



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).

This chapter includes the following sections:

- [Information About EIGRP, page 31-1](#)
- [Licensing Requirements for EIGRP, page 31-2](#)
- [Guidelines and Limitations, page 31-3](#)
- [Configuring EIGRP, page 31-3](#)
- [Customizing EIGRP, page 31-5](#)
- [Monitoring EIGRP, page 31-17](#)
- [Configuration Example for EIGRP, page 31-18](#)
- [Feature History for EIGRP, page 31-19](#)

Information About EIGRP

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, or configure the Hello Interval in ASDM, 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 includes 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 discovery/recovery, Reliable Transport Protocol (RTP), and DUAL, which is 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 not 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.

Using Clustering

For information about using clustering with EIGRP, see [Dynamic Routing and Clustering, page 26-9](#).

Licensing Requirements for EIGRP

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Firewall Mode Guidelines

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

Failover Guidelines

Supports Stateful Failover in single and multiple context mode.

IPv6 Guidelines

Does not support IPv6.

Clustering Guidelines

- Supports Spanned EtherChannel and Individual Interface clustering when configured to use both EIGRP and OSPFv2.
- In a Individual Interface cluster setup, EIGRP adjacencies can only be established between two contexts on a shared interface on the master unit. You can manually configure multiple neighbor statements corresponding to each cluster node separately to work around this issue.

Additional Guidelines

- EIGRP instances cannot form adjacencies with each other across shared interfaces because inter-context exchange of multicast traffic is not supported.
- A maximum of one EIGRP process is supported.

Configuring EIGRP

This section describes how to enable the EIGRP process on your system. After you have enabled EIGRP, see the following sections to learn how to customize the EIGRP process on your system.

- [Enabling EIGRP, page 31-4](#)
- [Enabling EIGRP Stub Routing, page 31-4](#)

Enabling EIGRP

You can only enable one EIGRP routing process on the ASA.

To enable EIGRP, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	router eigrp <i>as-num</i>	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.
	Example: ciscoasa(config)# router eigrp 2	The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	network <i>ip-addr</i> [<i>mask</i>]	Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.
	Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	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 have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configuring Interfaces for EIGRP, page 31-6 .

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 correct 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 <i>as-num</i>	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.
	Example: ciscoasa(config)# router eigrp 2	The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	network <i>ip-addr</i> [<i>mask</i>]	Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.
	Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	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 have participate in EIGRP routing, but that is attached to a network that you want advertised, see section Configuring Passive Interfaces, page 31-8 .
Step 3	eigrp stub { receive-only [connected] [redistributed] [static] [summary]}	Configures 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.
	Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# eigrp stub {receive-only [connected] [redistributed] [static] [summary]}	



Note

A stub routing process does not maintain a full topology table. At a minimum, stub routing needs a default route to a distribution router, which makes the routing decisions.

Customizing EIGRP

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

- [Defining a Network for an EIGRP Routing Process, page 31-6](#)
- [Configuring Interfaces for EIGRP, page 31-6](#)
- [Configuring the Summary Aggregate Addresses on Interfaces, page 31-9](#)
- [Changing the Interface Delay Value, page 31-9](#)
- [Enabling EIGRP Authentication on an Interface, page 31-10](#)
- [Defining an EIGRP Neighbor, page 31-11](#)
- [Redistributing Routes Into EIGRP, page 31-12](#)

- [Filtering Networks in EIGRP, page 31-13](#)
- [Customizing the EIGRP Hello Interval and Hold Time, page 31-14](#)
- [Disabling Automatic Route Summarization, page 31-15](#)
- [Configuring Default Information in EIGRP, page 31-15](#)
- [Disabling EIGRP Split Horizon, page 31-16](#)
- [Restarting the EIGRP Process, page 31-17](#)

Defining a Network for an EIGRP Routing Process

The Network table lets you specify the networks used by the EIGRP routing process. For an interface to participate in EIGRP routing, it must fall within the range of addresses defined by the network entries. For directly connected and static networks to be advertised, they must also fall within the range of the network entries.

