional References for EIGRP Nonstop Forwarding Awareness, on page 110
- Feature Information for EIGRP Nonstop Forwarding Awareness, on page 110

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP Nonstop Forwarding Awareness

This module 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 software that supports NSF awareness or NSF capabilities must be installed.

Restrictions for EIGRP Nonstop Forwarding Awareness

- All neighboring devices that are participating in EIGRP NSF must be NSF-capable or NSF-aware.
- EIGRP NSF awareness does not support two neighbors that are performing an NSF restart operation at the same time. However, both neighbors will still re-establish peering sessions after the NSF restart operation is complete.

Information About EIGRP Nonstop Forwarding Awareness

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. 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.

Note NSF supports IPv4 in classic mode and named mode. NSF supports IPv6 in named mode. For more information about EIGRP IPv6 NSF, see the “EIGRP IPv6 NSF/GR” module in the *IP Routing: EIGRP Configuration Guide*.

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, to maintain the peering session with this neighbor, to retain known routes, and to continue to forward packets for these routes. The deployment of EIGRP NSF awareness can minimize the effects 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 graceful-restart purge-time 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 graceful-restart purge-time** 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 graceful-restart purge-time timer expires. If the graceful-restart purge-time 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 Timers

NSF/GR supports three types of timers: namely, signal timer, converge timer, and graceful-restart purge-time timer.

The signal timer can be configured to adjust the maximum time of the initial restart period where the restarting router sends hello packets with the restart(RS)-bit set. When the timer expires, if the restarting router has not learnt about any neighbor, or has not learnt about any NSF-aware neighbor, or has not received all the updates from the neighbors, the routing information base is notified for convergence. The default value for the signal timer is 20 seconds. The **timers nsf signal** command is used to configure the signal timer.

The converge timer can be configured to adjust the maximum time the restarting router waits for the end-of-table (EOT) indications from all the neighbors. The default value for the converge timer is 120 seconds. The **timers nsf converge** command is used to configure the converge timer.

The graceful-restart purge-time timer can be configured to adjust the maximum waiting time to receive the convergent signal from the restarting router. The graceful-restart purge-timer is used when the NSF-aware peer does not receive the EOT indication from the restarting neighbor. When the graceful-restart purge-timer expires, the EIGRP peer scans the topology table for the stale routes from the restarting neighbor and changes the stale routes to active, thereby allowing EIGRP peers to find alternate routes instead of waiting during a long switchover operation. The default value for the graceful-restart purge-time timer is 240 seconds. The **timers graceful-restart purge-time** command is used to configure the graceful-restart purge-timer. The **timers graceful-restart purge-time** command is accepted under router configuration mode for IPv4 EIGRP classic mode and under address-family configuration mode for EIGRP named mode.

How to Configure EIGRP Nonstop Forwarding Awareness

Enabling EIGRP Nonstop Forwarding Awareness

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **address-family ipv4 autonomous-system** *number*
5. **nsf**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Configures an EIGRP routing process in classic mode and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *number* **Example:**	Enters address-family configuration mode to configure an EIGRP routing instance.

	Command or Action	Purpose
	`Device(config-router)# address-family ipv4 autonomous-system 1`	
Step 5	**nsf** **Example:** `Device(config-router-af)# nsf`	Enables NSF for the specific address family on the router.

Step 6	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address-family configuration mode and returns to privileged EXEC mode.

Modifying EIGRP Nonstop Forwarding Awareness Timers

Perform this task to modify EIGRP NSF timers. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *name*
4. **address-family ipv4 autonomous-system** *number*
5. **timers nsf signal** *seconds*
6. **timers nsf converge** *seconds*
7. **timers graceful-restart purge-time** *seconds*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *name* **Example:** `Device(config)# router eigrp e1`	Configures an EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**address-family ipv4 autonomous-system** *number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 1`	Enters address-family configuration mode to configure an EIGRP routing instance.
Step 5	**timers nsf signal** *seconds* **Example:** `Device(config-router-af)# timers nsf signal 15`	Sets the initial restart period wherein the restarting router sends hello packets with the RS-bit set. The default is 20 seconds.
Step 6	**timers nsf converge** *seconds* **Example:** `Device(config-router-af)# timers nsf converge 60`	Sets the maximum time that the restarting router has to wait for the EOT indications from all neighbors. The default is 120 seconds.
Step 7	**timers graceful-restart purge-time** *seconds* **Example:** `Device(config-router-af)# timers graceful-restart purge-time 150`	Sets the graceful-restart purge time to determine the period for which an NSF-aware router that is running EIGRP will hold routes for an inactive peer. The default is 240 seconds.

Step 8	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address-family configuration mode and returns to 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 neighbors** command will need to be entered before normal redistribution will occur.

Monitoring EIGRP NSF Debug Events and Notifications

Use the following steps to monitor EIGRP NSF debug events and notifications on an NSF-aware router.

The **debug eigrp nsf** and **debug ip eigrp notifications** commands do not need to be issued together or even in the same session because 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 ip eigrp notifications**
4. **debug eigrp address-family ipv4 notifications**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eigrp nsf** **Example:** `Device# debug eigrp nsf`	Displays NSF notifications and information about NSF events in an EIGRP network on the console of the router.
Step 3	**debug ip eigrp notifications** **Example:** `Device# 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.
Step 4	**debug eigrp address-family ipv4 notifications** **Example:** `Device# debug eigrp address-family ipv4 notifications`	Displays debugging information about EIGRP address-family IPv4 event notifications.

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	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip protocols** **Example:** `Device# 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

Example: EIGRP Graceful-Restart Purge-Time Timer Configuration

The following example shows how to set the graceful-restart purge-time timer to 2 minutes:

```
Device(config-router)# timers graceful-restart purge-time 120
```

Example: Monitoring EIGRP NSF Debug Events and Notifications Configuration

The following example output shows that an NSF-aware router has received a restart notification. The NSF-aware router waits for EOT to be sent from the restarting (NSF-capable) neighbor.

```
Device# debug ip eigrp notifications

*Oct  4 11:39:18.092:EIGRP:NSF:AS2. Rec RS update from 10.100.10.1,
00:00:00. Wait for EOT.
*Oct  4 11:39:18.092:%DUAL-5-NBRCHANGE:IP-EIGRP(0) 2:Neighbor
10.100.10.1 (POS3/0) is up:peer NSF restarted
*Sep 23 18:49:07.578: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 1.1.2.1
(GigabitEthernet1/0/0) is resync: peer graceful-restart
```

Example: 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 graceful-restart purge-time timer is set to 240 seconds, which is the default value.

```
Device# show ip protocols

*** IP Routing is NSF aware ***
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 EIGRP Nonstop Forwarding Awareness

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
CEF commands	*Cisco IOS IP Switching Command Reference*
EIGRP commands	*Cisco IOS IP Routing: EIGRP Command Reference*
Nonstop forwarding (NSF)	• Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide • “Cisco Nonstop Forwarding” module in *High Availability Configuration Guide* • “EIGRP IPv6 NSF/GR” module in *IP Routing: EIGRP Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Nonstop Forwarding Awareness

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 13: Feature Information for EIGRP Nonstop Forwarding Awareness

Feature Name	Releases	Feature Information
EIGRP Nonstop Forwarding (NSF) Awareness	Cisco IOS XE Release 2.1	The EIGRP Nonstop Forwarding Awareness feature allows an NSF-aware router that is running 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. The following commands were introduced or modified: **debug eigrp nsf**, **debug ip eigrp notifications**, **show ip eigrp neighbors**, **show ip protocols**, **timers graceful-restart purge-time**, **timers nsf route-hold**.

CHAPTER 7

EIGRP Nonstop Forwarding

EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. NSF works with the SSO feature in Cisco software to minimize the amount of time that 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.

Note Throughout this document, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

- Finding Feature Information, on page 113
- Prerequisites for EIGRP Nonstop Forwarding, on page 113
- Restrictions for EIGRP Nonstop Forwarding, on page 114
- Information About EIGRP Nonstop Forwarding, on page 114
- How to Configure EIGRP Nonstop Forwarding, on page 116
- Configuration Examples for EIGRP Nonstop Forwarding, on page 119
- Additional References, on page 119
- Feature Information for EIGRP Nonstop Forwarding, on page 121

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP Nonstop Forwarding

- The networking device that is to be configured for NSF must first be configured for SSO. For more information, see the "Configuring Stateful Switchover" chapter in the *High Availability Configuration Guide*.

- All neighboring devices must be NSF-capable or NSF-aware.
- An NSF-aware device must be completely converged with the network before it can assist an NSF-capable device in an NSF restart operation.
- On platforms that support the Route Switch Processor (RSP), and where the Cisco Express Forwarding (CEF) switching mode is configurable, configure distributed CEF (dCEF) switching mode using the **ip cef distributed** command.

Note Distributed platforms that run a supporting version of Cisco software can support full NSF capabilities. These devices can perform a restart operation and can support other NSF capable peers.

Restrictions for EIGRP Nonstop Forwarding

- An NSF-aware device cannot support two NSF-capable peers that are performing an NSF restart operation at the same time. However, both neighbors will reestablish peering sessions after the NSF restart operation is complete.
- Single processor platforms that run a supporting version of Cisco software support only NSF awareness. These devices maintain adjacency and hold known routes for the NSF-capable neighbor until it signals that it is ready for the NSF-aware device to send its topology table or until the route-hold timer expires.

Information About EIGRP Nonstop Forwarding

Nonstop Forwarding

Note In the following content, the term Route Processor (RP) is used to describe the route processing engine on all networking devices, regardless of the platform designation, unless otherwise noted.

NSF works with the SSO feature in Cisco software 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 an RP switchover.

Usually, when a networking device restarts, all routing peers of that device detect that the device went down and then came back up. This transition results in what is called a routing flap, which could spread across multiple routing domains. Routing flaps caused by routing restarts create routing instabilities, which are detrimental to the overall network performance. NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

NSF allows for the forwarding of data packets to continue along known routes while the routing protocol information is being restored following a switchover. With NSF, peer networking devices do not experience routing flaps. Data traffic is forwarded through intelligent line cards or dual forwarding processors (FPs) while the standby RP assumes control from the failed active RP during a switchover. The ability of line cards and

FPs to remain up through a switchover and to be kept current with the Forwarding Information Base (FIB) on the active RP is key to NSF operation.

The NSF feature provides the following benefits:

- Improved network availability—NSF continues forwarding network traffic and application state information so that user session information is maintained after a switchover.
- Overall network stability—Network stability may be improved with the reduction in the number of route flaps that had been created when devices in the network failed and lost their routing tables.
- Neighboring devices do not detect link flapping—Because the interfaces remain up across a switchover, neighboring devices do not detect a link flap (that is, the link does not go down and come back up).
- Prevention of routing flaps—Because SSO continues forwarding network traffic in the event of a switchover, routing flaps are avoided.
- No loss of user sessions—User sessions established prior to the switchover are maintained.

NSF always runs together with SSO. SSO supported protocols and applications must be high-availability (HA)-aware. A feature or protocol is HA-aware if it maintains, either partially or completely, undisturbed operation during an RP switchover. For some HA-aware protocols and applications, state information is synchronized from the active to the standby processor.

EIGRP NSF Operations

Cisco NSF is supported by the EIGRP protocol for routing and by CEF for forwarding. EIGRP 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.

EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. The NSF-capable device notifies its neighbors that an NSF restart operation has started by setting the restart (RS) bit in a hello packet. When an NSF-aware device receives notification from an NSF-capable neighbor that an NSF-restart operation is in progress, the NSF-capable and NSF-aware devices immediately exchange their topology tables. The NSF-aware device sends an end-of-table (EOT) update packet when the transmission of its topology table is complete. The NSF-aware device then performs the following actions to assist the NSF-capable device:

- The EIGRP hello hold timer is expired to reduce the time interval set for hello packet generation and transmission. This allows the NSF-aware device to reply to the NSF-capable device more quickly reducing the amount of time required for the NSF-capable device to rediscover neighbors and rebuild the topology table.
- The route-hold timer is started. This timer is used to set the period of time that the NSF-aware device will hold known routes for the NSF-capable neighbor.
- The NSF-aware device 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 device to send its topology table or the route-hold timer expires. If the route-hold timer expires on the NSF-aware device, the NSF-aware device will discard held routes and treat the NSF-capable device as a new device joining the network and reestablishing adjacency accordingly.
- The NSF-aware device will continue to send queries to the NSF-capable device that is still converging after switchover, effectively extending the time before a stuck-in-active (SIA) condition can occur.

When the switchover operation is complete, the NSF-capable device notifies its neighbors that it has reconverged and has received all of their topology tables by sending an EOT update packet to the assisting devices. The NSF-capable device then returns to normal operation. The NSF-aware device will look for alternate paths (go active) for any routes that are not refreshed by the NSF-capable (restarting device). The NSF-aware device will then return to normal operation. If all paths are refreshed by the NSF-capable device, the NSF-aware device will immediately return to normal operation.

NSF-aware devices are completely compatible with non-NSF-aware or non-NSF-capable neighbors in an EIGRP network. A non-NSF-aware neighbor will ignore NSF capabilities and reset adjacencies and otherwise maintain the peering sessions normally.

How to Configure EIGRP Nonstop Forwarding

Configuring and Verifying EIGRP NSF

Repeat this task on each peer device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *as-number*
4. **nsf**
5. **timers nsf converge** *seconds*
6. **timers nsf signal** *seconds*
7. **timers graceful-restart purge-time** *seconds*
8. **end**
9. **show ip protocols**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Device(config)# router eigrp 109`	Enables an EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**nsf** **Example:** `Device(config-router)# nsf`	Enables NSF capabilities. • This command is enabled by default. To disable nonstop forwarding capability, use the **no** form of this command.
Step 5	**timers nsf converge** *seconds* **Example:** `Device(config-router)# timers nsf converge 120`	Use this optional command to adjust the maximum time that the restarting device will wait for the EOT notification from an NSF-capable or NSF-aware peer. • Enter this command on NSF-capable devices only.
Step 6	**timers nsf signal** *seconds* **Example:** `Device(config-router)# timers nsf signal 20`	Use this optional command to adjust the maximum time for the initial restart period. • Enter this command on NSF-capable devices only.
Step 7	**timers graceful-restart purge-time** *seconds* **Example:** `Device(config-router)# timers graceful-restart purge-time 240`	Use this optional command to set the route-hold timer to determine how long an NSF-aware EIGRP device will hold routes for an inactive peer.

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Returns to privileged EXEC mode.

Step 9	**show ip protocols** **Example:** `Device# show ip protocols`	Displays the parameters and current state of the active routing protocol process.

Troubleshooting EIGRP Nonstop Forwarding

Use the following commands in any order to troubleshoot issues with nonstop forwarding using the EIGRP protocol.

SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug ip eigrp notifications**
4. **show cef nsf**
5. **show cef state**
6. **show ip cef**
7. **show ip eigrp neighbors detail**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **debug eigrp nsf**

Example:

```
Device# debug eigrp nsf
```

Displays notifications and information about NSF events for an EIGRP routing process.

Step 3 **debug ip eigrp notifications**

Example:

```
Device# debug ip eigrp notifications
```

Displays information and notifications for an EIGRP routing process. This output includes NSF notifications and events.

Step 4 **show cef nsf**

Example:

```
Device# show cef nsf
```

Displays the current NSF state of CEF on both the active and standby RPs.

Step 5 **show cef state**

Example:

```
Device# show cef state
```

Displays the CEF state on a networking device.

Step 6 **show ip cef**

Example:

```
Device# show ip cef
```

Displays entries in the FIB that are unresolved or displays a FIB summary.

Step 7 **show ip eigrp neighbors detail**

Example:

```
Device# show ip eigrp neighbors detail
```

Displays detailed information about neighbors discovered by EIGRP.

Configuration Examples for EIGRP Nonstop Forwarding

Example: EIGRP NSF

The following sample output shows that EIGRP NSF support is present in the installed software image.

- “EIGRP NSF-aware route hold timer is . . .” is displayed in the output for either NSF-aware or NSF-capable devices, and the default or user-defined value for the route-hold timer is displayed.
- “EIGRP NSF enabled” or “EIGRP NSF disabled” appears in the output only when the NSF capability is supported by the device.

```
Device# show ip protocols

Routing Protocol is "eigrp 100"
  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 100
  EIGRP NSF-aware route hold timer is 240s
  EIGRP NSF enabled
     NSF signal timer is 20s
     NSF converge timer is 120s
  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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
EIGRP commands	IP Routing: EIGRP Command Reference

Related Topic	Document Title
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks feature	"Mobile Ad Hoc Networks for Router-to-Radio Communications" module of *the IP Mobility Configuration Guide*
EIGRP Technology Support	Enhanced Interior Gateway Routing Protocol
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol
IPv6 Routing EIGRP Support	*EIGRP Configuration Guide*
Protocol-independent features that work with EIGRP	*IP Routing: Protocol-Independent Configuration Guide*
Service Advertisement Framework	*Service Advertisement Framework Configuration Guide*
Service Advertisement Framework commands	Service Advertisement Framework Command Reference

Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	*SECURE HASH STANDARD (SHS)*
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Nonstop Forwarding

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 14: Feature Information for EIGRP Nonstop Forwarding

Feature Name	Releases	Feature Information
NSF – EIGRP		EIGRP nonstop forwarding (NSF) capabilities are exchanged by EIGRP peers in hello packets. NSF works with the SSO feature in Cisco software to minimize the amount of time that 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. The following commands were introduced or modified: **debug ip eigrp notifications**, **nsf (EIGRP)**, **router eigrp**, and **show ip eigrp neighbors**.

CHAPTER 8

EIGRP IPv6 NSF/GR

The EIGRP IPv6 NSF/GR feature allows a Nonstop Forwarding (NSF)-aware device that is running Enhanced Interior Gateway Routing Protocol (EIGRP) to forward IPv6 packets while EIGRP restarts after recovering from a failure.

- Finding Feature Information, on page 123
- Prerequisites for EIGRP IPv6 NSF/GR, on page 123
- Restrictions for EIGRP IPv6 NSF/GR, on page 124
- Information About EIGRP IPv6 NSF/GR, on page 124
- How to Configure EIGRP IPv6 NSF/GR, on page 125
- Configuration Examples for EIGRP IPv6 NSF/GR, on page 128
- Additional References for EIGRP IPv6 NSF/GR, on page 129
- Feature Information for EIGRP IPv6 NSF/GR, on page 130

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP IPv6 NSF/GR

- EIGRP (Enhanced Interior Gateway Routing Protocol) IPv6 must be configured on devices. You need not specify the **network** *network-number* command in EIGRP named mode. By default, EIGRP IPv6 enables EIGRP on all interfaces configured with an IPv6 address.

- Cisco software that supports Nonstop Forwarding (NSF) awareness or NSF capabilities must be installed.

- A redundant facility must be configured to notify EIGRP during a switchover and to notify whether the restart is due to a switchover or a device reboot.

- An NSF-aware device must be up and completely converged with the network before it can assist an NSF-capable device in an NSF restart operation.

- All neighboring devices participating in EIGRP NSF must be NSF-capable or NSF-aware.

Restrictions for EIGRP IPv6 NSF/GR

- Nonstop Forwarding (NSF) is supported on platforms that support high-availability systems.
- An Enhanced Interior Gateway Routing Protocol (EIGRP) NSF-aware network does not allow two neighbors to perform an NSF restart operation at the same time. However, neighbors can re-establish peering sessions after the NSF restart operation is complete.
- NSF for IPv6 is supported only in EIGRP named mode configurations.

Information About EIGRP IPv6 NSF/GR

EIGRP IPv6 NSF/GR

The EIGRP IPv6 NSF/GR feature allows a Nonstop Forwarding (NSF)-aware device that is running Enhanced Interior Gateway Routing Protocol (EIGRP) to forward IPv6 packets along routes that are known to a device that is performing a switchover operation. EIGRP peers retain adjacencies and routes learned from a restarting peer (the device that is undergoing a switchover), and the EIGRP peers continue to forward IPv6 packets to the restarting peer. The high-availability systems on the device retain the forwarding table and continue to forward IPv6 packets until the control plane (EIGRP) has converged on the restarting device.

NSF allows forwarding of IPv6 packets while the device restarts after a failure. Graceful Restart (GR) allows topology databases to resynchronize while maintaining neighbor relationships and forwarding paths.

Note NSF supports IPv4 in EIGRP classic mode and named mode configurations. NSF supports IPv6 in named mode. For more information about the EIGRP IPv4 NSF feature, see the “EIGRP Nonstop Forwarding Awareness” module in the *IP Routing: EIGRP Configuration Guide*.

EIGRP IPv6 NSF Timers

The EIGRP IPv6 NSF/GR feature supports three types of timers: the signal timer, the converge timer, and the graceful-restart purge-time timer.

Configure the signal timer to adjust the maximum time of the initial restart period. The restarting device sends hello packets with the restart-signal (RS) bit set. If the restarting device has not learned about any neighbor or any Nonstop Forwarding (NSF)-aware neighbor or has not received all updates from neighbors when the timer expires, the Routing Information Base (RIB) is notified for convergence. The default value for the signal timer is 20 seconds. The **timers nsf signal** command is used to configure the signal timer.

Configure the converge timer to adjust the maximum time that a restarting device waits for the end-of-table (EOT) indications from all neighbors. The default value for the converge timer is 120 seconds. The **timers nsf converge** command is used to configure the converge timer.

Configure the graceful-restart purge-time timer to adjust the maximum waiting time to receive the convergent signal from a restarting device. The graceful-restart purge-time timer is used when the NSF-aware peer does not receive the EOT indication from the restarting neighbor. When the graceful-restart purge-time timer expires, the Enhanced Interior Gateway Routing Protocol (EIGRP) peer scans the topology table for stale routes from the restarting neighbor and changes the stale routes to active. This process allows EIGRP peers to find alternate routes instead of waiting during a long switchover operation. The default value for the graceful-restart purge-time timer is 240 seconds. The **timers graceful-restart purge-time** command is used to configure the graceful-restart purge-time timer.

How to Configure EIGRP IPv6 NSF/GR

Enabling EIGRP IPv6 NSF/GR

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *name*
4. **address-family ipv6 autonomous-system** *number*
5. **nsf**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *name* **Example:** `Device(config)# router eigrp e1`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 4	**address-family ipv6 autonomous-system** *number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP IPv6 routing instance.
Step 5	**nsf** **Example:**	Enables Nonstop Forwarding (NSF) for the specific address family on the device.

	Command or Action	Purpose
	`Device(config-router-af)# nsf`	

Step 6	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Modifying EIGRP IPv6 NSF Timers

Perform this task to modify EIGRP IPv6 NSF timers. This task is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *name*
4. **address-family ipv6 autonomous-system** *number*
5. **timers nsf signal** *seconds*
6. **timers nsf converge** *seconds*
7. **timers graceful-restart purge-time** *seconds*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *name* **Example:** `Device(config)# router eigrp e1`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 4	**address-family ipv6 autonomous-system** *number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP IPv6 routing instance.

	Command or Action	Purpose
Step 5	**timers nsf signal** *seconds* **Example:** `Device(config-router-af)# timers nsf signal 15`	Sets the initial restart period, in seconds, for the restarting device to send hello packets with the restart-signal (RS) bit set.
Step 6	**timers nsf converge** *seconds* **Example:** `Device(config-router-af)# timers nsf converge 60`	Sets the maximum time, in seconds, that the restarting device must wait for end-of-table (EOT) indications from all neighbors.
Step 7	**timers graceful-restart purge-time** *seconds* **Example:** `Device(config-router-af)# timers graceful-restart purge-time 150`	Sets the graceful-restart purge-time timer to determine the period, in seconds, for which a Nonstop Forwarding (NSF)-aware device that is running EIGRP must hold routes for an inactive peer.

