

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, on page 1
- Guidelines for EIGRP, on page 2
- Configure an EIGRP Process, on page 3
- Configure EIGRP, on page 4
- Customize EIGRP, on page 6
- Monitoring for EIGRP, on page 19
- History for EIGRP, on page 20

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.

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

EIGRP does not form neighbor relationships with cluster peers in individual interface mode.

IPv6 Guidelines

Does not support IPv6.

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 an EIGRP Process

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP**.

Step 2 Enable the EIGRP routing process by checking the **Enable this EIGRP process** check box on the Process Instances tab. See Enable EIGRP, on page 4 or Enable EIGRP Stub Routing, on page 5.

Step 3 Define the networks and interfaces that will participate in EIGRP routing on the Setup > Networks tab. See Define a Network for an EIGRP Routing Process, on page 7 for more information.

Step 4 (Optional) Define route filters on the Filter Rules pane. Route filtering provides more control over the routes that are allowed to be sent or received in EIGRP updates. See Filter Networks in EIGRP, on page 14 for more information.

Step 5 (Optional) Define route redistribution in the Redistribution pane.

You can redistribute routes discovered by RIP and OSPF to the EIGRP routing process. You can also redistribute static and connected routes to the EIGRP routing process. See Redistribute Routes Into EIGRP, on page 12 for more information.

Step 6 (Optional) Define static EIGRP neighbors on the Static Neighbor pane.

See Define an EIGRP Neighbor, on page 11 for more information.

Step 7 (Optional) Define summary addresses on the Summary Address pane.

See Configure the Summary Aggregate Addresses on Interfaces, on page 9 for more information about defining summary addresses.

Step 8 (Optional) Define interface-specific EIGRP parameters on the Interfaces pane. These parameters include EIGRP message authentication, hold time, hello interval, delay metric, and the use of split-horizon. See Configure Interfaces for EIGRP, on page 7 for more information.

Step 9 (Optional) Control the sending and receiving of default route information in EIGRP updates on the Default Information pane. By default, default routes are sent and accepted. See Configure Default Information in EIGRP, on page 16 for more information.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The EIGRP Setup pane appears.

The three tabs on the main EIGRP Setup pane used to enable EIGRP are as follows:

- The Process Instances tablets you enable an EIGRP routing process for each context. Single context mode and multiple context mode are both supported. See Enable EIGRP, on page 4 and the Enable EIGRP Stub Routing, on page 5 for more information.
- The Networks tablets 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. See Define a Network for an EIGRP Routing Process, on page 7 for more information.

- The Passive Interfaces tablets you configure one or more interfaces as passive interfaces. In EIGRP, a passive interface does not send or receive routing updates.The Passive Interface table lists each interface that is configured as a passive interface.

Step 2 Check the **Enable this EIGRP process** check box.

You can only enable one EIGRP routing process on the device. You must enter an autonomous system number (AS) for the routing process in the EIGRP Process field before you can save your changes.

Step 3 In the EIGRP Process field, enter the autonomous system (AS) number for the EIGRP process. The AS number can be from 1 to 65535.

Step 4 (Optional) Click **Advanced** to configure the EIGRP process settings, such as the router ID, default metrics, stub routing, neighbor changes, and the administrative distances for the EIGRP routes.

Step 5 Click the **Networks** tab.

Step 6 To add a new network entry, click **Add**.

The **Add EIGRP Network** dialog box appears. To remove a network entry, choose an entry in the table and click **Delete**.

Step 7 Choose the AS number of the EIGRP routing process from the drop-down list.

Step 8 Enter the IP address of the networks to participate in the EIGRP routing process in the IP Address field.

Note
To change a network entry, you must first remove the entry and then add a new one. You cannot edit existing entries.

Step 9 Enter a network mask to apply to the IP address in the Network Mask field.

Step 10 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the autonomous system (AS) number for the EIGRP process. The AS number can be from 1 to 65535.

Step 4 Click **Advanced** to configure the EIGRP stub routing process.

The **Edit EIGRP Process Advanced Properties** dialog box appears.

Step 5 In the **Stub** area on the **Edit EIGRP Process Advanced Properties** dialog box, choose one or more of the following EIGRP stub routing processes:

- Stub Receive only—Configures the EIGRP stub routing process to receive route information from the neighbor routers but does not send route information to the neighbors. If this option is selected, you cannot select any of the other stub routing options.
- Stub Connected—Advertises connected routes.
- Stub Static—Advertises static routes.
- Stub Redistributed—Advertises redistributed routes.
- Stub Summary—Advertises summary routes.

Step 6 Click **OK**.

Step 7 Click the **Networks** tab.

Step 8 Click **Add** to add a new network entry.

The **Add EIGRP Network** dialog box appears. To remove a network entry, choose the entry in the table and click **Delete**.