The Network table displays the networks configured for the EIGRP routing process. Each row of the table displays the network address and associated mask configured for the specified EIGRP routing process.

To add or define a network, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	<code>router eigrp as-num</code>	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.
	Example: <code>ciscoasa(config)# router eigrp 2</code>	The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	<code>network ip-addr [mask]</code>	Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.
	Example: <code>ciscoasa(config)# router eigrp 2</code> <code>ciscoasa(config-router)# network 10.0.0.0</code> <code>255.0.0.0</code>	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 have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configuring Passive Interfaces, page 31-8 .

Configuring Interfaces for EIGRP

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

To configure interfaces for EIGRP, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	<p>router eigrp <i>as-num</i></p> <p>Example: ciscoasa(config)# router eigrp 2</p>	<p>Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.</p> <p>The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.</p>
Step 2	<p>ciscoasa(config-router)# network <i>ip-addr</i> [<i>mask</i>]</p> <p>Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0</p>	<p>Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.</p> <p>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.</p> <p>If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Defining a Network for an EIGRP Routing Process, page 31-6.</p>
Step 3	<p>(Optional) Do one of the following to customize an interface to participate in EIGRP routing:</p> <p>no default-information {in out WORD}</p> <p>Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# no default-information {in out WORD}</p> <p>authentication mode eigrp <i>as-num</i> md5</p> <p>Example: ciscoasa(config)# authentication mode eigrp 2 md5</p> <p>delay <i>value</i></p> <p>Example: ciscoasa(config-if)# delay 200</p>	<p>Allows you to control the sending or receiving of candidate default route information.</p> <p>Entering the no default-information in command causes the candidate default route bit to be blocked on received routes. Entering the no default-information out command disables the setting of the default route bit in advertised routes.</p> <p>see Configuring Default Information in EIGRP, page 31-15 for more information on this particular option.</p> <p>Enables MD5 authentication of EIGRP packets.</p> <p>The <i>as-num</i> 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:</p> <pre>% System(100) specified does not exist</pre> <p>see Enabling EIGRP Authentication on an Interface, page 31-10 for more information on this particular option.</p> <p>The <i>value</i> argument entered is in tens of microseconds. To set the delay for 2000 microseconds, you enter a <i>value</i> of 200.</p> <p>To view the delay value assigned to an interface, use the show interface command.</p> <p>see Changing the Interface Delay Value, page 31-9 for more information on this particular option.</p>

Command	Purpose
hello-interval eigrp <i>as-num seconds</i> Example: <pre>ciscoasa(config)# hello-interval eigrp 2 60</pre>	Allows you to change the hello interval. see Customizing the EIGRP Hello Interval and Hold Time, page 31-14 for more information on this particular option.
hold-time eigrp <i>as-num seconds</i> Example: <pre>ciscoasa(config)# hold-time eigrp 2 60</pre>	Allows you to change the hold time. see Customizing the EIGRP Hello Interval and Hold Time, page 31-14 for more information on this particular option.

Configuring Passive Interfaces

You can configure one or more interfaces as passive interfaces. In EIGRP, a passive interface does not send or receive routing updates.

To configure passive interfaces, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	router eigrp <i>as-num</i> Example: <pre>ciscoasa(config)# router eigrp 2</pre>	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process. The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	<pre>ciscoasa(config-router)# network ip-addr [mask]</pre> Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0</pre>	Configures 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 have participate in EIGRP routing, but that is attached to a network that you want advertised, see Defining a Network for an EIGRP Routing Process, page 31-6 .
Step 3	passive-interface { default <i>if-name</i> } Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# passive-interface {default}</pre>	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 use multiple passive-interface commands in your EIGRP router configuration.

