



Configuring EIGRP

- [Information About EIGRP, on page 1](#)
- [How to Configure EIGRP, on page 4](#)
- [Monitoring and Maintaining EIGRP, on page 11](#)

Information About EIGRP

Enhanced IGRP (EIGRP) is a Cisco proprietary enhanced version of the IGRP. EIGRP uses the same distance vector algorithm and distance information as IGRP; however, the convergence properties and the operating efficiency of EIGRP are significantly improved.

The convergence technology employs an algorithm referred to as the Diffusing Update Algorithm (DUAL), which guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.

IP EIGRP provides increased network width. With RIP, the largest possible width of your network is 15 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. EIGRP increments the transport control field only when an IP packet has traversed 15 routers and the next hop to the destination was learned through EIGRP. When a RIP route is used as the next hop to the destination, the transport control field is incremented as usual.

EIGRP Features

EIGRP offers these features:

- Fast convergence.
- Incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table, minimizing the bandwidth required for EIGRP packets.
- Less CPU usage because full update packets need not be processed each time they are received.
- Protocol-independent neighbor discovery mechanism to learn about neighboring routers.
- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.
- EIGRP scales to large networks.

EIGRP Components

EIGRP has these four basic components:

- Neighbor discovery and recovery is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery and recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can learn that a neighbor is alive and functioning. When this status is determined, the neighboring routers can exchange routing information.
- The reliable transport protocol is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably, and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet), it is not necessary to send hellos 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 shown in the packet. The reliable transport has a provision to send multicast packets quickly when there are unacknowledged packets pending. Doing so helps ensure that convergence time remains low in the presence of varying speed links.
- The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors, but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time it takes to recompute the route affects the convergence time. Recomputation is processor-intensive; it is advantageous to avoid recomputation if it is not necessary. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, it uses any it finds to avoid unnecessary recomputation.
- The protocol-dependent modules are responsible for network layer protocol-specific tasks. An example is the IP EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. EIGRP is also responsible for redistributing routes learned by other IP routing protocols.



Note To enable EIGRP, the Device or active switch must be running the Network Advantage license.

EIGRP Nonstop Forwarding

The Device stack supports two levels of EIGRP nonstop forwarding:

- EIGRP NSF Awareness
- EIGRP NSF Capability

EIGRP NSF Awareness

The Network Advantage license supports EIGRP NSF Awareness for IPv4. When the neighboring router is NSF-capable, the Layer 3 Device continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

This feature cannot be disabled. For more information on this feature, see the “EIGRP Nonstop Forwarding (NSF) Awareness” section of the *Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*.

EIGRP NSF Capability

The Network Advantage license supports EIGRP Cisco NSF routing to speed up convergence and to eliminate traffic loss after a stack's active switch changeover.

The Network Advantage license also supports EIGRP NSF-capable routing for IPv4 for better convergence and lower traffic loss following an active switch changeover. When an EIGRP NSF-capable active switch restarts or a new active switch starts up and NSF restarts, the Device has no neighbors, and the topology table is empty. The Device must bring up the interfaces, reacquire neighbors, and rebuild the topology and routing tables without interrupting the traffic directed toward the Device stack. EIGRP peer routers maintain the routes learned from the new active switch and continue forwarding traffic through the NSF restart process.

To prevent an adjacency reset by the neighbors, the new active switch uses a new Restart (RS) bit in the EIGRP packet header to show the restart. When the neighbor receives this, it synchronizes the stack in its peer list and maintains the adjacency with the stack. The neighbor then sends its topology table to the active switch with the RS bit set to show that it is NSF-aware and is aiding the new active switch.

If at least one of the stack peer neighbors is NSF-aware, the active switch receives updates and rebuilds its database. Each NSF-aware neighbor sends an end of table (EOT) marker in the last update packet to mark the end of the table content. The active switch recognizes the convergence when it receives the EOT marker, and it then begins sending updates. When the active switch has received all EOT markers from its neighbors or when the NSF converge timer expires, EIGRP notifies the routing information database (RIB) of convergence and floods its topology table to all NSF-aware peers.

