CHAPTER 23

Configuring EIGRP

This chapter describes how to configure the ASA to route data, perform authentication, and redistribute routing information, using the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol.

This chapter includes the following sections:

Overview

EIGRP is an enhanced version of IGRP developed by Cisco. Unlike IGRP and RIP, EIGRP does not send out periodic route updates. EIGRP updates are sent out only when the network topology changes. Key capabilities that distinguish EIGRP from other routing protocols include fast convergence, support for variable-length subnet mask, support for partial updates, and support for multiple network layer protocols.

A router running EIGRP stores all the neighbor routing tables so that it can quickly adapt to alternate routes. If no appropriate route exists, EIGRP queries its neighbors to discover an alternate route. These queries propagate until an alternate route is found. Its support for variable-length subnet masks permits routes to be automatically summarized on a network number boundary. In addition, EIGRP can be configured to summarize on any bit boundary at any interface. EIGRP does not make periodic updates. Instead, it sends partial updates only when the metric for a route changes. Propagation of partial updates is automatically bounded so that only those routers that need the information are updated. As a result of these two capabilities, EIGRP consumes significantly less bandwidth than IGRP.

Neighbor discovery is the process that the ASA uses to dynamically learn of other routers on directly attached networks. EIGRP routers send out multicast hello packets to announce their presence on the network. When the ASA receives a hello packet from a new neighbor, it sends its topology table to the neighbor with an initialization bit set. When the neighbor receives the topology update with the initialization bit set, the neighbor sends its topology table back to the ASA.

The hello packets are sent out as multicast messages. No response is expected to a hello message. The exception to this is for statically defined neighbors. If you use the **neighbor** command to configure a neighbor, the hello messages sent to that neighbor are sent as unicast messages. Routing updates and acknowledgements are sent out as unicast messages.

Once this neighbor relationship is established, routing updates are not exchanged unless there is a change in the network topology. The neighbor relationship is maintained through the hello packets. Each hello packet received from a neighbor contains a hold time. This is the time in which the ASA can expect to receive a hello packet from that neighbor. If the ASA does not receive a hello packet from that neighbor within the hold time advertised by that neighbor, the ASA considers that neighbor to be unavailable.

The EIGRP protocol uses four key algorithm technologies, four key technologies, including neighbor discover/recovery, Reliable Transport Protocol (RTP), and the fourth one, DUAL being important for route computations. DUAL saves all routes to a destination in the topology table, not just the least-cost route. The least-cost route is inserted into the routing table. The other routes remain in the topology table. If the main route fails, another route is chosen from the feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination. The feasibility calculation guarantees that the path is not part of a routing loop.

If a feasible successor is not found in the topology table, a route recomputation must occur. During route recomputation, DUAL queries the EIGRP neighbors for a route, who in turn query their neighbors. Routers that do no have a feasible successor for the route return an unreachable message.

During route recomputation, DUAL marks the route as active. By default, the ASA waits for three minutes to receive a response from its neighbors. If the ASA does not receive a response from a neighbor, the route is marked as stuck-in-active. All routes in the topology table that point to the unresponsive neighbor as a feasibility successor are removed.

Note EIGRP neighbor relationships are not supported through the IPSec tunnel without a GRE tunnel.

Licensing Requirements for EIGRP

Model	License Requirement
All models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single context mode.

Firewall Mode Guidelines

Supported only in routed firewall mode. Transparent mode is not supported.

IPv6 Guidelines

Does not support IPv6.

Additional Guidelines

A maximum of one EIGRP process is supported.

Configuring EIGRP

This section explains how to enable and restart the EIGRP process on your system. After enabling see the section, to learn how to customize the EIGRP process on your system.

- Enabling EIGRP, page 23-3
- Enabling EIGRP Stub Routing, page 23-3
- Restarting the EIGRP Process, page 23-4

Enabling EIGRP

You can only enable one EIGRP routing process on the ASA. To enable EIGRP, perform the following detailed steps.

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** `hostname(config)# router eigrp 2`	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2	**network** *ip-addr* [*mask*]
	
	Example:
	`hostname(config)# router eigrp 2`
	`hostname(config-router)# network 10.0.0.0 255.0.0.0`
		This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command.
		
		Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.
		
		If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces in EIGRP.

Enabling EIGRP Stub Routing

You can enable, and configure the ASA as an EIGRP stub router. Stub routing decreases memory and processing requirements on the ASA. As a stub router, the ASA does not need to maintain a complete EIGRP routing table because it forwards all nonlocal traffic to a distribution router. Generally, the distribution router need not send anything more than a default route to the stub router.

Only specified routes are propagated from the stub router to the distribution router. As a stub router, the ASA responds to all queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message "inaccessible." When the ASA is configured as a stub, it sends a special peer information packet to all neighboring routers to report its status as a stub router. Any neighbor that receives a packet informing it of the stub status will not query the stub router for any routes, and a router that has a stub peer will not query that peer. The stub router depends on the distribution router to send the proper updates to all peers.

To enable the ASA as an EIGRP stub routing process, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** `hostname(config)# router eigrp 2`	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2	**network** *ip-addr* [*mask*]
	
	Example:
	`hostname(config)# router eigrp 2`
	`hostname(config-router)# network 10.0.0.0 255.0.0.0`
		This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command.
		
		Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process.
		
		If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces for EIGRP.

Step 3	**eigrp stub** {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]}
	
	Example:
	`hostname(config)# router eigrp 2`
	`hostname(config-router)# network 10.0.0.0 255.0.0.0`
	`hostname(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static] [summary]}`
		This step configure the stub routing process. You must specify which networks are advertised by the stub routing process to the distribution router. Static and connected networks are not automatically redistributed into the stub routing process.

Restarting the EIGRP Process

To restart an EIGRP process, clear redistribution, or counters, enter the following command:

```
hostname(config)# clear eigrp pid {<1-65535> | neighbors | topology | events)}
```

Customizing EIGRP

This section describes how to customize the EIGRP routing, and includes the following topics:

- Configuring Interfaces for EIGRP, page 23-5

Configuring Interfaces for EIGRP

If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, you can configure a **network** command that covers the network the interface is attached to, and use the **passive-interface** command to prevent that interface from sending or receiving EIGRP updates.

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# router eigrp 2	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	hostname(config-router)# **network** *ip-addr* [*mask*] **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0	This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command. Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process. If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces for EIGRP.
Step 3	Do one of the following to customize an interface to participate in EIGRP routing:	

Command	Purpose
passive-interface {**default** | *if-name*} **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0 hostname(config-router)# passive-interface {default}	This step prevents an interface from sending or receiving EIGRP routing message. Using the **default** keyword disables EIGRP routing updates on all interfaces. Specifying an interface name, as defined by the **nameif** command, disables EIGRP routing updates on the specified interface. You can have multiple **passive-interface** commands in your EIGRP router configuration.
no default-information {**in** | **out** | **WORD**} **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0 hostname(config-router)# no default-information {in | out | WORD}	This allows you to control the sending or receiving of candidate default route information. Configuring **no default-information in** causes the candidate default route bit to be blocked on received routes. Configuring **no default-information out** disables the setting of th edefault route bit in advertised routes.

Configuring the Summary Aggregate Addresses on Interfaces

You can configure a summary addresses on a per-interface basis. You need to manually define summary addresses if you want to create summary addresses that do not occur at a network number boundary or if you want to use summary addresses on a ASA with automatic route summarization disabled. If any more specific routes are in the routing table, EIGRP will advertise the summary address out the interface with a metric equal to the minimum of all more specific routes.

To create a summary address, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**interface** *phy_if* **Example:** hostname(config)# **interface** *phy_if*	Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
Step 2	**summary-address eigrp** *as-num address mask* [*distance*] **Example:** hostname(config-if)# **summary-address eigrp** *2 address mask* [*20*]	This step creates the summary address. By default, EIGRP summary addresses that you define have an administrative distance of 5. You can change this value by specifying the optional *distance* argument in the **summary-address** command.

