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).

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 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.

EIGRPv6

EIGRP for IPv6 can be configured just like EIGRP IPv4. EIGRPv6 communicates only with IPv6 peers and advertises only IPv6 routes. EIGRPv6 is similar to EIGRPv4 in many ways than one:

- DUAL is used for route calculation and selection with the same metrics.
- It is scalable to large network implementations.
- Neighbor, routing, and topology tables are maintained.
- Both equal-cost load balancing and unequal-cost load balancing are offered.

However, EIGRPv6 differ from EIGRPv4 in many ways, such as:

- The network command is not used in IPv6; EIGRP is configured using links.
- You must explicitly enable EIGRPv6 on each interface during configuration.

Null0 and EIGRP

By default, EIGRP advertises the Null0 route to the peer as summary route to prevent the router that is advertising the summary, from forwarding any packets that it does not have a route.

For example, consider the two routers, R1 and R2. The three interfaces on R1 have these networks- 192.168.0.0/24, 192.168.1.0/24, and 192.168.3.0/24. Configure R1 with summary route 192.168.0.0/22 and

advertise it to R2. When R2 has an IP packet for 192.168.2.x, it would forward it to R1. R1, would drop the packet as it does not have 192.168.2.x in its routing table. However, if R1 is also connected to an ISP and it has a default route pointing to the ISP, the 192.168.2.x packet is forwarded to the ISP. To prevent this forwarding action, EIGRP generates an entry that matches the summary route, pointing to Null0. Thus, when packets for 192.168.2.x are received, R1 will drop the packet instead of using the default route.

Guidelines for EIGRP

Firewall Mode Guidelines

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

Cluster Guidelines

For a cluster in individual interface mode, EIGRP can form neighbor relationships with cluster peers using cluster pools as router IDs.

IPv6 Guidelines

Supports IPv6 routing.

Context Guidelines

- EIGRP instances cannot form adjacencies with each other across shared interfaces because, by default, inter-context exchange of multicast traffic is not supported across shared interfaces. However, you can use the static neighbor configuration under EIGRP process configuration under EIGRP process to bring up EIGRP neighbourship on a shared interface.
- Inter-context EIGRP on separate interfaces is supported.

Redistribution Guidelines

When EIGRP is configured on a device that is a part of OSPF network or vice versa, ensure that OSPF-router is configured to tag the route (EIGRP does not support route tag).

When redistributing EIGRP into OSPF and OSPF into EIGRP, a routing loop occurs when there is an outage on one of the links, interfaces, or even when the route originator is down. To prevent the redistribution of routes from one domain back into the same domain, a router can tag a route that belongs to a domain while it is redistributing, and those routes can be filtered on the remote router based on the same tag. Because the routes will not be installed into the routing table, they will not be redistributed back into the same domain.

Additional Guidelines

- A maximum of one EIGRP process is supported.
- EIGRP adjacency flap occurs whenever a configuration change is applied which results in modifying the routing information (sent or received) from neighbors especially in distribute lists, offset lists, and changes to summarization. After the routers are synchronized, EIGRP reestablishes the adjacency between neighbors. When an adjacency is torn down and reestablished, all learned routes between the neighbors are erased and the entire synchronization between the neighbors is performed newly with the new distribute list.

- There is no restriction on the maximum number of EIGRP neignbours. However, to prevent unnecessary EIGRP flap, we recommend you to limit the number to 500 per unit.

Configure 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.

Enable EIGRP

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

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

To enable EIGRP IPv6 routing process, enter the following command:

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

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 Configure Interfaces for EIGRP, on page 7.

Enable 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

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 section Configure Passive Interfaces, on page 9.

Step 3 Configure the stub routing process:

eigrp stub {**receive-only** | [**connected**] [**redistributed**] [**static**] [**summary**]}

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]}
```

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.

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.

Customize EIGRP

This section describes how to customize the EIGRP routing.

Define 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

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 Configure Passive Interfaces, on page 9.

Configure 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

To enable EIGRP IPv6 routing process, enter the following command:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

You can configure one or more network statements with this command. However, the **network** command is not used in EIGRP IPv6.

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 Define a Network for an EIGRP Routing Process, on page 6.

Step 3 Control the sending or receiving of candidate default route information:

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}
```

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.

For more information see, Configure Default Information in EIGRP, on page 19.