Step 8	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Verifying the EIGRP IPv6 NSF/GR Configuration

SUMMARY STEPS

1. **enable**
2. **show ipv6 protocols**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 protocols** **Example:** `Device# show ipv6 protocols`	Displays parameters and the current state of the active IPv6 routing protocol process. • The output of this command can be used to verify the EIGRP IPv6 NSF/GR configuration.

Monitoring EIGRP IPv6 NSF/GR Events

SUMMARY STEPS

1. **enable**
2. **debug eigrp nsf**
3. **debug eigrp address-family ipv6 notifications**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug eigrp nsf** **Example:** `Device# debug eigrp nsf`	Displays debugging information about NSF events on the console of the router.
Step 3	**debug eigrp address-family ipv6 notifications** **Example:** `Device# debug eigrp address-family ipv6 notifications`	Displays debugging information about Enhanced Interior Gateway Routing Protocol (EIGRP) address family IPv6 event notifications.

Configuration Examples for EIGRP IPv6 NSF/GR

Example: Configuring an EIGRP NSF Converge Timer

The following example shows how to adjust the maximum time that the restarting router waits for end-of-table (EOT) indications from all neighbors:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv6 autonomous system 1
Device(config-router-af)# timers nsf converge 60
Device(config-router-af)# end
```

Example: Verifying the Configuration of EIGRP IPv6 NSF/GR on an NSF-Aware Device

The following is a sample output from the **show ipv6 protocols** command, which shows that EIGRP NSF is enabled, the graceful-restart purge-time timer is set to 260 seconds, the signal timer is set to 15 seconds, and the converge timer is set to 65 seconds:

```
Device> enable
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
     NSF signal timer is 15s
     NSF converge timer is 65s
  Router-ID: 10.1.1.1
  Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 16
    Maximum hopcount 100
    Maximum metric variance 1
    Total Prefix Count: 0
    Total Redist Count: 0

  Interfaces:
  Redistribution:
    None
```

Additional References for EIGRP IPv6 NSF/GR

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco Express Forwarding (formerly known as CEF) commands	Cisco IOS IP Switching Command Reference
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference

Related Topic	Document Title
Nonstop Forwarding (NSF)	• "Cisco Nonstop Forwarding" module in the Stateful Switchover Deployment Guide • "Cisco Nonstop Forwarding" module in the *High Availability Configuration Guide* • "EIGRP Nonstop Forwarding Awareness" module in the *IP Routing: EIGRP Configuration Guide*
Command Lookup Tool	http://tools.cisco.com/Support/CLILookup

Standards and RFCs

Standard/RFC	Title
RFC 4724	*Graceful Restart Mechanism for BGP*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP IPv6 NSF/GR

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 15: Feature Information for EIGRP IPv6 NSF/GR

Feature Name	Releases	Feature Information
EIGRP IPv6 NSF/GR		The EIGRP IPv6 NSF/GR feature allows an NSF-aware router that is running EIGRP to forward IPv6 packets while the control plane restarts after recovering from a failure. The following commands were introduced or modified: **debug eigrp nsf**, **nsf**, **show ipv6 protocols**, **timers graceful-restart purge-time**, **timers nsf converge**, **timers nsf signal**.

CHAPTER 9

EIGRP Prefix Limit Support

The EIGRP Prefix Limit Support feature introduces the capability to limit the number of prefixes per VPN routing/forwarding instance (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 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 and Customer Edge feature.

For more information about EIGRP MPLS VPN configuration, refer to the EIGRP MPLS VPN PE-CE Site of Origin module.

- Finding Feature Information, on page 133
- Prerequisites for EIGRP Prefix Limit Support, on page 133
- Restrictions for EIGRP Prefix Limit Support, on page 134
- Information About EIGRP Prefix Limit Support, on page 134
- How to Configure the Maximum-Prefix Limit, on page 136
- Configuration Examples for Configuring the Maximum-Prefix Limit, on page 148
- Additional References, on page 150
- Feature Information for EIGRP Prefix Limit Support, on page 152

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for EIGRP Prefix Limit Support

- Multiprotocol 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.
- The EIGRP Prefix Limiting Support feature is enabled only under the IPv4 VRF address-family. 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

Misconfigured VPN Peers

In MPLS VPNs, the number of routes that are permitted in the 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 effect on the local router by consuming all available system resources (CPU and memory) in processing prefix updates. 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 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.

External Peer Router Protection

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.

Redistributed Prefix Number Limiting

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.

EIGRP Process Level Router Protection

This feature can 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 through redistribution are discarded, and redistribution and peering are suspended for the default or user-defined time period.

EIGRP Prefix Limiting 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 XE system logging configuration options.

EIGRP Prefix Limiting Restart Reset and Dampening Timers and Counters

The EIGRP Prefix Limit Support feature provides two user-configurable timers, a restart counter, and a dampening mechanism. 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 manual intervention is taken.

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 three.

Caution After the restart count limit has been crossed, you will need to enter the **clear ip route ***, **clear ip eigrp neighbor**, or **clear eigrp address-family neighbor**command to restore normal peering and 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 an 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.

How to Configure the Maximum-Prefix Limit

Configuring the Maximum Number of Prefixes Accepted from Peering Sessions Autonomous System Configuration

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.

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.

Before you begin

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Note

- This task can be configured only in IPv4 VRF address family configuration mode.
- When you configure 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*] **autonomous-system** *autonomous-system-number*
5. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*
6. **neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]
7. **neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**]
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Enters router configuration mode and creates an EIGRP routing process. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**address-family ipv4** [**unicast**][**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv4 vrf vrf1 autonomous-system 4453`	Enters address family configuration mode and creates a session for the VRF.
Step 5	**neighbor** {*ip-address* | *peer-group-name*} **description** *text* **Example:** `Router(config-router-af)# neighbor 172.16.2.3 description peer with example.com`	(Optional) Associates a description with a neighbor.
Step 6	**neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**] **Example:** `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.
Step 7	**neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**]	Limits the number of prefixes that are accepted from all EIGRP neighbors.

	Command or Action	Purpose
	Example: `Router(config-router-af)# neighbor maximum-prefix 10000 80 warning-only`	

Step 8	**end**
	Example:
	`Router(config-router-af)# end`
		Exits address family configuration mode and enters privileged EXEC mode.

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 Accepted from Peering Sessions Named Configuration

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.

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.

Before you begin

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Note

- This task can be configured only in IPv4 VRF address family configuration mode.
- When you configure the **neighbor maximum-prefix** command to protect a single peering session, only the maximum-prefix limit, the percentage threshold, and 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** *virtual-instance-name*
4. **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **neighbor** {*ip-address* | *peer-group-name*} **description** *text*
6. **neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]
7. **neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] \| **warning-only**]
8. **exit-address-family**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp virtual-name1`	Enters router configuration mode and creates an EIGRP routing process. - A maximum of 30 EIGRP routing processes can be configured.

Step 4	**address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Router(config-router)# address-family ipv4 vrf VRF1`
	` autonomous-system 45000`
		Enters address family configuration mode and creates a session for the VRF.

Step 5	**neighbor** {*ip-address* | *peer-group-name*} **description** *text* **Example:**	(Optional) Associates a description with a neighbor.

	Command or Action	Purpose
	`Router(config-router-af)# neighbor 172.16.2.3 description peer with example.com`	
Step 6	**neighbor** *ip-address* **maximum-prefix** *maximum* [*threshold*] [**warning-only**] **Example:** `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.
Step 7	**neighbor maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**] **Example:** `Router(config-router-af)# neighbor maximum-prefix 10000 80 warning-only`	Limits the number of prefixes that are accepted from all EIGRP neighbors.
Step 8	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address family configuration mode.

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 eigrp address-family neighbors** command before normal peering can be reestablished.

Configuring the Maximum Number of Prefixes Learned Through Redistribution Autonomous System Configuration

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 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.

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.

Before you begin

- VRFs have been created and configured.

- EIGRP peering is established through the MPLS VPN.

Note 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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Enters router configuration mode and creates an EIGRP routing process. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**address-family ipv4** [**unicast**] **vrf** *vrf-name* **Example:** `Router(config-router)# address-family ipv4 vrf VRF1`	Enters address family configuration mode and creates a session for the VRF.
Step 5	**redistribute maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**] **Example:** `Router(config-router-af)# redistribute maximum-prefix 10000 80 reset-time 10 restart 2`	Limits the number of prefixes redistributed into an EIGRP process.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`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 neighbors** command will need to be entered before normal redistribution will occur.

Configuring the Maximum Number of Prefixes Learned Through Redistribution Named Configuration

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 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.

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.

Before you begin

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Note This task can be configured only in IPv4 VRF address family topology configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **topology base**
7. **redistribute maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**]

8. **exit-af-topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp virtual-name1`	Enters router configuration mode and creates an EIGRP routing process. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000`	Enters address family configuration mode and creates a session for the VRF.
Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Router(config-router-af)# network 172.16.0.0`	Specifies the network for an EIGRP address family routing process.
Step 6	**topology base** **Example:** `Router(config-router-af)# topology base`	Configures an EIGRP process to route traffic under the specified topology instance and enters address family topology configuration mode.
Step 7	**redistribute maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**] **Example:** `Router(config-router-af-topology)# redistribute maximum-prefix 10000 80 reset-time 10 restart 2`	Limits the number of prefixes redistributed into an EIGRP process.
Step 8	**exit-af-topology** **Example:**	Exits address family topology configuration mode.

	Command or Action	Purpose
	`Router(config-router-af-topology)# exit-af-topology`	

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 eigrp address-family neighbors**command will need to be entered before normal redistribution will occur.

Configuring the Maximum-Prefix Limit for an EIGRP Process Autonomous System Configuration

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.

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.

Before you begin

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Note 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*[**autonomous-system** *autonomous-system-number*]
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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Enters router configuration mode and creates an EIGRP routing process. - A maximum of 30 EIGRP routing processes can be configured.
Step 4	**address-family ipv4** [**unicast**] **vrf** *vrf-name*[**autonomous-system** *autonomous-system-number*] **Example:** `Router(config-router)# address-family ipv4 vrf VRF1`	Enters address family configuration mode and creates a session for the VRF.

Step 5	**maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**]
	Example:
	`Router(config-router-af)# maximum-prefix 10000 80`
	` reset-time 10 restart 2`
		Limits the number of prefixes that are accepted under an address family by an EIGRP process.
		- The example configures a maximum-prefix limit of 10,000 prefixes, a reset time period of 10 minutes, a warning message to be displayed at 80 percent of the maximum-prefix limit, and a restart time period of 2 minutes.

Step 6	**end**
	Example:
	`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 neighbors** command will need to be entered before normal redistribution will occur.

Configuring the Maximum-Prefix Limit for an EIGRP Process Named Configuration

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.

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.

Before you begin

- VRFs have been created and configured.
- EIGRP peering is established through the MPLS VPN.

Note This task can be configured only in IPv4 VRF address family topology configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**]
6. **exit-address-family**
7. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **accounting**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp virtual-name1`	Creates an EIGRP routing process and enters router configuration mode. • A maximum of 30 EIGRP routing processes can be configured.
Step 4	**address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000`	Enters address family configuration mode and creates a session for the VRF.
Step 5	**maximum-prefix** *maximum* [*threshold*] [[**dampened**] [**reset-time** *minutes*] [**restart** *minutes*] [**restart-count** *number*] | **warning-only**] **Example:** `Router(config-router-af)# maximum- prefix 10000 80 reset-time 10 restart 2 warning-only`	Limits the number of prefixes that are accepted under an address family by an EIGRP process. • The example configures a maximum-prefix limit of 10,000 prefixes, a reset time period of 10 minutes, a warning message to be displayed at 80 percent of the maximum-prefix limit, and a restart time period of 2 minutes.
Step 6	**exit-address-family** **Example:** `Router(config-router-af)# exit-af-topology`	Exits address family configuration mode.
Step 7	**show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] **accounting** **Example:** `Router# show eigrp address-family ipv4 22 accounting`	(Optional) Displays prefix accounting information for EIGRP processes. **Note** Connected and summary routes are not listed individually in the output from this **show** command but are counted in the total aggregate count per process.

Example

The following is sample output from the **show eigrp address-family accounting** command:

```
Router# show eigrp address-family ipv4 22 accounting
EIGRP-IPv4 VR(saf) Accounting for AS(22)/ID(10.0.0.1)
Total Prefix Count: 3  States: A-Adjacency, P-Pending, D-Down
State Address/Source    Interface       Prefix   Restart  Restart/
                                        Count     Count   Reset(s)
 A    10.0.0.2          Et0/0               2         0        0
 P    10.0.2.4          Se2/0               0         2        114
 D    10.0.1.3          Et0/0               0         3        0
```

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 eigrp address-family neighbors**command will need to be entered before normal redistribution will occur.

Configuration Examples for Configuring the Maximum-Prefix Limit

Example Configuring the Maximum-Prefix Limit for a Single Peer--Autonomous System Configuration

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 VRF1
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# end
```

Example Configuring the Maximum-Prefix Limit for a Single Peer--Named Configuration

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 virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# neighbor 10.0.0.1 maximum-prefix 1000 80
Router(config-router-af)# exit-address-family
```

Example Configuring the Maximum-Prefix Limit for All Peers--Autonomous System Configuration

The following example, starting in global configuration mode, configures the maximum-prefix limit for all peers. The maximum limit is set to 10,000 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 VRF1
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60
 restart 4
Router(config-router-af)# end
```

Example Configuring the Maximum-Prefix Limit for All Peers--Named Configuration

The following example, starting in global configuration mode, configures the maximum-prefix limit for all peers. The maximum limit is set to 10,000 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 virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# neighbor maximum-prefix 10000 90 dampened reset-time 60
 restart 4
Router(config-router-af)# exit-address-family
```

Example Configuring the Maximum-Prefix Limit for Redistributed Routes--Autonomous System Configuration

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 95 percent. 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 VRF1
Router(config-router-af)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af)# end
```

Example Configuring the Maximum-Prefix Limit for Redistributed Routes--Named Configuration

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 95 percent. 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 virtual-name1
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# network 172.16.0.0
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute maximum-prefix 5000 95 warning-only
Router(config-router-af-topology)# exit-af-topology
```

Example Configuring the Maximum-Prefix Limit for an EIGRP Process--Autonomous System Configuration

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 50,000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), 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
```

Example Configuring the Maximum-Prefix Limit for an EIGRP Process--Named Configuration

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 50,000 prefixes. When the number of prefixes learned through redistribution reaches 37,500 (75 percent of 50,000), 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 virtual-name
Router(config-router)# address-family ipv4 vrf VRF1 autonomous-system 45000
Router(config-router-af)# maximum-prefix 50000
Router(config-router-af)# exit-address-family
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
EIGRP commands	*Cisco IOS IP Routing: EIGRP Command Reference*

Related Topic	Document Title
EIGRP autonomous system configuration and EIGRP named configuration	Configuring EIGRP module
BGP cost community configuration tasks for EIGRP MPLS VPN PE-CE	BGP Cost Community module of the *Cisco IOS IP Routing: BGP Configuration Guide*
Basic EIGRP configuration tasks	Configuring EIGRP module
EIGRP MPLS VPN configuration tasks	EIGRP MPLS VPN PE-CE Site of Origin (SoO) module
MPLS VPNs configuration tasks	Configuring MPLS Layer 3 VPNs module of the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

Standards

Standards	Title
None	--

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Prefix Limit Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 16: Feature Information for EIGRP Prefix Limit Support

Feature Name	Releases	Feature Information
EIGRP Prefix Limit Support	Cisco IOS XE Release 2.6	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 redistribution. In Cisco IOS XE Release 2.6, the following commands were introduced or modified: **maximum-prefix**, **neighbor description**, **neighbor maximum-prefix**, **redistribute maximum-prefix**(EIGRP).

CHAPTER 10

EIGRP Support for Route Map Filtering

The EIGRP Support for Route Map Filtering feature enables Enhanced Interior Gateway Routing Protocol (EIGRP) to interoperate with other protocols to leverage additional routing functionality by filtering inbound and outbound traffic based on complex route map options. Several extended filtering options are introduced to provide EIGRP-specific match choices.

- Finding Feature Information, on page 153
- Information About EIGRP Support for Route Map Filtering, on page 153
- How to Configure EIGRP Support for Route Map Filtering, on page 154
- Configuration Examples for EIGRP Support for Route Map Filtering, on page 164
- Additional References, on page 165
- Feature Information for EIGRP Support for Route Map Filtering, on page 166

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP Support for Route Map Filtering

EIGRP Route Map Support

EIGRP support for route map filtering enables EIGRP to interoperate with other protocols by filtering inbound and outbound traffic based on route map options. Additional EIGRP-specific match choices are available to allow flexibility in fine-tuning EIGRP network operations.

EIGRP supports the route map filtering capability that exists for other routing protocols to filter routes being redistributed into their protocol. For more details about understanding and configuring route maps, see the Enabling Policy Routing section of the Configuring IP Routing Protocol-Independent Features module of the *Cisco IOS XE IP Routing: Protocol-Independent Configuration Guide,* Release 2.

Match options allow EIGRP to filter internal and external routes based on source protocols, to match a metric against a range, and to match on an external protocol metric.

EIGRP can be configured to filter traffic using a route map and the **redistribute** or **distribute-list** command. Using a route map with the **redistribute** command allows routes that are redistributed from the routing table to be filtered with a route map before being admitted into an EIGRP topology table. Routes that are dynamically received from, or advertised to, EIGRP peers can be filtered by adding a route map option to the **distribute-list** command.

A route map may be configured with both the **redistribute** and the **distribute-list** commands in the same routing process. When a route map is used with a **distribute-list** command that is configured for inbound or outbound filtering, route packets that are learned from or advertised to EIGRP peers can be processed with the route map to provide better control of route selection during the route exchange process. Redistribution serves as a mechanism to import routes into the EIGRP topology table from a routing table. A route map configured with the **redistribute** command adds flexibility to the redistribution capability and results in a more specific redistributed route selection.

The use of route maps to filter traffic is the same for both autonomous-system configurations and named configurations. See the Configuring EIGRP module for more information about autonomous system and named configurations.

Demands for EIGRP to interoperate with other protocols and flexibility in fine-tuning network operation necessitate the capability to filter traffic using a route map.

How to Configure EIGRP Support for Route Map Filtering

Setting EIGRP Tags Using a Route Map for Autonomous System Configurations

Perform this task to set EIGRP tags for autonomous system configurations using a route map. The EIGRP metrics used for filtering are configured within a route map. The first match clause defines EIGRP routes that contain an external protocol metric between 400 and 600 inclusive; the second match clause defines EIGRP external routes that match a source protocol of BGP and the autonomous system 45000. When the two match clauses are true, a tag value of the destination routing protocol is set to 5. This route map can be used with the **distribute-list** command, see the Example Setting EIGRP Tags Using a Route Map--Autonomous System Configuration Examples, on page 164 for an example configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match metric** {*metric-value*| **external** *metric-value*} [**+-** *deviation-number*]
5. **match source-protocol** *source-protocol* [*autonomous-system-number*]
6. **set tag** *tag-value*
7. **exit**
8. **router eigrp** *as-number*
9. **network** *ip-address*
10. **distribute-list route-map** *map-tag* **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map metric-range`	Enters route-map configuration mode.
Step 4	**match metric** {*metric-value*| **external** *metric-value*} [**+-** *deviation-number*] **Example:** `Router(config-route-map)# match metric external 500 +- 100`	Specifies a match clause that filters inbound updates that match an internal or external protocol metric. • *metric-value* --Internal protocol metric, which can be an EIGRP five-part metric. The range is from 1 to 4294967295. • **external** --External protocol metric. The range is from 1 to 4294967295. • **+-** *deviation-number* --(Optional) Represents a standard deviation. The deviation can be any number. There is no default. **Note** When you specify a metric deviation with the **+** and **-** keywords, the router will match any metric that falls inclusively in that range. **Note** The external protocol metric is not the same as the EIGRP assigned route metric, which is a figure computed from EIGRP vectorized metric components (delay, bandwidth, reliability, load, and MTU).
Step 5	**match source-protocol** *source-protocol* [*autonomous-system-number*] **Example:** `Router(config-route-map)# match source-protocol bgp 45000`	Specifies a match clause that matches external routes from sources that match the source protocol. • *source-protocol* --Protocol to match. The valid keywords are **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip**, and **static**. There is no default. • *autonomous-system-number* --(Optional) Autonomous system number. The *autonomous-system-number* argument is not applicable to the **connected**, **static**,

	Command or Action	Purpose
		and **rip** keywords. The range is from 1 to 65535. There is no default.
Step 6	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 5`	Sets a tag value on the route in the destination routing protocol when all the match criteria of a route map are met.
Step 7	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 8	**router eigrp** *as-number* **Example:** `Router(config)# router eigrp 1`	Configures the EIGRP routing process and enters router configuration mode.
Step 9	**network** *ip-address* **Example:** `Router(config-router)# network 172.16.0.0`	Specifies a network for the EIGRP routing process.
Step 10	**distribute-list route-map** *map-tag* **in** **Example:** `Router(config-router)# distribute-list route-map metric-range in`	Filters networks received in updates.

Setting EIGRP Tags Using a Route Map for Named Configurations

Perform this task to set EIGRP tags for named configurations using a route map. The EIGRP metrics used for filtering are configured within a route map. The first match clause defines EIGRP routes that contain an external protocol metric between 400 and 600 inclusive; the second match clause defines EIGRP external routes that match a source protocol of BGP and the autonomous system 45000. When the two match clauses are true, a tag value of the destination routing protocol is set to 5. This route map can be used with the **distribute-list** command, see the Example Setting EIGRP Tags Using a Route Map--Named Configuration Examples, on page 164 for an example configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **set metric** *bandwidth delay reliability loading mtu*
5. **match ip route-source** {*access-list-number*| *access-list-name*} [*...access-list-number* | *...access-list-name*]
6. **match metric** {*metric-value*| **external** *metric-value*} [**+-** *deviation-number*]

7. **match source-protocol** *source-protocol* [*autonomous-system-number*]
8. **set tag** *tag-value*
9. **exit**
10. **router eigrp** *virtual-instance-name*
11. Do one of the following:
    - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
    - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
12. **network** *ip-address* [*wildcard-mask*]
13. **af-interface** {**default** | *interface-type interface-number*}
14. **next-hop-self**
15. **exit-af-interface**
16. **topology** {**base** | *topology-name* **tid** *number*}
17. **distribute-list route-map** *map-tag* **in**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map metric-range`	Enters route-map configuration mode.
Step 4	**set metric** *bandwidth delay reliability loading mtu* **Example:** `Router(config-route-map)# set metric 10000 10 255 1 1500`	(Optional) Sets the metric value for EIGRP in a route map.
Step 5	**match ip route-source** {*access-list-number*| *access-list-name*} [*...access-list-number* | *...access-list-name*] **Example:** `Router(config-route-map)# match ip route-source 5 80`	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.

