



## **IP Routing: EIGRP Configuration Guide, Cisco IOS XE Release 3E**

### **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.

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### CHAPTER 1

### EIGRP 1

Finding Feature Information	1
Information About Configuring EIGRP	2
EIGRP Features	2
EIGRP Autonomous System Configuration	2
EIGRP Named Configuration	2
EIGRP Neighbor Relationship Maintenance	3
Neighbor Authentication	3
DUAL Finite State Machine	3
Protocol-Dependent Modules	4
Goodbye Message	4
EIGRP Metric Weights	4
Mismatched K Values	5
Routing Metric Offset Lists	5
EIGRP Cost Metrics	6
Route Summarization	7
Summary Aggregate Addresses	8
Floating Summary Routes	8
Hello Packets and the Hold-Time Intervals	10
Split Horizon	11
EIGRP Dual DMVPN Domain Enhancement	11
Link Bandwidth Percentage	12
EIGRP vNETs	12
EIGRP vNET Interface and Command Inheritance	12
How to Configure EIGRP	13
Enabling EIGRP Autonomous System Configuration	13
Enabling the EIGRP Named Configuration	14
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	21
Configuring the EIGRP Route Summarization Autonomous System Configuration	22
Configuring the EIGRP Route Summarization Named Configuration	24
Configuring the EIGRP Event Logging Autonomous System Configuration	27
Configuring the EIGRP Event Logging Named Configuration	28
Configuring Equal and Unequal Cost Load Balancing Autonomous System Configuration	30
Configuring Equal and Unequal Cost Load Balancing Named Configuration	32
Adjusting the Interval Between Hello Packets and the Hold Time in an Autonomous System Configuration	33
Adjusting the Interval Between Hello Packets and the Hold Time in a Named Configuration	35
Disabling the Split Horizon Autonomous System Configuration	37
Disabling the Split Horizon and Next-Hop-Self Named Configuration	38
Monitoring and Maintaining the EIGRP Autonomous System Configuration	40
Monitoring and Maintaining the EIGRP Named Configuration	42
Configuration Examples for EIGRP	44
Example: Enabling EIGRP—Autonomous System Configuration	44
Example: Enabling EIGRP—Named Configuration	44
Example: EIGRP Parameters—Autonomous System Configuration	44
Example: EIGRP Parameters—Named Configuration	45
Example: EIGRP Redistribution—Autonomous System Configuration	45
Example: EIGRP Route Summarization—Autonomous System Configuration	45
Example: EIGRP Route Summarization—Named Configuration	46
Example: EIGRP Event Logging—Autonomous System Configuration	46
Example: EIGRP Event Logging—Named Configuration	46
Example: Equal and Unequal Cost Load Balancing—Autonomous System Configuration	47
Example: Equal and Unequal Cost Load Balancing—Named Configuration	47
Example: Adjusting the Interval Between Hello Packets and the Hold Time—Autonomous System Configuration	47
Example: Adjusting the Interval Between Hello Packets and the Hold Time—Named Configuration	47
Example: Disabling the Split Horizon—Autonomous System Configuration	48

Example: Disabling the Split Horizon and Next-Hop-Self—Named Configuration	48
Example: Command Inheritance and Virtual Network Interface Mode Override in an EIGRP Environment	48
Example: Monitoring and Maintaining the EIGRP Autonomous System Configuration	51
Example: Monitoring and Maintaining the EIGRP Named Configuration	53
Additional References for EIGRP	55
Feature Information for EIGRP	56

---

**CHAPTER 2**
**Configuring EIGRP 59**

Finding Feature Information	59
Information About Configuring EIGRP	60
EIGRP Features	60
EIGRP Autonomous System Configuration	60
EIGRP Named Configuration	60
EIGRP IPv6 VRF-Lite	61
EIGRP vNETs	61
EIGRP vNET Interface and Command Inheritance	61
EIGRP Neighbor Relationship Maintenance	62
Neighbor Authentication	62
DUAL Finite State Machine	63
Protocol-Dependent Modules	63
EIGRP Metric Weights	63
Mismatched K Values	64
EIGRP Wide Metrics	64
Goodbye Message	65
Routing Metric Offset Lists	66
EIGRP Cost Metrics	66
Route Summarization	68
Summary Aggregate Addresses	68
Floating Summary Routes	68
EIGRP Route Authentication	70
Hello Packets and the Hold-Time Intervals	71
Split Horizon	71
EIGRP Dual DMVPN Domain Enhancement	71
Link Bandwidth Percentage	72

EIGRP Stub Routing	72
Dual-Homed Remote Topology	73
EIGRP Stub Routing Leak Map Support	76
How to Configure EIGRP	76
Enabling EIGRP Autonomous System Configuration	76
Enabling the EIGRP Named Configuration	77
Enabling the EIGRP IPv6 VRF-Lite Named Configuration	79
Configuring Optional EIGRP Parameters in an Autonomous System Configuration	80
Configuring Optional EIGRP Parameters in a Named Configuration	82
Configuring the EIGRP Redistribution Autonomous System Configuration	85
Configuring the EIGRP Route Summarization Autonomous System Configuration	86
Configuring the EIGRP Route Summarization Named Configuration	88
Configuring the EIGRP Event Logging Autonomous System Configuration	91
Configuring the EIGRP Event Logging Named Configuration	92
Configuring Equal and Unequal Cost Load Balancing Autonomous System Configuration	94
Configuring Equal and Unequal Cost Load Balancing Named Configuration	96
Defining an Autonomous System for EIGRP Route Authentication	97
Defining a Named Configuration for EIGRP Route Authentication	100
Adjusting the Interval Between Hello Packets and the Hold Time in an Autonomous System Configuration	103
Adjusting the Interval Between Hello Packets and the Hold Time in a Named Configuration	105
Disabling the Split Horizon Autonomous System Configuration	106
Disabling the Split Horizon and Next-Hop-Self Named Configuration	107
Configuring the EIGRP Stub Routing Autonomous System Configuration	110
Configuring the EIGRP Stub Routing Named Configuration	111
Monitoring and Maintaining the EIGRP Autonomous System Configuration	113
Monitoring and Maintaining the EIGRP Named Configuration	114
Configuration Examples for EIGRP	117
Example: Enabling EIGRP—Autonomous System Configuration	117
Example: Enabling EIGRP—Named Configuration	117
Example: Enabling EIGRP IPv6 VRF-Lite—Named Configuration	117
Example: EIGRP Parameters—Autonomous System Configuration	117
Example: EIGRP Parameters—Named Configuration	118

Example: EIGRP Redistribution—Autonomous System Configuration	118
Example: EIGRP Route Summarization—Autonomous System Configuration	118
Example: EIGRP Route Summarization—Named Configuration	119
Example: EIGRP Event Logging—Autonomous System Configuration	119
Example: EIGRP Event Logging—Named Configuration	119
Example: Equal and Unequal Cost Load Balancing—Autonomous System Configuration	120
Example: Equal and Unequal Cost Load Balancing—Named Configuration	120
Example: EIGRP Route Authentication—Autonomous System Definition	120
Example: EIGRP Route Authentication—Named Configuration	121
Example: Adjusting the Interval Between Hello Packets and the Hold Time—Autonomous System Configuration	122
Example: Adjusting the Interval Between Hello Packets and the Hold Time—Named Configuration	123
Example: Disabling the Split Horizon—Autonomous System Configuration	123
Example: Disabling the Split Horizon and Next-Hop-Self—Named Configuration	123
Example: EIGRP Stub Routing—Autonomous System Configuration	123
Example: eigrp stub Command	124
Example: eigrp stub connected static Command	124
Example: eigrp stub leak-map Command	124
Example: eigrp stub receive-only Command	124
Example: eigrp stub redistributed Command	125
Example: EIGRP Stub Routing—Named Configuration	125
Example: eigrp stub Command	125
Example: eigrp stub connected static Command	125
Example: eigrp stub leak-map Command	126
Example: eigrp stub receive-only Command	126
Example: eigrp stub redistributed Command	126
Example: Command Inheritance and Virtual Network Interface Mode Override in an EIGRP Environment	126
Additional References	129
Feature Information for EIGRP	130

**CHAPTER 3****IPv6 Routing: EIGRP Support 133**

Finding Feature Information 133

Restrictions for IPv6 Routing EIGRP Support 133

Information About IPv6 Routing EIGRP Support	134
Cisco EIGRP for IPv6 Implementation	134
How to Configure IPv6 Routing EIGRP Support	136
Enabling EIGRP for IPv6 on an Interface	136
Configuring the Percentage of Link Bandwidth Used by EIGRP	138
Configuring Summary Addresses	139
Configuring EIGRP Route Authentication	140
Overriding the Next Hop in EIGRP	142
Adjusting the Interval Between Hello Packets in EIGRP for IPv6	143
Adjusting the Hold Time in EIGRP for IPv6	144
Disabling Split Horizon in EIGRP for IPv6	145
Configuring EIGRP Stub Routing for Greater Network Stability	146
Configuring a Device for EIGRP Stub Routing	147
Verifying EIGRP Stub Routing	148
Customizing an EIGRP for IPv6 Routing Process	148
Logging EIGRP Neighbor Adjacency Changes	148
Configuring Intervals Between Neighbor Warnings	149
Adjusting EIGRP for IPv6 Metric Weights	150
Deleting Entries from EIGRP for IPv6 Routing Tables	151
Configuration Examples for IPv6 Routing EIGRP Support	152
Example: Configuring EIGRP to Establish Adjacencies on an Interface	152
Additional References	152
Feature Information for IPv6 Routing: EIGRP Support	154

**CHAPTER 4****EIGRP Stub Routing 157**

Finding Feature Information	157
Information About EIGRP Stub Routing	158
EIGRP Stub Routing	158
Dual-Homed Remote Topology	159
How to Configure EIGRP Stub Routing	162
Configuring the EIGRP Stub Routing Autonomous System Configuration	162
Configuring the EIGRP Stub Routing Named Configuration	163
Configuration Examples for EIGRP Stub Routing	165
Example: EIGRP Stub Routing—Autonomous System Configuration	165
Example: eigrp stub Command	165



Example: eigrp stub connected static Command	166
Example: eigrp stub leak-map Command	166
Example: eigrp stub receive-only Command	166
Example: eigrp stub redistributed Command	166
Example: EIGRP Stub Routing—Named Configuration	166
Example: eigrp stub Command	167
Example: eigrp stub connected static Command	167
Example: eigrp stub leak-map Command	167
Example: eigrp stub receive-only Command	167
Example: eigrp stub redistributed Command	167
Additional References	168
Feature Information for EIGRP Stub Routing	168

**CHAPTER 5****EIGRP IPv6 VRF-Lite 171**

Finding Feature Information	171
Information About EIGRP IPv6 VRF-Lite	172
VRF-Lite for EIGRP IPv6	172
EIGRP Named Configuration	172
How to Configure EIGRP IPv6 VRF-Lite	173
Enabling the EIGRP IPv6 VRF-Lite Named Configuration	173
Configuration Examples for EIGRP IPv6 VRF-Lite	174
Example: Enabling EIGRP IPv6 VRF-Lite—Named Configuration	174
Additional References	174
Feature Information for EIGRP IPv6 VRF-Lite	175

**CHAPTER 6****IP EIGRP Route Authentication 177**

Finding Feature Information	177
Information About IP EIGRP Route Authentication	177
EIGRP Route Authentication	177
How to Configure IP EIGRP Route Authentication	178
Defining an Autonomous System for EIGRP Route Authentication	178
Defining a Named Configuration for EIGRP Route Authentication	180
Configuration Examples for IP EIGRP Route Authentication	184
Example: EIGRP Route Authentication—Autonomous System Definition	184
Example: EIGRP Route Authentication—Named Configuration	185

Additional References	186
Feature Information for IP EIGRP Route Authentication	187

---

**CHAPTER 7**

<b>EIGRP Nonstop Forwarding</b>	<b>189</b>
Finding Feature Information	189
Prerequisites for EIGRP Nonstop Forwarding	190
Restrictions for EIGRP Nonstop Forwarding	190
Information About EIGRP Nonstop Forwarding	190
Nonstop Forwarding	190
EIGRP NSF Operations	191
How to Configure EIGRP Nonstop Forwarding	192
Configuring and Verifying EIGRP NSF	192
Troubleshooting EIGRP Nonstop Forwarding	194
Configuration Examples for EIGRP Nonstop Forwarding	195
Example: EIGRP NSF	195
Additional References	196
Feature Information for EIGRP Nonstop Forwarding	197