Step 4 Enable MD5 authentication of EIGRP packets:

authentication mode eigrp as-num **md5**

Example:

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

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
```

For more information see Enable EIGRP Authentication on an Interface, on page 11.

Step 5 Set the delay value:

delay *value*

Example:

```
ciscoasa(config-if)# delay 200
```

The *value* argument entered is in tens of microseconds. To set the delay for 2000 microseconds, enter a *value* of 200.

To view the delay value assigned to an interface, use the **show interface** command.

For more information, see Change the Interface Delay Value, on page 10.

Step 6 Change the hello interval:

hello-interval eigrp as-num seconds

Example:

```
ciscoasa(config)# hello-interval eigrp 2 60
```

For more information see Customize the EIGRP Hello Interval and Hold Time, on page 17.

Step 7 Change the hold time:

hold-time eigrp as-num seconds

Example:

```
ciscoasa(config)# hold-time eigrp 2 60
```

For more information see Customize the EIGRP Hello Interval and Hold Time, on page 17.

Configure Passive Interfaces

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

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing. You can configure one or more **network** statements with this command:

network ip-addr [mask]

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 Define a Network for an EIGRP Routing Process, on page 6.

Step 3 Prevent an interface from sending or receiving EIGRP routing message:

passive-interface {**default** | if-name}

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

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.

Configure 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.

Procedure

Step 1 Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

interface phy_if

Example:

```
ciscoasa(config)# interface inside
```

Step 2 Create the summary address:

summary-address eigrp *as-num address mask* [*distance*]

Example:

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

To create the summary address for EIGRP IPv6:

ipv6 summary-address eigrp *as-num address mask* [*distance*]

Example:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 summary-address eigrp 1 4001::1/64 ?
interface mode commands/options:
  <1-255>  Administrative distance
```

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.

Change the Interface Delay Value

The interface delay value is used in EIGRP distance calculations. You can modify this value on a per-interface basis.

Procedure

Step 1 Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

interface phy_if

Example:

```
ciscoasa(config)# interface inside
```

Step 2 Set a delay value:

delay *value*

Example:

```
ciscoasa(config-if)# delay 200
```

The *value* argument entered is in tens of microseconds. To set the delay for 2000 microseconds, you enter a *value* of 200.

Note
To view the delay value assigned to an interface, use the **show interface** command.

Enable 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp *as-num*

Example:

```
ciscoasa(config)# router eigrp 2
```

The as-num argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network *ip-addr* [*mask*]

Example:

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

- 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 falls 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 Configure EIGRP, on page 4.

Step 3 Enter interface configuration mode for the interface on which you are configuring EIGRP message authentication:

interface *phy_if*

Example:

```
ciscoasa(config)# interface inside
```

Step 4 Enable MD5 authentication of EIGRP packets:

authentication mode eigrp *as-num* md5

Example:

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

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 Configure the key used by the MD5 algorithm:

authentication key eigrp *as-num key* key-id *key-id*

Example:

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- 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 include up to 16 characters, including alphabets, numbers and special characters.White spaces are not allowed, in the key argument.
- The key-id argument is a number that can range from 0 to 255.

Define 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.

Procedure

Step 1 Create an EIGRP routing process and enters router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

Step 3 Define the static neighbor:

neighbor *ip-addr* **interface** *if_name*

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

Example:

For EIGRP IPv6

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

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.

Note
You must configure the interfaces network that participate in the EIGRP routing for the neighborship configuration to be effective.

Redistribute 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 (Optional) Specifies the default metrics that should be applied to routes redistributed into the EIGRP routing process:

default-metric bandwidth delay reliability loading mtu

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

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 Redistribute connected routes into the EIGRP routing process:

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

Example:

```
ciscoasa(config-router)# redistribute connected [metric bandwidth delay reliability loading
 mtu] [route-map map_name]
```

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.