	Command or Action	Purpose
Step 6	**match metric** {*metric-value*| **external** *metric-value*} [**+-** *deviation-number*] **Example:** `Router(config-route-map)# match metric external 500 +- 100`	Specifies a match clause that includes EIGRP routes that match an internal or external protocol metric. • *metric-value* --Internal protocol metric, which can be an EIGRP five-part metric. The range is from 1 to 4294967295. • **external** --External protocol metric. The range is from 1 to 4294967295. • **+-** *deviation-number* --(Optional) Represents a standard deviation. The deviation can be any number. There is no default. **Note** When you specify a metric deviation with the **+** and **-** keywords, the router will match any metric that falls inclusively in that range. **Note** The external protocol metric is not the same as the EIGRP assigned route metric, which is a figure computed from EIGRP vectorized metric components (delay, bandwidth, reliability, load, and MTU).
Step 7	**match source-protocol** *source-protocol* [*autonomous-system-number*] **Example:** `Router(config-route-map)# match source-protocol bgp 45000`	Specifies a match clause that includes EIGRP external routes that match a source protocol. • *source-protocol* --Protocol to match. The valid keywords are **bgp**, **connected**, **eigrp**, **isis**, **ospf**, **rip**, and **static**. There is no default. • *autonomous-system-number* --(Optional) Autonomous system number. The *autonomous-system-number* argument is not applicable to the **connected**, **static**, and **rip** keywords. The range is from 1 to 65535. There is no default.
Step 8	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 5`	Sets a tag value on the route in the destination routing protocol when all the match criteria of a route map are met.
Step 9	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 10	**router eigrp** *virtual-instance-name* **Example:**	Configures the EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
	`Router(config)# router eigrp virtual-name1`	
Step 11	Do one of the following: - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv4 autonomous-system 45000`	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
Step 12	**network** *ip-address* [*wildcard-mask*] **Example:** `Router(config-router-af)# network 172.16.0.0`	Specifies a network for the EIGRP routing process.

Step 13	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Router(config-router-af)# af-interface default`
		Enters address family interface configuration mode to configure interface-specific EIGRP commands.

Step 14	**next-hop-self** **Example:** `Router(config-router-af-interface)# next-hop-self`	Enables EIGRP to advertise routes with the local outbound interface address as the next hop.
Step 15	**exit-af-interface** **Example:** `Router(config-router-af-interface)# exit-af-interface`	Exits address-family interface configuration mode.

Step 16	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Router(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 17	**distribute-list route-map** *map-tag* **in** **Example:** `Router(config-router-af-topology)# distribute-list route-map metric-range in`	Filters networks received in updates.

Configuring EIGRP Route-map for Distribute-list in IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **topology** {**base** | *topology-name* **tid** *number*}
6. **distribute-list route-map** *map-tag* **in**
7. **distribute-list route-map** *map-tag* **out**
8. **exit-af-toplogy**
9. **exit-address-family**
10. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
11. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
12. **set tag** *tag-value*
13. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
14. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
15. **set tag** *tag-value*
16. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
17. **match metric** *bandwidth delay reliability loading mtu*
18. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
19. **match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
20. **set tag** *tag-value*
21. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
22. **match interface** *interface-type interface-number* [*...interface-type interface-number*]
23. **set tag** *tag-value*
24. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
25. **match metric** *bandwidth delay reliability loading mtu*
26. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Router(config)# router eigrp virtual1`	Configures the EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number* **Example:** `Router(config-router)# address-family ipv6 autonomous-system 1`	Enters address family configuration mode to configure an EIGRP IPv6 routing instance.

Step 5	**topology** {**base** | *topology-name* **tid** *number*}
	Example:
	`Router(config-router-af)# topology base`
		Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

Step 6	**distribute-list route-map** *map-tag* **in** **Example:** `Router(config-router-af-topology)# distribute-list route-map map_in in`	Enables filtering of the networks received in EIGRP updates.
Step 7	**distribute-list route-map** *map-tag* **out** **Example:** `Router(config-router-af-topology)# distribute-list route-map map_out out`	Enables suppressing of networks from being advertised in the EIGRP updates.
Step 8	**exit-af-toplogy** **Example:** `Router(config-router-af-topology)# exit-af-topology`	Exits address-family topology configuration mode.
Step 9	**exit-address-family** **Example:** `Router(config-router-af)# exit-address-family`	Exits address-family configuration mode.
Step 10	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map1 permit 10`	Enters route-map configuration mode. • Specifies route map name and set action to redistribute the route if the match criteria are met.
Step 11	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*} **Example:**	Specifies an IPv6 access list to match for redistributing routes that have been advertised by routers and access servers.

	Command or Action	Purpose
	`Router(config-route-map)# match ipv6 address acl1`	
Step 12	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 10`	Sets a tag value for the route in the route map.
Step 13	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map1 permit 20`	Specifies route map name and set action to redistribute the route if the match criteria are met.
Step 14	**match interface** *interface-type interface-number* [*...interface-type interface-number*] **Example:** `Router(config-route-map)# match interface ethernet 0/0`	Specifies the next hop out of the interface to distribute the associated routes.
Step 15	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 20`	Sets a tag value for the route in the route map.
Step 16	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map1 permit 30`	Specifies route map name and set action to redistribute the route if the match criteria are met.
Step 17	**match metric** *bandwidth delay reliability loading mtu* **Example:** `Router(config-route-map)# match metric 10000 100 255 100 1500`	Specifies the metric value for EIGRP in a route map.
Step 18	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map2 permit 10`	Enters route-map configuration mode. • Specifies route map name and set action to redistribute the route if the match criteria are met.

Step 19	**match ipv6 address** {**prefix-list** *prefix-list-name* | *access-list-name*}
	Example:
	`Router(config-route-map)# match ipv6 address acl1`
		Specifies an IPv6 access list to match for redistributing routes that have been advertised by routers and access servers.

	Command or Action	Purpose
Step 20	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 10`	Sets a tag value for the route in the route map.
Step 21	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map2 permit 20`	Specifies route map name and set action to redistribute the route if the match criteria are met.
Step 22	**match interface** *interface-type interface-number* [...*interface-type interface-number*] **Example:** `Router(config-route-map)# match interface ethernet 0/0`	Specifies the next hop out of the interface to distribute the associated routes.
Step 23	**set tag** *tag-value* **Example:** `Router(config-route-map)# set tag 20`	Sets a tag value for the route in the route map.
Step 24	**route-map** *map-tag* [**permit** | **deny**] [*sequence-number*] **Example:** `Router(config)# route-map map2 permit 30`	Specifies route map name and set action to redistribute the route if the match criteria are met.
Step 25	**match metric** *bandwidth delay reliability loading mtu* **Example:** `Router(config-route-map)# match metric 1000 100 255 200 1800`	Specifies the metric value for EIGRP in a route map.

Step 26	**end**
	Example:
	`Router(config-route-map)# end`
		Exits route-map configuration mode and returns to privileged EXEC mode.

Configuration Examples for EIGRP Support for Route Map Filtering

Example Setting EIGRP Tags Using a Route Map--Autonomous System Configuration Examples

The following example shows how to configure a route map to match an EIGRP external protocol metric route with an allowable deviation of 100, a source protocol of BGP, and an autonomous system 45000. When the two match clauses are true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
Router(config)# route-map metric-range
Router(config-route-map)# match metric external 500 +- 100
Router(config-route-map)# match source-protocol bgp 45000
Router(config-route-map)# set tag 5
Router(config-route-map)# exit
Router(config)# router eigrp 1
Router(config-router)# network 172.16.0.0
Router(config-router)# distribute-list route-map metric_range in
```

The following example shows how to configure a route map to match EIGRP routes with a metric of 110, 200, or an inclusive range of 700 to 800. When the match clause is true, the tag value of the destination routing protocol is set to 10. The route map is used to redistribute EIGRP packets.

```
Router(config)# route-map metric-eigrp
Router(config-route-map)# match metric 110 200 750 +- 50
Router(config-route-map)# set tag 10
Router(config-route-map)# exit
Router(config)# router eigrp 1
Router(config-router)# network 172.21.1.0/24
Router(config-router)# redistribute eigrp route-map metric-eigrp
```

Example Setting EIGRP Tags Using a Route Map--Named Configuration Examples

The following example shows how to configure a route map to match an EIGRP external protocol metric route with an allowable deviation of 100, a source protocol of BGP, and an autonomous system 45000. When the two match clauses are true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
Router(config)# route-map metric_range
Router(config-route-map)# match metric external 500 +- 100
Router(config-route-map)# match source-protocol bgp 45000
Router(config-route-map)# set tag 5
Router(config-route-map)# exit
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.21.1.0/24
Router(config-router-af)# topology base
Router(config-router-af-topology)# distribute-list route-map metric_range in
```

The following example shows how to configure a route map to match EIGRP routes with a metric of 110, 200, or an inclusive range of 700 to 800. When the match clause is true, the tag value of the destination routing protocol is set to 10. The route map is used to redistribute EIGRP packets.

```
Router(config)# route-map metric_eigrp
Router(config-route-map)# match metric 110 200 750 +- 50
Router(config-route-map)# set tag 10
Router(config-route-map)# exit
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 45000
Router(config-router-af)# network 172.21.1.0/24
Router(config-router-af)# topology base
Router(config-router-af-topology)# distribute-list route-map metric-range in
```

Example Configuring EIGRP Route-map for Distribute-list in IPv6

The following example shows how to configure EIGRP route maps for distribute list in IPv6.

```
enable
configure terminal
router eigrp test
 address-family ipv6 unicast autonomous-system 1
 topology base
 distribute-list route-map map_in
 distribute-list route-map map_out
 exit-af-topology
 exit-address-family
route-map map_in permit 10
 match ipv6 address acl1
 set tag 15
 route-map map_in permit 20
 match interface Ethernet0/0
 set tag 25
 route-map map_in permit 30
 match metric 10000 1000 255 255 1024
 route-map map_out permit 20
 match ipv6 address acl1
 set tag 25
 route-map map_out permit 40
 match interface Ethernet0/0
 set tag 35
 route-map map_out permit 50
 match metric 10000 100 255 200 1024
end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
EIGRP overview and configuration	Configuring EIGRP
EIGRP commands including syntax, usage guidelines, and examples	*Cisco IOS IP Routing: EIGRP Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Support for Route Map Filtering

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 17: Feature Information for EIGRP Support for Route Map Filtering

Feature Name	Releases	Feature Information
EIGRPv6 Route-map support for Distribute-list	Cisco IOS XE Release 3.17S	The EIGRPv6 Route-map support for Distribute-list feature enables EIGRP route-map in the distribute list for IPv6 networks. The following commands were introduced or modified by this feature: **match metric**, **match tag**, **show interface**, **match ipv6 address**, **match route-type**, **match ipv6 next-hop**, **set tag set metric**, **address-family**, **topology**.
EIGRP Support for Route Map Filtering	Cisco IOS XE Release 2.1	The EIGRP Support for Route Map Filtering feature enables EIGRP to interoperate with other protocols by filtering inbound and outbound traffic based on complex route map options. Several extended filtering options are introduced to provide EIGRP-specific match choices. In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: **match metric** (IP), **match source-protocol**, **ip eigrp topology**. In Cisco IOS XE Release 2.5, the following command was introduced or modified for this feature: **show eigrp address-family topology**

CHAPTER 11

EIGRP Route Tag Enhancements

The EIGRP Route Tag Enhancements feature enables you to specify and display route tags in dotted-decimal format, filter routes using the route tag value with wildcard mask, and set a default route tag for all internal Enhanced Interior Gateway Routing Protocol (EIGRP) routes.

- Finding Feature Information, on page 169
- Restrictions for EIGRP Route Tag Enhancements, on page 169
- Information About EIGRP Route Tag Enhancements, on page 170
- How to Configure EIGRP Route Tag Enhancements, on page 170
- Configuration Examples for EIGRP Route Tag Enhancements, on page 177
- Additional References, on page 179
- Feature Information for EIGRP Route Tag Enhancements, on page 179

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EIGRP Route Tag Enhancements

- Default route tags are not supported in EIGRP autonomous system configurations.
- Route tags will not be displayed in dotted-decimal format if the **route-tag notation** global configuration command is not enabled on the device.

Information About EIGRP Route Tag Enhancements

EIGRP Route Tag Enhancements Overview

A route tag is a 32-bit value attached to routes. Route tags are used to filter routes and apply administrative policies, such as redistribution and route summarization, to tagged routes. You can tag routes within a route map by using the **set tag** command. You can match tagged routes and apply administrative policies to tagged routes within a route map by using the **match tag** or **match tag list** command. The **match tag list** command is used to match a list of route tags.

Prior to the EIGRP Route Tag Enhancements feature, EIGRP routes could only be tagged using plain decimals (range: 1 to 4294967295). This feature enables users to specify and display route tag values as dotted decimals (range: 0.0.0.0 to 255.255.255.255), similar to the format used by IPv4 addresses. This enhancement is intended to simplify the use of route tags as users can now filter routes by using the route tag wildcard mask.

This feature also allows you to configure a default route tag for all internal EIGRP routes without using route maps. Use the **eigrp default-route-tag** command in address family configuration mode to configure a default route tag for internal EIGRP routes.

How to Configure EIGRP Route Tag Enhancements

Enabling Dotted-Decimal Notation for Route Tags

Perform this task to enable route tags to be displayed as dotted decimals in **show** commands, irrespective of whether or not the tags were configured as dotted decimals.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-tag notation dotted-decimal**
4. **end**
5. Enter one of the following:
   - **show ip route tag**
   - **show ipv6 route tag**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-tag notation dotted-decimal** **Example:** `Device(config)# route-tag notation dotted-decimal`	Enables the display of route tags in dotted-decimal format.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits to privileged EXEC mode.

Step 5	Enter one of the following:
	• **show ip route tag**
	• **show ipv6 route tag**
	Example:
	`Device# show ip route tag`
	`Device# show ipv6 route tag`
		(Optional) Displays route tag entries for IPv4 or IPv6 routes.

Setting a Route Tag in a Route Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-name* **[permit | deny]** [*sequence-number*]
4. **set tag** {*tag-value* | *tag-value-dotted-decimal*}
5. **end**
6. **show route-map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-name* **[permit | deny]** [*sequence-number*] **Example:** `Device(config)# route-map rip-to-eigrp`	Configures a route map and enters route-map configuration mode.

Step 4	**set tag** {*tag-value* | *tag-value-dotted-decimal*}
	Example:
	`Device(config-route-map)# set tag 7.7.7.7`
		Sets a tag value for a route.
		Note In this example, all routes from Routing Information Protocol (RIP) to EIGRP are given a tag value of 7.7.7.7.

Step 5	**end**
	Example:
	`Device(config-route-map)# end`
		Exits to privileged EXEC mode.

Step 6	**show route-map** **Example:** `Device# show route-map`	(Optional) Displays static and dynamic route maps configured on the router.

Matching a Route Tag in a Route Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-name* **[permit | deny]** [*sequence-number*]
4. **match tag** {*tag-value* | *tag-value-dotted-decimal*} [**. . .** *tag-value* | *tag-value-dotted-decimal*]
5. **end**
6. **show route-map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-name* **[permit | deny]** [*sequence-number*] **Example:** `Device(config)# route-map eigrp-to-rip`	Configures a route map and enters route-map configuration mode.
Step 4	**match tag** {*tag-value* | *tag-value-dotted-decimal*} [**. . .** *tag-value* | *tag-value-dotted-decimal*] **Example:** `Device(config-route-map)# match tag 10.10.10.0`	Filters routes that match specific route tags.

Step 5	**end**
	Example:
	`Device(config-route-map)# end`
		Exits to privileged EXEC mode.

Step 6	**show route-map** **Example:** `Device# show route-map`	(Optional) Displays static and dynamic route maps configured on the device.

Creating a Route Tag List

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-tag list** *list-name* **{deny | permit | sequence** *number* **{deny | permit}}** *tag-dotted-decimal mask*
4. **end**
5. **show route-tag list** [*list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-tag list** *list-name* **{deny | permit | sequence** *number* **{deny | permit}}** *tag-dotted-decimal mask* **Example:** `Device(config)# route-tag list to-rip permit 10.10.10.0 0.0.0.7`	Creates a route tag list. - Route tag lists are used by route maps to match routes based on conditions specified in the route tag lists.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits to privileged EXEC mode.

Step 5	**show route-tag list** [*list-name*] **Example:** `Device(config-router)# show route-tag list to-rip`	(Optional) Displays information about route tag lists configured on the device. - Use the *list-name* argument to display information about a specific route tag list.

Matching a Route Tag List

Route tag lists are used in route maps to match routes based on conditions specified in the route tag lists. Multiple route tag and mask pair sequences can be configured to permit or deny any condition for a list of route tags.

Note You can match either a route tag or a route tag list within a single route map sequence.

Perform this task to match routes based on conditions specified in the route tag list.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-tag list** *list-name* **{deny | permit | sequence** *number* **{deny | permit}}** *tag-value-dotted-decimal mask*
4. **route-map** *map-name* **[permit | deny]** [*sequence-number*]
5. **match tag list** *list-name* [**. . .** *list-name*]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**route-tag list** *list-name* {**deny** | **permit** | **sequence** *number* {**deny** | **permit**}} *tag-value-dotted-decimal mask* **Example:** `Device(config)# route-tag list list1 permit 10.10.10.0 0.0.0.7`	Configures a route tag list.
Step 4	**route-map** *map-name* [**permit** | **deny**] [*sequence-number*] **Example:** `Device(config)# route-map to-ospf`	Configures a route map and enters route-map configuration mode.
Step 5	**match tag list** *list-name* [**. . .** *list-name*] **Example:** `Device(config-route-map)# match tag list list1`	Filters routes that match a specified route tag list.

Step 6	**end**
	Example:
	`Device(config-route-map)# end`
		Exits to privileged EXEC mode.

Setting a Default Route Tag for EIGRP Internal Routes

Perform this task to set a default route tag for all internal EIGRP routes without using a route map. Default route tags are supported only in EIGRP named mode configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. Enter one of the following:
    - **address-family ipv4 unicast autonomous-system** *autonomous-system-number*

- **address-family ipv6 unicast autonomous-system** *autonomous-system-number*

5. **eigrp default-route-tag** {*route-tag-plain-decimal* | *route-tag-dotted-decimal*}
6. **end**
7. Enter one of the following:
   - **show eigrp address-family ipv4 topology**
   - **show eigrp address-family ipv6 topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4 unicast autonomous-system** *autonomous-system-number*
	• **address-family ipv6 unicast autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 unicast autonomous-system 1`
	`Device(config-router)# address-family ipv6 unicast autonomous-system 1`
		Enters IPv4 or IPv6 address family configuration mode and configures an EIGRP routing instance.

Step 5	**eigrp default-route-tag** {*route-tag-plain-decimal* | *route-tag-dotted-decimal*}
	Example:
	`Device(config-router-af)# eigrp default-route-tag 10`
		Sets a default route tag for all internal EIGRP routes.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Device(config-router-af)# end`
		Exits to privileged EXEC mode.

Step 7	Enter one of the following:
	• **show eigrp address-family ipv4 topology**
	• **show eigrp address-family ipv6 topology**
	Example:
	`Device(config-router-af)# show eigrp address-family ipv4 topology`
	`Device(config-router-af)# show eigrp address-family ipv6 topology`
		(Optional) Displays entries of EIGRP address-family IPv4 or IPv6 topology tables.

Configuration Examples for EIGRP Route Tag Enhancements

Example: Enabling Dotted-Decimal Notation for Route Tags

The following example shows how to enable the display of route tags in dotted-decimal format by using the **route-tag notation** command. If you do not configure the **route-tag notation** command, route tags will be displayed as plain decimals in **show** commands even if the route tags were configured as dotted decimals. When you configure the **route-tag notation** command, route tags will be displayed as dotted decimals even if the route tags were configured as plain decimals.

```
Device# configure terminal
Device(config)# route-tag notation dotted-decimal
```

Example: Setting a Route Tag

The following example shows how to redistribute EIGRP routes into RIP and RIP routes into EIGRP by setting tags for routes within route maps:

```
Device(config)# route-map eigrp-to-rip
Device(config-route-map)# set tag 10.10.10.10
Device(config-route-map)# exit
Device(config)# route-map rip-to-eigrp
Device(config-route-map)# set tag 20.20.20.20
Device(config-route-map)# exit
Device(config)# router rip
Device(config-router)# redistribute eigrp 7 route-map eigrp-to-rip metric 5
Device(config-router)# exit
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 10
Device(config-router-af)# topology base
Device(config-router-af-topology)# redistribute rip route-map rip-to-eigrp 2 2 2 2 2
Device(config-router-af-topology)# end
```

Example: Matching a Route Tag

The following example shows how to redistribute EIGRP routes with a route tag value of 10.10.10.10 into a RIP domain:

```
Device(config)# route-map eigrp-to-rip
Device(config-route-map)# match tag 10.10.10.10
Device(config-route-map)# exit
Device(config)# router rip
Device(config-router)# redistribute eigrp 7 route-map eigrp-to-rip 5
Device(config-router)# end
```

Example: Configuring a Route Tag List

The following example shows how to configure a route tag list named TAG with various criteria for filtering routes. Route maps will use this list to match routes based on the criteria specified in the list. Route tag lists can accept route tags and wild card masks.

```
Device(config)# route-tag list TAG permit 1.1.1.1 0.0.0.1
Device(config)# route-tag list TAG seq 3 permit 2.2.2.2 0.0.0.3
Device(config)# route-tag list TAG seq 10 permit 3.3.3.3 0.0.0.7
Device(config)# route-tag list TAG seq 15 5.5.5.5 0.0.0.31
Device(config)# route-tag list TAG seq 20 deny 4.4.4.4 0.0.0.4
```

Example: Matching a Route Tag List

The following example shows how to use a route map to filter routes that match a specific route tag list. A single list can have multiple match criteria. All criteria must match before the route can be filtered. This example shows how to configure a route tag list named List1 in a route map and use the **match tag list** command to filter routes that match the criteria listed in the route tag list.

```
Device(config)# route-tag list List1 permit 10.10.10.0 0.0.0.7
Device(config)# route-map to-ospf
Device(config-route-map)# match tag list List1
Device(config-route-map)# exit
Device(config)# router ospf 10
Device(config-router)# redistribute eigrp 7 route-map to-ospf metric 20
Device(config-router)# end
```

Example: Setting a Default Route Tag

The following example shows how to set a default route tag for all internal EIGRP routes without using a route map. Default route tags are supported only in EIGRP named configurations.

```
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 unicast autonomous-system 1
Device(config-router-af)# eigrp default-route-tag 10.10.10.10
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
EIGRP commands	EIGRP Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Route Tag Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 18: Feature Information for Route Tag Enhancement

Feature Name	Releases	Feature Information
EIGRP Route Tag Enhancements		The EIGRP Route Tag Enhancements feature enables you to specify and display route tags in dotted-decimal format, filter routes using the route tag wildcard mask, and set a default route tag for all internal Enhanced Interior Gateway Routing Protocol (EIGRP) routes. The following commands were introduced or modified: **eigrp default-route-tag**, **match tag**, **match tag list**, **route-tag list**, **route-tag notation**, **set tag (IP)**, **show eigrp address-family topology**, **show ip eigrp topology**, **show ipv6 eigrp topology**, **show ip eigrp vrf topology, show ip route**, **show ip route tag**, **show ipv6 route tag**, **show ip route vrf**, **show ipv6 route vrf**, **show route map**, and **show route-tag list**.