---

**CHAPTER 8**

<b>EIGRP Nonstop Forwarding Awareness</b>	<b>199</b>
Finding Feature Information	199
Prerequisites for EIGRP Nonstop Forwarding Awareness	200
Restrictions for EIGRP Nonstop Forwarding Awareness	200
Information About EIGRP Nonstop Forwarding Awareness	200
Cisco NSF Routing and Forwarding Operation	200
Cisco Express Forwarding	201
EIGRP Nonstop Forwarding Awareness	201
EIGRP NSF-Capable and NSF-Aware Interoperation	202
Non-NSF Aware EIGRP Neighbors	202
EIGRP NSF Timers	203
How to Configure EIGRP Nonstop Forwarding Awareness	203
Enabling EIGRP Nonstop Forwarding Awareness	203
Modifying EIGRP Nonstop Forwarding Awareness Timers	204
Troubleshooting Tips	206
Monitoring EIGRP NSF Debug Events and Notifications	206
Verifying the Local Configuration of EIGRP NSF Awareness	207

Configuration Examples for EIGRP Nonstop Forwarding Awareness	208
Example: EIGRP Graceful-Restart Purge-Time Timer Configuration	208
Example: Monitoring EIGRP NSF Debug Events and Notifications Configuration	208
Example: Verifying Local Configuration of EIGRP NSF Awareness	208
Additional References for EIGRP Nonstop Forwarding Awareness	209
Feature Information for EIGRP Nonstop Forwarding Awareness	210





# 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, page 1](#)
- [Information About Configuring EIGRP, page 2](#)
- [How to Configure EIGRP, page 13](#)
- [Configuration Examples for EIGRP, page 44](#)
- [Additional References for EIGRP, page 55](#)
- [Feature Information for EIGRP, page 56](#)

## 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](http://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  $10^7/\text{minimum bandwidth in kilobits per second}$ . 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:

$$\text{EIGRP composite cost metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))$$

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: $(10^7 / \text{minimum bandwidth (Bw) in kilobits per second})$
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:

$(10^7 / \text{minimum Bw in kilobits per second})$

**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:

$$\text{Metric} = 256 * (10^7 / 128 + 84000 / 10) = 256 * 86525 = 22150400$$

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:

$$\text{Metric} = (256 * (10^7 / 128)) + (84000 * 256) / 10 = 20000000 + 2150400 = 22150400$$

## 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.

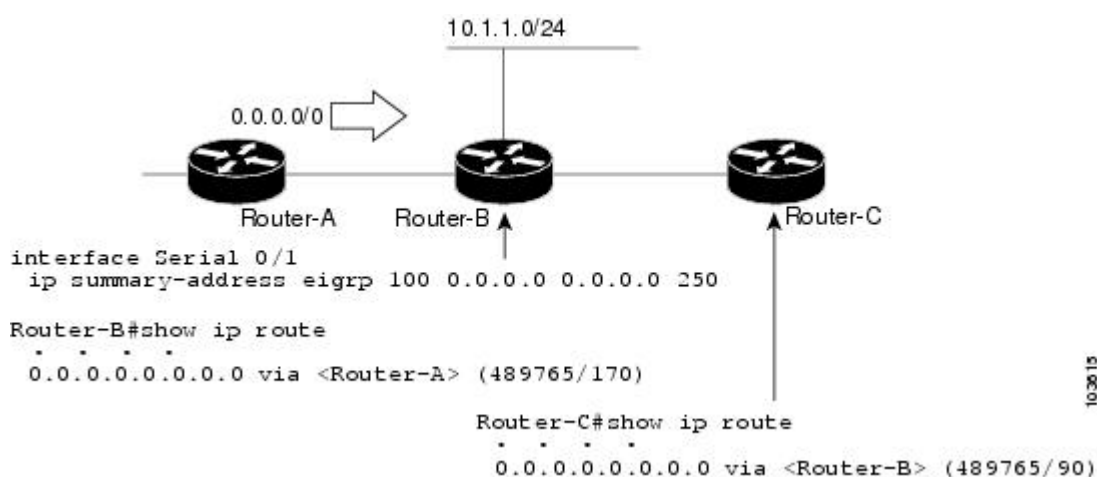
The figure below shows a network with three devices, Device-A, Device-B, and Device-C. Device-A learns a default route from elsewhere in the network and then advertises this route to Device-B. Device-B is configured so that only a default summary route is advertised to Device-C. The default summary route 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**



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
```

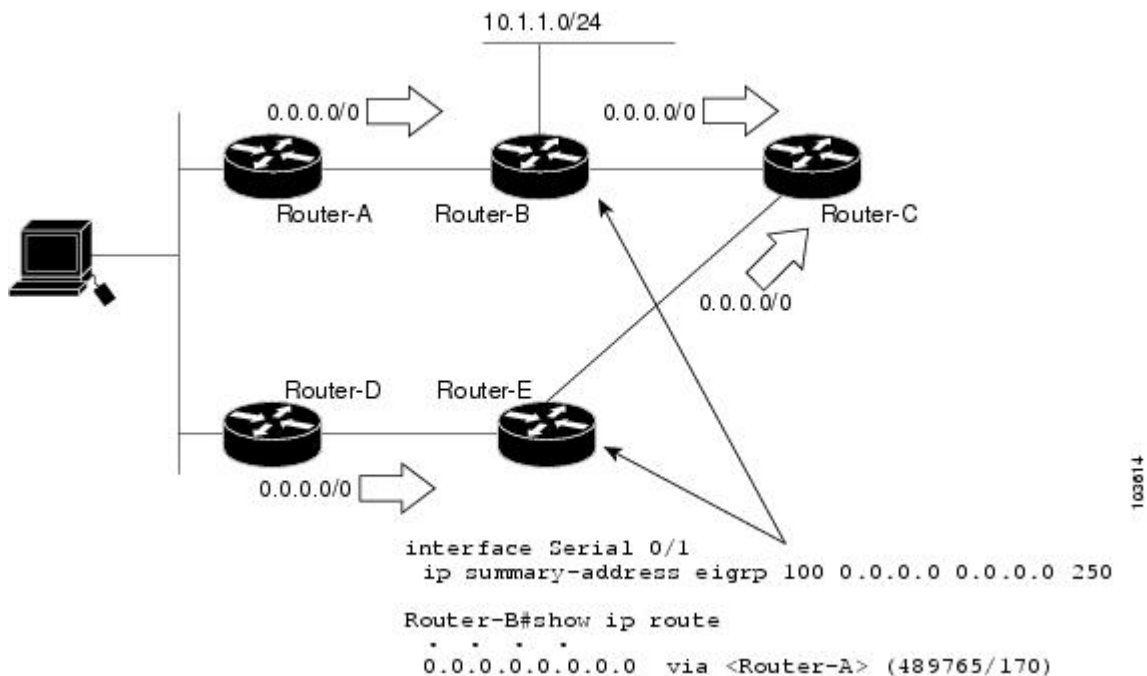
The administrative distance of 250, applied in the **summary-address** command, is now assigned to the discard route generated on Device-B. The 0.0.0.0/0, from Device-A, is learned through EIGRP and installed in the local routing table. Routing to Device-C is restored.

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**



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.

## 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp <i>autonomous-system-number</i></b>  <b>Example:</b> Device(config)# router eigrp 1	Configures an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
Step 4	<b>network <i>network-number</i></b>  <b>Example:</b> Device(config-router)# network 172.16.0.0	Associates a network with an EIGRP routing process.
Step 5	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Configures the EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>network</b> <i>ip-address</i> [<i>wildcard-mask</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# network 172.16.0.0</pre>	Specifies a network for the EIGRP routing process.
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# end</pre>	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
<b>Step 1</b>	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>router eigrp <i>autonomous-system</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp 1</pre>	<p>Enables an EIGRP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<p><b>network <i>ip-address</i> [<i>wildcard-mask</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# network 172.16.0.0</pre>	Associates networks with an EIGRP routing process.
<b>Step 5</b>	<p><b>passive-interface [default] [<i>interface-type interface-number</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# passive-interface</pre>	(Optional) Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.
<b>Step 6</b>	<p><b>offset-list [<i>access-list-number</i>   <i>access-list-name</i>] {in   out} <i>offset</i> [<i>interface-type interface-number</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# offset-list 21 in 10 gigabitethernet 0/0/1</pre>	(Optional) Applies an offset to routing metrics.
<b>Step 7</b>	<p><b>metric weights <i>tos k1 k2 k3 k4 k5</i></b></p> <p><b>Example:</b></p> <pre>Device(config-router)# metric weights 0 2 0 2 0 0</pre>	<p>(Optional) Adjusts the EIGRP metric or K value.</p> <ul style="list-style-type: none"> <li>EIGRP uses the following formula to determine the total metric to the network:</li> </ul> $\text{EIGRP Metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))$ <p><b>Note</b> If K5 is 0, then (K5 / (Reliability + K4)) is defined as 1.</p>
<b>Step 8</b>	<b>no auto-summary</b>	(Optional) Disables automatic summarization.

	Command or Action	Purpose
	<b>Example:</b> Device(config-router)# no auto-summary	<b>Note</b> Automatic summarization is enabled by default.
<b>Step 9</b>	<b>end</b>  <b>Example:</b> 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** {**default** | *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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
Step 4	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] [<b>multicast</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b> 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	<b>network</b> <i>ip-address</i> [ <i>wildcard-mask</i> ]  <b>Example:</b> Device(config-router-af)# network 172.16.0.0	Specifies a network for the EIGRP routing process.
Step 6	<b>metric weights</b> <i>tos k1 k2 k3 k4 k5 k6</i>  <b>Example:</b> Device(config-router-af)# metric weights 0 2 0 2 0 0 0	(Optional) Adjusts the EIGRP metric or K value. <ul style="list-style-type: none"> <li>• EIGRP uses the following formula to determine the total 32-bit metric to the network:  <math display="block">\text{EIGRP Metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))</math></li> <li>• EIGRP uses the following formula to determine the total 64-bit metric to the network:  <math display="block">\text{EIGRP Metric} = 256 * ((K1 * \text{Throughput}) + (K2 * \text{Throughput}) / (256 - \text{Load}) + (K3 * \text{Latency}) + (K6 * \text{Extended Attributes})) * (K5 / (\text{Reliability} + K4))</math></li> </ul>

	Command or Action	Purpose
		<b>Note</b> If K5 is 0, then $(K5 / (\text{Reliability} + K4))$ is defined as 1.
<b>Step 7</b>	<b>af-interface</b> { <b>default</b>   <i>interface-type interface-number</i> }  <b>Example:</b> Device(config-router-af)# af-interface gigabitethernet 0/0/1	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 8</b>	<b>passive-interface</b>  <b>Example:</b> 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.
<b>Step 9</b>	<b>bandwidth-percent</b> <i>maximum-bandwidth-percentage</i>  <b>Example:</b> 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.
<b>Step 10</b>	<b>exit-af-interface</b>  <b>Example:</b> Device(config-router-af-interface)# exit-af-interface	Exits address family interface configuration mode.
<b>Step 11</b>	<b>topology</b> { <b>base</b>   <i>topology-name tid number</i> }  <b>Example:</b> 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.
<b>Step 12</b>	<b>offset-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ] { <b>in</b>   <b>out</b> } <i>offset</i> [ <i>interface-type interface-number</i> ]  <b>Example:</b> Device(config-router-af-topology)# offset-list 21 in 10 gigabitethernet 6/2	(Optional) Applies an offset to routing metrics.
<b>Step 13</b>	<b>no auto-summary</b>  <b>Example:</b> Device(config-router-af-topology)# no auto-summary	(Optional) Disables automatic summarization.  <b>Note</b> Automatic summarization is enabled by default.
<b>Step 14</b>	<b>end</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> Device(config)# router eigrp 1	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>network</b> <i>ip-address [wildcard-mask]</i>  <b>Example:</b> Device(config-router)# network 172.16.0.0	Associates networks with an EIGRP routing process.
<b>Step 5</b>	<b>redistribute</b> <i>protocol</i>  <b>Example:</b> Device(config-router)# redistribute rip	Redistributes routes from one routing domain into another routing domain.
<b>Step 6</b>	<b>distance eigrp</b> <i>internal-distance external-distance</i>  <b>Example:</b> Device(config-router)# distance eigrp 80 130	Allows the use of two administrative distances—internal and external.
<b>Step 7</b>	<b>default-metric</b> <i>bandwidth delay reliability loading mtu</i>  <b>Example:</b> Device(config-router)# default-metric 1000 100 250 100 1500	Sets metrics for EIGRP.
<b>Step 8</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> 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.
<b>Step 4</b>	<b>no auto-summary</b>  <b>Example:</b> Device(config-router)# no auto-summary	Disables automatic summarization of subnet routes into network-level routes
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits router configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/3	Enters interface configuration mode.
<b>Step 7</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode
<b>Step 8</b>	<b>bandwidth</b> <i>kpbs</i>  <b>Example:</b> bandwidth 56	Sets the inherited and received bandwidth values for an interface
<b>Step 9</b>	<b>ip summary-address eigrp</b> <i>as-number ip-address mask</i> <i>[admin-distance] [leak-map name]</i>  <b>Example:</b> Device(config-if)# ip summary-address eigrp 100 10.0.0.0 0.0.0.0	(Optional) Configures a summary aggregate address.
<b>Step 10</b>	<b>ip bandwidth-percent eigrp</b> <i>as-number percent</i>  <b>Example:</b> Device(config-if)# ip bandwidth-percent eigrp 209 75	(Optional) Configures the percentage of bandwidth that may be used by EIGRP on an interface.
<b>Step 11</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>af-interface</b> {default   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# af-interface gigabitethernet 0/0/1</pre>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<p><b>summary-address</b> <i>ip-address mask [administrative-distance [leak-map leak-map-name]]</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0</pre>	Configures a summary address for EIGRP.
<b>Step 7</b>	<p><b>exit-af-interface</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# exit-af-interface</pre>	Exits address family interface configuration mode.
<b>Step 8</b>	<p><b>topology</b> {base   <i>topology-name tid number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.
<b>Step 9</b>	<p><b>summary-metric</b> <i>network-address subnet-mask bandwidth delay reliability load mtu</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# summary-metric 192.168.0.0/16 10000 10 255 1 1500</pre>	(Optional) Configures a fixed metric for an EIGRP summary aggregate address.
<b>Step 10</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# end</pre>	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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp <i>autonomous-system</i></b>  <b>Example:</b> Device(config)# router eigrp 101	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
Step 4	<b>eigrp event-log-size <i>size</i></b>  <b>Example:</b> Device(config-router)# eigrp event-log-size 5000010	(Optional) Sets the size of the EIGRP event log.
Step 5	<b>eigrp log-neighbor-changes</b>  <b>Example:</b> Device(config-router)# eigrp log-neighbor-changes	(Optional) Enables logging of EIGRP neighbor adjacency changes. <ul style="list-style-type: none"> <li>• By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.</li> </ul>

	Command or Action	Purpose
<b>Step 6</b>	<b>eigrp log-neighbor-warnings</b> <i>[seconds]</i>  <b>Example:</b>  Device(config-router)# eigrp log-neighbor-warnings 300	(Optional) Enables the logging of EIGRP neighbor warning messages.
<b>Step 7</b>	<b>end</b>  <b>Example:</b>  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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>



	Command or Action	Purpose
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>router eigrp</b> <i>virtual-instance-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp virtual-name1</pre>	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	<p>Enter one of the following:</p> <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [multicast] [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
<b>Step 5</b>	<p><b>eigrp log-neighbor-warnings</b> [<i>seconds</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# eigrp log-neighbor-warnings 300</pre>	(Optional) Enables the logging of EIGRP neighbor warning messages.
<b>Step 6</b>	<p><b>eigrp log-neighbor-changes</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# eigrp log-neighbor-changes</pre>	<p>(Optional) Enables logging of EIGRP neighbor adjacency changes.</p> <ul style="list-style-type: none"> <li>• By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.</li> </ul>
<b>Step 7</b>	<p><b>topology</b> {base   <i>topology-name tid number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

	Command or Action	Purpose
<b>Step 8</b>	<b>Command or Action</b> <code>eigrp event-log-size <i>size</i></code>  <b>Example:</b> <pre>Device(config-router-af-topology)# eigrp event-log-size 10000</pre>	(Optional) Sets the size of the EIGRP event log.
<b>Step 9</b>	<b>Command or Action</b> <code>end</code>  <b>Example:</b> <pre>Device(config-router-af-topology)# end</pre>	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
<b>Step 1</b>	<b>Command or Action</b> <code>enable</code>  <b>Example:</b> <pre>Device&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>Command or Action</b> <code>configure terminal</code>  <b>Example:</b> <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> Device(config)# router eigrp 101	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>traffic-share</b> <b>balanced</b>  <b>Example:</b> Device(config-router)# traffic-share balanced	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.
<b>Step 5</b>	<b>maximum-paths</b> <i>number-of-paths</i>  <b>Example:</b> Device(config-router)# maximum-paths 5	Controls the maximum number of parallel routes that an IP routing protocol can support.
<b>Step 6</b>	<b>variance</b> <i>multiplier</i>  <b>Example:</b> Device(config-router)# variance 1	Controls load balancing in an internetwork based on EIGRP.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>topology</b> {<b>base</b>   <i>topology-name</i> <b>tid</b> <i>number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.
<b>Step 6</b>	<p><b>traffic-share</b> <b>balanced</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# traffic-share balanced</pre>	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.
<b>Step 7</b>	<p><b>maximum-paths</b> <i>number-of-paths</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# maximum-paths 5</pre>	Controls the maximum number of parallel routes that an IP routing protocol can support.
<b>Step 8</b>	<p><b>variance</b> <i>multiplier</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# variance 1</pre>	Controls load balancing in an internetwork based on EIGRP.
<b>Step 9</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# end</pre>	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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> 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.
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits to global configuration mode.
<b>Step 5</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/9	Enters interface configuration mode.
<b>Step 6</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode

	Command or Action	Purpose
<b>Step 7</b>	<b>ip hello-interval eigrp</b> <i>autonomous-system-number seconds</i>  <b>Example:</b>  Device(config-if)# ip hello-interval eigrp 109 10	Configures the hello interval for an EIGRP routing process.
<b>Step 8</b>	<b>ip hold-time eigrp</b> <i>autonomous-system-number seconds</i>  <b>Example:</b>  Device(config-if)# ip hold-time eigrp 109 40	Configures the hold time for an EIGRP routing process.  <b>Note</b> Do not adjust the hold time without consulting your technical support personnel.
<b>Step 9</b>	<b>end</b>  <b>Example:</b>  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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following:  <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b>  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.
<b>Step 5</b>	<b>af-interface</b> { <b>default</b>   <i>interface-type interface-number</i> }  <b>Example:</b>  Device(config-router-af)# af-interface gigabitethernet 0/0/1	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<b>hello-interval</b> <i>seconds</i>  <b>Example:</b>  Device(config-router-af-interface)# hello-interval 10	Configures the hello interval for an EIGRP address family named configuration.



	Command or Action	Purpose
<b>Step 7</b>	<b>hold-time</b> <i>seconds</i>  <b>Example:</b> Device(config-router-af-interface)# hold-time 50	Configures the hold time for an EIGRP address family named configuration.
<b>Step 8</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface gigabitethernet 0/1	Configures an interface and enters interface configuration mode.
Step 4	<b>no ip split-horizon eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config-if)# no ip split-horizon eigrp 101	Disables split horizon.
Step 5	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b> 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.
<b>Step 5</b>	<b>af-interface</b> { <b>default</b>   <i>interface-type interface-number</i> }  <b>Example:</b> Device(config-router-af)# af-interface gigabitethernet 0/0/1	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<b>no split-horizon</b>  <b>Example:</b> Device(config-router-af-interface)# no split-horizon	Disables EIGRP split horizon.

	Command or Action	Purpose
<b>Step 7</b>	<b>no next-hop-self [no-ecmp-mode]</b>  <b>Example:</b>  <pre>Device(config-router-af-interface)# no next-hop-self no-ecmp-mode</pre>	(Optional) Instructs an EIGRP router to use the received next hop rather than the local outbound interface address as the next hop. <ul style="list-style-type: none"> <li>The <b>no-ecmp-mode</b> keyword is an enhancement to the <b>no next-hop-self</b> 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.</li> </ul>
<b>Step 8</b>	<b>end</b>  <b>Example:</b>  <pre>Device(config-router-af-interface)# end</pre>	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 GigabitEthernet 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 Count Restart Count Restart/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)