EIGRP Stub Routing

The EIGRP stub routing feature reduces resource utilization by moving routed traffic closer to the end user.



Note The EIGRP stub routing capability advertises connected or summary routes from the routing tables to other device in the network. The device uses EIGRP stub routing at the access layer to eliminate the need for other types of routing advertisements. On a device running the Network Essentials license, if you try to configure multi-VRF-CE and EIGRP stub routing at the same time, the configuration is not allowed. IPv6 EIGRP stub routing is not supported with the Network Essentials license.

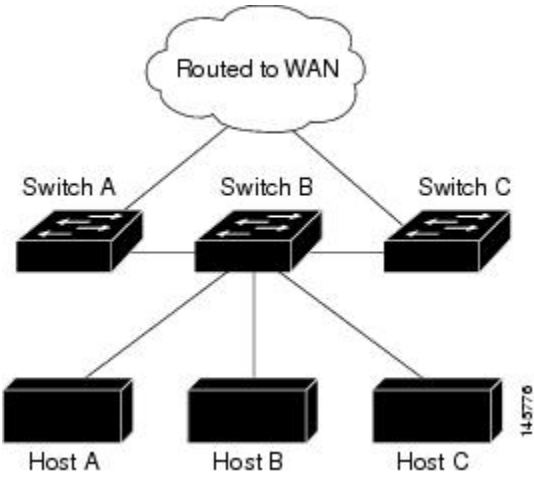
In a network using EIGRP stub routing, the only allowable route for IP traffic to the user is through a device that is configured with EIGRP stub routing. The device sends the routed traffic to interfaces that are configured as user interfaces or are connected to other devices.

When using EIGRP stub routing, you need to configure the distribution and remote routers to use EIGRP and to configure only the device as a stub. Only specified routes are propagated from the device. The device responds to all queries for summaries, connected routes, and routing updates.

Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes, and a router that has a stub peer does not query that peer. The stub router depends on the distribution router to send the proper updates to all peers.

In the figure given below, device B is configured as an EIGRP stub router. Devices A and C are connected to the rest of the WAN. Device B advertises connected, static, redistribution, and summary routes to Device A and C. Device B does not advertise any routes learned from Device A (and the reverse).

Figure 1: EIGRP Stub Router Configuration



For more information about EIGRP stub routing, see “Configuring EIGRP Stub Routing” section of the *Cisco IOS IP Configuration Guide, Volume 2 of 3: Routing Protocols*.

How to Configure EIGRP

To create an EIGRP routing process, you must enable EIGRP and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.



Note If you have routers on your network that are configured for IGRP, and you want to change to EIGRP, you must designate transition routers that have both IGRP and EIGRP configured. In these cases, perform Steps 1 through 3 in the next section and also see the “Configuring Split Horizon” section. You must use the same AS number for routes to be automatically redistributed.

Default EIGRP Configuration

Table 1: Default EIGRP Configuration

Feature	Default Setting
Auto summary	Disabled.

Feature	Default Setting
Default-information	Exterior routes are accepted and default information is passed between processes when doing redistribution.
Default metric	Only connected routes and interface static routes can be redistributed with a default metric. The metric includes: <ul style="list-style-type: none"> • Bandwidth: 0 or greater kb/s. • Delay (tens of microseconds): 0 or any positive number that is greater than 39.1 nanoseconds. • Reliability: any number between 0 and 255 (255 means 100 percent reliability). • Loading: effective bandwidth as a number between 0 and 255 (255 means 100 percent loading). • MTU: maximum transmission unit size of the route in bytes. 0 or any positive integer.
Distance	Internal distance: 90. External distance: 170.
EIGRP log-neighbor changes	Disabled. No adjacency changes logged.
IP authentication key-chain	No authentication provided.
IP authentication mode	No authentication provided.
IP bandwidth-percent	50 percent.
IP hello interval	For low-speed nonbroadcast multiaccess (NBMA) networks: 60 seconds. For other networks: 5 seconds.
IP hold-time	For low-speed NBMA networks: 180 seconds; all other networks: 10 seconds.
IP split-horizon	Enabled.
IP summary address	No summary aggregate addresses are predefined.
Metric weights	tos: 0; k1 and k3: 1; k2, k4, and k5: 0
Network	None specified.
Nonstop Forwarding (NSF) Awareness	Enabled for IPv4 on switches running the Network Advantage license. Layer 3 switches to continue forwarding packets from a neighboring router during hardware or software changes.
NSF capability	Disabled. Note The Device supports EIGRP NSF-capable routing for IPv4.
Offset-list	Disabled.