CHAPTER 12

BFD Support for EIGRP IPv6

The BFD Support for EIGRP IPv6 feature provides Bidirectional Forwarding Detection (BFD) support for Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 sessions, thereby facilitating rapid fault detection and alternate-path selection in EIGRP IPv6 topologies. BFD is a detection protocol that provides a consistent failure-detection method for network administrators, and network administrators use BFD to detect forwarding path failures at a uniform rate and not at variable rates for different routing protocol ‘Hello’ mechanisms. This failure-detection methodology ensures easy network profiling and planning and consistent and predictable reconvergence time. This document provides information about BFD support for EIGRP IPv6 networks and explains how to configure BFD support in EIGRP IPv6 networks.

- Finding Feature Information, on page 181
- Prerequisites for BFD Support for EIGRP IPv6, on page 181
- Restrictions for BFD Support for EIGRP IPv6, on page 182
- Information About BFD Support for EIGRP IPv6, on page 182
- How to Configure BFD Support for EIGRP IPv6, on page 182
- Configuration Examples for BFD Support for EIGRP IPv6, on page 186
- Additional References, on page 187
- Feature Information for BFD Support for EIGRP IPv6, on page 188

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for BFD Support for EIGRP IPv6

EIGRP IPv6 sessions have a shutdown option in router, address family, and address-family interface configuration modes. To enable BFD support on EIGRP IPv6 sessions, the routing process should be in no shut mode in the abovementioned modes.

Restrictions for BFD Support for EIGRP IPv6

- The BFD Support for EIGRP IPv6 feature is supported only in EIGRP named mode.
- EIGRP supports only single-hop Bidirectional Forwarding Detection (BFD).
- The BFD Support for EIGRP IPv6 feature is not supported on passive interfaces.

Information About BFD Support for EIGRP IPv6

BFD for EIGRP IPv6

Bidirectional Forwarding Detection (BFD) is a detection protocol that provides fast-forwarding, path-failure detection for all media types, encapsulations, topologies, and routing protocols. The BFD Support for EIGRP IPv6 feature enables BFD to interact with the Enhanced Interior Gateway Routing Protocol (EIGRP) to create BFDv6 sessions between EIGRP neighbors. In a BFD-enabled EIGRP IPv6 session, BFD constantly monitors the forwarding path (from a local device to a neighboring device) and provides consistent failure detection at a uniform rate. Because failure detection happens at a uniform rate and not at variable rates, network profiling and planning is easier, and the reconvergence time remains consistent and predictable.

BFD is implemented in EIGRP at multiple levels; it can be implemented per interface or on all interfaces. When BFD is enabled on a specific interface, all peer relationships formed through the EIGRP "Hello" mechanism on that interface are registered with the BFD process. Subsequently, BFD establishes a session with each of the peers in the EIGRP topology and notifies EIGRP through a callback mechanism of any change in the state of any peer. When a peer is lost, BFD sends a "peer down" notification to EIGRP, and EIGRP unregisters a peer from BFD. BFD does not send a "peer up" notification to EIGRP when the peer is up because BFD now has no knowledge of the state of the peer. This behavior prevents rapid neighbor bouncing and repetitive route computations. The EIGRP "Hello" mechanism will later allow peer rediscovery and reregistration with the BFD process.

How to Configure BFD Support for EIGRP IPv6

Configuring BFD Support on All Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ipv6 address** *ipv6-address/prefix-length*
6. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
7. **exit**
8. **router eigrp** *virtual-name*

9. **address-family ipv6 autonomous-system** *as-number*
10. **eigrp router-id** *ip-address*
11. **af-interface default**
12. **bfd**
13. **end**
14. **show eigrp address-family ipv6 neighbors**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet0/0/1`	Specifies the interface type and number, and enters the interface configuration mode.
Step 5	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:A:B::1/64`	Configures an IPv6 address.
Step 6	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Device(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Sets the baseline BFD session parameters on an interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Specifies an EIGRP routing process and enters router configuration mode.
Step 9	**address-family ipv6 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 3`	Enters address family configuration mode for IPv6 and configures an EIGRP routing instance.
Step 10	**eigrp router-id** *ip-address* **Example:** `Device(config-router-af)# eigrp router-id 172.16.1.3`	Sets the device ID used by EIGRP for this address family when EIGRP peers communicate with their neighbors.
Step 11	**af-interface default** **Example:** `Device(config-router-af)# af-interface default`	Configures interface-specific commands on all interfaces that belong to an address family in EIGRP named mode configurations, and enters address-family interface configuration mode.
Step 12	**bfd** **Example:** `Device(config-router-af-interface)# bfd`	Enables BFD on all interfaces.

Step 13	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address-family interface configuration mode and returns to privileged EXEC mode.

Step 14	**show eigrp address-family ipv6 neighbors** **Example:** `Device# show eigrp address-family ipv6 neighbors`	(Optional) Displays neighbors for which BFD has been enabled.

Configuring BFD Support on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **ipv6 address** *ipv6-address /prefix-length*
6. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
7. **exit**

8. **router eigrp** *virtual-name*
9. **address-family ipv6 autonomous-system** *as-number*
10. **eigrp router-id** *ip-address*
11. **af-interface** *interface-type interface-number*
12. **bfd**
13. **end**
14. **show eigrp address-family ipv6 neighbors**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet0/0/1`	Specifies the interface type and number, and enters the interface configuration mode.
Step 5	**ipv6 address** *ipv6-address /prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:A:B::1/64`	Configures an IPv6 address.
Step 6	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Device(config-if)# bfd interval 50 min_rx 50 multiplier 3`	Sets the baseline BFD session parameters on an interface.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Specifies an EIGRP routing process and enters router configuration mode.
Step 9	**address-family ipv6 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 3`	Enters address family configuration mode for IPv6 and configures an EIGRP routing instance.
Step 10	**eigrp router-id** *ip-address* **Example:** `Device(config-router-af)# eigrp router-id 172.16.1.3`	Sets the device ID used by EIGRP for this address family when EIGRP peers communicate with their neighbors.
Step 11	**af-interface** *interface-type interface-number* **Example:** `Device(config-router-af)# af-interface gigabitethernet0/0/1`	Configures interface-specific commands on an interface that belongs to an address family in an EIGRP named mode configuration, and enters address-family interface configuration mode.
Step 12	**bfd** **Example:** `Device(config-router-af-interface)# bfd`	Enables BFD on the specified interface.

Step 13	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address-family interface configuration mode and returns to privileged EXEC mode.

Step 14	**show eigrp address-family ipv6 neighbors** **Example:** `Device# show eigrp address-family ipv6 neighbors`	(Optional) Displays neighbors for which BFD has been enabled.

Configuration Examples for BFD Support for EIGRP IPv6

Example: Configuring BFD Support on All Interfaces

```
Device(config)# ipv6 unicast-routing
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ipv6 address 2001:0DB8:1::12/64
Device(config-if)# bfd interval 50 min_rx 50 multiplier 3
Device(config-if)# exit
Device(config)# router eigrp name
Device(config-router)# address-family ipv6 unicast autonomous-system 1
Device(config-router-af)# eigrp router-id 172.16.0.1
Device(config-router-af)# af-interface default
Device(config-router-af-interface)# bfd
Device(config-router-af-interface)# end
```

Example: Configuring BFD Support on an Interface

```
Device(config)# ipv6 unicast-routing
Device(config)# GigabitEthernet0/0/1
Device(config-if)# ipv6 address 2001:DB8:A:B::1/64
Device(config-if)# bfd interval 50 min_rx 50 multiplier 3
Device(config-if)# exit
Device(config)# router eigrp name
Device(config-router)# address-family ipv6 autonomous-system 3
Device(config-router-af)# af-interface GigabitEthernet0/0/1
Device(config-router-af-interface)# bfd
Device(config-router-af-interface)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Commands List, All Releases
BFD commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples.	IP Routing: Protocol-Independent Command Reference
EIGRP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples.	IP Routing: EIGRP Command Reference
Configuring EIGRP	"Configuring EIGRP" chapter in *IP Routing: EIGRP Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BFD Support for EIGRP IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 19: Feature Information for BFD Support for EIGRP IPv6

Feature Name	Releases	Feature Information
BFD Support for EIGRP IPv6		Bidirectional Forwarding Detection (BFD) is a detection protocol that provides fast-forwarding, path-failure detection for all media types, encapsulations, topologies, and routing protocols. BFD helps network administrators to ensure easier network profiling and planning and consistent and predictable reconvergence time. BFD interacts with Enhanced Interior Gateway Routing Protocol (EIGRP) to create sessions (IPv4 type sessions) between EIGRP neighbors for fast-forwarding, path-failure detections. Each session tests the forwarding path for a single route from a local router to a neighboring router. For any change in state (forwarding path goes down or forwarding path comes up) for any of the sessions, BFD notifies EIGRP of the new state for that route. Support has been added for EIGRP IPv6 neighbors to use BFD as a fall-over mechanism. The following commands were introduced or modified: **bfd**, **show eigrp address-family neighbors**, **show eigrp address-family interfaces**.

CHAPTER 13

EIGRP Loop-Free Alternate Fast Reroute

The EIGRP Loop-Free Alternate Fast Reroute feature allows the Enhanced Interior Gateway Routing Protocol (EIGRP) to reduce the routing transition time to less than 50 ms by precomputing repair paths or backup routes and installing these paths or routes in the Routing Information Base (RIB). Fast Reroute (FRR) is the mechanism that enables traffic that traverses a failed link to be rerouted around the failure. In EIGRP networks, precomputed backup routes or repair paths are known as feasible successors or loop-free alternates (LFAs). This module describes how to configure the EIGRP Loop-Free Alternate Fast Reroute feature and enable load-sharing and tie-breaking configurations for the feasible successors or LFAs that are identified by EIGRP.

- Finding Feature Information, on page 189
- Restrictions for EIGRP Loop-Free Alternate Fast Reroute, on page 189
- Information About EIGRP Loop-Free Alternate Fast Reroute, on page 190
- How to Configure EIGRP Loop-Free Alternate Fast Reroute, on page 191
- Configuration Examples for EIGRP Loop-Free Alternate Fast Reroute, on page 195
- Additional References, on page 196
- Feature Information for EIGRP Loop-Free Alternate Fast Reroute, on page 197

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EIGRP Loop-Free Alternate Fast Reroute

- Only paths that are reachable through point-to-point interfaces are protected.
- IPv6 is not supported.

Information About EIGRP Loop-Free Alternate Fast Reroute

Repair Paths Overview

When a link or a device fails, distributed routing algorithms compute new routes or repair paths. The time taken for this computation is called routing transition. Until the transition is complete and all devices are converged on a common view of the network, the connectivity between the source and destination pairs of devices is interrupted. Repair paths forward traffic during a routing transition.

When a link or a device fails, initially only the neighboring devices are aware of the failure. All other devices in the network are unaware of the nature and location of this failure until information about this failure is propagated through the routing protocol. The propagation of this information may take several hundred milliseconds. Meanwhile, packets affected by the network failure need to be steered to their destinations. A device adjacent to the failed link employs a set of repair paths for packets that would have used the failed link. These repair paths are used from the time the router detects the failure until the routing transition is complete. By the time the routing transition is complete, all devices in the network revise their forwarding data and the failed link is eliminated from the routing computation. Routing protocols precompute repair paths in anticipation of failures so that the repair paths can be activated the moment a failure is detected. In Enhanced Interior Gateway Routing Protocol (EIGRP) networks, precomputed repair paths or backup routes are known as feasible successors or loop-free alternates (LFAs).

LFA Computation

A loop-free alternate (LFA) is a precomputed next-hop route that delivers a packet to its destination without looping back. Traffic is redirected to an LFA after a network failure and the LFA makes the forwarding decision without any knowledge of the failure.

Interior Gateway Protocols (IGPs) compute LFAs in the following two ways:

- Per-link (link-based) computation: In link-based LFAs, all prefixes (networks) that are reachable through the primary (protected) link share the same backup information. This means that the whole set of prefixes sharing the primary link also share the repair or the Fast Reroute (FRR) ability. The per-link approach protects only the next-hop address. It need not necessarily protect the destination node. Therefore, the per-link approach is suboptimal and not the best approach for capacity planning because all traffic from the primary link is redirected to the next hop instead of being spread over multiple paths. Redirecting all traffic to the next hop may lead to congestion on the link to the next hop

- Per-prefix (prefix-based) computation: Prefix-based LFAs allow computing backup information per prefix (network) and protect the destination address. The per-prefix approach is preferred over the per-link approach because of its greater applicability and better bandwidth utilization. Per-prefix computations provide better load sharing and better protection coverage than per-link computations because per-prefix computations evaluate all possible LFAs and use tie-breakers to select the best LFA from among the available LFAs.

Note The repair or backup information computed for a primary path by using prefix-based LFAs may be different from that computed by using link-based LFAs.

EIGRP always computes prefix-based LFAs. EIGRP uses the Diffusing Update Algorithm (DUAL) to calculate the successor and feasible successors. EIGRP uses the successor as the primary path and feasible successors as repair paths or LFAs.

LFA Tie-Breaking Rules

When there are multiple candidate LFAs for a given primary path, EIGRP uses a tie-breaking rule to select one LFA per primary path per prefix. A tie-breaking rule considers LFAs that satisfy certain conditions or have certain attributes. EIGRP uses the following four attributes to implement tie-breaking rules:

- Interface-disjoint—Eliminates LFAs that share the outgoing interface with the protected path.
- Linecard-disjoint—Eliminates LFAs that share the line card with the protected path.
- Lowest-repair-path-metric—Eliminates LFAs whose metric to the protected prefix is high. Multiple LFAs with the same lowest path metric may remain in the routing table after this tie-breaker is applied.
- Shared Risk Link Group (SRLG)-disjoint—Eliminates LFAs that belong to any of the protected path SRLGs. SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may also fail. Therefore, links in a group share risks.

How to Configure EIGRP Loop-Free Alternate Fast Reroute

Configuring LFA FRRs per Prefix

Perform this task to configure loop-free alternate (LFA) Fast Reroutes (FRRs) per prefix in an Enhanced Interior Gateway Routing Protocol (EIGRP) network. You can enable LFAs for all available prefixes in the EIGRP topology or for prefixes specified by route maps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *autonomous-system-number*
5. **topology base**
6. **fast-reroute per-prefix** {**all** | **route-map** *route-map-name*}
7. **end**
8. **show ip eigrp topology frr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 1`	Enters IPv4 VRF address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology base** **Example:** `Device(config-router-af)# topology base`	Configures a base EIGRP topology and enters router address family topology configuration mode.

Step 6	**fast-reroute per-prefix {all | route-map** *route-map-name***}**
	Example:
	`Device(config-router-af-topology)# fast-reroute per-prefix all`
		Enables FRR for all prefixes in the topology.
		• Enter the **route-map** keyword to enable FRR on prefixes specified by a route map.

Step 7	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits router address family topology configuration mode and returns to privileged EXEC mode.

Step 8	**show ip eigrp topology frr** **Example:** `Device# show ip eigrp topology frr`	Displays the list of configured LFAs in the EIGRP topology table.

Disabling Load Sharing Among Prefixes

When the primary path is an Equal Cost Multipath (ECMP) path with multiple LFAs, prefixes (networks) are distributed equally among the LFAs because the default behavior for ECMP paths is load sharing. However, you can control the selection of LFAs by enabling tie-breaking configurations. To enable tie-breaking configurations, you should disable load sharing among prefixes. Perform this task to disable load sharing among prefixes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *autonomous-system-number*

5. **topology base**
6. **fast-reroute load-sharing disable**
7. **end**
8. **show ip eigrp topology frr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 1`	Enters IPv4 VRF address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology base** **Example:** `Device(config-router-af)# topology base`	Configures a base EIGRP topology and enters router address family topology configuration mode.
Step 6	**fast-reroute load-sharing disable** **Example:** `Device(config-router-af-topology)# fast-reroute load-sharing disable`	Disables load sharing among prefixes.

Step 7	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits router address family topology configuration mode and returns to privileged EXEC mode.

Step 8	**show ip eigrp topology frr** **Example:** `Device# show ip eigrp topology frr`	Displays the list of configured feasible successors or LFAs in the EIGRP topology table.

Enabling Tie-Breaking Rules for EIGRP LFAs

Perform this task to enable tie-breaking rules to select a single loop-free alternate (LFA) when there are multiple LFAs for a given primary path. The Enhanced Interior Gateway Routing Protocol (EIGRP) allows you to use four attributes to configure tie-breaking rules. Each of the following keywords of the **fast-reroute tie-break** command allows you to configure a tie-breaking rule based on a specific attribute: **interface-disjoint**, **linecard-disjoint**, **lowest-backup-path-metric**, and **srlg-disjoint**. You can assign a priority value for each attribute. Tie-breaking rules are applied on the basis of the priority assigned to each attribute. The lower the assigned priority value the higher the priority of the tie-breaking attribute.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *autonomous-system-number*
5. **topology base**
6. **fast-reroute tie-break {interface-disjoint | linecard-disjoint | lowest-backup-path-metric | srlg-disjoint}** *priority-number*
7. **end**
8. **show ip eigrp topology frr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 1`	Enters IPv4 VRF address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology base** **Example:** `Device(config-router-af)# topology base`	Configures a base EIGRP topology and enters router address family topology configuration mode.

	Command or Action	Purpose
Step 6	**fast-reroute tie-break {interface-disjoint | linecard-disjoint | lowest-backup-path-metric | srlg-disjoint}** *priority-number* **Example:** `Device(config-router-af-topology)# fast-reroute tie-break lowest-backup-path-metric 2`	Enables EIGRP to select an LFA by configuring a tie-breaking attribute and assigning a priority to that attribute. • You cannot configure an attribute more than once in an address family.

Step 7	**end**
	Example:
	`Device(config-router-af-topology)# end`
		Exits router address family topology configuration mode and returns to privileged EXEC mode.

Step 8	**show ip eigrp topology frr** **Example:** `Device# show ip eigrp topology frr`	Displays the list of configured feasible successors or LFAs in the EIGRP topology table.

Configuration Examples for EIGRP Loop-Free Alternate Fast Reroute

Example: Configuring LFA FRRs Per Prefix

The following example shows how to configure Enhanced Interior Gateway Routing Protocol (EIGRP) loop-free alternate (LFA) Fast Reroutes (FRRs) for prefixes specified by the route map named map1:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute per-prefix route-map map1
Device(config-router-af-topology)# end
```

Example: Disabling Load Sharing Among Prefixes

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute load-sharing disable
Device(config-router-af-topology)# end
```

Example: Enabling Tie-Breaking Rules

The following examples show how to enable tie-breaking configurations to allow the Enhanced Interior Gateway Routing Protocol (EIGRP) to select a loop-free alternate (LFA) when there are multiple candidate LFAs for a given primary path. The following example shows how to enable the tie-breaking rule that eliminates LFAs that share the outgoing interface with the primary path:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute tie-break interface-disjoint 2
Device(config-router-af-topology)# end
```

The following example shows how to enable the tie-breaking rule that eliminates LFAs that share the linecard with the primary path:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute tie-break linecard-disjoint 3
Device(config-router-af-topology)# end
```

The following example shows how to enable the tie-breaking rule that selects the LFA with the lowest metric to the the protected prefix:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute tie-break lowest-backup-path-metric 4
Device(config-router-af-topology)# end
```

The following example shows how to enable the tie-breaking rule that eliminates LFAs that share any SRLGs with the primary path:

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 1
Device(config-router-af)# topology base
Device(config-router-af-topology)# fast-reroute tie-break srlg-disjoint 1
Device(config-router-af-topology)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases

Related Topic	Document Title
EIGRP commands	EIGRP Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Loop-Free Alternate Fast Reroute

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 20: Feature Information for EIGRP Loop-Free Alternate Fast Reroute

Feature Name	Releases	Feature Information
EIGRP Loop-Free Alternate Fast Reroute		The EIGRP Loop-Free Alternate Fast Reroute feature allows the Enhanced Interior Gateway Routing Protocol (EIGRP) to reduce the routing transition time to less than 50 ms by precomputing repair paths or backup routes and installing these paths or routes in the Routing Information Base (RIB). In EIGRP networks, the precomputed backup routes are known as feasible successors or loop-free alternates (LFAs). The following commands were introduced or modified: **debug eigrp frr**, **fast-reroute load-sharing disable (EIGRP)**, **fast-reroute per-prefix (EIGRP)**, **fast-reroute tie-break (EIGRP)**, and **show ip eigrp topology**.

CHAPTER 14

Add Path Support in EIGRP

The Add Path Support in EIGRP feature enables hubs in a single Dynamic Multipoint VPN (DMVPN) domain to advertise multiple best paths to connected spokes when the Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol between the hubs and the spokes. This module provides information about the Add Path Support in EIGRP feature and explains how to configure it.

- Finding Feature Information, on page 199
- Prerequisites for Add Path Support in EIGRP, on page 199
- Restrictions for Add Path Support in EIGRP, on page 200
- Information About Add Path Support in EIGRP, on page 200
- How to Configure Add Path Support in EIGRP, on page 202
- Configuration Examples for Add Path Support in EIGRP, on page 205
- Additional References for Add Path Support in EIGRP, on page 205
- Feature Information for Add Path Support in EIGRP, on page 206

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Add Path Support in EIGRP

All interfaces in an Enhanced Interior Gateway Routing Protocol (EIGRP) topology are by default configured with the **next-hop-self** command. This command enables EIGRP to set the local outbound interface as the next-hop value while advertising a route to a peer, even when advertising routes out of the interface on which the routes were learned. This default EIGRP behavior may interfere with the **add-paths**command that helps configure the Add Path Support in EIGRP feature. Therefore, before you configure this feature on a hub device in a Dynamic Multipoint VPN (DMVPN) domain, you must disable the **next-hop-self** command that is configured on the hub interface that connects to spokes in the DMVPN domain.

Restrictions for Add Path Support in EIGRP

- The Add Path Support in EIGRP feature can be enabled only in Enhanced Interior Gateway Routing Protocol (EIGRP) named mode configurations.
- The **variance** command should not be configured when the Add Path Support in EIGRP feature is enabled. The **variance** command alters the metrics of routes in an EIGRP topology, thereby enabling EIGRP to balance traffic among desired paths. Therefore, if you configure the **variance** command on a hub device, the command may interfere with the configuration of this feature.

Information About Add Path Support in EIGRP

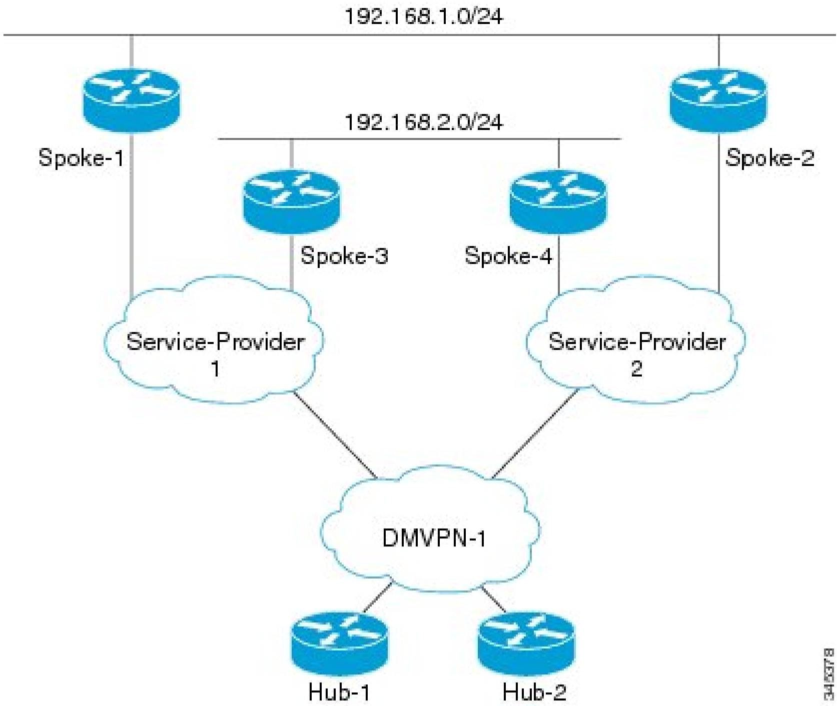
EIGRP Add Path Support Overview

In most Dynamic Multipoint VPN (DMVPN) domains, two or more spokes are connected to the same LAN segment. These spokes connect to more than one hub (for hub redundancy) through different service providers (for service-provider redundancy). In a single DMVPN domain, a hub connects to all spokes through one tunnel interface. In Enhanced Interior Gateway Routing Protocol (EIGRP) topologies, when a hub has more than one path (with the same metric but through different spokes) to reach the same network, both paths are chosen as best paths. However, by default, EIGRP advertises only one path as the best path to connected spokes. With the implementation of the Add Path Support in EIGRP feature, hubs in an EIGRP-DMVPN domain can advertise up to four additional best paths to connected spokes, thereby allowing load balancing and path redundancy. This feature supports both IPv4 and IPv6 configurations.