```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending 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 (sec)	SRTT (ms)	RTO	Q Cnt	Seq 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), GigabitEthernet0/0
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 Count Restart Count Restart/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 Cnt Num
(sec) (ms) (ms)
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	<a href="#">Master Commands List, All Releases</a>
EIGRP commands	<a href="#">IP Routing: EIGRP Command Reference</a>
EIGRP FAQ	<a href="#">EIGRP Frequently Asked Questions</a>
EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks feature	“Mobile Ad Hoc Networks for Router-to-Radio Communications” module of <i>the IP Mobility Configuration Guide</i>
EIGRP Technology Support	<a href="#">Enhanced Interior Gateway Routing Protocol</a>
EIGRP Technology White Papers	<a href="#">Enhanced Interior Gateway Routing Protocol</a>
IPv6 Routing EIGRP Support	<i>IPv6 Routing: EIGRP Support</i>
Protocol-independent features that work with EIGRP	<i>IP Routing: Protocol-Independent Configuration Guide</i>
Service Advertisement Framework	<i>Service Advertisement Framework Configuration Guide</i>
Service Advertisement Framework commands	<a href="#">Service Advertisement Framework Command Reference</a>

### Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	<i>SECURE HASH STANDARD (SHS)</i>

Standard/RFC	Title
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 3: Feature Information for EIGRP Features

Feature Name	Releases	Feature Information
EIGRP	Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified:</p> <p><b>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).</b></p>

Feature Name	Releases	Feature Information
EIGRP Dual DMVPN Domain Enhancement	Cisco IOS XE Release 3.6E	<p>The EIGRP Dual DMVPN Domain Enhancement feature supports the no next-hop-self functionality on dual DMVPN domains in both IPv4 and IPv6 configurations.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified by this feature:  <b>ip next-hop-self eigrp</b>, <b>ipv6 next-hop-self eigrp</b>, <b>next-hop-self</b>, <b>show ip eigrp interfaces</b>, <b>show ipv6 eigrp interfaces</b>, <b>show ip eigrp topology</b>, <b>show ipv6 eigrp topology</b>.</p>
Named mode for EIGRP vNETs IPv4	Cisco IOS XE Release 3.6E	<p>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.</p> <p>The following command was modified: <b>vnet</b>.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>



## CHAPTER 2

# Configuring 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 referred to as 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](#), page 59
- [Information About Configuring EIGRP](#), page 60
- [How to Configure EIGRP](#), page 76
- [Configuration Examples for EIGRP](#), page 117
- [Additional References](#), page 129
- [Feature Information for EIGRP](#), 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](http://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 255 hops, and the EIGRP metric is large enough to support thousands of hops. The default maximum number of EIGRP hops is 100.
- Fast convergence—The DUAL algorithm allows routing information to converge quickly.
- Partial updates—EIGRP sends incremental updates (instead of sending the entire contents of the routing table) when the state of a destination changes. This feature minimizes the bandwidth required for EIGRP packets.
- Neighbor discovery mechanism—This is a simple, protocol-independent hello mechanism used to learn about neighboring devices.
- Variable-Length Subnet Masks (VLSMs).
- Arbitrary route summarization.
- 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 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.

## 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.

## 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.

## 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.

## 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  $10^7/\text{minimum bandwidth in kilobits per second}$ . 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.

## 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.

$$\text{Metric} = [(K1 * \text{Minimum Throughput} + \{K2 * \text{Minimum Throughput}\} / 256 - \text{Load}) + (K3 * \text{Total Latency}) + (K6 * \text{Extended Attributes})] * [K5 / (K4 + \text{Reliability})]$$

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:

$$\text{Composite Cost Metric} = (K1 * \text{Minimum Throughput}) + (K3 * \text{Total Latency})$$

Minimum Throughput =  $(10^7 * 65536) / \text{Bw}$ , where 65536 is the wide-scale constant.

Total Latency for bandwidths below 1 gigabit =  $(\text{Delay} * 65536) / 10$ , where 65536 is the wide-scale constant.

Total Latency for bandwidths above 1 gigabit =  $(10^7 * 65536 / 10) / \text{Bw}$ , 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.

## 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.

## 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:

$$\text{EIGRP composite cost metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))$$

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

**Table 4: 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: $(10^7 / \text{minimum bandwidth (Bw) in kilobits per second})$
delay	Route delay, in tens of microseconds.