Feature	Default Setting
Router EIGRP	Disabled.
Set metric	No metric set in the route map.
Traffic-share	Distributed proportionately to the ratios of the metrics.
Variance	1 (equal-cost load-balancing).

Configuring Basic EIGRP Parameters

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	router eigrp autonomous-system Example: Device(config)# <code>router eigrp 10</code>	Enables an EIGRP routing process, and enter router configuration mode. The AS number identifies the routes to other EIGRP routers and is used to tag routing information.
Step 3	nsf Example: Device(config-router)# <code>nsf</code>	(Optional) Enables EIGRP NSF. Enter this command on the active switch and on all of its peers.
Step 4	network network-number Example: Device(config-router)# <code>network 192.168.0.0</code>	Associate networks with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.
Step 5	eigrp log-neighbor-changes Example: Device(config-router)# <code>eigrp log-neighbor-changes</code>	(Optional) Enables logging of EIGRP neighbor changes to monitor routing system stability.
Step 6	metric weights <i>tos k1 k2 k3 k4 k5</i> Example: Device(config-router)# <code>metric weights 0 2 0 2 0 0</code>	(Optional) Adjust the EIGRP metric. Although the defaults have been carefully set to provide excellent operation in most networks, you can adjust them. Caution Setting metrics is complex and is not recommended without guidance from an experienced network designer.

	Command or Action	Purpose
Step 7	offset-list [<i>access-list number name</i>] { in out } <i>offset</i> <i>[type number]</i> Example: Device(config-router)# offset-list 21 out 10	(Optional) Applies an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through EIGRP. You can limit the offset list with an access list or an interface.
Step 8	auto-summary Example: Device(config-router)# auto-summary	(Optional) Enables automatic summarization of subnet routes into network-level routes.
Step 9	interface <i>interface-id</i> Example: Device(config-router)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 10	ip summary-address eigrp <i>autonomous-system-number</i> <i>address mask</i> Example: Device(config-if)# ip summary-address eigrp 1 192.168.0.0 255.255.0.0	(Optional) Configures a summary aggregate.
Step 11	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 12	show ip protocols Example: Device# show ip protocols	Verifies your entries. For NSF awareness, the output shows: *** IP Routing is NSF aware *** EIGRP NSF enabled
Step 13	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring EIGRP Interfaces