How Add Path Support in EIGRP Works

A typical single Dynamic Multipoint VPN (DMVPN) domain consists of dual hubs (for hub redundancy) connected to more than one service provider (for service-provider redundancy). In the figure below, two hub devices—Hub-1 and Hub-2—are connected through tunnel interfaces to a DMVPN domain.

Figure 3: Single DMVPN Domain



The DMVPN domain is in turn connected to two service providers—Service-Provider 1 and Service-Provider 2. Four spoke devices in this DMVPN domain—Spoke-1, Spoke-2, Spoke-3, and Spoke-4. Spoke-1 and Spoke-3 are connected to Service-Provider 1, and Spoke-2 and Spoke-4 are connected to Service-Provider 2. The Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol between the hubs and the spokes over the tunnel interfaces.

Spoke-1 and Spoke-2 are connected to a LAN with the network address 192.168.1.0/24. Both these spokes are connected to both the hubs through two different service providers, and hence, these spokes advertise the same LAN network to both hubs. Typically, spokes on the same LAN advertise the same metric; therefore, based on the metric, Hub-1 and Hub-2 have dual Equal-Cost Multipath (ECMP) routes to reach network 192.168.1.0/24. However, because EIGRP is a distance vector protocol, it advertises only one best path to the destination. Therefore, in this EIGRP-DMVPN domain, the hubs advertise only one route (for example, through Spoke-1) to reach network 192.168.1.0/24. When clients in subnet 192.168.2.0/24 communicate with clients in subnet 192.168.1.0/24, all traffic is directed to Spoke-1. Because of this default EIGRP behavior, there is no load balancing on Spoke-3 and Spoke-4. Additionally, if Spoke-1 fails or if the network of Service-Provider 1 goes down, EIGRP must reconverge to provide connectivity to 192.168.1.0/24.

The Add Path Support in EIGRP feature enables EIGRP to advertise up to four additional paths to connected spokes in a single DMVPN domain. If you configure this feature in the example topology discussed above, both Spoke-1 and Spoke-2 will be advertised to Spoke-3 and Spoke-4 as best paths to network 192.168.1.0, thereby allowing load balancing among all spokes in this DMVPN domain.

How to Configure Add Path Support in EIGRP

Configuring IPv4 Add Path Support on a Hub

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **af-interface** {**default** | *interface-type interface-number*}
6. **no next-hop-self** [**no-ecmp-mode**]
7. **add-paths** *number*
8. **end**
9. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 3`	Enters address family configuration mode and configures an EIGRP routing instance.

Step 5	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface tunnel 0`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

	Command or Action	Purpose
Step 6	**no next-hop-self** [**no-ecmp-mode**] **Example:** `Device(config-router-af-interface)# no next-hop-self no-ecmp-mode`	Instructs EIGRP to use the received next hop and not the local outbound interface address as the next hop to be advertised to neighboring devices.
Step 7	**add-paths** *number* **Example:** `Device(config-router-af-interface)# add-paths 4`	Enables EIGRP to advertise multiple paths as best paths to connected spokes in a single Dynamic Multipoint VPN (DMVPN) domain.

Step 8	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address family interface configuration mode and returns to privileged EXEC mode.

Step 9	**show running-config** **Example:** `Device# show running-config | section eigrp`	Displays contents of the current running configuration file. • Use the output modifier "|" to display the EIGRP section of the running configuration, and to verify whether the **add-paths** command is enabled in the configuration.

Configuring IPv6 Add Path Support on a Hub

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **router eigrp** *virtual-name*
5. **address-family ipv6 autonomous-system** *as-number*
6. **af-interface** {**default** | *interface-type interface-number*}
7. **no next-hop-self** [**no-ecmp-mode**]
8. **add-paths** *number*
9. **end**
10. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Device(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 4	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name`	Configures an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process and enters router configuration mode.
Step 5	**address-family ipv6 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv6 autonomous-system 3`	Enters address family configuration mode and configures an EIGRP routing instance.

Step 6	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface tunnel 0`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 7	**no next-hop-self** [**no-ecmp-mode**] **Example:** `Device(config-router-af-interface)# no next-hop-self no-ecmp-mode`	Instructs EIGRP to use the received next-hop address and not the local outbound interface address as the next hop to be advertised to neighboring devices.
Step 8	**add-paths** *number* **Example:** `Device(config-router-af-interface)# add-paths 4`	Enables EIGRP to advertise multiple paths as best paths to connected spokes in a single Dynamic Multipoint VPN (DMVPN) domain.

Step 9	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address family interface configuration mode and returns to privileged EXEC mode.

Step 10	**show running-config** **Example:** `Device# show running-config | section eigrp`	Displays contents of the current running configuration file. • Use the output modifier "|" to display the EIGRP section of the running configuration, and to verify whether the **add-paths** command is enabled in the configuration.

Configuration Examples for Add Path Support in EIGRP

Example: Configuring IPv4 Add Path Support on a Hub

```
Device(config)# router eigrp name
Device(config-router)# address-family ipv4 autonomous-system 10
Device(config-router-af)# af-interface tunnel 0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
Device(config-router-af-interface)# add-paths 4
Device(config-router-af-interface)# end
```

Example: Configuring IPv6 Add Path Support on a Hub

```
Device(config)# ipv6 unicast-routing
Device(config)# router eigrp name
Device(config-router)# address-family ipv6 autonomous-system 10
Device(config-router-af)# af-interface tunnel 0
Device(config-router-af-interface)# no next-hop-self no-ecmp-mode
Device(config-router-af-interface)# add-paths 4
Device(config-router-af-interface)# end
```

Additional References for Add Path Support in EIGRP

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP technology white papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Add Path Support in EIGRP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 21: Feature Information for Add Path Support in EIGRP

Feature Name	Releases	Feature Information
Add Path Support in EIGRP		The Add Path Support in EIGRP feature enables a hub in a single Dynamic Multipoint VPN (DMVPN) domain to advertise multiple paths to connected spokes when the Enhanced Interior Gateway Routing Protocol (EIGRP) is the routing protocol between the hub and the spokes. The following command was introduced or modified: **add-paths**.

CHAPTER 15

EIGRP Wide Metrics

The EIGRP Wide Metrics feature supports 64-bit metric calculations and Routing Information Base (RIB) scaling in Enhanced Interior Gateway Routing Protocol (EIGRP) topologies. The 64-bit calculations work only in EIGRP named mode configurations. EIGRP classic mode configurations use 32-bit calculations. This module provides an overview of the EIGRP Wide Metrics feature.

- Information About EIGRP Wide Metrics, on page 207
- Additional References, on page 211
- Feature Information for EIGRP Wide Metrics, on page 211

Information About EIGRP Wide Metrics

EIGRP Composite Cost Metrics

The Enhanced Interior Gateway Routing Protocol (EIGRP) uses bandwidth, delay, reliability, load, and K values (various constants that can be configured by a user to produce varying routing behaviors) to calculate the composite cost metric for local Routing Information Base (RIB) installation and route selections. The EIGRP composite cost metric is calculated using the following formula:

EIGRP composite cost metric = 256*((K1*Scaled Bw) + (K2*Scaled Bw)/(256 – Load) + (K3*Scaled Delay)*(K5/(Reliability + K4)))

EIGRP uses one or more vector metrics to calculate the composite cost metric. The table below lists EIGRP vector metrics and their descriptions.

Table 22: EIGRP Vector Metrics

Vector Metric	Description
bandwidth	The minimum bandwidth (Bw) of the route, in kilobits per second. It can be 0 or any positive integer. The bandwidth for the formula is scaled and inverted by using the following formula: Scaled Bw = (10^7/minimum bandwidth (Bw) in kilobits per second)
delay	Route delay, in tens of microseconds. Scaled Delay = (Delay/10)

Vector Metric	Description
load	The effective load of the route, expressed as a number from 0 to 255 (255 is 100 percent loading).
mtu	The minimum maximum transmission unit (MTU) size of the route, in bytes. It can be 0 or any positive integer.
reliability	The likelihood of successful packet transmission, expressed as a number between 0 and 255, where 255 means 100 percent reliability and 0 means no reliability.

EIGRP monitors metric weights, by using K values, on an interface to allow the tuning of EIGRP metric calculations and to indicate the type of service (ToS). K values are integers from 0 to 128; these integers, in conjunction with variables like bandwidth and delay, are used to calculate the overall EIGRP composite cost metric. The table below lists the K values and their defaults.

Table 23: EIGRP K-Value Defaults

Setting	Default Value
K1	1
K2	0
K3	1
K4	0
K5	0

Although you can configure K values to produce varying routing behaviors, most configurations use only the delay and bandwidth metrics by default, with bandwidth taking precedence, to produce a single 32-bit metric. Use of the default constants effectively reduces the above-mentioned composite cost metric formula to the following default formula: 256*(Scaled Bw + Scaled Delay).

For example, let us consider a link whose bandwidth to a particular destination is 128 kb/s and the delay is 84,000 microseconds. By using the default formula, you can simplify the EIGRP composite cost metric calculation to 256*(Scaled Bw + Scaled Delay), thus resulting in the following value:

Metric = 256*(10^7/128 + 84000/10) = 256*86525 = 22150400

EIGRP Wide Metrics

The Enhanced Interior Gateway Routing Protocol (EIGRP) composite cost metric (calculated using the bandwidth, delay, reliability, load, and K values) is not scaled correctly for high-bandwidth interfaces or Ethernet channels, resulting in incorrect or inconsistent routing behavior. The lowest delay that can be configured for an interface is 10 microseconds. As a result, high-speed interfaces, such as 10 Gigabit Ethernet (GE) interfaces, or high-speed interfaces channeled together (GE ether channel) will appear to EIGRP as a single GE interface. This may cause undesirable equal-cost load balancing. To resolve this issue, the EIGRP Wide Metrics feature supports 64-bit metric calculations and Routing Information Base (RIB) scaling that provide the ability to support interfaces (either directly or via channeling techniques like port channels or ether channels) up to approximately 4.2 terabits.

Note The 64-bit metric calculations work only in EIGRP named mode configurations. EIGRP classic mode uses 32-bit metric calculations.

To accommodate interfaces with bandwidths above 1 gigabit and up to 4.2 terabits and to allow EIGRP to perform path selections, the EIGRP composite cost metric formula is modified. The paths are selected based on the computed time. The time that information takes to travel through links is measured in picoseconds. The interfaces can be directly capable of these high speeds, or the interfaces can be bundles of links with an aggregate bandwidth greater than 1 gigabit.

Metric = [(K1*Minimum Throughput + {K2*Minimum Throughput} / 256-Load) + (K3*Total Latency) + (K6*Extended Attributes)]* [K5/(K4 + Reliability)]

Default K values are as follows:

- K1 = K3 = 1
- K2 = K4 = K5 = 0
- K6 = 0

The EIGRP Wide Metrics feature also introduces K6 as an additional K value for future use.

By default, the path selection scheme used by EIGRP is a combination of throughput (rate of data transfer) and latency (time taken for data transfer), and the formula for calculating the composite cost metric is as follows:

Composite Cost Metric = (K1*Minimum Throughput) + (K3*Total Latency)

Minimum Throughput = (10^7* 65536)/Bw), where 65536 is the wide-scale constant.

Total Latency for bandwidths below 1 gigabit = (Delay*65536)/10, where 65536 is the wide-scale constant.

Total Latency for bandwidths above 1 gigabit = (10^7* 65536/10)/ Bw, 65536 is the wide-scale constant.

With the calculation of larger bandwidths, EIGRP can no longer fit the computed metric into a 4-byte unsigned long value that is needed by the Cisco RIB. To set the RIB scaling factor for EIGRP, use the **metric rib-scale** command. When you configure the **metric rib-scale** command, all EIGRP routes in the RIB are cleared and replaced with the new metric values.

EIGRP Metric Weights

You can use the **metric weights** command to adjust the default behavior of Enhanced Interior Gateway Routing Protocol (EIGRP) routing and metric computations. EIGRP metric defaults (K values) 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 K values without guidance from an experienced network designer.

By default, the EIGRP composite cost metric is a 32-bit quantity that is the sum of segment delays and the lowest segment bandwidth (scaled and inverted) for a given route. The formula used to scale and invert the bandwidth value is 10^7/minimum bandwidth in kilobits per second. However, with the EIGRP Wide Metrics feature, the EIGRP composite cost metric is scaled to include 64-bit metric calculations for EIGRP named mode configurations.

For a network of homogeneous media, this metric reduces to a hop count. For a network of mixed media (FDDI, Gigabit Ethernet (GE), 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

EIGRP K values are the metrics that EIGRP uses to calculate routes. Mismatched K values can prevent neighbor relationships from being established and can negatively impact network convergence. The example given below explains this behavior between two EIGRP peers (Device-A and Device-B).

The following configuration is applied to Device-A. The K values are changed using the **metric weights** command. A value of 2 is entered for the *k1* argument to adjust the bandwidth calculation. A value of 1 is entered for the *k3* argument to adjust the delay calculation.

```
Device(config)# hostname Device-A
Device-A(config)# interface serial 0
Device-A(config-if)# ip address 10.1.1.1 255.255.255.0
Device-A(config-if)# exit
Device-A(config)# router eigrp name1
Device-A(config-router)# address-family ipv4 autonomous-system 4533
Device-A(config-router-af)# network 10.1.1.0 0.0.0.255
Device-A(config-router-af)# metric weights 0 2 0 1 0 0 1
```

The following configuration is applied to Device-B, and the default K values are used. The default K values are 1, 0, 1, 0, 0, and 0.

```
Device(config)# hostname Device-B
Device-B(config)# interface serial 0
Device-B(config-if)# ip address 10.1.1.2 255.255.255.0
Device-B(config-if)# exit
Device-B(config)# router eigrp name1
Device-B(config-router)# address-family ipv4 autonomous-system 4533
Device-B(config-router-af)# network 10.1.1.0 0.0.0.255
Device-B(config-router-af)# metric weights 0 1 0 1 0 0 0
```

The bandwidth calculation is set to 2 on Device-A and set to 1 (by default) on Device-B. This configuration prevents these peers from forming a neighbor relationship.

The following error message is displayed on the console of Device-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
```

The following are two scenarios where the above error message can be displayed:

- Two devices are connected on the same link and configured to establish a neighbor relationship. However, each device is configured with different K values.
- One of two peers has transmitted a “peer-termination” message (a message that is broadcast when an EIGRP routing process is shut down), and the receiving device does not support this message. The receiving device will interpret this message as a K-value mismatch.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Wide Metrics

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 24: Feature Information for EIGRP Wide Metrics

Feature Name	Releases	Feature Information
EIGRP Wide Metrics		The EIGRP Wide Metrics feature introduces 64-bit metric calculations and RIB scaling in Enhanced Interior Gateway Routing Protocol (EIGRP) topologies. The following commands were introduced or modified by this feature: **metric rib-scale, metric weights**, **show eigrp address-family neighbors**, **show eigrp address-family topology**, **show eigrp plugins**, **show eigrp protocols**, **show eigrp tech-support**, **show ip eigrp neighbors**, and **show ip eigrp topology**.

CHAPTER 16

EIGRP/SAF HMAC-SHA-256 Authentication

The EIGRP/SAF HMAC-SHA-256 Authentication feature enables packets in an Enhanced Interior Gateway Routing Protocol (EIGRP) topology or a Service Advertisement Framework (SAF) domain to be authenticated using Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) message authentication codes. This module discusses this feature from an EIGRP perspective; it gives a brief overview of this feature and explains how to configure it.

- Finding Feature Information, on page 213
- Information About EIGRP/SAF HMAC-SHA-256 Authentication, on page 213
- How to Configure EIGRP/SAF HMAC-SHA-256 Authentication, on page 215
- Configuration Examples for EIGRP/SAF HMAC-SHA-256 Authentication, on page 217
- Additional References, on page 217
- Feature Information for EIGRP/SAF HMAC-SHA-256 Authentication, on page 218

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP/SAF HMAC-SHA-256 Authentication

EIGRP Neighbor Relationship Maintenance

Neighbor relationship maintenance is the process that devices use to dynamically learn of other devices on their directly attached networks. Devices must also discover when their neighbors become unreachable or inoperative. Neighbor relationship maintenance is achieved with low overhead by devices when they periodically send small hello packets to each other. As long as hello packets are received, the Cisco software can determine whether a neighbor is alive and functioning. After the status of the neighbor is determined, neighboring devices can exchange routing information.

The reliable transport protocol is responsible for the guaranteed, ordered delivery of Enhanced Interior Gateway Routing Protocol (EIGRP) packets to all neighbors. The reliable transport protocol supports intermixed transmission of multicast and unicast packets. Some EIGRP packets (such as updates) must be sent reliably; this means that the packets require acknowledgment from the destination. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities, hello packets need not be sent reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello packet with an indication in the packet informing receivers that the packet need not be acknowledged. The reliable transport protocol can send multicast packets quickly when unacknowledged packets are pending, thereby ensuring that the convergence time remains low in the presence of varying speed links.

Some EIGRP remote unicast-listen (any neighbor that uses unicast to communicate) and remote multicast-group neighbors may peer with any device that sends a valid hello packet, thus causing security concerns. By authenticating the packets that are exchanged between neighbors, you can ensure that a device accepts packets only from devices that know the preshared authentication key.

HMAC-SHA-256 Authentication

Packets exchanged between neighbors must be authenticated to ensure that a device accepts packets only from devices that have the same preshared authentication key. Enhanced Interior Gateway Routing Protocol (EIGRP) authentication is configurable on a per-interface basis; this means that packets exchanged between neighbors connected through an interface are authenticated. EIGRP supports message digest algorithm 5 (MD5) authentication to prevent the introduction of unauthorized information from unapproved sources. MD5 authentication is defined in RFC 1321. EIGRP also supports the Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication method. When you use the HMAC-SHA-256 authentication method, a shared secret key is configured on all devices attached to a common network. For each packet, the key is used to generate and verify a message digest that gets added to the packet. The message digest is a one-way function of the packet and the secret key. For more information on HMAC-SHA-256 authentication, see FIPS PUB 180-2, SECURE HASH STANDARD (SHS), for the SHA-256 algorithm and RFC 2104 for the HMAC algorithm.

If HMAC-SHA-256 authentication is configured in an EIGRP network, EIGRP packets will be authenticated using HMAC-SHA-256 message authentication codes. The HMAC algorithm takes as input the data to be authenticated (that is, the EIGRP packet) and a shared secret key that is known to both the sender and the receiver; the algorithm gives a 256-bit hash output that is used for authentication. If the hash value provided by the sender matches the hash value calculated by the receiver, the packet is accepted by the receiver; otherwise, the packet is discarded.

Typically, the shared secret key is configured to be identical between the sender and the receiver. To protect against packet replay attacks because of a spoofed source address, the shared secret key for a packet is defined as the concatenation of the user-configured shared secret (identical across all devices participating in the authenticated domain) with the IPv4 or IPv6 address (which is unique for each device) from which the packet is sent.

The device sending a packet calculates the hash to be sent based on the following:

- Key part 1—the configured shared secret.
- Key part 2—the local interface address from which the packet will be sent.
- Data—the EIGRP packet to be sent (prior to the addition of the IP header).

The device receiving the packet calculates the hash for verification based on the following:

- Key part 1—the configured shared secret.

- Key part 2—the IPv4 or IPv6 source address in the IPv4 or IPv6 packet header.
- Data—the EIGRP packet received (after removing the IP header).

For successful authentication, all of the following must be true:

- The sender and receiver must have the same shared secret.
- The source address chosen by the sender must match the source address in the IP header that the receiver receives.
- The EIGRP packet data that the sender transmits must match the EIGRP packet data that the receiver receives.

Authentication cannot succeed if any of the following is true:

- The sender does not know the shared secret expected by the receiver.
- The IP source address in the IP header is modified in transit.
- Any of the EIGRP packet data is modified in transit.

How to Configure EIGRP/SAF HMAC-SHA-256 Authentication

Configuring HMAC-SHA-256 Authentication

Before you begin

Perform this task to configure an interface to use basic Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication with an encrypted password—password1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **af-interface** {**default** | *interface-type interface-number*}
7. **authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	- **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	- **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 46000`
		Enters IPv4 or IPv6 VRF address family configuration mode and configures an EIGRP routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Associates a network with an EIGRP routing process. **Note** This command is used only while configuring an IPv4 routing instance.

Step 6	**af-interface** {**default** | *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface ethernet 0/0`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 7	**authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
	Example:
	`Device(config-router-af-interface)# authentication mode hmac-sha-256 7 password1`
		Specifies the type of authentication to be used in an EIGRP address family for the EIGRP instance. In this case, the HMAC-SHA-256 authentication method is used.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits address family interface configuration mode and returns to global configuration mode.

Configuration Examples for EIGRP/SAF HMAC-SHA-256 Authentication

Example: Configuring HMAC-SHA-256 Authentication

The following example shows how to configure Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) authentication with password password1.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp name1
Device(config-router)# address-family ipv6 autonomous-system 45000
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# authentication mode hmac-sha-256 0 password1
Device(config-router-af-interface)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	*SECURE HASH STANDARD (SHS)*

Standard/RFC	Title
RFC 1321	*The MD5 Message-Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Message Authentication*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP/SAF HMAC-SHA-256 Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 25: Feature Information for EIGRP/SAF HMAC-SHA-256 Authentication

Feature Name	Releases	Feature Information
EIGRP/SAF HMAC-SHA-256 Authentication		The EIGRP/SAF HMAC-SHA-256 Authentication feature enables packets in an Enhanced Interior Gateway Routing Protocol (EIGRP) topology or a Service Advertisement Framework (SAF) domain to be authenticated using Hashed Message Authentication Code-Secure Hash Algorithm-256 (HMAC-SHA-256) message authentication codes. The following command was introduced or modified by this feature: **authentication mode** (EIGRP).

CHAPTER 17

IP EIGRP Route Authentication

The IP Enhanced IGRP Route Authentication feature provides 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.

- Finding Feature Information, on page 219
- Information About IP EIGRP Route Authentication, on page 219
- How to Configure IP EIGRP Route Authentication, on page 220
- Configuration Examples for IP EIGRP Route Authentication, on page 225
- Additional References, on page 227
- Feature Information for IP EIGRP Route Authentication, on page 228

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP EIGRP Route Authentication

EIGRP Route Authentication

EIGRP route authentication provides 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.

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 the MD5 authentication key in use.

You can configure multiple keys with specific lifetimes. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in the order from lowest to highest, and uses the first valid key that it encounters. Note that the device needs to know the time to configure keys with lifetimes.

How to Configure IP EIGRP Route Authentication

Defining an Autonomous System for EIGRP Route Authentication

Before you begin

Before you configure EIGRP route authentication, you must enable EIGRP. In this task, EIGRP is defined with an autonomous system number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no switchport**
5. **ip authentication mode eigrp** *autonomous-system* **md5**
6. **ip authentication key-chain eigrp** *autonomous-system key-chain*
7. **exit**
8. **key chain** *name-of-chain*
9. **key** *key-id*
10. **key-string** *text*
11. **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
12. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0/9`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	Puts an interface into Layer 3 mode
Step 5	**ip authentication mode eigrp** *autonomous-system* **md5** **Example:** `Device(config-if)# ip authentication mode eigrp 1 md5`	Enables MD5 authentication in EIGRP packets.
Step 6	**ip authentication key-chain eigrp** *autonomous-system key-chain* **Example:** `Device(config-if)# ip authentication key-chain eigrp 1 keychain1`	Enables authentication of EIGRP packets.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits to global configuration mode.
Step 8	**key chain** *name-of-chain* **Example:** `Device(config)# key chain keychain1`	Identifies a key chain and enters key chain configuration mode.
Step 9	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies the key number and enters key chain key configuration mode.
Step 10	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string 0987654321`	Identifies the key string.

Step 11	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
	Example:
	`Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite`
		(Optional) Specifies the time period during which the key can be received.

Step 12	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:**	(Optional) Specifies the time period during which the key can be sent.

	Command or Action	Purpose
	`Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite`	

Step 13	**end**
	Example:
	`Device(config-keychain-key)# end`
		Exits key chain key configuration mode and returns to privileged EXEC mode.

Defining a Named Configuration for EIGRP Route Authentication

Before you begin

Before you configure EIGRP route authentication, you must enable EIGRP. In this task, EIGRP is defined with a virtual instance name.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [*wildcard-mask*]
6. **af-interface** {**default** | *interface-type interface-number*}
7. **authentication key-chain** *name-of-chain*
8. **authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
9. **exit-af-interface**
10. **exit-address-family**
11. **exit**
12. **key chain** *name-of-chain*
13. **key** *key-id*
14. **key-string** *text*
15. **accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
16. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [*wildcard-mask*] **Example:** `Device(config-router-af)# network 172.16.0.0`	Associates networks with an EIGRP routing process.
Step 6	**af-interface** {**default** | *interface-type interface-number*} **Example:**	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 7	**authentication key-chain** *name-of-chain* **Example:** `Device(config-router-af-interface)# authentication key-chain SITE1`	Specifies an authentication key chain for EIGRP.

Step 8	**authentication mode** {**hmac-sha-256** *encryption-type password* | **md5**}
	Example:
	`Device(config-router-af-interface)# authentication mode md5`
		Specifies the type of authentication used in an EIGRP address family for the EIGRP instance.

	Command or Action	Purpose
Step 9	**exit-af-interface** **Example:** `Device(config-router-af-interface)# exit-af-interface`	Exits address family interface configuration mode.
Step 10	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode.
Step 11	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.
Step 12	**key chain** *name-of-chain* **Example:** `Device(config)# key chain keychain1`	Identifies a key chain and enters key chain configuration mode.
Step 13	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Identifies the key number and enters key chain key configuration mode.
Step 14	**key-string** *text* **Example:** `Device(config-keychain-key)# key-string 0987654321`	Identifies the key string.

Step 15	**accept-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
	Example:
	`Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite`
		(Optional) Specifies the time period during which the key can be received.

Step 16	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
	Example:
	`Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite`
		(Optional) Specifies the time period during which the key can be sent.

Step 17	**end** **Example:**	Exits key chain key configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-keychain-key)# end`	

Configuration Examples for IP EIGRP Route Authentication

Example: EIGRP Route Authentication—Autonomous System Definition

The following example shows how to enable MD5 authentication on EIGRP packets in autonomous system 1.

Device 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. Device A will send all EIGRP packets with key 2.

Device B will accept key 1 or key 2 and will use key 1 to send MD5 authentication because key 1 is the first valid key of the key chain. Key 1 is not valid after December 4, 2006. After this date, key 2 is used to send MD5 authentication, and this key is valid until January 4, 2007.

The figure below shows the scenario.

Device A Configuration