Step 4 Redistribute static routes into the EIGRP routing process:

redistribute static [**route-map** map_name]

Example:

```
ciscoasa(config-router)# redistribute static [route-map map_name]
```

This command will pass all the static routes to EIGRP. To redistribute selective static routes, ensure to create an access-list with the static route and then include it in a route-map:

Example:

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

After creating the route-map, include it in the redistribute command as follows:

Example:

```
ciscoasa(config)#router eigrp 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

Step 5 Redistribute routes from an OSPF routing process 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:

```
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]
```

Step 6 Redistribute routes from a RIP routing process into the EIGRP routing process:

redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

Example:

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

Filter 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

ciscoasa(config-router)# **network** ip-addr [mask]

Example:

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

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 Configure Interfaces for EIGRP, on page 7.

Step 3 Filter networks sent in EIGRP routing updates:

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

Example:

```
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]
```

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.

Step 4 Filter networks received in EIGRP routing updates:

distribute-list acl **in** [**interface** if_name]

Example:

```
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]
```

You can specify an interface to apply the filter to only those updates that are received by that interface.

Customize 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.

Procedure

Step 1 Enter interface configuration mode for the interface on which you are configuring the hello interval or advertised hold time:

interface phy_if

Example:

```
ciscoasa(config)# interface inside
```

Step 2 Change the hello interval:

hello-interval eigrp as-num seconds

Example:

```
ciscoasa(config)# hello-interval eigrp 2 60
```

To change the hello interval for EIGRP IPv6:

ipv6 hello-interval eigrp as-num seconds

Example:

```
ciscoasa(config)# ipv6 hello-interval eigrp 2 60
```

Step 3 Change the hold time:

hold-time eigrp as-num seconds

Example:

```
ciscoasa(config)# hold-time eigrp 2 60
```

To change the hold time for EIGRP IPv6:

ipv6 hold-time eigrp as-num seconds

Example:

```
ciscoasa(config)# ipv6 hold-time eigrp 2 60
```

Disable 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Disable automatic route summarization:

no auto-summary

Example:

```
ciscoasa(config-router)# no auto-summary
```

Automatic summary addresses have a default administrative distance of 5.

Configure 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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

router eigrp as-num

Example:

```
ciscoasa(config)# router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Configure the interfaces and networks that participate in EIGRP routing:

network ip-addr [mask]

Example:

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

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 Configure Interfaces for EIGRP, on page 7.

Step 3 Control the sending or receiving of candidate default route information:

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}
```

Note
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.

Disable 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:

Procedure

Step 1 Enter interface configuration mode for the interface on which you are changing the delay value used by EIGRP:

interface phy_if

Example:

```
ciscoasa(config)# interface phy_if
```

Step 2 Disable the split horizon:

no split-horizon eigrp *as-number*

Example:

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

To disable the split horizon for EIGRP IPv6:

no ipv6 split-horizon eigrp *as-number*

Example:

```
ciscoasa(config-if)# no ipv6 split-horizon eigrp 2
```

Restart the EIGRP Process

You can restart an EIGRP process or clear redistribution or clear counters.

Procedure

Restart an EIGRP process or clear redistribution or clear counters:

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

Example:

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

Configure an EIGRPv6 Process

This section describes how to enable and configure the EIGRP IPv6 process on your system.

Enable EIGRPv6

You can only enable one EIGRPv6 routing process on the ASA.

Procedure

Create an EIGRP for IPv6 routing process and enter router configuration mode for this EIGRP process:

ipv6 router eigrp *as-num*

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Filter Rules in EIGRPv6

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.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Apply a prefix list to EIGRP for IPv6 routing updates that are advertised from an interface:

distribute-list prefix-list name **out interface** if_name

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl out interface interface2
```

You can enter multiple **distribute-list** commands in your EIGRPv6 router configuration.

Step 3 Apply a prefix list to EIGRP for IPv6 routing updates that are received on an interface:

distribute-list prefix-list name **in** [**interface** if_name]

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl in interface interface1
```

Configure Interfaces for EIGRPv6

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 the ASA 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.

Procedure

Step 1 Create an EIGRP IPv6 routing process and enter router configuration mode for this EIGRP process:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Control the sending or receiving of candidate default route information:

no default-information {**in** | **out** | **WORD**}

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

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.

For more information see, Configure Default Information in EIGRP, on page 19.

Step 3 Change the hello interval:

ipv6 hello-interval eigrp as-num seconds

Example:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hello-interval eigrp 2 60
```

For more information see Customize the EIGRP Hello Interval and Hold Time, on page 17.

Step 4 Change the hold time:

ipv6 hold-time eigrp as-num seconds

Example:

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hold-time eigrp 2 60
```

For more information see Customize the EIGRP Hello Interval and Hold Time, on page 17.

Configure Passive Interfaces for EIGRPv6

You can configure one or more interfaces as passive interfaces. In EIGRPv6, a passive interface does not send or receive routing updates.

Procedure

Step 1 Create an EIGRPv6 routing process and enter router configuration mode for this EIGRP process:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

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

passive-interface {**default** | if-name}

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# passive-interface {default}
```

Using the **default** keyword disables EIGRPv6 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 EIGRPv6 router configuration.