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 an 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	<code>interface phy_if</code> Example: <code>ciscoasa(config)# interface inside</code>	Enters interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
Step 2	<code>summary-address eigrp as-num address mask [distance]</code> Example: <code>ciscoasa(config-if)# summary-address eigrp 2 address mask [20]</code>	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 <i>distance</i> 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 interface delay value, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	<code>interface phy_if</code> Example: <code>ciscoasa(config)# interface inside</code>	Enters interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
Step 2	<code>delay value</code> Example: <code>ciscoasa(config-if)# delay 200</code>	The <i>value</i> argument entered is in tens of microseconds. To set the delay for 2000 microseconds, you enter a <i>value</i> 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

	Command	Purpose
Step 1	<p>router eigrp <i>as-num</i></p> <p>Example: hostname(config)# router eigrp 2</p>	<p>Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.</p> <p>The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.</p>
Step 2	<p>network <i>ip-addr [mask]</i></p> <p>Example: hostname(config)# router eigrp 2 hostname(config-router)# network 10.0.0.0 255.0.0.0</p>	<p>Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.</p> <p>Directly connected and static networks that fall within the defined network are advertised by the ASA. Additionally, only interfaces with an IP address that falls within the defined network participate in the EIGRP routing process.</p> <p>If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configuring EIGRP, page 31-3.</p>
Step 3	<p>interface <i>phy_if</i></p> <p>Example: hostname(config)# interface inside</p>	<p>Enters interface configuration mode for the interface on which you are configuring EIGRP message authentication.</p>

	Command	Purpose
Step 4	<p>authentication mode eigrp <i>as-num</i> md5</p> <p>Example: <pre>hostname(config)# authentication mode eigrp 2 md5</pre></p>	<p>Enables MD5 authentication of EIGRP packets.</p> <p>The <i>as-num</i> 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:</p> <pre>% Asystem(100) specified does not exist</pre>
Step 5	<p>authentication key eigrp <i>as-num</i> key key-id <i>key-id</i></p> <p>Example: <pre>hostname(config)# authentication key eigrp 2 cisco key-id 200</pre></p>	<p>Configures the key used by the MD5 algorithm.</p> <p>The <i>as-num</i> 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:</p> <pre>% Asystem(100) specified does not exist%</pre> <p>The <i>key</i> argument can include up to 16 characters, including alphabets, numbers and special characters.</p> <p> Note White spaces are not allowed, in the key argument.</p> <p>The <i>key-id</i> argument is a number that can range from 0 to 255.</p>

Defining an EIGRP Neighbor

EIGRP hello packets are sent as multicast packets. If an EIGRP neighbor is located across a non broadcast 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	<p>router eigrp <i>as-num</i></p> <p>Example: <pre>ciscoasa(config)# router eigrp 2</pre></p>	<p>Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.</p> <p>The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.</p>
Step 2	<p>neighbor <i>ip-addr</i> interface <i>if_name</i></p> <p>Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1</pre></p>	<p>Defines the static neighbor.</p> <p>The <i>ip-addr</i> argument is the IP address of the neighbor.</p> <p>The <i>if_name</i> 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.</p>

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 28, “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	<p>router eigrp <i>as-num</i></p> <p>Example: ciscoasa(config)# router eigrp 2</p>	<p>Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.</p> <p>The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.</p>
Step 2	<p>default-metric <i>bandwidth delay reliability loading mtu</i></p> <p>Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# default-metric <i>bandwidth delay reliability loading mtu</i></p>	<p>(Optional) Specifies the default metrics that should be applied to routes redistributed into the EIGRP routing process.</p> <p>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.</p>
Step 3	<p>Do one of the following to redistribute the selected route type into the EIGRP routing process:</p> <p>redistribute connected [metric <i>bandwidth delay reliability loading mtu</i>] [route-map <i>map_name</i>]</p> <p>Example: ciscoasa(config-router): redistribute connected [<i>metric bandwidth delay reliability loading mtu</i>] [<i>route-map map_name</i>]</p> <p>redistribute static [metric <i>bandwidth delay reliability loading mtu</i>] [route-map <i>map_name</i>]</p> <p>Example: ciscoasa(config-router): redistribute static [<i>metric bandwidth delay reliability loading mtu</i>] [<i>route-map map_name</i>]</p>	<p>Redistributes connected routes into the EIGRP routing process.</p> <p>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.</p> <p>Redistributes static routes into the EIGRP routing process.</p>