Vector Metric	Description
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 5: 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:

$(10^7 / \text{minimum Bw in kilobits per second})$



**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:

$$\text{Metric} = (256 * (10^7 / 128)) + (84000 * 256) / 10 = 20000000 + 2150400 = 22150400$$

## 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
```

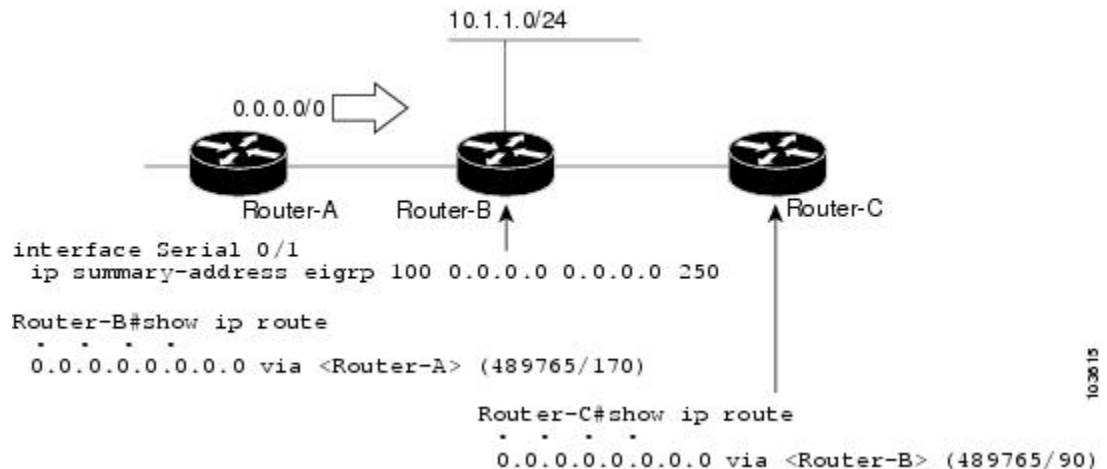
The default summary route is applied to serial interface 0/1 on Device-B with the following named configuration:

```
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 3: Floating Summary Route Applied to Device-B**