```
Device> enable
Device(config)# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Gigabitethernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# ip authentication mode eigrp 1 md5
Device(config-if)# ip authentication key-chain eigrp 1 key1
Device(config-if)# exit
Device(config)# key chain key1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 04:48:00 Dec 4 1996
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Device B Configuration

```
Device> enable
Device(config)# configure terminal
Device(config)# router eigrp 1
Device(config-router)# exit
Device(config)# interface Gigabitethernet 1/0/9
Device(config-if)# no switchport
Device(config-if)# ip authentication mode eigrp 1 md5
Device(config-if)# ip authentication key-chain eigrp 1 key2
Device(config-if)# exit
Device(config)# key chain key2
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Example: EIGRP Route Authentication—Named Configuration

The following example shows how to enable MD5 authentication on EIGRP packets in a named configuration.

Device 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. Device A will send all EIGRP packets with key 2.

Device B will accept key 1 or key 2 and will use key 1 to send MD5 authentication because key 1 is the first valid key of the key chain. Key 1 is not valid after December 4, 2006. After this date, key 2 will be used to send MD5 authentication because it is valid until January 4, 2007.

Device A Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# af-interface Gigabitethernet 1/0/1
Device(config-router-af-interface)# authentication key-chain SITE1
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)# exit-address-family
Device(config-router)# exit
Device(config)# key chain SITE1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string 1234567890
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:45:00 Jan 4 2007 infinite
```

Device B Configuration

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name2
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# af-interface ethernet 0/0
Device(config-router-af-interface)# authentication key-chain SITE2
Device(config-router-af-interface)# authentication mode md5
Device(config-router-af-interface)# exit-af-interface
Device(config-router-af)# exit-address-family
Device(config-router)# exit
Device(config)# key chain SITE2
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string 0987654321
Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite
Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite
```

The following example shows how to configure advanced SHA authentication with password password1 and several key strings that will be rotated as time passes:

```
!
key chain chain1
 key 1
  key-string securetraffic
  accept-lifetime 04:00:00 Dec 4 2006 infinite
  send-lifetime 04:00:00 Dec 4 2010 04:48:00 Dec 4 2008
 !
 key 2
  key-string newertraffic
  accept-lifetime 01:00:00 Dec 4 2010 infinite
  send-lifetime 03:00:00 Dec 4 2010 infinite
 exit
!
router eigrp virtual-name
  address-family ipv6 autonomous-system 4453
    af-interface ethernet 0
       authentication mode hmac-sha-256 0 password1
       authentication key-chain key1
  !
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

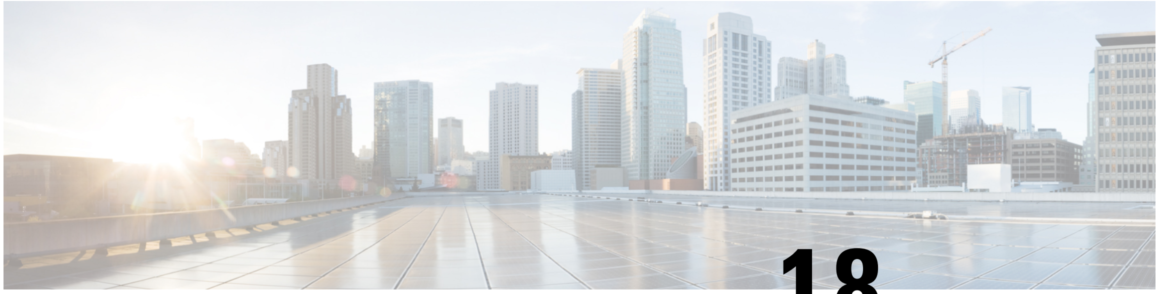
Feature Information for IP EIGRP Route Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 26: Feature Information for IP EIGRP Route Authentication

Feature Name	Releases	Feature Information
IP Enhanced IGRP Route Authentication		EIGRP route authentication provides 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. The following commands were introduced or modified: **ip authentication key-chain eigrp**, **ip authentication mode eigrp**, **show ip eigrp interfaces**.



CHAPTER 18

EIGRP IPv6 VRF-Lite

The EIGRP IPv6 VRF-Lite feature provides EIGRP IPv6 support for multiple VRFs and simplifies the management and troubleshooting of traffic belonging to a specific VRF.

Note The EIGRP IPv6 VRF-Lite feature is available only in EIGRP named configurations.

- Finding Feature Information, on page 229
- Information About EIGRP IPv6 VRF-Lite, on page 229
- How to Configure EIGRP IPv6 VRF-Lite, on page 230
- Configuration Examples for EIGRP IPv6 VRF-Lite, on page 231
- Additional References, on page 232
- Feature Information for EIGRP IPv6 VRF-Lite, on page 232

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP IPv6 VRF-Lite

VRF-Lite for EIGRP IPv6

The EIGRP IPv6 VRF-Lite feature provides separation between routing and forwarding, which supports an additional level of security because communication between devices belonging to different VRFs is not allowed, unless explicitly configured. While the EIGRP IPv6 VRF-Lite feature supports multiple VRFs, the feature also simplifies the management and troubleshooting of traffic belonging to a specific VRF.

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over a service provider backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table. A VPN routing table is called a VPN routing/forwarding (VRF) table.

VRF-lite allows a service provider to support two or more VPNs with an overlapping IP address using one interface. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but a Layer 3 interface cannot belong to more than one VRF at any time.

Note The EIGRP IPv6 VRF-Lite feature is available only in EIGRP named configurations.

EIGRP Named Configuration

Configuring the **router eigrp** command with the *virtual-instance-name* argument creates an EIGRP configuration referred to as the EIGRP named configuration or EIGRP named mode. An EIGRP named configuration does not create an EIGRP routing instance by itself; it is a base configuration that is required to define address-family configurations that are used for routing.

In EIGRP named configurations, EIGRP VPNs can be configured in IPv4 and IPv6 named configurations. A VRF instance and a route distinguisher must be defined before the address family session can be created.

A single EIGRP routing process can support multiple VRFs. The number of VRFs that can be configured is limited only by the available system resources on the device, which is determined by the number running processes and available memory. However, only a single VRF can be supported by each VPN, and redistribution between different VRFs is not supported.

How to Configure EIGRP IPv6 VRF-Lite

Enabling the EIGRP IPv6 VRF-Lite Named Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. **address-family ipv6 vrf** *vrf-name* **autonomous-system** *autonomous-system-number*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Configures the EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv6 vrf** *vrf-name* **autonomous-system** *autonomous-system-number* **Example:** `Device(config-router)# address-family ipv6 vrf vrf1 autonomous-system 45000`	Enables EIGRP IPv6 VRF-Lite and enters address family configuration mode.

Step 5	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Configuration Examples for EIGRP IPv6 VRF-Lite

Example: Enabling EIGRP IPv6 VRF-Lite—Named Configuration

The following example shows how to enable the EIGRP IPv6 VRF-lite feature:

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 100:1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit
Device(config-vrf)# exit
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv6 vrf vrf1 autonomous-system 45000
Device(config-router-af)#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP IPv6 VRF-Lite

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 27: Feature Information for EIGRP IPv6 VRF-Lite

Feature Name	Releases	Feature Information
EIGRP IPv6 VRF-Lite		The EIGRP IPv6 VRF-Lite feature provides EIGRP IPv6 support for multiple VRFs and simplifies the management and troubleshooting of traffic belonging to a specific VRF. **Note** The EIGRP IPv6 VRF-Lite feature is available only in EIGRP named configurations. There are no new or modified commands for this feature.

CHAPTER 19

EIGRP Stub Routing

The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration.

Stub routing is commonly used in hub-and-spoke network topologies. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote device (the spoke) that is connected to one or more distribution devices (the hub). The remote device is adjacent to one or more distribution devices. The only route for IP traffic to reach the remote device is through a distribution device.

- Finding Feature Information, on page 235
- Information About EIGRP Stub Routing, on page 235
- How to Configure EIGRP Stub Routing, on page 239
- Configuration Examples for EIGRP Stub Routing, on page 242
- Additional References, on page 245
- Feature Information for EIGRP Stub Routing, on page 246

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP Stub Routing

EIGRP Stub Routing

The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration.

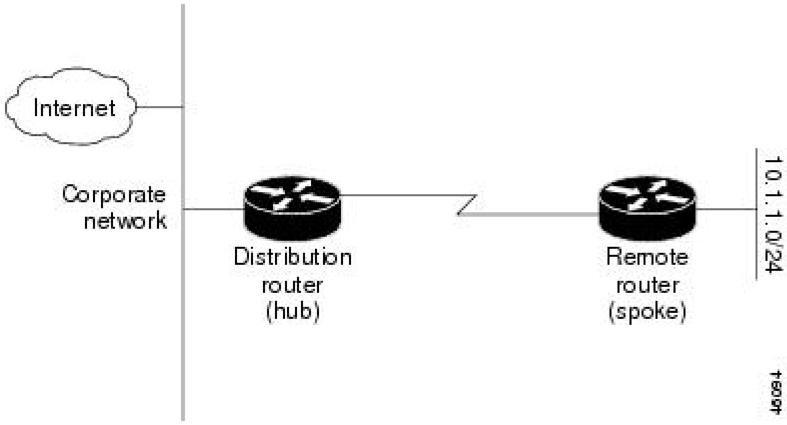
Stub routing is commonly used in hub-and-spoke network topologies. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote device (the spoke) that is connected to one or more distribution devices (the hub). The remote device is adjacent to one or more distribution devices. The only route for IP traffic to reach the remote device is through a distribution device. This type of configuration is commonly used in WAN topologies, where the distribution device is directly connected to a WAN. The distribution device can be connected to many remote devices, which is often the case. In a hub-and-spoke topology, the remote device must forward all nonlocal traffic to a distribution device, so it becomes unnecessary for the remote device to have a complete routing table. Generally, the distribution device need not send anything more than a default route to the remote device.

When using the EIGRP stub routing feature, you need to configure the distribution and remote devices to use EIGRP and configure only the remote device as a stub. Only specified routes are propagated from the remote (stub) device. The stub device responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message "inaccessible." A device that is configured as a stub will send a special peer information packet to all neighboring devices to report its status as a stub device.

Any neighbor that receives a packet informing it of the stub status will not query the stub device for any routes, and a device that has a stub peer will not query that peer. The stub device will depend on the distribution device to send proper updates to all peers.

The figure below shows a simple hub-and-spoke network.

Figure 5: Simple Hub-and-Spoke Network



The stub routing feature by itself does not prevent routes from being advertised to the remote device. In the above example, the remote device can access the corporate network and the Internet only through the distribution device. Having a complete route table on the remote device would serve no functional purpose because the path to the corporate network and the Internet would always be through the distribution device. The large route table would only reduce the amount of memory required by the remote device. Bandwidth and memory can be conserved by summarizing and filtering routes in the distribution device. The remote device need not receive routes that have been learned from other networks because the remote device must send all nonlocal traffic, regardless of the destination, to the distribution device. If a true stub network is desired, the distribution device should be configured to send only a default route to the remote device. The EIGRP stub routing feature does not automatically enable summarization on distribution devices. In most cases, the network administrator will need to configure summarization on distribution devices.

Note When configuring the distribution device to send only a default route to the remote device, you must use the **ip classless** command on the remote device. By default, the **ip classless** command is enabled in all Cisco images that support the EIGRP stub routing feature.

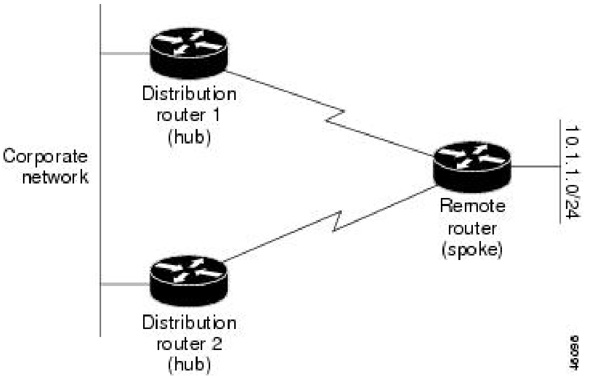
Without the EIGRP stub routing feature, even after routes that are sent from the distribution device to the remote device have been filtered or summarized, a problem might occur. If a route is lost somewhere in the corporate network, EIGRP could send a query to the distribution device, which in turn would send a query to the remote device, even if routes are being summarized. If there is a communication problem (over the WAN link) between the distribution device and the remote device, 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 device.

Dual-Homed Remote Topology

In addition to a simple hub-and-spoke network, where a remote device is connected to a single distribution device, the remote device can be dual-homed to two or more distribution devices. This configuration adds redundancy and introduces unique issues, and the stub feature helps to address some of these issues.

A dual-homed remote device will have two or more distribution (hub) devices. However, the principles of stub routing are the same as they are with a hub-and-spoke topology. The figure below shows a common dual-homed remote topology with one remote device: however, 100 or more devices could be connected on the same interfaces on distribution Device 1 and distribution Device 2. The remote device will use the best route to reach its destination. If distribution Device 1 experiences a failure, the remote device can still use distribution Device 2 to reach the corporate network.

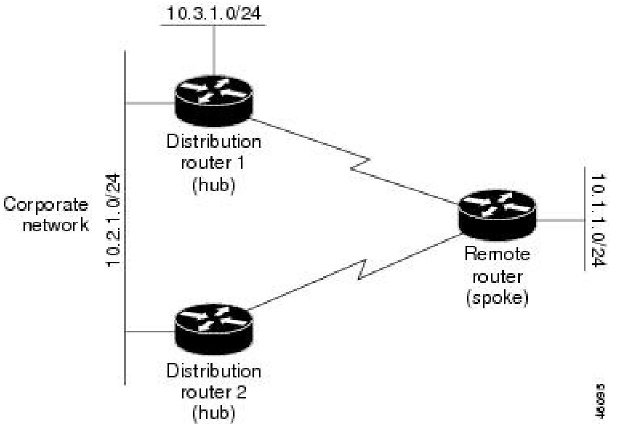
Figure 6: Simple Dual-Homed Remote Topology



The figure above shows a simple dual-homed remote topology with one remote device and two distribution devices. Both distribution devices 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 the figure below, distribution Device 1 is directly connected to network 10.3.1.0/24. If summarization or filtering is applied on distribution Device 1, the device will advertise network 10.3.1.0/24 to all of its directly connected EIGRP neighbors (distribution Device 2 and the remote device).

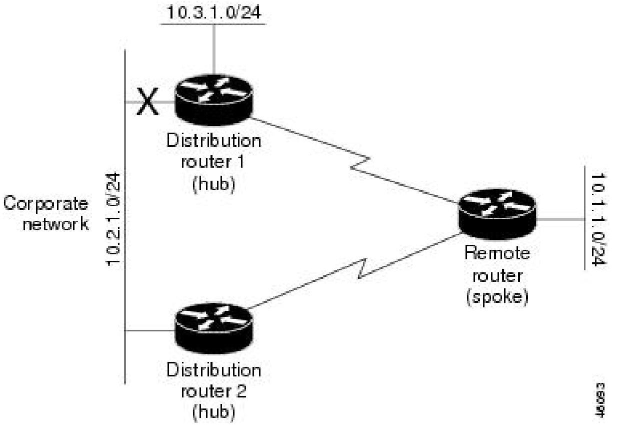
Figure 7: Dual-Homed Remote Topology with Distribution Device 1 Connected to Two Networks



The figure above shows a simple dual-homed remote topology, where distribution Device 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 Device 1 and distribution Device 2 fails, the lowest cost path to network 10.3.1.0/24 from distribution Device 2 will be through the remote device (see the figure below). 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 overutilization of the lower bandwidth WAN connection can cause many problems that might affect the entire corporate network. The use of the lower bandwidth route that passes through the remote device may cause WAN EIGRP distribution devices to be dropped. Serial lines on distribution and remote devices may also be dropped, and EIGRP SIA errors on the distribution and core devices can occur.

Figure 8: Dual-Homed Remote Topology with a Failed Route to a Distribution Device



It is not desirable for traffic from distribution Device 2 to travel through any remote device to reach network 10.3.1.0/24. Backup routes can be used if links are sized to manage the load. However, most networks, of the type shown in the figure above, have remote devices located at remote offices with relatively slow links. To ensure that traffic from distribution devices are not routed through a remote device, you can configure route summarization on the distribution device and the remote device.

It is typically undesirable for traffic from a distribution device to use a remote device as a transit path. A typical connection from a distribution device to a remote device would have much less bandwidth than a connection at the network core. Attempting to use a remote device with a limited bandwidth connection as a transit path would generally produce excessive congestion at the remote device. The EIGRP stub routing feature can prevent this problem by preventing the remote device from advertising core routes back to the distribution devices. In the above example, routes learned by the remote device from distribution Device 1 will not be advertised to distribution Device 2. Therefore, distribution Device 2 will not use the remote device as a transit for traffic destined to the network core.

The EIGRP stub routing feature provides network stability. If the network is not stable, this feature prevents EIGRP queries from being sent over limited bandwidth links to nontransit devices. Instead, distribution devices to which the stub device is connected answer queries on behalf of the stub device. 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 devices to prevent those devices from appearing as transit paths to hub devices.

Caution The EIGRP stub routing feature should be used only on stub devices. A stub device is defined as a device connected to the network core or distribution layer through which core transit traffic should not flow. A stub device should not have any EIGRP neighbors other than distribution devices. Ignoring this restriction will cause undesirable behavior.

Note Multiaccess interfaces such as ATM, Gigabit Ethernet, Frame Relay, ISDN PRI, and X.25 are supported by the EIGRP stub routing feature only when all devices on that interface, except the hub, are configured as stub devices.

How to Configure EIGRP Stub Routing

Configuring the EIGRP Stub Routing Autonomous System Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *autonomous-system-number*
4. **network** *ip-address* [**wildcard-mask**]
5. **eigrp stub** [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**]
6. **end**
7. **show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *autonomous-system-number* **Example:** `Device(config)# router eigrp 1`	Configures a remote or distribution device to run an EIGRP process and enters router configuration mode.
Step 4	**network** *ip-address* [**wildcard-mask**] **Example:** `Device(config-router)# network 172.16.0.0`	Specifies the network address of the EIGRP distribution device.
Step 5	**eigrp stub** [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**] **Example:** `Device(config-router)# eigrp stub connected static`	Configures a remote device as an EIGRP stub device.

Step 6	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Step 7	**show ip eigrp neighbors** [*interface-type* | *as-number* | **static** | **detail**] **Example:** `Device# show ip eigrp neighbors detail`	(Optional) Verifies that a remote device has been configured as a stub device with EIGRP. • Enter this command on the distribution device. The last line of the output displays the stub status of the remote or spoke device.

Configuring the EIGRP Stub Routing Named Configuration

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*

5. **network** *ip-address* [**wildcard-mask**]
6. **eigrp stub** [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**]
7. **exit-address-family**
8. **end**
9. **show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] [**neighbors**] [**static**] [**detail**] [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [**wildcard-mask**] **Example:** `Device(config-router-af)# network 172.16.0.0`	Specifies the network address of the EIGRP distribution device.
Step 6	**eigrp stub** [**receive-only**] [**leak-map** *name*] [**connected**] [**static**] [**summary**] [**redistributed**] **Example:** `Device(config-router-af) eigrp stub leak-map map1`	Configures a device as a stub using EIGRP.
Step 7	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode.