Command	Purpose
<p>redistribute ospf <i>pid</i> [match {internal external [1 2] nssa-external [1 2]}}] [metric <i>bandwidth delay reliability loading mtu</i>] [route-map <i>map_name</i>]</p> <p>Example: <pre>ciscoasa(config-router): redistribute ospf pid [match {internal external [1 2] nssa-external [1 2]}}] [metric bandwidth delay reliability loading mtu] [route-map map_name]</pre></p>	Redistributes routes from an OSPF routing process into the EIGRP routing process.
<p>redistribute rip [metric <i>bandwidth delay reliability load mtu</i>] [route-map <i>map_name</i>]</p> <p>Example: <pre>(config-router): redistribute rip [metric bandwidth delay reliability load mtu] [route-map map_name]</pre></p>	Redistributes 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 ACL that defines the routes that you want to advertise. That is, create a standard ACL that defines the routes that you want to filter from sending or receiving updates.

To filter networks in EIGRP, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	<p>router eigrp <i>as-num</i></p> <p>Example: <pre>ciscoasa(config)# router eigrp 2</pre></p>	<p>Creates an EIGRP routing process and enters router configuration mode for this EIGRP process.</p> <p>The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.</p>
Step 2	<p>ciscoasa(config-router)# network <i>ip-addr</i> [<i>mask</i>]</p> <p>Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0</pre></p>	<p>Configures the interfaces and networks that participate in EIGRP routing. You can configure one or more network statements with this command.</p> <p>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.</p> <p>If you have an interface that you do not want to have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configuring Interfaces for EIGRP, page 31-6.</p>
Step 3	Do one of the following to filter networks sent or received in EIGRP routing updates:	

Command	Purpose
distribute-list <i>acl</i> out [connected ospf rip static interface <i>if_name</i>]	Filters networks sent in EIGRP routing updates. You can specify an interface to apply the filter to only those updates that are sent by that specific interface. You can enter multiple distribute-list commands in your EIGRP router configuration.
Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router): distribute-list acl out [connected]</pre>	
distribute-list <i>acl</i> in [interface <i>if_name</i>]	Filters networks received in EIGRP routing updates. You can specify an interface to apply the filter to only those updates that are received by that interface.
Example: <pre>ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router): distribute-list acl in [interface interface1]</pre>	

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 <i>phy_if</i> Example: <pre>ciscoasa(config)# interface inside</pre>	Enters interface configuration mode for the interface on which you are configuring the hello interval or advertised hold time.
Step 2	hello-interval eigrp <i>as-num seconds</i> Example: <pre>ciscoasa(config)# hello-interval eigrp 2 60</pre>	Changes the hello interval.
Step 3	hold-time eigrp <i>as-num seconds</i> Example: <pre>ciscoasa(config)# hold-time eigrp 2 60</pre>	Changes 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 noncontiguous 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 route summarization, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	<code>router eigrp as-num</code> Example: <code>ciscoasa(config)# router eigrp 2</code>	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process. The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	<code>no auto-summary</code> Example: <code>ciscoasa(config-router)# no auto-summary</code>	You cannot configure this value. Automatic summary addresses have an administrative distance of 5.

Configuring Default Information in EIGRP

You can control the sending and receiving of default route information in EIGRP updates. By default, default routes are sent and accepted. Configuring the ASA to disallow default information to be received causes the candidate default route bit to be blocked on received routes. Configuring the ASA to disallow default information to be sent disables the setting of the default route bit in advertised routes.