Changing the Interface Delay Value

The interface delay value is used in EIGRP distance calculations. You can modify this value on a per-interface basis. To change the delay value, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**interface** *phy_if* **Example:** hostname(config)# **interface** *phy_if*	Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
Step 2	**delay** *value* **Example:** hostname(config-if)# **delay** *200*	The *value* entered is in tens of microseconds. So, to set the delay for 2000 microseconds, you would enter a *value* of 200. To view the delay value assigned to an interface, use the **show interface** command.

Enabling EIGRP Authentication on an Interface

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.

EIGRP route authentication is configured on a per-interface basis. All EIGRP neighbors on interfaces configured for EIGRP message authentication must be configured with the same authentication mode and key for adjacencies to be established.

Note Before you can enable EIGRP route authentication, you must enable EIGRP.

To enable EIGRP authentication on an interface, perform the following steps:

Detailed Steps

Step 1	**router eigrp** *as-num* **Example:** hostname(config)# **router eigrp** *2*	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	**network** *ip-addr* [*mask*] **Example:** hostname(config)# **router eigrp 2** hostname(config-router)# **network 10.0.0.0 255.0.0.0**	This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command. Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process. If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces in EIGRP.
Step 3	**interface** *phy_if* **Example:** hostname(config)# **interface** *phy_if*	Enter interface configuration mode for the interface on which you are configuring EIGRP message authentication.
Step 4	**authentication mode eigrp** *as-num* **md5** **Example:** hostname(config)# **authentication mode eigrp** *2* **md5**	Enable MD5 authentication of EIGRP packets. The *as-num* argument is the autonomous system number of the EIGRP routing process configured on the ASA. If EIGRP is not enabled or if you enter the wrong number, the ASA returns the following error message: `% Asystem(100) specified does not exist`
Step 5	**authentication key eigrp** *as-num key* **key-id** *key-id* **Example:** hostname(config)# **authentication key eigrp** *2 cisco* **key-id** *200*	Configure the key used by the MD5 algorithm. The *as-num* argument is the autonomous system number of the EIGRP routing process configured on the ASA. If EIGRP is not enabled or if you enter the wrong number, the ASA returns the following error message: `% Asystem(100) specified does not exist` The *key* argument can contain up to 16 characters. The *key-id* argument is a number from 0 to 255

Defining an EIGRP Neighbor

EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a nonbroadcast network, such as a tunnel, you must manually define that neighbor. When you manually define an EIGRP neighbor, hello packets are sent to that neighbor as unicast messages.

To manually define an EIGRP neighbor, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# **router eigrp** *2*	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	**neighbor** *ip-addr* **interface** *if_name* **Example:** hostname(config)# **router eigrp 2** hostname(config-router)# **neighbor 10.0.0.0 interface** *interface1*	This step defines the static neighbor. The *ip-addr* argument is the IP address of the neighbor. The *if-name* argument is the name of the interface, as specified by the **nameif** command, through which that neighbor is available. You can define multiple neighbors for an EIGRP routing process.

Redistributing Routes Into EIGRP

You can redistribute routes discovered by RIP and OSPF into the EIGRP routing process. You can also redistribute static and connected routes into the EIGRP routing process. You do not need to redistribute connected routes if they fall within the range of a **network** statement in the EIGRP configuration.

Note **For RIP only**: Before you begin this procedure, you must create a route-map to further define which routes from the specified routing protocol are redistributed in to the RIP routing process. See Chapter 20, "Defining Route Maps," for more information about creating a route map.

To redistribute routes into the EIGRP routing process, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# **router eigrp** *2*	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	**default-metric** *bandwidth delay reliability loading mtu* **Example:** hostname(config)# **router eigrp** *2* hostname(config-router)# **default-metric** *bandwidth delay reliability loading mtu*	(Optional) Specify the default metrics that should be applied to routes redistributed into the EIGRP routing process. If you do not specify a **default-metric** in the EIGRP router configuration, you must specify the metric values in each **redistribute** command. If you specify the EIGRP metrics in the **redistribute** command and have the **default-metric** command in the EIGRP router configuration, the metrics in the **redistribute** command are used.
Step 3	Do one of the following to redistribute the selected route type into the EIGRP routing process. You must specify the EIGRP metric values in the **redistribute** command if you do not have a **default-metric** command in the EIGRP router configuration.	