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
```

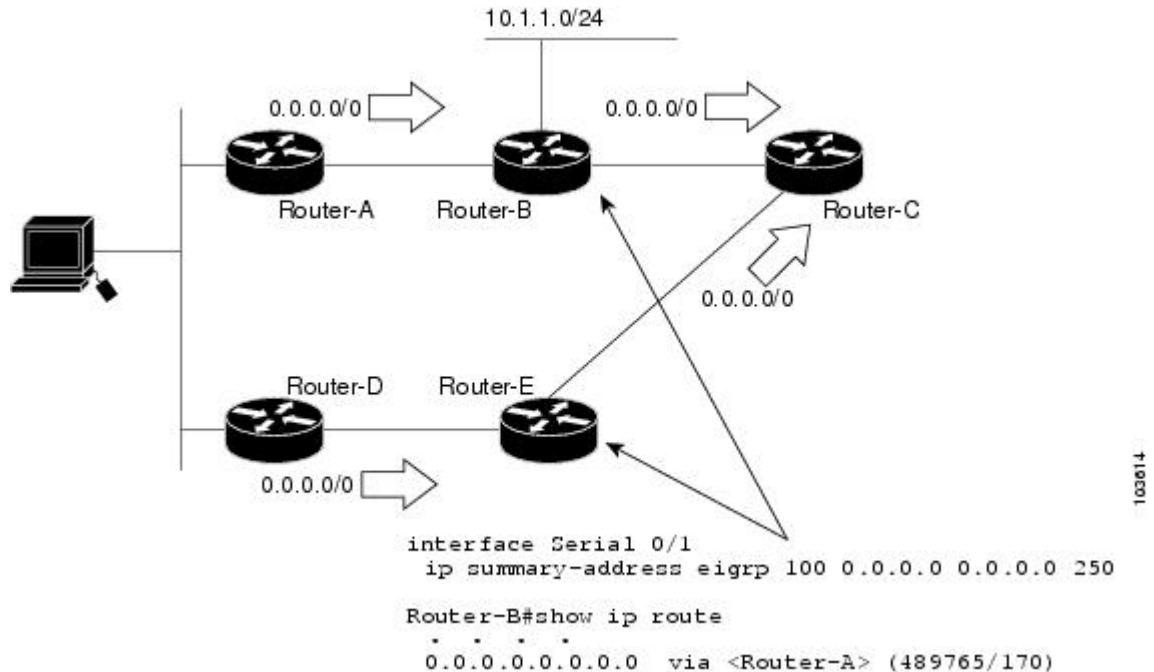
The administrative distance of 250, applied in the **summary-address** command, is now assigned to the discard route generated on Device-B. The 0.0.0.0/0, from Device-A, is learned through EIGRP and installed in the local routing table. Routing to Device-C is restored.

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 4: Floating Summary Route Applied for Dual-Homed Remotes**



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).

## 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.

## 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 Stub Routing

The EIGRP stub routing feature improves network stability, reduces resource utilization, and simplifies the stub device configuration.

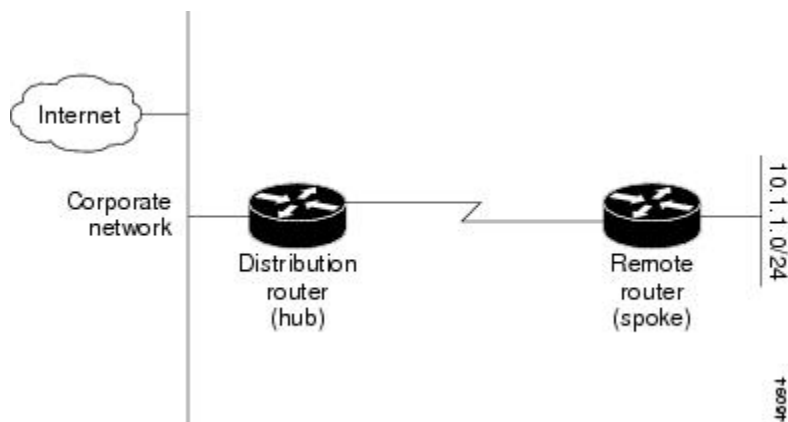
Stub routing is commonly used in hub-and-spoke network topologies. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote device (the spoke) that is connected to one or more distribution devices (the hub). The remote device is adjacent to one or more distribution devices. 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.

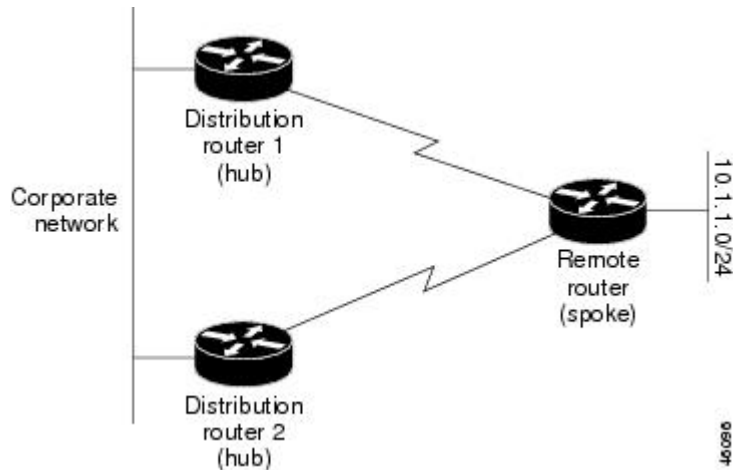
## Dual-Homed Remote Topology

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.

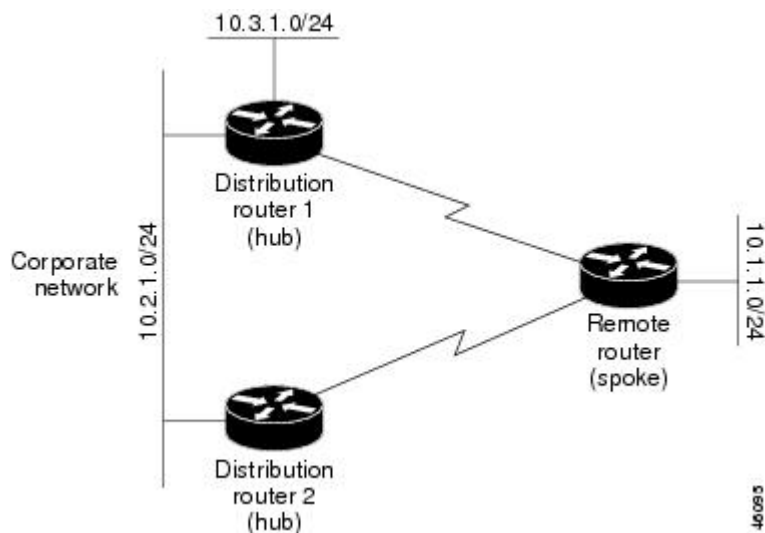
**Figure 6: Simple Dual-Homed Remote Topology**



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).

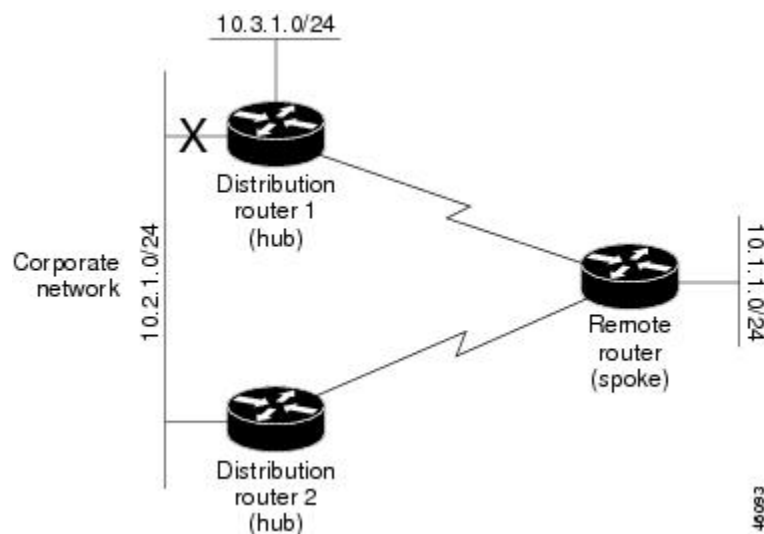
**Figure 7: Dual-Homed Remote Topology with Distribution Device 1 Connected to Two Networks**



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.

## EIGRP Stub Routing Leak Map Support

In EIGRP stub routing configurations where there is a remote site with more than one device, only one of the remote devices can be configured as the stub device. If you have two distribution layer devices and two devices at a remote site, there is no way to declare both remote devices as stub devices. If one remote device is configured as a stub device, the other remote device can neither learn routes towards the network core if the link between the stub device and the distribution layer device fails nor route around the failed link.

The stub device cannot readvertise routes learned from any neighboring EIGRP device. To resolve this issue, a leak map configuration that allows a selected set of learned routes to be readvertised to other peers can be added to the EIGRP stub routing feature. The set of routes allowed through the stub device are specified using a standard route map so that routes can be matched based on tags, prefixes, or interfaces. These routes are marked using the site-of-origin code mechanism, which prevents routes permitted through the stub from being readvertised into the core of the network.

Use the **eigrp stub leak-map** command to configure the EIGRP stub routing feature to reference a leak map that identifies routes that are allowed to be advertised on an EIGRP stub device that would normally have been suppressed.

## 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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config)# router eigrp 1	Configures an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>network</b> <i>network-number</i>  <b>Example:</b> Device(config-router)# network 172.16.0.0	Associates a network with an EIGRP routing process.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Configures the EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>network</b> <i>ip-address</i> [<i>wildcard-mask</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# network 172.16.0.0</pre>	Specifies a network for the EIGRP routing process.
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# end</pre>	Exits address family configuration mode and returns to privileged EXEC mode.

## 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
<b>Step 1</b>	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Configures the EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	<b>address-family ipv6 vrf</b> <i>vrf-name</i> <b>autonomous-system</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config-router)# address-family ipv6 vrf vrf1 autonomous-system 45000	Enables EIGRP IPv6 VRF-Lite and enters address family configuration mode.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>router eigrp <i>autonomous-system</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp 1</pre>	<p>Enables an EIGRP routing process and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<p><b>network <i>ip-address</i> [<i>wildcard-mask</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# network 172.16.0.0</pre>	Associates networks with an EIGRP routing process.
<b>Step 5</b>	<p><b>passive-interface [default] [<i>interface-type interface-number</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# passive-interface</pre>	(Optional) Suppresses EIGRP hello packets and routing updates on interfaces while still including the interface addresses in the topology database.
<b>Step 6</b>	<p><b>offset-list [<i>access-list-number</i>   <i>access-list-name</i>] {in   out} <i>offset</i> [<i>interface-type interface-number</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# offset-list 21 in 10 gigabitethernet 0/0/1</pre>	(Optional) Applies an offset to routing metrics.
<b>Step 7</b>	<p><b>metric weights <i>tos k1 k2 k3 k4 k5</i></b></p> <p><b>Example:</b></p> <pre>Device(config-router)# metric weights 0 2 0 2 0 0</pre>	<p>(Optional) Adjusts the EIGRP metric or K value.</p> <ul style="list-style-type: none"> <li>EIGRP uses the following formula to determine the total metric to the network:</li> </ul> $\text{EIGRP Metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))$ <p><b>Note</b> If K5 is 0, then (K5 / (Reliability + K4)) is defined as 1.</p>
<b>Step 8</b>	<b>no auto-summary</b>	(Optional) Disables automatic summarization.

	Command or Action	Purpose
	<b>Example:</b> Device(config-router)# no auto-summary	<b>Note</b> Automatic summarization is enabled by default.
<b>Step 9</b>	<b>end</b>  <b>Example:</b> 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** {**default** | *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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
Step 4	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] [<b>multicast</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b> 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	<b>network</b> <i>ip-address</i> [ <i>wildcard-mask</i> ]  <b>Example:</b> Device(config-router-af)# network 172.16.0.0	Specifies a network for the EIGRP routing process.
Step 6	<b>metric weights</b> <i>tos k1 k2 k3 k4 k5 k6</i>  <b>Example:</b> Device(config-router-af)# metric weights 0 2 0 2 0 0 0	(Optional) Adjusts the EIGRP metric or K value. <ul style="list-style-type: none"> <li>• EIGRP uses the following formula to determine the total 32-bit metric to the network:  <math display="block">\text{EIGRP Metric} = 256 * ((K1 * Bw) + (K2 * Bw) / (256 - \text{Load}) + (K3 * \text{Delay}) * (K5 / (\text{Reliability} + K4)))</math></li> <li>• EIGRP uses the following formula to determine the total 64-bit metric to the network:  <math display="block">\text{EIGRP Metric} = 256 * ((K1 * \text{Throughput}) + (K2 * \text{Throughput}) / (256 - \text{Load}) + (K3 * \text{Latency}) + (K6 * \text{Extended Attributes})) * (K5 / (\text{Reliability} + K4))</math></li> </ul>

	Command or Action	Purpose
		<b>Note</b> If K5 is 0, then $(K5 / (\text{Reliability} + K4))$ is defined as 1.
<b>Step 7</b>	<b>af-interface</b> { <b>default</b>   <i>interface-type interface-number</i> }  <b>Example:</b> Device(config-router-af)# af-interface gigabitethernet 0/0/1	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 8</b>	<b>passive-interface</b>  <b>Example:</b> 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.
<b>Step 9</b>	<b>bandwidth-percent</b> <i>maximum-bandwidth-percentage</i>  <b>Example:</b> 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.
<b>Step 10</b>	<b>exit-af-interface</b>  <b>Example:</b> Device(config-router-af-interface)# exit-af-interface	Exits address family interface configuration mode.
<b>Step 11</b>	<b>topology</b> { <b>base</b>   <i>topology-name tid number</i> }  <b>Example:</b> 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.
<b>Step 12</b>	<b>offset-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ] { <b>in</b>   <b>out</b> } <i>offset</i> [ <i>interface-type interface-number</i> ]  <b>Example:</b> Device(config-router-af-topology)# offset-list 21 in 10 gigabitethernet 6/2	(Optional) Applies an offset to routing metrics.
<b>Step 13</b>	<b>no auto-summary</b>  <b>Example:</b> Device(config-router-af-topology)# no auto-summary	(Optional) Disables automatic summarization.  <b>Note</b> Automatic summarization is enabled by default.
<b>Step 14</b>	<b>end</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> Device(config)# router eigrp 1	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>network</b> <i>ip-address [wildcard-mask]</i>  <b>Example:</b> Device(config-router)# network 172.16.0.0	Associates networks with an EIGRP routing process.
<b>Step 5</b>	<b>redistribute</b> <i>protocol</i>  <b>Example:</b> Device(config-router)# redistribute rip	Redistributes routes from one routing domain into another routing domain.
<b>Step 6</b>	<b>distance eigrp</b> <i>internal-distance external-distance</i>  <b>Example:</b> Device(config-router)# distance eigrp 80 130	Allows the use of two administrative distances—internal and external.
<b>Step 7</b>	<b>default-metric</b> <i>bandwidth delay reliability loading mtu</i>  <b>Example:</b> Device(config-router)# default-metric 1000 100 250 100 1500	Sets metrics for EIGRP.
<b>Step 8</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> 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.
<b>Step 4</b>	<b>no auto-summary</b>  <b>Example:</b> Device(config-router)# no auto-summary	Disables automatic summarization of subnet routes into network-level routes
<b>Step 5</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits router configuration mode.

	Command or Action	Purpose
<b>Step 6</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/3	Enters interface configuration mode.
<b>Step 7</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode
<b>Step 8</b>	<b>bandwidth</b> <i>kpbs</i>  <b>Example:</b> bandwidth 56	Sets the inherited and received bandwidth values for an interface
<b>Step 9</b>	<b>ip summary-address eigrp</b> <i>as-number ip-address mask</i> <i>[admin-distance] [leak-map name]</i>  <b>Example:</b> Device(config-if)# ip summary-address eigrp 100 10.0.0.0 0.0.0.0	(Optional) Configures a summary aggregate address.
<b>Step 10</b>	<b>ip bandwidth-percent eigrp</b> <i>as-number percent</i>  <b>Example:</b> Device(config-if)# ip bandwidth-percent eigrp 209 75	(Optional) Configures the percentage of bandwidth that may be used by EIGRP on an interface.
<b>Step 11</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following:  • <b>address-family ipv4</b> [ <b>multicast</b> ] [ <b>unicast</b> ] [ <b>vrf vrf-name</b> ] <b>autonomous-system</b> <i>autonomous-system-number</i>  • <b>address-family ipv6</b> [ <b>unicast</b> ] [ <b>vrf vrf-name</b> ] <b>autonomous-system</b> <i>autonomous-system-number</i>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>af-interface</b> {default   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# af-interface gigabitethernet 0/0/1</pre>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<p><b>summary-address</b> <i>ip-address mask [administrative-distance [leak-map leak-map-name]]</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# summary-address 192.168.0.0 255.255.0.0</pre>	Configures a summary address for EIGRP.
<b>Step 7</b>	<p><b>exit-af-interface</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# exit-af-interface</pre>	Exits address family interface configuration mode.
<b>Step 8</b>	<p><b>topology</b> {base   <i>topology-name tid number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.
<b>Step 9</b>	<p><b>summary-metric</b> <i>network-address subnet-mask bandwidth delay reliability load mtu</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# summary-metric 192.168.0.0/16 10000 10 255 1 1500</pre>	(Optional) Configures a fixed metric for an EIGRP summary aggregate address.
<b>Step 10</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# end</pre>	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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp <i>autonomous-system</i></b>  <b>Example:</b> Device(config)# router eigrp 101	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
Step 4	<b>eigrp event-log-size <i>size</i></b>  <b>Example:</b> Device(config-router)# eigrp event-log-size 5000010	(Optional) Sets the size of the EIGRP event log.
Step 5	<b>eigrp log-neighbor-changes</b>  <b>Example:</b> Device(config-router)# eigrp log-neighbor-changes	(Optional) Enables logging of EIGRP neighbor adjacency changes. <ul style="list-style-type: none"> <li>• By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.</li> </ul>

	Command or Action	Purpose
<b>Step 6</b>	<b>eigrp log-neighbor-warnings</b> <i>[seconds]</i>  <b>Example:</b>  Device(config-router)# eigrp log-neighbor-warnings 300	(Optional) Enables the logging of EIGRP neighbor warning messages.