To configure default routing information, perform the following steps:

Detailed Steps

	Command	Purpose
Step 1	router eigrp <i>as-num</i> Example: ciscoasa(config)# router eigrp 2	Creates an EIGRP routing process and enters router configuration mode for this EIGRP process. The <i>as-num</i> argument is the autonomous system number of the EIGRP routing process.
Step 2	ciscoasa(config-router)# network <i>ip-addr</i> [<i>mask</i>] Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0	Configures 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 have participate in EIGRP routing, but that is attached to a network that you want advertised, see Configuring Interfaces for EIGRP, page 31-6 .
Step 3	no default-information {in out WORD} Example: ciscoasa(config)# router eigrp 2 ciscoasa(config-router)# network 10.0.0.0 255.0.0.0 ciscoasa(config-router)# no default-information {in out WORD}	Controls the sending or receiving of candidate default route information. Entering the no default-information in command causes the candidate default route bit to be blocked on received routes. Entering the no default-information out command disables the setting of the default route bit in advertised routes.

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 <i>phy_if</i>	Enters interface configuration mode for the interface on which you are changing the delay value used by EIGRP.
	Example: ciscoasa(config)# interface <i>phy_if</i>	
Step 2	no split-horizon eigrp <i>as-number</i>	Disables the split horizon.
	Example: ciscoasa(config-if)# no split-horizon eigrp 2	

Restarting the EIGRP Process

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

Command	Purpose
clear eigrp pid {1-65535 neighbors topology events }	Restarts an EIGRP process or clears redistribution or counters.
Example: ciscoasa(config)# clear eigrp pid 10 neighbors	

Monitoring EIGRP

You can use the following commands to monitor the EIGRP routing process. For examples and descriptions of the command output, see the command reference. Additionally, you can disable the logging of neighbor change messages and neighbor warning messages.

To monitor or disable various EIGRP routing statistics, enter one of the following commands:

Command	Purpose
Monitoring EIGRP Routing	
router-id	Displays the router-id for this EIGRP process.
show eigrp [<i>as-number</i>] events [{ <i>start end</i> } type]	Displays the EIGRP event log.
show eigrp [<i>as-number</i>] interfaces [<i>if-name</i>] [detail]	Displays the interfaces participating in EIGRP routing.
show eigrp [<i>as-number</i>] neighbors [detail static] [<i>if-name</i>]	Displays the EIGRP neighbor table.

Command (continued)	Purpose (continued)
<code>show eigrp [as-number] topology [ip-addr [mask] active all-links pending summary zero-successors]</code>	Displays the EIGRP topology table.
<code>show eigrp [as-number] traffic</code>	Displays EIGRP traffic statistics.
<code>show mfib cluster</code>	Displays MFIB information in terms of forwarding entries and interfaces.
<code>show route cluster</code>	Displays additional route synchronization details for clustering.
Disabling EIGRP Logging Messages	
<code>no eigrp log-neighbor-changes</code>	Disables the logging of neighbor change messages. Enter this command in router configuration mode for the EIGRP routing process.
<code>no eigrp log-neighbor-warnings</code>	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 To enable EIGRP, enter the following commands:

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

Step 2 To configure an interface from sending or receiving EIGRP routing messages, enter the following command:

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

Step 3 To define an EIGRP neighbor, enter the following command:

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

Step 4 To configure the interfaces and networks that participate in EIGRP routing, enter the following command:

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

Step 5 To change the interface delay value used in EIGRP distance calculations, enter the following commands:

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

Feature History for EIGRP

Table 31-1 lists each feature change and the platform release in which it was implemented.

Table 31-1 Feature History for EIGRP

Feature Name	Platform Releases	Feature Information
EIGRP Support	7.0(1)	Support was added for routing data, performing authentication, and redistributing and monitoring routing information using the Enhanced Interior Gateway Routing Protocol (EIGRP). We introduced the following command: route eigrp .
Dynamic Routing in Multiple Context Mode	9.0(1)	EIGRP routing is supported in multiple context mode.
Clustering	9.0(1)	For EIGRP, bulk synchronization, route synchronization, and layer 2 load balancing are supported in the clustering environment. We introduced or modified the following commands: show route cluster , debug route cluster , show mfib cluster , debug mfib cluster .
EIGRP Auto-Summary	9.2(1)	For EIGRP, the Auto-Summary field is now disabled by default.