	Command or Action	Purpose

Step 8	**end**
	Example:
	`Device(config-router)# end`
		Exits router configuration mode and returns to privileged EXEC mode.

Step 9	**show eigrp address-family** {**ipv4** | **ipv6**} [**vrf** *vrf-name*] [*autonomous-system-number*] [**multicast**] [**neighbors**] [**static**] [**detail**] [*interface-type interface-number*] **Example:** `Device# show eigrp address-family ipv4 neighbors detail`	(Optional) Displays neighbors discovered by EIGRP.

Configuration Examples for EIGRP Stub Routing

Example: EIGRP Stub Routing—Autonomous System Configuration

A device that is configured as a stub with the **eigrp stub** command shares connected and summary routing information with all neighbor devices by default. The following six keywords can be used with the **eigrp stub** command to modify this behavior:

- **connected**
- **leak-map**
- **receive-only**
- **redistributed**
- **static**
- **summary**

This section provides configuration examples for all forms of the **eigrp stub** command for an EIGRP autonomous system configuration.

Example: eigrp stub Command

In the following example, the **eigrp stub** command is used to configure the device as a stub that advertises connected and summary routes:

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# eigrp stub
```

Example: eigrp stub connected static Command

In the following example, the **eigrp stub** command is used with the **connected** and **static** keywords to configure the device as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# eigrp stub connected static
```

Example: eigrp stub leak-map Command

In the following example, the **eigrp stub** command is issued with the **leak-map** *name* keyword-argument pair to configure the device to reference a leak map that identifies routes that would have been suppressed:

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# eigrp stub leak-map map1
```

Example: eigrp stub receive-only Command

In the following example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the device as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# eigrp stub receive-only
```

Example: eigrp stub redistributed Command

In the following example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the device to advertise other protocols and autonomous systems:

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# eigrp stub redistributed
```

Example: EIGRP Stub Routing—Named Configuration

A device that is configured as a stub with the **eigrp stub** command shares connected and summary routing information with all neighbor devices by default. The following six keywords can be used with the **eigrp stub** command to modify this behavior:

- **connected**
- **leak-map**
- **receive-only**

- **redistributed**
- **static**
- **summary**

This section provides configuration examples for all forms of the **eigrp stub** command for an EIGRP named configuration.

Example: eigrp stub Command

In the following example, the **eigrp stub** command is used to configure the device as a stub that advertises connected and summary routes:

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af) eigrp stub
```

Example: eigrp stub connected static Command

In the following named configuration example, the **eigrp stub** command is issued with the **connected** and **static** keywords to configure the device as a stub that advertises connected and static routes (sending summary routes will not be permitted):

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# eigrp stub connected static
```

Example: eigrp stub leak-map Command

In the following named configuration example, the **eigrp stub** command is issued with the **leak-map** *name* keyword-argument pair to configure the device to reference a leak map that identifies routes that would normally have been suppressed:

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# eigrp stub leak-map map1
```

Example: eigrp stub receive-only Command

In the following named configuration example, the **eigrp stub** command is issued with the **receive-only** keyword to configure the device as a receive-only neighbor (connected, summary, and static routes will not be sent):

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af)# eigrp stub receive-only
```

Example: eigrp stub redistributed Command

In the following named configuration example, the **eigrp stub** command is issued with the **redistributed** keyword to configure the device to advertise other protocols and autonomous systems:

```
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# network 10.0.0.0
Device(config-router-af) eigrp stub redistributed
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP Technology White Papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Stub Routing

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 28: Feature Information for EIGRP Stub Routing

Feature Name	Releases	Feature Information
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 following command was introduced or modified: **eigrp stub**.

CHAPTER 20

EIGRP Support for 6PE/6VPE

The EIGRP Support for 6PE/6VPE feature enables native IPv6 Enhanced Interior Gateway Routing Protocol (EIGRP) routes to preserve their original characteristics (metric and other attributes like type, delay, bandwidth, and maximum transmission unit [MTU]) while being redistributed from one IPv6 EIGRP site to another over a service-provider VPN cloud or an IPv6 provider edge (6PE) Multiprotocol Label Switching-VPN (MPLS-VPN) network. The Border Gateway Protocol (BGP) is used as the external routing protocol to transfer IPv6 EIGRP routes across the VPN cloud or the 6PE MPLS-VPN network. This module explains the EIGRP 6PE/6VPE feature.

- Finding Feature Information, on page 247
- Information About EIGRP Support for 6PE/6VPE, on page 247
- Additional References for EIGRP Support for 6PE/6VPE, on page 250
- Feature Information For EIGRP Support for 6PE/6VPE, on page 250

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP Support for 6PE/6VPE

BGP Extended Communities

For the Enhanced Interior Gateway Routing Protocol (EIGRP) to recreate route metrics derived from the originating customer site, the original metrics are encoded into Border Gateway Protocol (BGP) Extended Communities by the provider-edge (PE) device that receives the routes from the transmitting customer-edge (CE) device. These extended communities are then transported across the Multiprotocol Label Switching-VPN (MPLS-VPN) backbone by BGP from one customer site to the other (peering customer site). After the peering customer site receives the routes, BGP redistributes the routes into EIGRP. EIGRP, then, extracts the BGP Extended Community information and reconstructs the routes as they appeared in the original customer site.

The following rules govern BGP Extended Communities:

Non-EIGRP-Originated Routes: If a non-EIGRP-originated route is received through BGP and the route has no extended community information for EIGRP, BGP advertises the route to the receiving CE as an external EIGRP route by using the route's default metric. If no default metric is configured, BGP does not advertise the route to the CE.

EIGRP-Originated Internal Routes: If an EIGRP-originated internal route is received through BGP and the route has extended community information for EIGRP, the PE sets the route type to "internal" if the source autonomous system number matches the autonomous system number configured for this VPN routing and forwarding (VRF) instance. BGP, then, reconstructs and advertises the route to the receiving CE as an internal EIGRP route by using the extended community information. If there is no autonomous system match, these routes are treated as non-EIGRP-originated routes.

EIGRP-Originated External Routes: If an EIGRP-originated external route is received through BGP and the route has extended community information for EIGRP, the PE sets the route type to "external" if the source autonomous system number matches the autonomous system number configured for this VRF instance. BGP, then, reconstructs and advertises this external route to the receiving CE as an external EIGRP route by using the extended community information. If there is no autonomous system match, these routes are treated as non-EIGRP-originated routes.

Preserving Route Metrics

The EIGRP 6PE/6VPE feature manages native and non-native Enhanced Interior Gateway Routing Protocol (EIGRP) routes by using the **redistribute** and the **default metric** commands, respectively. By using the **redistribute bgp** *as-number* command, you can ensure that only Border Gateway Protocol (BGP) routes with BGP Extended Community information are distributed into EIGRP. EIGRP uses this information to recreate the original EIGRP route. If the BGP Extended Community information is missing and the default metric is not specified, EIGRP will not learn the route from BGP.

By using the **redistribute bgp** *as-number* **metric-type** *type-value* command, you can ensure that the metric values configured using this command are used only for BGP routes redistributed into EIGRP. EIGRP looks for BGP Extended Community information, and if this information is found, EIGRP uses this information to recreate the original EIGRP route. If the Extended Community information is missing, EIGRP uses the metric values configured using this command to determine whether the route is the preferred route.

By using the **default-metric** *bandwidth delay reliability loading mtu* command, you can ensure that the metric values configured using this command are used for any non-EIGRP routes being redistributed into EIGRP. If the received route is a BGP route, EIGRP looks for BGP Extended Community information, and if this information is found, EIGRP uses this information to recreate the original EIGRP route. If the extended community information is missing, EIGRP uses the metric values configured to determine whether the route is the preferred route.

EIGRP 6PE/6VPE SoO

The EIGRP 6PE/6VPE Site of Origin (SoO) functionality allows an Enhanced Interior Gateway Routing Protocol (EIGRP) network to support complex topologies, such as Multiprotocol Label Switching-VPN (MPLS-VPN) links between sites with backdoor links, customer-edge (CE) devices that are dual-homed to different provider-edge (PE) devices, and PEs supporting CEs from different sites within the same VPN routing and forwarding (VRF) instance. Path selection within the EIGRP network containing PE-CE links is based on route metrics that allow either the link through the VPN or the EIGRP backdoor to act as the primary (best) link or the backup link, if the primary link fails. EIGRP accomplishes this path selection by retrieving the Site of Origin (SoO) attribute from routes redistributed from the Border Gateway Protocol (BGP) network.

This BGP/EIGRP interaction takes place through the use of the BGP Cost Community Extended Community attribute.

When routes are redistribued into EIGRP from a BGP network, BGP Cost Community Extended Community attributes are added to the routes. These attributes include the SoO attribute. The SoO attribute is used to identify the site of origin of a route and prevent advertisement of the route back to the source site. To enable the EIGRP SoO functionality, you must configure the **ip vrf sitemap** command on the PE interface that is connected to the CE device. This command enables SoO filtering on the interface. When EIGRP on the PE device receives CE routes on the interface that has a SoO value defined, EIGRP checks each route to determine whether there is an SoO value associated with the route that matches the interface SoO value. If the SoO values match, the route will be filtered. This filtering is done to stop routing loops.

When EIGRP on the PE receives a route that does not contain an SoO value or contains an SoO value that does not match the interface SoO value, the route will be accepted into the topology table so that it can be redistributed into BGP. When the PE redistributes an EIGRP route that does not contain an SoO value into BGP, the SoO value that is defined on the interface used to reach the next hop (CE) is included in the Extended Communities attribute associated with the route. If the EIGRP topology table entry already has an SoO value associated with the route, this SoO value, instead of the interface SoO value, will be included with the route when it is redistributed into the BGP table. Any BGP peer that receives these prefixes will also receive the SoO value associated with each prefix, identifying the site, where each prefix originated.

The EIGRP SoO functionality ensures that BGP does not follow its normal path-selection behavior, where locally derived routes (such as native EIGRP routes redistributed into BGP) are preferred over BGP-derived routes.

For more information on the Site of Origin functionality, see the “EIGRP MPLS VPN PE-CE Site of Origin” chapter in the *IP Routing: EIGRP Configuration Guide*.

Backdoor Devices

Backdoor devices are EIGRP devices that connect one EIGRP site to another, but not through the Multiprotocol Label Switching-VPN (MPLS-VPN) network. Typically, a backdoor link is used as a backup path between peering EIGRP sites if the MPLS-VPN link is down or unavailable. The metric on the backdoor link is set high enough so that the path through the backdoor will not be selected unless there is a VPN link failure. You can define Site of Origin (SoO) values on the backdoor device on interfaces connecting the device to the peering sites, thus identifying the local-site identity of the link.

When a backdoor device receives EIGRP updates or replies from a neighbor, the device checks each received route to verify that the route does not contain an SoO value that matches the ones defined on its interfaces. If the device finds a route with a SoO value that matches the value defined on any of its interfaces, the route is rejected and not included in the topology table. Typically, the reason that a route is received with a matching SoO value is that the route is learned by the other peering site through the MPLS-VPN connection and is being advertised back to the original site over the backdoor link. By filtering such routes based on the SoO value defined on the backdoor link, you can avoid short-term, invalid routing.

Additional References for EIGRP Support for 6PE/6VPE

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQs	EIGRP Frequently Asked Questions
EIGRP technology white papers	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information For EIGRP Support for 6PE/6VPE

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 29: Feature Information for EIGRP Support for 6PE/6VPE

Feature Name	Releases	Feature Information
EIGRP Support for 6PE/6VPE		The EIGRP Support for 6PE/6VPE feature enables native IPv6 Enhanced Interior Routing Protocol (EIGRP) routes to preserve their original characteristics while being redistributed from one IPv6 EIGRP site to another over a service-provider VPN cloud or an IPv6 Provider Edge (6PE) Multiprotocol Label Switching-VPN (MPLS-VPN) network. No commands were introduced or modified by this feature.

CHAPTER 21

EIGRP Over the Top

The EIGRP Over the Top feature enables a single end-to-end routing domain between two or more Enhanced Interior Gateway Routing Protocol (EIGRP) sites that are connected using a private or a public WAN connection. This module provides information about the EIGRP Over the Top feature and how to configure it.

- Finding Feature Information, on page 253
- Information About EIGRP Over the Top, on page 253
- How to Configure EIGRP Over the Top, on page 255
- Configuration Examples for EIGRP Over the Top, on page 259
- Feature Information for EIGRP Over the Top, on page 260

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP Over the Top

EIGRP Over the Top Overview

The EIGRP Over the Top feature enables a single end-to-end Enhanced Interior Gateway Routing Protocol (EIGRP) routing domain that is transparent to the underlying public or private WAN transport that is used for connecting disparate EIGRP customer sites. When an enterprise extends its connectivity across multiple sites through a private or a public WAN connection, the service provider mandates that the enterprise use an additional routing protocol, typically the Border Gateway Protocol (BGP), over the WAN links to ensure end-to-end routing. The use of an additional protocol causes additional complexities for the enterprise, such as additional routing processes and sustained interaction between EIGRP and the routing protocol to ensure connectivity, for the enterprise. With the EIGRP Over the Top feature, routing is consolidated into a single protocol (EIGRP) across the WAN, which provides the following benefits:

- There is no dependency on the type of WAN connection used.
- There is no dependency on the service provider to transfer routes.
- There is no security threat because the underlying WAN has no knowledge of enterprise routes.
- This feature simplifies dual carrier deployments and designs by eliminating the need to configure and manage EIGRP-BGP route distribution and route filtering between customer sites.
- This feature allows easy transition between different service providers.
- This feature supports both IPv4 and IPv6 environments.

How EIGRP Over the Top Works

The EIGRP Over the Top solution can be used to ensure connectivity between disparate Enhanced Interior Gateway Routing Protocol (EIGRP) sites. This feature uses EIGRP on the control plane and Locator ID Separation Protocol (LISP) encapsulation on the data plane to route traffic across the underlying WAN architecture. EIGRP is used to distribute routes between customer edge (CE) devices within the network, and the traffic forwarded across the WAN architecture is LISP encapsulated. Therefore, to connect disparate EIGRP sites, you must configure the **neighbor** command with LISP encapsulation on every CE in the network.

If your network has many CEs, then you can use EIGRP Route Reflectors (E-RRs) to form a half-mesh topology and ensure connectivity among all CEs in the network. An E-RR is an EIGRP peer that receives EIGRP route updates from CEs in the network and reflects these updates to other EIGRP CE neighbors without changing the next hop or metrics for the routes. An E-RR can also function as a CE in the network. You must configure E-RRs with the **remote-neighbors source** command to enable E-RRs to listen to unicast messages from peer CE devices and reflect the messages to other EIGRP CE neighbors. You must configure the CEs with the **neighbor** command to allow them to identify the E-RRs in their network and exchange routes with the E-RRs. Upon learning routes from E-RRs, the CEs install these routes into their routing information base (RIB). You can use dual or multiple E-RRs for redundancy. The CEs form adjacencies with all E-RRs configured in the network, thus enabling multihop remote neighborship amongst themselves.

Security Groups and SGTs

A security group is a grouping of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the ACS. As new users and devices are added to the Cisco TrustSec (CTS) domain, the authentication server assigns these new entities to appropriate security groups. CTS assigns to each security group a unique 16-bit security group number whose scope is global within a CTS domain. The number of security groups in the router is limited to the number of authenticated network entities. Security group numbers do not need to be manually configured.

Once a device is authenticated, CTS tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT throughout the network within the CTS header. The SGT is a single label that determines the privileges of the source within the entire CTS domain. The SGT is identified as the source because it contains the security group of the source. The destination device is assigned a destination group tag (DGT).

Note The CTS packet tag does not contain the security group number of the destination device.

EIGRP OTP Support to Propagate SGT

The EIGRP OTP Support enables to propagate SGT from site-to-site across WAN using OTP transport. OTP uses LISP to send the data traffic. OTP carries the SGT over the Layer 3 (L3) clouds across multiple connections/network and also provides access control at a remote site.

How to Configure EIGRP Over the Top

Configuring EIGRP Over the Top on a CE Device

You must enable the EIGRP Over the Top feature on all customer edge (CE) devices in the network so that the CEs know how to reach the Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector configured in the network. Perform the following task to configure the EIGRP Over the Top feature on a CE device and enable Locator ID Separation Protocol (LISP) encapsulation for traffic across the underlying WAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops* [**lisp-encap** [*lisp-id*]]]
6. **network** *ip-address*[*wildcard-mask*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp test`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:**	Enters address family configuration mode and configures an EIGRP routing instance.

	Command or Action	Purpose
	`Device(config-router)# address-family ipv4 autonomous-system 100`	
Step 5	**neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** *maximum-hops* [**lisp-encap** [*lisp-id*]]] **Example:** `Device(config-router-af)# neighbor 10.0.0.1 gigabitethernet 0/0/1 remote 2 lisp-encap 1`	Defines a neighboring device with which an EIGRP device can exchange routing information.
Step 6	**network** *ip-address*[*wildcard-mask*] **Example:** `Device(config-router-af)# network 192.168.0.0 255.255.0.0`	Specifies the network for the EIGRP routing process. In this case, configure all routes that the CE needs to be aware of.

Step 7	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Configuring EIGRP Route Reflectors

Perform this task to configure a customer edge (CE) device in a network to function as an Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 unicast autonomous-system** *as-number*
5. **af-interface** *interface-type interface-number*
6. **no next-hop-self**
7. **no split-horizon**
8. **exit**
9. **remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap**
10. **network** *ip-address*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp test`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 unicast autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 unicast autonomous-system 100`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**af-interface** *interface-type interface-number* **Example:** `Device(config-router-af)# af-interface gigabitethernet 0/0/1`	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 6	**no next-hop-self** **Example:** `Device(config-router-af-interface)# no next-hop-self`	Instructs EIGRP to use the received next hop and not the local outbound interface address as the next hop to be advertised to neighboring devices. **Note** If **no next-hop-self** is not configured, the data traffic will flow through the EIGRP Route Reflector.
Step 7	**no split-horizon** **Example:** `Device(config-router-af-interface)# no split-horizon`	Disables EIGRP split horizon.
Step 8	**exit** **Example:** `Device(config-router-af-interface)# exit`	Exits address family interface configuration mode and returns to address family configuration mode.
Step 9	**remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap** **Example:**	Enables remote neighbors to accept inbound connections from any remote IP address.

	Command or Action	Purpose
	`Device(config-router-af)# remote-neighbors source gigabitethernet 0/0/1 unicast-listen lisp-encap`	
Step 10	**network** *ip-address* **Example:** `Device(config-router-af)# network 192.168.0.0`	Specifies a network for the EIGRP routing process. • Enter all network routes that the EIGRP Route Reflector needs to be aware of.

Step 11	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode

Configuring EIGRP OTP Support to Propagate SGT

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual instance name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **topology base**
6. **cts propagate sgt**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual instance name* **Example:** `Device (config)# router eigrp kmd`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:** `Device (config-router)# address-family ipv4 autonomous-system 100`	Enters address family configuration mode and configures an EIGRP routing instance.

	Command or Action	Purpose
Step 5	**topology base** **Example:** `Device (config-router-af)# topology base`	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.
Step 6	**cts propagate sgt** **Example:** `Device (config-router-af)# cts propagate sgt`	Enables Security Group Tag (SGT) propagation over L3 network.

Step 7	**end**
	Example:
	`Device (config-router-af)# end`
		Exits address family topology configuration mode and returns to privileged EXEC mode.

Configuration Examples for EIGRP Over the Top

Example: Configuring EIGRP Over the Top on a CE Device

The following example shows you how to configure the customer edge (CE) device in the network to advertise local routes to the Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflectors.

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast autonomous-system 100
Device(config-router-af)# neighbor 10.0.0.2 gigabitethernet 0/0/1 remote 3 lisp-encap 1
Device(config-router-af)# network 192.168.0.0
Device(config-router-af)# network 192.168.1.0
Device(config-router-af)# network 192.168.2.0
Device(config-router-af)# end
```

Example: Configuring EIGRP Route Reflectors

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 unicast autonomous-system 100
Device(config-router-af)# af-interface gigabitethernet 0/0/1
Device(config-router-af-interface)# no next-hop-self
Device(config-router-af-interface)# no split-horizon
Device(config-router-af-interface)# exit
Device(config-router-af)# remote-neighbors source gigabitethernet 0/0/1 unicast-listen
lisp-encap 1
Device(config-router-af)# network 192.168.0.0
Device(config-router-af)# end
```

Example: Configuring EIGRP OTP Support to Propagate SGT

The following example shows how to configure EIGRP OTP to propagate SGT.

```
router eigrp kmd
!
address-family ipv4 unicast autonomous-system 100
  !
  topology base
   cts propagate sgt
  exit-af-topology
exit-address-family
```

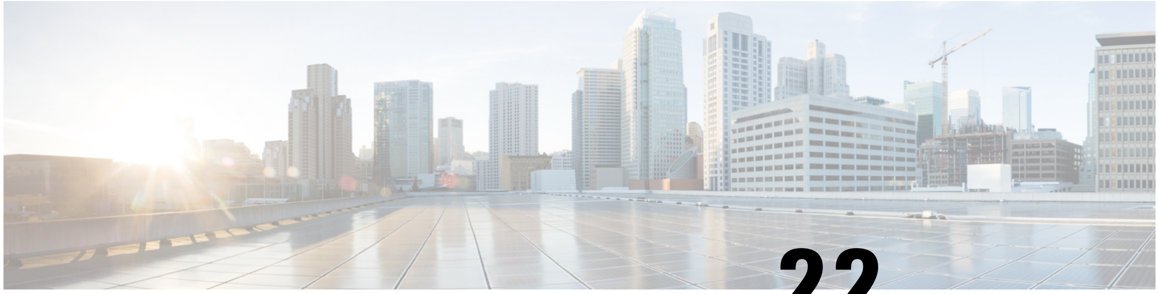
Feature Information for EIGRP Over the Top

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 30: Feature Information for EIGRP Over the Top

Feature Name	Releases	Feature Information
EIGRP Over the Top		The EIGRP Over the Top feature enables a single end-to-end routing domain between two or (EIGRP) more Enhanced Interior Gateway Routing Protocol sites that are connected using a private or public WAN connection. EIGRP OTP also supports the propagation of SGT over L3 network. The following commands were introduced or modified: **remote-neighbor** (EIGRP), **neighbor** (EIGRP), **cts propagate sgt** ,and **show ip eigrp neighbors**.



CHAPTER 22

EIGRP OTP VRF Support

The EIGRP OTP VRF support feature extends VPN routing and forwarding (VRF) support to the EIGRP OTP feature thereby retaining and carrying VRF information over WAN.

- Prerequisites for EIGRP OTP VRF Support, on page 261
- Restrictions for EIGRP OTP VRF Support, on page 261
- Information About EIGRP OTP VRF Support, on page 261
- How to Configure EIGRP OTP VRF Support, on page 263
- Configuration Examples for EIGRP OTP VRF Support, on page 267
- Additional References for EIGRP OTP VRF Support, on page 268
- Feature Information for Configuring EIGRP OTP VRF Support, on page 268

Prerequisites for EIGRP OTP VRF Support

The EIGRP Over the Top feature must be configured.