Command	Purpose
redistribute connected [metric *bandwidth delay reliability loading mtu***] [route-map** *map_name***]** **Example:** hostname(config-router): **redistribute connected [metric** *bandwidth delay reliability loading mtu***] [route-map** *map_name***]**	To redistribute connected routes into the EIGRP routing process.
redistribute static [metric *bandwidth delay reliability loading mtu***] [route-map** *map_name***]** **Example:** hostname(config-router): **redistribute static [metric** *bandwidth delay reliability loading mtu***] [route-map** *map_name***]**	To redistribute static routes into the EIGRP routing process.
redistribute ospf *pid* **[match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric** *bandwidth delay reliability loading mtu***] [route-map** *map_name***]** **Example:** hostname(config-router): **redistribute ospf** *pid* **[match {internal | external [1 | 2] | nssa-external [1 | 2]}] [metric** *bandwidth delay reliability loading mtu***] [route-map** *map_name***]**	To redistribute routes from an OSPF routing process into the EIGRP routing process.
redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**] **Example:** (config-router): **redistribute rip** [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]	To redistribute routes from a RIP routing process into the EIGRP routing process.

Filtering Networks in EIGRP

Note Before you begin this process, you must create a standard access list that defines the routes you want to advertise. That is, create a standard access list that defines the routes you want to filter from sending or receiving updates. For more information on creating standard access lists, see the chapter, “Identifying Traffic with Access Lists”.

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# router eigrp 2	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	hostname(config-router)# **network** *ip-addr* [*mask*] **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0	This step configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command. Directly-connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that fall within the defined network participate in the EIGRP routing process. If you have an interface that you do not want to participate in EIGRP routing, but that is attached to a network that you want advertised, see the section Configuring Interfaces for EIGRP.
Step 3	Do one of the following to filter networks sent or received in EIGRP routing updates. You can enter multiple **distribute-list** commands in your EIGRP router configuration.	
	distribute-list *acl* **out** [**connected** | **ospf** | **rip** | **static** | **interface** *if_name*] **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0 hostname(config-router): distribute-list acl out [connected]	This allows you to filter networks sent in EIGRP routing updates. You can specify an interface to apply the filter to only those updates sent by that specific interface.
	distribute-list *acl* **in** [**interface** *if_name*] **Example:** hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0 hostname(config-router): distribute-list acl in [interface interface1]	This allows you to filter networks received in EIGRP routing updates. You can specify an interface to apply the filter to only those updates received by that interface.

Customizing the EIGRP Hello Interval and Hold Time

The ASA periodically sends hello packets to discover neighbors and to learn when neighbors become unreachable or inoperative. By default, hello packets are sent every 5 seconds.

The hello packet advertises the ASA hold time. The hold time indicates to EIGRP neighbors the length of time the neighbor should consider the ASA reachable. If the neighbor does not receive a hello packet within the advertised hold time, then the ASA is considered unreachable. By default, the advertised hold time is 15 seconds (three times the hello interval).

Both the hello interval and the advertised hold time are configured on a per-interface basis. We recommend setting the hold time to be at minimum three times the hello interval.

To configure the hello interval and advertised hold time, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**interface** *phy_if* **Example:** hostname(config)# interface *phy_if*	Enter interface configuration mode for the interface on which you are configuring hello interval or advertised hold time.
Step 2	**hello-interval eigrp** *as-num seconds* **Example:** hostname(config)# hello-interval eigrp *2 60*	This step allows you to change the hello interval.
Step 3	**hold-time eigrp** *as-num seconds* **Example:** hostname(config)# hold-time eigrp *2 60*	This step allows you to change the hold time.

Disabling Automatic Route Summarization

Automatic route summarization is enabled by default. The EIGRP routing process summarizes on network number boundaries. This can cause routing problems if you have non-contiguous networks.

For example, if you have a router with the networks 192.168.1.0, 192.168.2.0, and 192.168.3.0 connected to it, and those networks all participate in EIGRP, the EIGRP routing process creates the summary address 192.168.0.0 for those routes. If an additional router is added to the network with the networks 192.168.10.0 and 192.168.11.0, and those networks participate in EIGRP, they will also be summarized as 192.168.0.0. To prevent the possibility of traffic being routed to the wrong location, you should disable automatic route summarization on the routers creating the conflicting summary addresses.