<b>Step 7</b>	<b>end</b>  <b>Example:</b>  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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>



	Command or Action	Purpose
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>router eigrp</b> <i>virtual-instance-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp virtual-name1</pre>	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	<p>Enter one of the following:</p> <ul style="list-style-type: none"> <li><b>address-family ipv4</b> [multicast] [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li><b>address-family ipv6</b> [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
<b>Step 5</b>	<p><b>eigrp log-neighbor-warnings</b> [<i>seconds</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# eigrp log-neighbor-warnings 300</pre>	(Optional) Enables the logging of EIGRP neighbor warning messages.
<b>Step 6</b>	<p><b>eigrp log-neighbor-changes</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# eigrp log-neighbor-changes</pre>	<p>(Optional) Enables logging of EIGRP neighbor adjacency changes.</p> <ul style="list-style-type: none"> <li>By default, the system logs EIGRP neighbor adjacency changes to help you monitor the stability of the routing system and detect problems.</li> </ul>
<b>Step 7</b>	<p><b>topology</b> {base   <i>topology-name tid number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

	Command or Action	Purpose
<b>Step 8</b>	<b>eigrp event-log-size</b> <i>size</i>  <b>Example:</b> Device(config-router-af-topology)# eigrp event-log-size 10000	(Optional) Sets the size of the EIGRP event log.
<b>Step 9</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system</i>  <b>Example:</b> Device(config)# router eigrp 101	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>traffic-share</b> <b>balanced</b>  <b>Example:</b> Device(config-router)# traffic-share balanced	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.
<b>Step 5</b>	<b>maximum-paths</b> <i>number-of-paths</i>  <b>Example:</b> Device(config-router)# maximum-paths 5	Controls the maximum number of parallel routes that an IP routing protocol can support.
<b>Step 6</b>	<b>variance</b> <i>multiplier</i>  <b>Example:</b> Device(config-router)# variance 1	Controls load balancing in an internetwork based on EIGRP.
<b>Step 7</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>topology</b> {<b>base</b>   <i>topology-name</i> <b>tid</b> <i>number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# topology base</pre>	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.
<b>Step 6</b>	<p><b>traffic-share</b> <b>balanced</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# traffic-share balanced</pre>	Controls how traffic is distributed among routes when multiple routes for the same destination network have different costs.
<b>Step 7</b>	<p><b>maximum-paths</b> <i>number-of-paths</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# maximum-paths 5</pre>	Controls the maximum number of parallel routes that an IP routing protocol can support.
<b>Step 8</b>	<p><b>variance</b> <i>multiplier</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# variance 1</pre>	Controls load balancing in an internetwork based on EIGRP.
<b>Step 9</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-topology)# end</pre>	Exits address family topology configuration mode and returns to privileged EXEC mode.

## 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/9	Configures an interface type and enters interface configuration mode.
<b>Step 4</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode
<b>Step 5</b>	<b>ip authentication mode eigrp</b> <i>autonomous-system md5</i>  <b>Example:</b> Device(config-if)# ip authentication mode eigrp 1 md5	Enables MD5 authentication in EIGRP packets.

	Command or Action	Purpose
<b>Step 6</b>	<b>ip authentication key-chain eigrp</b> <i>autonomous-system</i> <i>key-chain</i>  <b>Example:</b> Device(config-if)# ip authentication key-chain eigrp 1 keychain1	Enables authentication of EIGRP packets.
<b>Step 7</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits to global configuration mode.
<b>Step 8</b>	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Device(config)# key chain keychain1	Identifies a key chain and enters key chain configuration mode.
<b>Step 9</b>	<b>key</b> <i>key-id</i>  <b>Example:</b> Device(config-keychain)# key 1	Identifies the key number and enters key chain key configuration mode.
<b>Step 10</b>	<b>key-string</b> <i>text</i>  <b>Example:</b> Device(config-keychain-key)# key-string 0987654321	Identifies the key string.
<b>Step 11</b>	<b>accept-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.
<b>Step 12</b>	<b>send-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.
<b>Step 13</b>	<b>end</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>



	Command or Action	Purpose
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p><b>router eigrp</b> <i>virtual-instance-name</i></p> <p><b>Example:</b></p> <pre>Device(config)# router eigrp virtual-name1</pre>	Enables an EIGRP routing process and enters router configuration mode.
Step 4	<p>Enter one of the following:</p> <ul style="list-style-type: none"> <li><b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li><b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
Step 5	<p><b>network</b> <i>ip-address</i> [<i>wildcard-mask</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# network 172.16.0.0</pre>	Associates networks with an EIGRP routing process.
Step 6	<p><b>af-interface</b> {<b>default</b>   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
Step 7	<p><b>authentication key-chain</b> <i>name-of-chain</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# authentication key-chain SITE1</pre>	Specifies an authentication key chain for EIGRP.
Step 8	<p><b>authentication mode</b> {<b>hmac-sha-256</b> <i>encryption-type password</i>   <b>md5</b>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# authentication mode md5</pre>	Specifies the type of authentication used in an EIGRP address family for the EIGRP instance.

	Command or Action	Purpose
<b>Step 9</b>	<b>exit-af-interface</b>  <b>Example:</b> Device(config-router-af-interface)# exit-af-interface	Exits address family interface configuration mode.
<b>Step 10</b>	<b>exit-address-family</b>  <b>Example:</b> Device(config-router-af)# exit-address-family	Exits address family configuration mode.
<b>Step 11</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits router configuration mode and returns to global configuration mode.
<b>Step 12</b>	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Device(config)# key chain keychain1	Identifies a key chain and enters key chain configuration mode.
<b>Step 13</b>	<b>key</b> <i>key-id</i>  <b>Example:</b> Device(config-keychain)# key 1	Identifies the key number and enters key chain key configuration mode.
<b>Step 14</b>	<b>key-string</b> <i>text</i>  <b>Example:</b> Device(config-keychain-key)# key-string 0987654321	Identifies the key string.
<b>Step 15</b>	<b>accept-lifetime</b> <i>start-time</i> {infinite   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.
<b>Step 16</b>	<b>send-lifetime</b> <i>start-time</i> {infinite   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.

	Command or Action	Purpose
Step 17	<b>end</b>  <b>Example:</b> Device(config-keychain-key)# end	Exits key chain key 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config)# router eigrp 101	Enables an EIGRP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>• A maximum of 30 EIGRP routing processes can be configured.</li> </ul>
<b>Step 4</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits to global configuration mode.
<b>Step 5</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/9	Enters interface configuration mode.
<b>Step 6</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode
<b>Step 7</b>	<b>ip hello-interval eigrp</b> <i>autonomous-system-number seconds</i>  <b>Example:</b> Device(config-if)# ip hello-interval eigrp 109 10	Configures the hello interval for an EIGRP routing process.
<b>Step 8</b>	<b>ip hold-time eigrp</b> <i>autonomous-system-number seconds</i>  <b>Example:</b> Device(config-if)# ip hold-time eigrp 109 40	Configures the hold time for an EIGRP routing process.  <b>Note</b> Do not adjust the hold time without consulting your technical support personnel.
<b>Step 9</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	<p>Enter one of the following:</p> <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [multicast] [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
<b>Step 5</b>	<p><b>af-interface</b> {default   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# af-interface gigabitethernet 0/0/1</pre>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<p><b>hello-interval</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# hello-interval 10</pre>	Configures the hello interval for an EIGRP address family named configuration.
<b>Step 7</b>	<p><b>hold-time</b> <i>seconds</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# hold-time 50</pre>	Configures the hold time for an EIGRP address family named configuration.
<b>Step 8</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# end</pre>	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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>type number</i></b>  <b>Example:</b> Device(config)# interface gigabitethernet 0/1	Configures an interface and enters interface configuration mode.
<b>Step 4</b>	<b>no ip split-horizon eigrp <i>autonomous-system-number</i></b>  <b>Example:</b> Device(config-if)# no ip split-horizon eigrp 101	Disables split horizon.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.



	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	
<b>Step 5</b>	<p><b>af-interface</b> {<b>default</b>   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# af-interface gigabitethernet 0/0/1</pre>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 6</b>	<p><b>no split-horizon</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# no split-horizon</pre>	Disables EIGRP split horizon.
<b>Step 7</b>	<p><b>no next-hop-self [no-ecmp-mode]</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# no next-hop-self no-ecmp-mode</pre>	<p>(Optional) Instructs an EIGRP router to use the received next hop rather than the local outbound interface address as the next hop.</p> <ul style="list-style-type: none"> <li>The <b>no-ecmp-mode</b> keyword is an enhancement to the <b>no next-hop-self</b> 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.</li> </ul>
<b>Step 8</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# end</pre>	Exits address family interface configuration mode and returns to privileged EXEC mode.

## 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config)# router eigrp 1	Configures a remote or distribution device to run an EIGRP process and enters router configuration mode.
<b>Step 4</b>	<b>network</b> <i>ip-address</i> [ <b>wildcard-mask</b> ]  <b>Example:</b> Device(config-router)# network 172.16.0.0	Specifies the network address of the EIGRP distribution device.
<b>Step 5</b>	<b>eigrp stub</b> [ <b>receive-only</b> ] [ <b>leak-map</b> <i>name</i> ] [ <b>connected</b> ] [ <b>static</b> ] [ <b>summary</b> ] [ <b>redistributed</b> ]  <b>Example:</b> Device(config-router)# eigrp stub connected static	Configures a remote device as an EIGRP stub device.

	Command or Action	Purpose
Step 6	<b>end</b>  <b>Example:</b> Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 7	<b>show ip eigrp neighbors</b> [ <i>interface-type</i>   <i>as-number</i>   <b>static</b>   <b>detail</b> ]  <b>Example:</b> Device# show ip eigrp neighbors detail	(Optional) Verifies that a remote device has been configured as a stub device with EIGRP. <ul style="list-style-type: none"> <li>• Enter this command on the distribution device. The last line of the output displays the stub status of the remote or spoke device.</li> </ul>

## 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
Step 4	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b> 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	<b>network</b> <i>ip-address</i> [ <b>wildcard-mask</b> ]  <b>Example:</b> Device(config-router-af)# network 172.16.0.0	Specifies the network address of the EIGRP distribution device.
Step 6	<b>eigrp stub</b> [ <b>receive-only</b> ] [ <b>leak-map</b> <i>name</i> ] [ <b>connected</b> ] [ <b>static</b> ] [ <b>summary</b> ] [ <b>redistributed</b> ]  <b>Example:</b> Device(config-router-af) eigrp stub leak-map map1	Configures a device as a stub using EIGRP.
Step 7	<b>exit-address-family</b>  <b>Example:</b> Device(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 8	<b>end</b>  <b>Example:</b> Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.
Step 9	<b>show eigrp address-family</b> { <b>ipv4</b>   <b>ipv6</b> } [ <b>vrf vrf-name</b> ] [ <b>autonomous-system-number</b> ] [ <b>multicast</b> ] [ <b>neighbors</b> ] [ <b>static</b> ] [ <b>detail</b> ] [ <b>interface-type interface-number</b> ]	(Optional) Displays neighbors discovered by EIGRP.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device# show eigrp address-family ipv4 neighbors detail</pre>	

## 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: Enabling EIGRP IPv6 VRF-Lite—Named Configuration