Redistribute Routes Into EIGRPv6

You can redistribute routes discovered OSPF, BGP, ISIS into the EIGRP IPv6 routing process. You can also redistribute static and connected routes into the EIGRP routing process.

Procedure

Step 1 Create an EIGRP routing process and enter router configuration mode for this EIGRP process:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 (Optional) Specifies the default metrics that should be applied to routes redistributed into the EIGRP routing process:

default-metric[bandwidth | delay | reliability | loading | mtu]

Example:

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth 10 delay 20
```

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.

Note
When you specify the default-metric, the show run-config command in ASA will not display the default-metric configuration.

Step 3 Redistribute connected routes into the EIGRP routing process:

redistribute connected [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

Example:

```
ciscoasa(config-router)# redistribute connected [metric bandwidth 100] [route-map map_name]
```

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.

Step 4 Redistribute static routes into the EIGRP routing process:

redistribute static [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

Example:

```
ciscoasa(config-router): redistribute static [route-map map_name]
```

Step 5 Redistribute routes from an OSPF routing process 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:

```
ciscoasa(config-router)# redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}][route-map map_name]
```

Step 6 Redistribute routes from a BGP routing process into the EIGRP routing process:

redistribute bgp [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

Example:

```
ciscoasa(config-router)# redistribute bgp [route-map map_name]
```

Step 7 Redistribute routes from a ISIS routing process into the EIGRP routing process:

redistribute isis [**level-1 | level-2 | level-1-2**][**include-connected | metric number | metric-type | tag | route-map map_name**]

Example:

```
ciscoasa(config-router)# redistribute isis [level-1] [metric delay 20 [route-map map_name]]
```

Define an EIGRPv6 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.

Procedure

Step 1 Create an EIGRP routing process and enters router configuration mode for this EIGRP process:

ipv6 router eigrp as-num

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
```

The *as-num* argument is the autonomous system number of the EIGRP routing process.

Step 2 Define the static neighbor:

neighbor *ip-addr* **interface** *if_name*

Example:

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

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.

Monitoring for 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:

- **router-id**

  Displays the router-id for this EIGRP process.

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  Displays the EIGRP event log.

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  Displays the interfaces participating in EIGRP routing.

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  Displays the EIGRP neighbor table.

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Displays the EIGRP topology table.

- **show eigrp** [*as-number*] **traffic**

  Displays EIGRP traffic statistics.

- **show mfib cluster**

  Displays MFIB information in terms of forwarding entries and interfaces.

- **show route cluster**

  Displays additional route synchronization details for clustering.

- **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.

- **show ipv6 eigrp** *as-number* **interface** *interface*

  Displays the EIGRP IPv6 topology table.

- **show ipv6 eigrp** [*as-number*] **traffic**

  Displays EIGRP IPv6 traffic statistics.

- **show ipv6 eigrp** [as-number] **neighbors** [*if-name*]

  Displays the EIGRP IPv6 neighbor table.

- **show ipv6 eigrp interfaces** [*if-name*]

  Displays neighbor related information with respect to given interface.

- **show ipv6 eigrp** [*as-number*] **topology** [*ipv6-address* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  Displays the EIGRP IPv6 topology table.

- **show ipv6 eigrp** [*as-number*] **events** [{*start - end*} | **type**]

  Displays the EIGRP IPv6 event log.

- **show ipv6 eigrp timers**

  Displays the configured hello timer and hold timer.

Example for EIGRP

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

Procedure

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
```

History for EIGRP

Table 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.
EIGRPv6 Support	9.20(1)	IPv6 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: **ipv6 eigrp**, **ipv6 hello-interval eigrp**, **ipv6 hold-time eigrp**, **ipv6 split-horizon eigrp**, **show ipv6 eigrp interface**, **show ipv6 eigrp traffic**, **show ipv6 eigrp neighbors**, **show ipv6 eigrp interface**, **ipv6 summary-address eigrp**, **show ipv6 eigrp topology**, **show ipv6 eigrp events**, **show ipv6 eigrp timers**, **clear ipv6 eigrp**, and **clear configure ipv6 router eigrp**.