To disable automatic router summarization, enter the following command in router configuration mode for the EIGRP routing process:

Detailed Steps

	Command	Purpose
Step 1	**router eigrp** *as-num* **Example:** hostname(config)# router eigrp *2*	This creates an EIGRP routing process, and the user enters router configuration mode for this EIGRP process. The *as-num* argument is the autonomous system number of the EIGRP routing process.
Step 2	**no auto-summary** **Example:** hostname(config-router)# no auto-summary	Automatic summary addresses have an adminstrative distance of 5. You cannot configure this value.

Disabling EIGRP Split Horizon

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

By default, split horizon is enabled on all interfaces.

Split horizon blocks route information from being advertised by a router out of any interface from which that information originated. This behavior usually optimizes communications among multiple routing devices, particularly when links are broken. However, with nonbroadcast networks, there may be situations where this behavior is not desired. For these situations, including networks in which you have EIGRP configured, you may want to disable split horizon.

If you disable split horizon on an interface, you must disable it for all routers and access servers on that interface.

To disable EIGRP split-horizon, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	**interface** *phy_if* **Example:** hostname(config)# **interface** *phy_if*	Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
Step 2	**no split-horizon eigrp** *as-number* **Example:** hostname(config-if)# **no split-horizon eigrp** *2*	This step disables the split horizon.

Monitoring EIGRP

You can use the following commands to monitor the EIGRP routing process. For examples and descriptions of the command output, see the *Cisco Security Appliance Command Reference*. Additionally, you can disable the logging of neighbor change message and neighbor warning messages

To monitor or disable various EIGRP routing statistics, perform one of the following tasks:

Command	Purpose
Monitoring EIGRP Routing	
show eigrp [*as-number*] **events** [{*start end*} | **type**]	Displays the EIGRP event log.
show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]	Displays the EIGRP neighbor table.
show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]	Displays the interfaces participating in EIGRP routing.
show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]	Displays the EIGRP topology table.

Command	Purpose
show eigrp [*as-number*] **traffic**	Displays EIGRP traffic statistics.
router-id	Displays the router-id for this EIGRP process.
Disabling EIGRP Logging Messages	
no eigrp log-neighbor-changes	Disables the logging of neighbor change messages. Enter this command in router configuration mode for the EIGRP routing process.
no eigrp log-neighbor-warnings	Disables the logging of neighbor warning messages.

Note By default neighbor change, and neighbor warning messages are logged.

Configuration Example for EIGRP

The following example shows how to enable and configure EIGRP with various optional processes:

Step 1 Enable EIGRP:

```
hostname(config)# router eigrp 2
hostname(config-router)# network 10.0.0.0 255.0.0.0
```

Step 2 Configure an interface from sending or receiving EIGRP routing message:

```
hostname(config-router)# passive-interface {default}
```

Step 3 Define an EIGRP neighbor:

```
hostname(config-router)# neighbor 10.0.0.0 interface interface1
```

Step 4 Configure the interfaces and networks that participate in EIGRP routing:

```
hostname(config-router)# network 10.0.0.0 255.0.0.0
```

Step 5 Change the interface delay value is used in EIGRP distance calculations:

```
hostname(config-router)# exit
hostname(config)# interface phy_if
hostname(config-if)# delay 200
```

Feature History for EIGRP

Table 23-1 lists the release history for this feature.

Table 23-1 Feature History for EIGRP

Feature Name	Releases	Feature Information
router eigrp	7.0	This feature allows you to route data, perform authentication, redistribute and monitor routing information, using the Enhanced Interior Gateway Routing Protocol (EIGRP) routing protocol.

Additional References

For additional information related to routing, see the following:

- Related Documents, page 23-15

Related Documents

Related Topic	Document Title
Routing Overview	Information About Routing
How to configure OSPF	Configuring OSPF
How to configure RIP	Configuring RIP
How to configure a static or default route	Configuring Static and Default Routes
How to configure a route map	Defining Route Maps
How to configure multicast routing	Configuring Multicast Routing