```
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
```

## 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: 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
!
!
```

## 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 GigabitEthernet 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: 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
```

## 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

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
CEF commands	<i>Cisco IOS IP Switching Command Reference</i>
EIGRP commands	<i>Cisco IOS IP Routing: EIGRP Command Reference</i>
NSF with SSO deployment	<a href="#">Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide</a>

**Standards**

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

**MIBs**

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFCs**

RFCs	Title
RFC 4724	<i>Graceful Restart Mechanism for BGP</i>

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 6: Feature Information for Configuring EIGRP**

Feature Name	Releases	Feature Information
EIGRP Dual DMVPN Domain Enhancement	Cisco IOS XE Release 3.3SE Cisco IOS XE Release 3.5E	<p>The EIGRP Dual DMVPN Domain Enhancement feature supports the no next-hop-self functionality on dual DMVPN domains in both IPv4 and IPv6 configurations.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified by this feature:  <b>ip next-hop-self eigrp,</b>  <b>ipv6 next-hop self eigrp,next-hop-self, show ip eigrp interfaces, show ipv6 eigrp interfaces, show ip eigrp topology, show ipv6 eigrp topology.</b></p>







## 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, page 133](#)
- [Restrictions for IPv6 Routing EIGRP Support, page 133](#)
- [Information About IPv6 Routing EIGRP Support, page 134](#)
- [How to Configure IPv6 Routing EIGRP Support, page 136](#)
- [Configuration Examples for IPv6 Routing EIGRP Support, page 152](#)
- [Additional References, page 152](#)
- [Feature Information for IPv6 Routing: EIGRP Support, page 154](#)

### 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](http://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. **router-id** *{ip-address | ipv6-address}*
10. **exit**
11. **show ipv6 eigrp** [*as-number*] **interfaces** [*type number*] [*as-number*]

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 unicast-routing</b>  <b>Example:</b> Device(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.

	Command or Action	Purpose
<b>Step 4</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is to be configured.
<b>Step 5</b>	<b>no shut</b>  <b>Example:</b> Device(config-if)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 6</b>	<b>ipv6 enable</b>  <b>Example:</b> Device(config-if)# ipv6 enable	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
<b>Step 7</b>	<b>ipv6 eigrp</b> <i>as-number</i>  <b>Example:</b> Device(config-if)# ipv6 eigrp 1	Enables EIGRP for IPv6 on a specified interface.
<b>Step 8</b>	<b>ipv6 router eigrp</b> <i>as-number</i>  <b>Example:</b> Device(config-if)# ipv6 router eigrp 1	Enters router configuration mode and creates an EIGRP IPv6 routing process.
<b>Step 9</b>	<b>router-id</b> <i>{ip-address   ipv6-address}</i>  <b>Example:</b> Device(config-router)# 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.
<b>Step 10</b>	<b>exit</b>  <b>Example:</b> Device(config-router) exit	Enter three times to return to privileged EXEC mode.
<b>Step 11</b>	<b>show ipv6 eigrp</b> [ <i>as-number</i> ] <b>interfaces</b> [ <i>type number</i> ] [ <i>as-number</i> ]  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>ipv6 bandwidth-percent eigrp</b> <i>as-number percent</i>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>ipv6 summary-address eigrp</b> <i>as-number ipv6-address [admin-distance]</i>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>ipv6 authentication mode eigrp</b> <i>as-number</i> <b>md5</b>  <b>Example:</b> Device(config-if)# ipv6 authentication mode eigrp 1 md5	Specifies the type of authentication used in EIGRP for IPv6 packets.
<b>Step 6</b>	<b>ipv6 authentication key-chain eigrp</b> <i>as-number key-chain</i>  <b>Example:</b> Device(config-if)# ipv6 authentication key-chain eigrp 1 chain1	Enables authentication of EIGRP for IPv6 packets.
<b>Step 7</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits to global configuration mode.
<b>Step 8</b>	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Device(config)# key chain chain1	Identifies a group of authentication keys. <ul style="list-style-type: none"> <li>• Use the name specified in Step 5.</li> </ul>
<b>Step 9</b>	<b>key</b> <i>key-id</i>  <b>Example:</b> Device(config-keychain)# key 1	Identifies an authentication key on a key chain.
<b>Step 10</b>	<b>key-string</b> <i>text</i>  <b>Example:</b> Device(config-keychain-key)# key-string chain 1	Specifies the authentication string for a key.

	Command or Action	Purpose
<b>Step 11</b>	<b>accept-lifetime</b> <i>start-time</i> <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>  <b>Example:</b>  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.
<b>Step 12</b>	<b>send-lifetime</b> <i>start-time</i> <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>  <b>Example:</b>  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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b>  Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>no ipv6 next-hop-self eigrp</b> <i>as-number</i>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>interface <i>type number</i></b>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
Step 4	<b>ipv6 hello-interval eigrp <i>as-number seconds</i></b>  <b>Example:</b> 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	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<b>Example:</b> Device> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface type number</b>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>ipv6 hold-time eigrp as-number seconds</b>  <b>Example:</b> 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**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Device(config)# interface GigabitEthernet 0/0/0	Specifies the interface on which EIGRP is configured.
<b>Step 4</b>	<b>no shut</b>  <b>Example:</b> Device(config)# no shut	Enables no shut mode so the routing process can start running.
<b>Step 5</b>	<b>no ipv6 split-horizon eigrp</b> <i>as-number</i>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 router eigrp <i>as-number</i></b>  <b>Example:</b> Device(config)# ipv6 router eigrp 1	Specifies the EIGRP for IPv6 routing process to be configured.
<b>Step 4</b>	<b>eigrp stub receive-only   leak-map   connected   static   summary   redistributed</b>  <b>Example:</b> 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
<b>Step 1</b>	<p><code>enable</code></p> <p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><code>show ipv6 eigrp neighbors detail interface-type   as-number   static</code></p> <p><b>Example:</b></p> <pre>Device# show ipv6 eigrp neighbors detail</pre>	<p>Displays the neighbors discovered by EIGRP for IPv6.</p> <p>This command is performed on the distribution layer device to view the status of the remote device.</p>

## 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>ipv6 router eigrp <i>as-number</i></b>  <b>Example:</b> Device(config)# ipv6 router eigrp 1	Specifies the EIGRP for IPv6 routing process to be configured.
Step 4	<b>eigrp log-neighbor-changes</b>  <b>Example:</b> 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	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<p><b>ipv6 router eigrp <i>as-number</i></b></p> <p><b>Example:</b></p> <pre>Device(config)# ipv6 router eigrp 1</pre>	Specifies the EIGRP for IPv6 routing process to be configured.
<b>Step 4</b>	<p><b>eigrp log-neighbor-warnings [<i>seconds</i>]</b></p> <p><b>Example:</b></p> <pre>Device(config-router)# eigrp log-neighbor-warnings 300</pre>	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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 router eigrp</b> <i>as-number</i>  <b>Example:</b> Device(config)# ipv6 router eigrp 1	Specifies the EIGRP for IPv6 routing process to be configured.
<b>Step 4</b>	<b>metric weights</b> <i>tos k1 k2 k3 k4 k5</i>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>clear ipv6 eigrp</b> [ <i>as-number</i> ] [ <b>neighbor</b> [ <i>ipv6-address</i>   <i>interface-type interface-number</i> ] ]  <b>Example:</b> 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	<a href="#">Cisco IOS Master Commands List, All Releases</a>
CEF commands	<i>Cisco IOS IP Switching Command Reference</i>
EIGRP commands	<i>Cisco IOS IP Routing: EIGRP Command Reference</i>

Related Topic	Document Title
NSF with SSO deployment	<a href="#">Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide</a>

### Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

### MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
RFC 4724	<i>Graceful Restart Mechanism for BGP</i>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 7: Feature Information for IPv6 Routing: EIGRP Support**

Feature Name	Releases	Feature Information
IPv6 Routing: EIGRP Support	Cisco IOS XE Release 3.5E	<p>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.</p> <p>The following commands were introduced or modified:</p> <p><b>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.</b></p>

Feature Name	Releases	Feature Information
EIGRP IPv6 VRF Lite	Cisco IOS XE Release 3.6E	<p>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.</p> <p>The EIGRP IPv6 VRF Lite feature is available only in EIGRP named configurations.</p> <p>There are no new or modified commands for this feature.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>







## 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, page 157](#)
- [Information About EIGRP Stub Routing, page 158](#)
- [How to Configure EIGRP Stub Routing, page 162](#)
- [Configuration Examples for EIGRP Stub Routing, page 165](#)
- [Additional References, page 168](#)
- [Feature Information for EIGRP Stub Routing, page 168](#)

### 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](http://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.

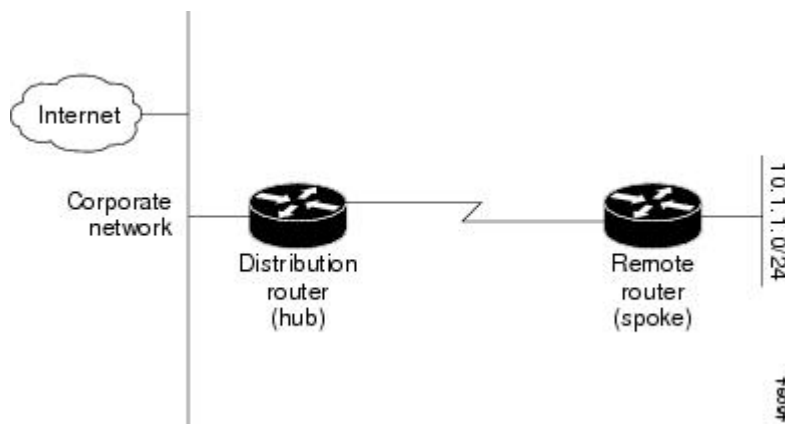
Stub routing is commonly used in hub-and-spoke network topologies. In a hub-and-spoke network, one or more end (stub) networks are connected to a remote device (the spoke) that is connected to one or more distribution devices (the hub). The remote device is adjacent to one or more distribution devices. 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 10: 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.

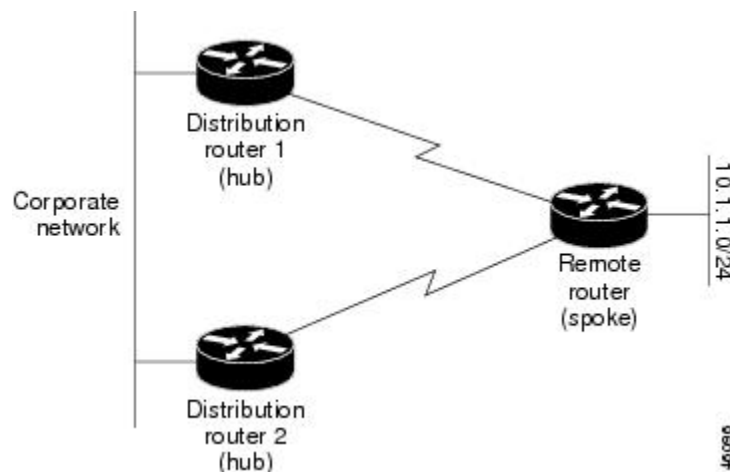
Without the EIGRP stub routing feature, even after routes that are sent from the distribution device to the remote device have been filtered or summarized, a problem might occur. If a route is lost somewhere in the corporate network, EIGRP could send a query to the distribution device, which in turn 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.

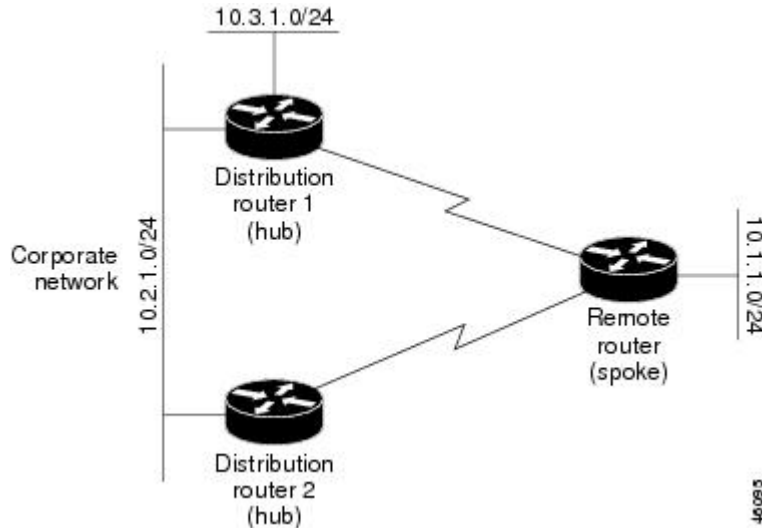
**Figure 11: Simple Dual-Homed Remote Topology**



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 12: Dual-Homed Remote Topology with Distribution Device 1 Connected to Two Networks**

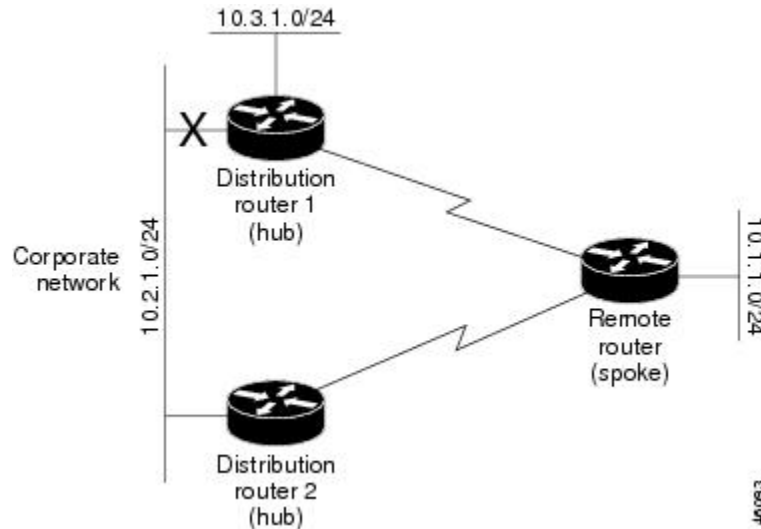


The figure above shows a simple dual-homed remote topology, where distribution Device 1 is connected to both network 10.3.1.0/24 and network 10.2.1.0/24.

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 13: 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config)# router eigrp 1	Configures a remote or distribution device to run an EIGRP process and enters router configuration mode.
<b>Step 4</b>	<b>network</b> <i>ip-address</i> [ <b>wildcard-mask</b> ]  <b>Example:</b> Device(config-router)# network 172.16.0.0	Specifies the network address of the EIGRP distribution device.

	Command or Action	Purpose
<b>Step 5</b>	<b>eigrp stub</b> [receive-only] [leak-map <i>name</i> ] [connected] [static] [summary] [redistributed]  <b>Example:</b> <pre>Device(config-router)# eigrp stub connected static</pre>	Configures a remote device as an EIGRP stub device.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> <pre>Device(config-router)# end</pre>	Exits router configuration mode and returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ip eigrp neighbors</b> [ <i>interface-type</i>   <i>as-number</i>   static   detail]  <b>Example:</b> <pre>Device# show ip eigrp neighbors detail</pre>	(Optional) Verifies that a remote device has been configured as a stub device with EIGRP. <ul style="list-style-type: none"> <li>Enter this command on the distribution device. The last line of the output displays the stub status of the remote or spoke device.</li> </ul>

## Configuring the EIGRP Stub Routing Named Configuration

### SUMMARY STEPS

- enable**
- configure terminal**
- router eigrp** *virtual-instance-name*
- 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*
- network** *ip-address* [wildcard-mask]
- eigrp stub** [receive-only] [leak-map *name*] [connected] [static] [summary] [redistributed]
- exit-address-family**
- end**
- 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.
Step 4	Enter one of the following: <ul style="list-style-type: none"> <li>• <b>address-family ipv4</b> [<b>multicast</b>] [<b>unicast</b>] [<b>vrf vrf-name</b>]  <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li>• <b>address-family ipv6</b> [<b>unicast</b>] [<b>vrf vrf-name</b>]  <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <b>Example:</b> 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	<b>network</b> <i>ip-address</i> [ <b>wildcard-mask</b> ]  <b>Example:</b> Device(config-router-af)# network 172.16.0.0	Specifies the network address of the EIGRP distribution device.
Step 6	<b>eigrp stub</b> [ <b>receive-only</b> ] [ <b>leak-map</b> <i>name</i> ] [ <b>connected</b> ] [ <b>static</b> ] [ <b>summary</b> ] [ <b>redistributed</b> ]  <b>Example:</b> Device(config-router-af) eigrp stub leak-map map1	Configures a device as a stub using EIGRP.
Step 7	<b>exit-address-family</b>  <b>Example:</b> Device(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 8	<b>end</b>  <b>Example:</b> Device(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.



	Command or Action	Purpose
Step 9	<pre>show eigrp address-family {ipv4   ipv6} [vrf vrf-name] [autonomous-system-number] [multicast] [neighbors] [static] [detail] [interface-type interface-number]</pre> <p><b>Example:</b></p> <pre>Device# show eigrp address-family ipv4 neighbors detail</pre>	(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	<a href="#">Cisco IOS Master Command List, All Releases</a>
EIGRP commands	<a href="#">Cisco IOS IP Routing: EIGRP Command Reference</a>
EIGRP FAQ	<a href="#">EIGRP Frequently Asked Questions</a>
EIGRP Technology White Papers	<a href="#">Enhanced Interior Gateway Routing Protocol</a>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/cisco/featurenavigator](#). An account on Cisco.com is not required.

**Table 8: Feature Information for EIGRP Stub Routing**

Feature Name	Releases	Feature Information
EIGRP Stub Routing	Cisco IOS XE Release 3.3SE Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p>The following command was introduced or modified: <b>eigrp stub</b>.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>





## 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, page 171](#)
- [Information About EIGRP IPv6 VRF-Lite, page 172](#)
- [How to Configure EIGRP IPv6 VRF-Lite, page 173](#)
- [Configuration Examples for EIGRP IPv6 VRF-Lite, page 174](#)
- [Additional References, page 174](#)
- [Feature Information for EIGRP IPv6 VRF-Lite, page 175](#)