Restrictions for EIGRP OTP VRF Support

- The WAN facing interface should not be in VRF.

Information About EIGRP OTP VRF Support

Overview of EIGRP OTP VRF Support

The EIGRP Over the Top is a WAN solution with EIGRP in control plane and LISP in data plane, in which route distribution between two EIGRP customer-edge devices is performed using EIGRP protocol. LISP encapsulates the data that is sent over WAN. To support VRF functionality, the routes from each VRF must be carried over the control plane and installed in the correct VRF tables in the CE devices and EIGRP Route Reflector (E-RR).

How EIGRP OTP VRF Support Works

A CE device supports multiple VRFs on a LAN. On a WAN, the WAN interface in the default VRF and the CE device forms a remote EIGRP neighborship with another CE or E-RR device. The neighbors are formed in a single EIGRP process. One EIGRP process handles multiple, distinct neighbor formations in various VRFs on the LAN side and at the same time, also forms a neighbor on the WAN side with an OTP peer. The receiving peer picks routes that are applicable for the topologies that are present on the receiving peer. Routes from any other topologies are dropped.

Various routes learnt from peers in different VRFs are updated in the respective topologies on the CE and are transported to the OTP peer with the topology information for each route. Each topology represents a configured VRF on the device.

Each topology is associated with a unique ID, called the TID (Topology ID). The TID identifies the topology across various remote customer sites as the VRF name could be different on each CE device. For the CE devices to exchange the right information, the TID must be the same on all CEs.

The LISP Id (LISP Instance ID) also is mapped to a VRF and TID. As LISP carries different VRF packets using different virtual LISP interfaces, the LISP ID per VRF must be unique and must be same across the CE devices for packet delivery.

Use the **topology** command to configure a unique topology ID on customer site.

Data Encapsulation

Data encapsulation is achieved using LISP and is configured using the same **topology** command. Each VRF is associated with a LISP virtual interface. Data packets from one VRF will be encapsulated between the CE devices per VRF.

Each CE device is the edge device for a customer site, having various VRFs in a network. When customer sites connect via EIGRP OTP, each CE device is a neighbor to another CE device. In case of E-RR deployment, the CE s neighbors with the E-RR. The routes in a VRF in one customer site are carried to its peer and updated in the appropriate peer VRF table. If routes are received from a particular topology is absent in a peer, the peer drops the routes.

The E-RR reflects all topologies that are configured on the E-RR. Routes from topologies that are absent on the E-RR are not reflected. This is the reason that the E-RR is expected to have a super set of all VRFs present in the network.

Interfaces and Topology Command

When the **topology** command is used, all the interfaces under that VRF are enabled with EIGRP, thereby forming neighbors on all interfaces under a VRF. However, there may be interfaces on which EIGRP should not be enabled. To disable the formation of peers on such interfaces, use the **topo-interface** command and disable the interface on which EIGRP must not be enabled via **passive-interface** command.

Differences between EIGRP OTP Feature and EIGRP OTP VRF Support Feature

Table 31: EIGRP OTP Feature and EIGRP VRF Support Feature Differences

EIGRP OTP Feature	EIGRP OTP VRF Support Feature
Supports the default VRF only.	Multiple VRFs can be configured. Each VRF is considered as a topology and the topology related information is carried across associated with a TID (topology ID).
Neighbors are formed on only those interfaces that are configured with the **network** command.	Neighbors are formed across all interfaces in a particular VRF configured with the **topology** command.
The **network** command is required on the WAN interface to form an OTP neighbor.	The **network** command is not required.

How to Configure EIGRP OTP VRF Support

Configuring EIGRP OTP VRF Support on a CE Device

You must enable the EIGRP OTP VRF Support feature on all customer edge (CE) devices in the network so that the CEs know how to reach the Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector configured in the network. Perform the following task to configure the EIGRP OTP VRF Support feature on a CE device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **topology vrf** *vrf-name* **tid** *number* **lisp-instance-id** *number*
6. **topo-interface** *interface-name interface-number*
7. **passive-interface**
8. **exit**
9. **exit**
10. **neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** [**lisp-encap** [*lisp-id*]]]
11. **end**
12. **show ip eigrp topology**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp test`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 10`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology vrf** *vrf-name* **tid** *number* **lisp-instance-id** *number* **Example:** `Device(config-router-af)# topology vrf vrf1 tid 10 lisp-instance-id 122`	Enters address-family topology configuration mode and assigns a topology to a VRF.
Step 6	**topo-interface** *interface-name interface-number* **Example:** `Device(config-router-af-topology)# #topo-interface GigabitEthernet0/0/0`	(Optional) Enters address family interface configuration mode and the interface on which EIGRP must not be enabled.
Step 7	**passive-interface** **Example:** `Device(config-router-af-topology-interface)# passive-interface`	Makes the interface passive.
Step 8	**exit** **Example:** `Device(config-router-af-topology-interface)# exit`	Exits address family interface configuration mode and returns to address-family topology configuration mode.
Step 9	**exit** **Example:** `Device(config-router-af-topology)# exit`	Exits address-family topology configuration mode and returns to address family configuration mode.
Step 10	**neighbor**{*ip-address* | *ipv6-address*} *interface-type interface-number* [**remote** [**lisp-encap** [*lisp-id*]]] **Example:** `Device(config-router-af)# neighbor 10.0.0.1 ATM0/3/0 remote lisp-encap 122`	Defines a neighboring device with which an EIGRP device can exchange routing information.

Step 11	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 12	**show ip eigrp topology** **Example:** `Router# show ip eigrp topology`	Displays EIGRP topology table entries.

Example

The following is a sample output from the show ip eigrp topology command.

```
Device# show ip eigrp topology

EIGRP-IPv4 VR(otp) Topology Table for AS(1)/ID(10.0.0.11)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 10.0.0.0/24, 1 successors, FD is 131072000
        via Connected, Ethernet0/1
EIGRP-IPv4 VR(otp) Topology Table for AS(1)/ID(10.0.0.11)
           Topology(red) TID(20) VRF(red)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 21.0.0.0/24, 1 successors, FD is 12161609142
        via 20.0.0.11 (12161609142/12096073142), Ethernet0/1
P 1.11.11.11/32, 1 successors, FD is 12161691062
        via 20.0.0.11 (12161691062/12096155062), Ethernet0/1
P 11.0.0.0/24, 1 successors, FD is 131072000
        via Connected, Ethernet0/0
P 1.1.1.1/32, 1 successors, FD is 131153920
        via 11.0.0.10 (131153920/163840), Ethernet0/0
EIGRP-IPv4 VR(otp) Topology Table for AS(1)/ID(10.0.0.11)
           Topology(green) TID(30) VRF(green)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2.222.222.222/32, 1 successors, FD is 12161691062
        via 30.0.0.11 (12161691062/12096155062), Ethernet0/1
P 12.0.0.0/24, 1 successors, FD is 131072000
        via Connected, Ethernet0/2
P 31.0.0.0/24, 1 successors, FD is 12161609142
        via 30.0.0.11 (12161609142/12096073142), Ethernet0/1
P 11.22.11.22/32, 1 successors, FD is 12161691062
        via 30.0.0.11 (12161691062/12096155062), Ethernet0/1
P 2.2.2.2/32, 1 successors, FD is 131153920
        via 12.0.0.10 (131153920/163840), Ethernet0/2
P 22.0.0.0/24, 1 successors, FD is 12161609142
        via 20.0.0.11 (12161609142/12096073142), Ethernet0/1
P 2.22.22.22/32, 1 successors, FD is 12161691062
        via 20.0.0.11 (12161691062/12096155062), Ethernet0/1
EIGRP-IPv4 VR(otp) Topology Table for AS(1)/ID(10.0.0.11)
           Topology(blue) TID(40) VRF(blue)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 13.0.0.0/24, 1 successors, FD is 131072000
        via Connected, Ethernet0/3
P 32.0.0.0/24, 1 successors, FD is 12161609142
        via 30.0.0.11 (12161609142/12096073142), Ethernet0/1
P 3.33.33.33/32, 1 successors, FD is 12161691062
        via 30.0.0.11 (12161691062/12096155062), Ethernet0/1
P 3.3.3.3/32, 1 successors, FD is 131153920
        via 13.0.0.10 (131153920/163840), Ethernet0/3
```

Configuring EIGRP OTP VRF Support on EIGRP Route Reflectors

Perform this task to configure a customer edge (CE) device in a network to function as an Enhanced Interior Gateway Routing Protocol (EIGRP) Route Reflector.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-name*
4. **address-family ipv4 autonomous-system** *as-number*
5. **topology vrf** *vrf-name* **tid** *number* **lisp-instance-id** *number*
6. **exit**
7. **remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap** *LISP-instance-ID*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router eigrp** *virtual-name* **Example:** `Device(config)# router eigrp test`	Configures an EIGRP routing process and enters router configuration mode.
Step 4	**address-family ipv4 autonomous-system** *as-number* **Example:** `Device(config-router)# address-family ipv4 autonomous-system 10`	Enters address family configuration mode and configures an EIGRP routing instance.
Step 5	**topology vrf** *vrf-name* **tid** *number* **lisp-instance-id** *number* **Example:** `Device((config-router-af)# topology vrf vrf1 tid 10 lisp-instance-id 122`	Assigns a topology to a VRF and enters address-family topology configuration mode.
Step 6	**exit** **Example:**	Exits address-family topology configuration mode and returns to address family configuration mode.

	Command or Action	Purpose
	`Device((config-router-af-topology)# exit`	
Step 7	**remote-neighbors source** *interface-type interface-number* **unicast-listen lisp-encap** *LISP-instance-ID* **Example:** `Device(config-router-af)# remote-neighbors source ATM0/3/0 unicast-listen lisp-encap 122`	Enables remote neighbors to accept inbound connections from any remote IP address.

Step 8	**end**
	Example:
	`Device(config-router-af)# end`
		Exits address family configuration mode and returns to privileged EXEC mode.

Configuration Examples for EIGRP OTP VRF Support

Example: Configuring EIGRP OTP VRF Support on a CE Device

```
Router> enable
Router# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 autonomous-system 10
Device((config-router-af)# topology vrf vrf1 tid 10 lisp-instance-id 122
Device(config-router-af-topology)# topo-interface GigabitEthernet0/0/0
Device(config-router-af-topology-interface)# passive-interface
Device(config-router-af-topology-interface)# exit
Device((config-router-af-topology)# exit
Device(config-router-af)# neighbor 10.0.0.1 ATM0/3/0 remote lisp-encap 122
Device(config-router-af)# end
```

Example: Configuring EIGRP OTP VRF Support on EIGRP Route Reflectors

```
Device> enable
Device# configure terminal
Device(config)# router eigrp test
Device(config-router)# address-family ipv4 autonomous-system 10
Device(config-router-af)# topology vrf vrf1 tid 10 lisp-instance-id 122
Device(config-router-af-topology)# exit
Device(config-router-af)# remote-neighbors source ATM0/3/0 unicast-listen lisp-encap 122
Device(config-router-af)# end
```

Additional References for EIGRP OTP VRF Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Routing: EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring EIGRP OTP VRF Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 32: Feature Information for Configuring EIGRP OTP VRF Support

Feature Name	Releases	Feature Information
EIGRP OTP VRF Support	Cisco IOS XE Release 3.15S	The EIGRP OTP VRF support feature extends VPN routing and forwarding (VRF) support to the EIGRP OTP feature thereby retaining and carrying VRF information over WAN. The following commands were introduced or modified: **neighbors**, **remote-neighbors**, **show ip eigrp topology**, **show ip route vrf**, **topology**.

CHAPTER 23

EIGRP Classic to Named Mode Conversion

The EIGRP Classic to Named Mode Conversion feature allows you to upgrade Enhanced Interior Gateway Routing Protocol (EIGRP) classic mode configurations to named mode configurations without causing network flaps or requiring the EIGRP process to restart. This feature supports both IPv4 and IPv6.

- Finding Feature Information, on page 269
- Restrictions for EIGRP Classic to Named Mode Conversions, on page 269
- Information About EIGRP Classic to Named Mode Conversion, on page 270
- Additional References for EIGRP Classic to Named Mode, on page 271
- Feature Information for EIGRP Classic to Named Mode Conversion, on page 271

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for EIGRP Classic to Named Mode Conversions

- You must use the **eigrp upgrade-cli** command to convert Enhanced Interior Gateway Routing Protocol (EIGRP) configurations from classic mode to named mode. If multiple classic mode configurations exist, you must use this command per EIGRP autonomous system number in classic mode.
- The **eigrp upgrade-cli** command blocks the router from accepting any other command until the conversion is complete (the console is locked). The time taken to complete the conversion depends on the size of the configuration. However, the conversion is a one-time activity.
- The **eigrp upgrade-cli** command is available only under EIGRP classic router configuration mode. Therefore, you can convert configurations from classic mode to named mode but not vice-versa.
- After conversion, the running configuration on the device will show only named mode configurations; you will be unable to see any classic mode configurations. To revert to classic mode configurations, you can reload the router without saving the running configuration to the startup configuration.

- The new configurations are available only in the running configuration; they will not be saved to the startup configuration. If you want to add them to the startup configuration, you must explicitly save them using the **write memory** or the **copy running-config startup-config** command.
- After conversion, the **copy startup-config running-config** command will fail because you cannot have both the classic and named mode for the same autonomous system.
- After conversion, all neighbors (under the converted router EIGRP) will undergo graceful restart and sync all routes.

Information About EIGRP Classic to Named Mode Conversion

-

EIGRP Classic to Named Mode Conversion - Overview

The Enhanced Interior Gateway Routing Protocol (EIGRP) can be configured using either the classic mode or the named mode. The classic mode is the old way of configuring EIGRP. In classic mode, EIGRP configurations are scattered across the router mode and the interface mode. The named mode is the new way of configuring EIGRP; this mode allows EIGRP configurations to be entered in a hierarchical manner under the router mode.

Each named mode configuration can have multiple address families and autonomous system number combinations. In the named mode, you can have similar configurations across IPv4 and IPv6. We recommend that you upgrade to EIGRP named mode because all new features, such as Wide Metrics, IPv6 VRF Lite, and EIGRP Route Tag Enhancements, are available only in EIGRP named mode.

Use the **eigrp upgrade-cli** command to upgrade from classic mode to named mode. You must use the **eigrp upgrade-cli** command for all classic router configurations to ensure that these configurations are upgraded to the named mode. Therefore, if multiple classic configurations exist, you must use this command per autonomous system number. You must use this command separately for IPv4 and IPv6 configurations.

Prior to the EIGRP Classic to Named Mode Conversion feature, upgrading to EIGRP named mode required that the user manually unconfigure the classic mode using the **no router eigrp** *autonomous-system-number* command and then reconfigure EIGRP configurations under named mode using the **router eigrp** *virtual name* command. This method may lead to network churn and neighborship or network flaps.

The EIGRP Classic to Named Mode Conversion feature allows you to convert from classic mode to named mode without causing network flaps or the EIGRP process to restart. With this feature, you can move an entire classic mode configuration to a router named mode configuration, and consequently, all configurations under interfaces will be moved to the address-family interface under the appropriate address family and autonomous-system number. After conversion, the **show running-config** command will show only named mode configurations; you will not see any old classic mode configurations.

Additional References for EIGRP Classic to Named Mode

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference
EIGRP FAQ	EIGRP Frequently Asked Questions
EIGRP technology white paper	Enhanced Interior Gateway Routing Protocol

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP Classic to Named Mode Conversion

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 33: Feature Information for EIGRP Classic to Named Mode Conversion

Feature Name	Releases	Feature Information
EIGRP Classic to Named Mode Conversion	15.4(1)S 15.4(2)T	The EIGRP Classic to Named Mode Conversion feature allows you to upgrade Enhanced Interior Gateway Routing Protocol (EIGRP) classic mode configurations to named mode without causing network flaps or requiring EIGRP process restart. The following command was introduced: **eigrp upgrade-cli**.

CHAPTER 24

EIGRP Scale for DMVPN

The EIGRP Scale for DMVPN feature provides an increase in hub scalability for Dynamic Multipoint VPN (DMVPN). Cisco DMVPN is a security solution for building scalable enterprise VPNs that support distributed applications such as voice and video.

- Finding Feature Information, on page 273
- Information About EIGRP Scale for DMVPN, on page 273
- Additional References for EIGRP Scale for DMVPN, on page 274
- Feature Information for EIGRP Scale for DMVPN, on page 274

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP Scale for DMVPN

EIGRP Scale for DMVPN Overview

Dynamic Multipoint VPN (DMVPN) improves the usage of spoke-to-spoke networks. However, scaling of routing protocols and optimization of routing updates in large scale DMVPN networks remain a challenge. These challenges pertain to neighbor discovery, overhead reduction, and building upon the recent enhancements in the area of scaling routing over DMVPN. IPSEC tunnels, Next Hop Resolution Protocol (NHRP) and Enhanced Interior Gateway Routing Protocol (EIGRP) are established during initial startup of a DMVPN network. It is possible that EIGRP may not process and respond to inbound packets waiting in the interface or socket queue causing the spokes to time out and retransmit which worsens the resource contention issue. The EIGRP Scale for DMVPN feature provides an increase in the scalability of the hub device to 2500 sessions. The increase in the number of sessions reduces the adverse impact on CPU, system buffers, interface buffers, and queues and it reduces resource contention on the hub during initial startup of a DMVPN network. In a typical EIGRP DMVPN setup, spokes are configured as stubs.

This EIGRP Scale for DMVPN feature is enabled by default and does not have a configuration task.

Additional References for EIGRP Scale for DMVPN

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for EIGRP Scale for DMVPN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Name	Releases	Feature Information
EIGRP Scale for DMVPN	Cisco IOS XE Release 3.12S	The EIGRP Scale for DMVPN feature provides an increase in hub scalability for Dynamic Multipoint VPN (DMVPN).

CHAPTER 25

EIGRP IWAN Simplification

EIGRP is widely deployed on DMVPN networks. The EIGRP IWAN Simplification feature implements stub site behavior for EIGRP deployed on DMVPN networks.

- Finding Feature Information, on page 275
- Information About EIGRP IWAN Simplification, on page 275
- How to Configure EIGRP IWAN Simplification, on page 276
- Configuration Examples for EIGRP IWAN Simplification, on page 278
- Additional References for EIGRP IWAN Simplification, on page 278
- Feature Information for EIGRP IWAN Simplification, on page 279

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About EIGRP IWAN Simplification

Stub Site ID Configuration

The EIGRP Stub Routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration on the spoke. EIGRP Stub routing is commonly used over DMVPN networks having multiple sites with single device in each site. Site devices acting as stub result in reducing the query domain thereby enhancing improved performance. On the other hand, branch EIGRP routing is simple for a single router default-gateway site. When a the branch adds a second router or becomes larger and needs routing within the campus the configuration becomes complex.

The EIGRP IWAN Simplification feature implements stub site behavior on devices that are connected to the WAN interfaces on branch routing via the configuration of stub site ID on EIGRP address family. Use the **eigrp stub-site** command in the address family configuration mode. The stub site ID is applied to all incoming routes on WAN interfaces.

Note The **eigrp stub-site** command is mutually exclusive with the **eigrp stub** command. You cannot execute both commands on a device. This **eigrp stub-site** command resets the peers on WAN interfaces and initiates relearning of routes from WAN neighbors.

Interfaces connected towards hub or WAN are identified so that routes learnt through neighbors on such interfaces are part of a list of a given route. This is achieved via the **stub-site wan-interface** command configured in the address family interface configuration mode.

Note On the identified interfaces, neighbors treat WAN interfaces as stub.

How to Configure EIGRP IWAN Simplification

Configuring the Stub Site ID

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router eigrp** *virtual-instance-name*
4. Enter one of the following:
   - **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
   - **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
5. **network** *ip-address* [**wildcard-mask**]
6. **eigrp stub-site**
7. **af-interface** *interface-type interface-number*}
8. **stub-site wan-interface**
9. **end**
10. **show ip eigrp vrf** *vrf-name* **topology** [*ip-address* [*mask*]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	**Purpose**
Step 3	**router eigrp** *virtual-instance-name* **Example:** `Device(config)# router eigrp virtual-name1`	Enables an EIGRP routing process and enters router configuration mode.

Step 4	Enter one of the following:
	• **address-family ipv4** [**multicast**] [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	• **address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **autonomous-system** *autonomous-system-number*
	Example:
	`Device(config-router)# address-family ipv4 autonomous-system 45000`
	`Device(config-router)# address-family ipv6 autonomous-system 45000`
		Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

Step 5	**network** *ip-address* [**wildcard-mask**] **Example:** `Device(config-router-af)# network 172.16.0.0`	Specifies the network address of the EIGRP distribution device.
Step 6	**eigrp stub-site** **Example:** `Device(config-router-af)# eigrp stub-site 101:100`	Specifies a stub site for the address family in the following formats: • ASN:nn • IP-address:nn • 4BASN:nn • aa:nn

Step 7	**af-interface** *interface-type interface-number*}
	Example:
	`Device(config-router-af)# af-interface gigabitethernet 0/0/1`
		Enters address family interface configuration mode and configures interface-specific EIGRP commands.

Step 8	**stub-site wan-interface** **Example:** `Device(config-router-af-interface)# stub-site wan-interface`	Specifies a stub site for the WAN interfaces.

Step 9	**end**
	Example:
	`Device(config-router-af-interface)# end`
		Exits the address family interface configuration mode and returns to privileged EXEC mode.

Step 10	**show ip eigrp vrf** *vrf-name* **topology** [*ip-address* [*mask*]] **Example:**	Displays VPN routing and forwarding (VRF) entries in the EIGRP topology table.

	Command or Action	Purpose
	`Device# show ip eigrp vrf vrf1 topology 109.1.0.6/32`	

Example

The following is a sample output from the **show ip eigrp vrf topology** command

```
Device# show ip eigrp vrf vrf1 topology 109.1.0.6/32

EIGRP-IPv4 Topology Entry for AS(1)/ID(109.1.0.2) VRF(vrf1)
EIGRP-IPv4(1): Topology base(0) entry for 109.1.0.6/32
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2713600
  Descriptor Blocks:
  104.1.1.58 (Tunnel1), from 104.1.1.1, Send flag is 0x0
      Composite metric is (2713600/1408256), route is Internal
      Vector metric:
        Minimum bandwidth is 100000 Kbit
       Total delay is 105000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 200
        Hop count is 2
        Originating router is 109.1.0.6
      Extended Community: StubSite:101:100
```

Configuration Examples for EIGRP IWAN Simplification

Example: Configuring the Stub Site ID

```
Device> enable
Device# configure terminal
Device(config)# router eigrp virtual-name1
Device(config-router)# address-family ipv4 autonomous-system 45000
Device(config-router-af)# network 172.16.0.0
Device(config-router-af)# eigrp stub-site 101:100
Device(config-router-af)# af-interface gigabitethernet 0/0/1
Device(config-router-af-interface)# stub-site wan-interface
Device(config-router-af-interface)# end
```

Additional References for EIGRP IWAN Simplification

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
EIGRP commands	Cisco IOS IP Routing: EIGRP Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for EIGRP IWAN Simplification

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 34: Feature Information for EIGRP IWAN Simplification

Feature Name	Releases	Feature Information
EIGRP IWAN Simplification		EIGRP is widely deployed on DMVPN networks. The EIGRP IWAN Simplification feature implements stub site behavior for EIGRP deployed on DMVPN networks. The following commands were introduced by this feature: **eigrp stub-site**, **stub-site wan-interface**, **show ip eigrp**.