Other optional EIGRP parameters can be configured on an interface basis.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>interface interface-id</p> <p>Example:</p> <pre>Device(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 3	<p>ip bandwidth-percent eigrp percent</p> <p>Example:</p> <pre>Device(config-if)# ip bandwidth-percent eigrp 60</pre>	(Optional) Configures the percentage of bandwidth that can be used by EIGRP on an interface. The default is 50 percent.
Step 4	<p>ip summary-address eigrp autonomous-system-number address mask</p> <p>Example:</p> <pre>Device(config-if)# ip summary-address eigrp 109 192.161.0.0 255.255.0.0</pre>	(Optional) Configures a summary aggregate address for a specified interface (not usually necessary if auto-summary is enabled).
Step 5	<p>ip hello-interval eigrp autonomous-system-number seconds</p> <p>Example:</p> <pre>Device(config-if)# ip hello-interval eigrp 109 10</pre>	(Optional) Change the hello time interval for an EIGRP routing process. The range is 1 to 65535 seconds. The default is 60 seconds for low-speed NBMA networks and 5 seconds for all other networks.
Step 6	<p>ip hold-time eigrp autonomous-system-number seconds</p> <p>Example:</p> <pre>Device(config-if)# ip hold-time eigrp 109 40</pre>	<p>(Optional) Change the hold time interval for an EIGRP routing process. The range is 1 to 65535 seconds. The default is 180 seconds for low-speed NBMA networks and 15 seconds for all other networks.</p> <p>Caution Do not adjust the hold time without consulting Cisco technical support.</p>
Step 7	<p>no ip split-horizon eigrp autonomous-system-number</p> <p>Example:</p> <pre>Device(config-if)# no ip split-horizon eigrp 109</pre>	(Optional) Disables split horizon to allow route information to be advertised by a router out any interface from which that information originated.
Step 8	<p>end</p> <p>Example:</p>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config)# end	
Step 9	show ip eigrp interface Example: Device# show ip eigrp interface	Displays which interfaces EIGRP is active on and information about EIGRP relating to those interfaces.
Step 10	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring EIGRP Route Authentication

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol to prevent the introduction of unauthorized or false routing messages from unapproved sources.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	interface interface-id Example: Device(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 3	ip authentication mode eigrp autonomous-system md5 Example: Device(config-if)# ip authentication mode eigrp 104 md5	Enables MD5 authentication in IP EIGRP packets.
Step 4	ip authentication key-chain eigrp autonomous-system key-chain Example: Device(config-if)# ip authentication key-chain eigrp 105 chain1	Enables authentication of IP EIGRP packets.

	Command or Action	Purpose
Step 5	<p>exit</p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	Returns to global configuration mode.
Step 6	<p>key chain <i>name-of-chain</i></p> <p>Example:</p> <pre>Device(config)# key chain chain1</pre>	Identify a key chain and enter key-chain configuration mode. Match the name configured in Step 4.
Step 7	<p>key number</p> <p>Example:</p> <pre>Device(config-keychain)# key 1</pre>	In key-chain configuration mode, identify the key number.
Step 8	<p>key-string <i>text</i></p> <p>Example:</p> <pre>Device(config-keychain-key)# key-string key1</pre>	In key-chain key configuration mode, identify the key string.
Step 9	<p>accept-lifetime <i>start-time</i> {infinite <i>end-time</i> duration <i>seconds</i>}</p> <p>Example:</p> <pre>Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200</pre>	<p>(Optional) Specifies the time period during which the key can be received.</p> <p>The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i>. The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and duration is infinite.</p>
Step 10	<p>send-lifetime <i>start-time</i> {infinite <i>end-time</i> duration <i>seconds</i>}</p> <p>Example:</p> <pre>Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600</pre>	<p>(Optional) Specifies the time period during which the key can be sent.</p> <p>The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i>. The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and duration is infinite.</p>
Step 11	<p>end</p> <p>Example:</p> <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 12	<p>show key chain</p> <p>Example:</p> <pre>Device# show key chain</pre>	Displays authentication key information.

	Command or Action	Purpose
Step 13	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring and Maintaining EIGRP

You can delete neighbors from the neighbor table. You can also display various EIGRP routing statistics. The table given below lists the privileged EXEC commands for deleting neighbors and displaying statistics. For explanations of fields in the resulting display, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*.

Table 2: IP EIGRP Clear and Show Commands

clear ip eigrp neighbors [<i>if-address</i> <i>interface</i>]	Deletes neighbors from the neighbor table.
show ip eigrp interface [<i>interface</i>] [<i>as number</i>]	Displays information about interfaces participating in EIGRP.
show ip eigrp neighbors [<i>type-number</i>]	Displays EIGRP discovered neighbors.
show ip eigrp topology [<i>autonomous-system-number</i>] [[<i>ip-address</i>] <i>mask</i>]	Displays the EIGRP topology table.
show ip eigrp traffic [<i>autonomous-system-number</i>]	Displays the number of packets sent and received by the EIGRP process.