## 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](http://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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Configures the EIGRP routing process and enters router configuration mode.
<b>Step 4</b>	<b>address-family ipv6 vrf</b> <i>vrf-name</i> <b>autonomous-system</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config-router)# address-family ipv6 vrf vrf1 autonomous-system 45000	Enables EIGRP IPv6 VRF-Lite and enters address family configuration mode.
<b>Step 5</b>	<b>end</b>  <b>Example:</b> 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	<a href="#">Cisco IOS Master Command List, All Releases</a>
EIGRP commands	<a href="#">Cisco IOS IP Routing: EIGRP Command Reference</a>
EIGRP FAQ	<a href="#">EIGRP Frequently Asked Questions</a>
EIGRP Technology White Papers	<a href="#">Enhanced Interior Gateway Routing Protocol</a>

**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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 9: Feature Information for EIGRP IPv6 VRF-Lite**

Feature Name	Releases	Feature Information
EIGRP IPv6 VRF-Lite	Cisco IOS XE Release 3.3SE	<p>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.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p><b>Note</b> The EIGRP IPv6 VRF-Lite feature is available only in EIGRP named configurations. There are no new or modified commands for this feature.</p>





## CHAPTER 6

# 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, page 177](#)
- [Information About IP EIGRP Route Authentication, page 177](#)
- [How to Configure IP EIGRP Route Authentication, page 178](#)
- [Configuration Examples for IP EIGRP Route Authentication, page 184](#)
- [Additional References, page 186](#)
- [Feature Information for IP EIGRP Route Authentication, page 187](#)

## 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](http://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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b>  Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>interface type number</b>  <b>Example:</b> Device(config)# interface GigabitEthernet 1/0/9	Configures an interface type and enters interface configuration mode.
<b>Step 4</b>	<b>no switchport</b>  <b>Example:</b> Device(config-if)# no switchport	Puts an interface into Layer 3 mode
<b>Step 5</b>	<b>ip authentication mode eigrp autonomous-system md5</b>  <b>Example:</b> Device(config-if)# ip authentication mode eigrp 1 md5	Enables MD5 authentication in EIGRP packets.
<b>Step 6</b>	<b>ip authentication key-chain eigrp autonomous-system key-chain</b>  <b>Example:</b> Device(config-if)# ip authentication key-chain eigrp 1 keychain1	Enables authentication of EIGRP packets.
<b>Step 7</b>	<b>exit</b>  <b>Example:</b> Device(config-if)# exit	Exits to global configuration mode.
<b>Step 8</b>	<b>key chain name-of-chain</b>  <b>Example:</b> Device(config)# key chain keychain1	Identifies a key chain and enters key chain configuration mode.
<b>Step 9</b>	<b>key key-id</b>  <b>Example:</b> Device(config-keychain)# key 1	Identifies the key number and enters key chain key configuration mode.

	Command or Action	Purpose
<b>Step 10</b>	<p><b>key-string</b> <i>text</i></p> <p><b>Example:</b></p> <pre>Device(config-keychain-key)# key-string 0987654321</pre>	Identifies the key string.
<b>Step 11</b>	<p><b>accept-lifetime</b> <i>start-time</i> {<b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>}</p> <p><b>Example:</b></p> <pre>Device(config-keychain-key)# accept-lifetime 04:00:00 Jan 4 2007 infinite</pre>	(Optional) Specifies the time period during which the key can be received.
<b>Step 12</b>	<p><b>send-lifetime</b> <i>start-time</i> {<b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>}</p> <p><b>Example:</b></p> <pre>Device(config-keychain-key)# send-lifetime 04:00:00 Dec 4 2006 infinite</pre>	(Optional) Specifies the time period during which the key can be sent.
<b>Step 13</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Device(config-keychain-key)# end</pre>	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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp</b> <i>virtual-instance-name</i>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Enables an EIGRP routing process and enters router configuration mode.

	Command or Action	Purpose
<b>Step 4</b>	<p>Enter one of the following:</p> <ul style="list-style-type: none"> <li><b>address-family ipv4</b> [multicast] [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> <li><b>address-family ipv6</b> [unicast] [vrf <i>vrf-name</i>] <b>autonomous-system</b> <i>autonomous-system-number</i></li> </ul> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 autonomous-system 45000  Device(config-router)# address-family ipv6 autonomous-system 45000</pre>	Enters address family configuration mode to configure an EIGRP IPv4 or IPv6 routing instance.
<b>Step 5</b>	<p><b>network</b> <i>ip-address</i> [<i>wildcard-mask</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# network 172.16.0.0</pre>	Associates networks with an EIGRP routing process.
<b>Step 6</b>	<p><b>af-interface</b> {<b>default</b>   <i>interface-type interface-number</i>}</p> <p><b>Example:</b></p>	Enters address family interface configuration mode and configures interface-specific EIGRP commands.
<b>Step 7</b>	<p><b>authentication key-chain</b> <i>name-of-chain</i></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# authentication key-chain SITE1</pre>	Specifies an authentication key chain for EIGRP.
<b>Step 8</b>	<p><b>authentication mode</b> {<b>hmac-sha-256</b> <i>encryption-type password</i>   <b>md5</b>}</p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# authentication mode md5</pre>	Specifies the type of authentication used in an EIGRP address family for the EIGRP instance.
<b>Step 9</b>	<p><b>exit-af-interface</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af-interface)# exit-af-interface</pre>	Exits address family interface configuration mode.
<b>Step 10</b>	<p><b>exit-address-family</b></p> <p><b>Example:</b></p> <pre>Device(config-router-af)# exit-address-family</pre>	Exits address family configuration mode.

	Command or Action	Purpose
<b>Step 11</b>	<b>exit</b>  <b>Example:</b> Device(config-router)# exit	Exits router configuration mode and returns to global configuration mode.
<b>Step 12</b>	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Device(config)# key chain keychain1	Identifies a key chain and enters key chain configuration mode.
<b>Step 13</b>	<b>key</b> <i>key-id</i>  <b>Example:</b> Device(config-keychain)# key 1	Identifies the key number and enters key chain key configuration mode.
<b>Step 14</b>	<b>key-string</b> <i>text</i>  <b>Example:</b> Device(config-keychain-key)# key-string 0987654321	Identifies the key string.
<b>Step 15</b>	<b>accept-lifetime</b> <i>start-time</i> {infinite   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.
<b>Step 16</b>	<b>send-lifetime</b> <i>start-time</i> {infinite   <i>end-time</i>   <b>duration</b> <i>seconds</i> }  <b>Example:</b> 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.
<b>Step 17</b>	<b>end</b>  <b>Example:</b> Device(config-keychain-key)# end	Exits key chain key configuration mode and returns to privileged EXEC mode.

# 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	<a href="#">Cisco IOS Master Command List, All Releases</a>
EIGRP commands	<a href="#">Cisco IOS IP Routing: EIGRP Command Reference</a>
EIGRP FAQ	<a href="#">EIGRP Frequently Asked Questions</a>
EIGRP Technology White Papers	<a href="#">Enhanced Interior Gateway Routing Protocol</a>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 10: Feature Information for IP EIGRP Route Authentication**

Feature Name	Releases	Feature Information
IP Enhanced IGRP Route Authentication	Cisco IOS XE Release 3.3SE Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified:</p> <p><b>ip authentication key-chain eigrp,</b> <b>ip authentication mode eigrp,</b> <b>show ip eigrp interfaces.</b></p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p>







## 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](#), page 189
- [Prerequisites for EIGRP Nonstop Forwarding](#), page 190
- [Restrictions for EIGRP Nonstop Forwarding](#), page 190
- [Information About EIGRP Nonstop Forwarding](#), page 190
- [How to Configure EIGRP Nonstop Forwarding](#), page 192
- [Configuration Examples for EIGRP Nonstop Forwarding](#), page 195
- [Additional References](#), page 196
- [Feature Information for EIGRP Nonstop Forwarding](#), 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](http://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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp as-number</b>  <b>Example:</b> Device(config)# router eigrp 109	Enables an EIGRP routing process and enters router configuration mode.
Step 4	<b>nsf</b>  <b>Example:</b> Device(config-router)# nsf	Enables NSF capabilities. <ul style="list-style-type: none"> <li>• This command is enabled by default. To disable nonstop forwarding capability, use the <b>no</b> form of this command.</li> </ul>
Step 5	<b>timers nsf converge seconds</b>  <b>Example:</b> 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. <ul style="list-style-type: none"> <li>• Enter this command on NSF-capable devices only.</li> </ul>
Step 6	<b>timers nsf signal seconds</b>  <b>Example:</b> Device(config-router)# timers nsf signal 20	Use this optional command to adjust the maximum time for the initial restart period. <ul style="list-style-type: none"> <li>• Enter this command on NSF-capable devices only.</li> </ul>
Step 7	<b>timers graceful-restart purge-time seconds</b>  <b>Example:</b> 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	<b>end</b>  <b>Example:</b> Device(config-router)# end	Returns to privileged EXEC mode.
Step 9	<b>show ip protocols</b>  <b>Example:</b> 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	<a href="#">Master Commands List, All Releases</a>
EIGRP commands	<a href="#">IP Routing: EIGRP Command Reference</a>
EIGRP FAQ	<a href="#">EIGRP Frequently Asked Questions</a>
EIGRP L2/L3 API and Tunable Metric for Mobile Adhoc Networks feature	“Mobile Ad Hoc Networks for Router-to-Radio Communications” module of <i>the IP Mobility Configuration Guide</i>
EIGRP Technology Support	<a href="#">Enhanced Interior Gateway Routing Protocol</a>
EIGRP Technology White Papers	<a href="#">Enhanced Interior Gateway Routing Protocol</a>
IPv6 Routing EIGRP Support	<i>EIGRP Configuration Guide</i>
Protocol-independent features that work with EIGRP	<i>IP Routing: Protocol-Independent Configuration Guide</i>
Service Advertisement Framework	<i>Service Advertisement Framework Configuration Guide</i>
Service Advertisement Framework commands	<a href="#">Service Advertisement Framework Command Reference</a>

### Standards and RFCs

Standard/RFC	Title
FIPS PUB 180-2	<i>SECURE HASH STANDARD (SHS)</i>
RFC 1321	<i>The MD5 Message-Digest Algorithm</i>



Standard/RFC	Title
RFC 2104	<i>HMAC: Keyed-Hashing for Message Authentication</i>

#### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/cisco/web/featurenavigator/index.html](#). An account on Cisco.com is not required.

**Table 11: Feature Information for EIGRP Nonstop Forwarding**

Feature Name	Releases	Feature Information
NSF – EIGRP	Cisco IOS XE Release 3.3SE Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified: <b>debug ip eigrp notifications</b>, <b>nsf (EIGRP)</b>, <b>router eigrp</b>, and <b>show ip eigrp neighbors</b>.</p>



## 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, page 199](#)
- [Prerequisites for EIGRP Nonstop Forwarding Awareness, page 200](#)
- [Restrictions for EIGRP Nonstop Forwarding Awareness, page 200](#)
- [Information About EIGRP Nonstop Forwarding Awareness, page 200](#)
- [How to Configure EIGRP Nonstop Forwarding Awareness, page 203](#)
- [Configuration Examples for EIGRP Nonstop Forwarding Awareness, page 208](#)
- [Additional References for EIGRP Nonstop Forwarding Awareness, page 209](#)
- [Feature Information for EIGRP Nonstop Forwarding Awareness, page 210](#)

### 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](http://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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>router eigrp <i>virtual-instance-name</i></b>  <b>Example:</b> Device(config)# router eigrp virtual-name1	Configures an EIGRP routing process in classic mode and enters router configuration mode.
<b>Step 4</b>	<b>address-family ipv4 autonomous-system <i>number</i></b>  <b>Example:</b> Device(config-router)# address-family ipv4 autonomous-system 1	Enters address-family configuration mode to configure an EIGRP routing instance.
<b>Step 5</b>	<b>nsf</b>  <b>Example:</b> Device(config-router-af)# nsf	Enables NSF for the specific address family on the router.
<b>Step 6</b>	<b>end</b>  <b>Example:</b> 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	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router eigrp <i>name</i></b>  <b>Example:</b> Device(config)# router eigrp e1	Configures an EIGRP routing process and enters router configuration mode.
Step 4	<b>address-family ipv4 autonomous-system <i>number</i></b>  <b>Example:</b> Device(config-router)# address-family ipv4 autonomous-system 1	Enters address-family configuration mode to configure an EIGRP routing instance.
Step 5	<b>timers nsf signal <i>seconds</i></b>  <b>Example:</b> 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.

	Command or Action	Purpose
<b>Step 6</b>	<b>timers nsf converge <i>seconds</i></b>  <b>Example:</b> 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.
<b>Step 7</b>	<b>timers graceful-restart purge-time <i>seconds</i></b>  <b>Example:</b> 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.
<b>Step 8</b>	<b>end</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>debug eigrp nsf</b>  <b>Example:</b> Device# debug eigrp nsf	Displays NSF notifications and information about NSF events in an EIGRP network on the console of the router.
<b>Step 3</b>	<b>debug ip eigrp notifications</b>  <b>Example:</b> 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.
<b>Step 4</b>	<b>debug eigrp address-family ipv4 notifications</b>  <b>Example:</b> 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
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>show ip protocols</b>  <b>Example:</b> 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	<a href="#">Cisco IOS Master Command List, All Releases</a>
CEF commands	<i>Cisco IOS IP Switching Command Reference</i>
EIGRP commands	<i>Cisco IOS IP Routing: EIGRP Command Reference</i>
Nonstop forwarding (NSF)	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Nonstop Forwarding with Stateful Switchover Deployment Guide</a></li> <li>• “Cisco Nonstop Forwarding” module in <i>High Availability Configuration Guide</i></li> <li>• “EIGRP IPv6 NSF/GR” module in <i>IP Routing: EIGRP Configuration Guide</i></li> </ul>

### 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.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

**Table 12: Feature Information for EIGRP Nonstop Forwarding Awareness**

Feature Name	Releases	Feature Information
EIGRP Nonstop Forwarding (NSF) Awareness	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SE Cisco IOS XE Release 3.6E	<p>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.</p> <p>In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.</p> <p>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches.</p> <p>The following commands were introduced or modified: <b>debug eigrp nsf</b>, <b>debug ip eigrp notifications</b>, <b>show ip eigrp neighbors</b>, <b>show ip protocols</b>, <b>timers graceful-restart purge-time</b>, <b>timers nsf route-hold</b>.</p>