Step 9 Choose the AS number of the EIGRP routing process from the drop-down list.

Step 10 Enter the IP address of the networks to participate in the EIGRP routing process in the **IP Address** field.

Note
To change a network entry, you must first remove the entry and then add a new one. You cannot edit existing entries.

Step 11 Enter a network mask to apply to the IP address in the **Network Mask** field.

Step 12 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the autonomous system (AS) number for the EIGRP process. The AS number can be from 1 to 65535.

Step 4 Click the **Networks** tab.

Step 5 Click **Add** to add a new network entry.

The **Add EIGRP Network** dialog box appears. To remove a network entry, choose the entry in the table and click **Delete**.

Step 6 Choose the AS number of the EIGRP routing process from the drop-down list.

Step 7 Enter the IP address of the networks to participate in the EIGRP routing process in the **IP Address** field.

Note
To change a network entry, you must first remove the entry and then add a new one. You cannot edit existing entries.

Step 8 Enter a network mask to apply to the IP address in the **Network Mask** field.

Step 9 Click **OK**.

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 the ASA that includes the network to which the interface is attached, and prevent that interface from sending or receiving EIGRP updates.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 Click **OK**.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interfaces**.

The **Interface** pane appears and displays the EIGRP interface configurations. The **Interface Parameters** table displays all of the interfaces on the ASA and lets you modify the following settings on a per-interface basis:

- Authentication key and mode.
- The EIGRP hello interval and hold time.
- The interface delay metric used in EIGRP metric calculations.
- The use of split-horizon on the interface.

Step 5 Choose an interface entry by double-clicking an interface entry, or choose the entry and click **Edit**.

The **Edit EIGRP Interface Entry** dialog box appears.

Step 6 In the **EIGRP Process** field, enter the AS number for the EIGRP process. The AS number can range from 1 to 65535.

Step 7 In the **Hello Interval** field, enter the interval between EIGRP hello packets sent on an interface.

Valid values range from 1 to 65535 seconds. The default value is 5 seconds.

Step 8 In the **Hold Time** field, enter the hold time, in seconds. Valid values range from 1 to 65535 seconds. The default value is 15 seconds.

Step 9 Check the **Enable** check box for Split Horizon.

Step 10 In the **Delay** field, enter the delay value. The delay time is in tens of microseconds. Valid values range from 1 to 16777215.

Step 11 Check the **Enable MD5 Authentication** check box to enable MD5 authentication of EIGRP process messages.

Step 12 Enter the Key or Key ID values.

- In the **Key** field, enter the key to authenticate EIGRP updates. The key can contain up to 16 characters.
- In the **Key ID** field, enter the key identification value. Valid values range from 1 to 255.

Step 13 Click **OK**.

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. In ASDM, the Passive Interface table lists each interface that is configured as a passive interface.

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 Click **OK**.

Step 4 Click the **Passive Interfaces** tab.

Step 5 Choose the interface that you want to configure from the drop-down list.

Step 6 Check the **Suppress routing updates on all interfaces** check box to specify all interfaces as passive. Even if an interface is not shown in the Passive Interface table, it will be configured as passive when the check box is checked.

Step 7 Click **Add** to add a passive interface entry.

The **Add EIGRP Passive Interface** dialog box appears. Choose the interface that you want to make passive and click **Add**. To remove a passive interface, choose the interface in the table and click **Delete**.

Step 8 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interfaces**.

The **Interface** pane shows the EIGRP interface configurations. The Interface Parameters table shows all of the interfaces on the ASA and lets you modify the settings on a per-interface basis. For more information about these settings, see Configure Interfaces for EIGRP, on page 7.

Step 2 To configure the EIGRP parameters for an interface, double-click an interface entry or select the entry and click **Edit**.

Step 3 Click **OK**.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Summary Address**.

The **Summary Address** pane displays a table of the statically-defined EIGRP summary addresses. By default, EIGRP summarizes subnet routes to the network level. You can create statically defined EIGRP summary addresses to the subnet level from the **Summary Address** pane.

Step 5 Click **Add** to add a new EIGRP summary address, or to click **Edit** to edit an existing EIGRP summary address in the table.

The **Add Summary Address** or **Edit Summary Address** dialog box appears. You can also double-click an entry in the table to edit that entry.

Step 6 In the **EIGRP Process** field, enter the autonomous system (AS) number for the EIGRP process. The AS number can be from 1 to 65535.

Step 7 In the **Interface** drop-down list, choose the interface from which the summary address is advertised.

Step 8 In the **IP Address** field, enter the IP address of the summary route.

Step 9 In the **Netmask** field, choose or enter the network mask to apply to the IP address.

Step 10 Enter the administrative distance for the route in the **Administrative Distance** field. If left blank, the route has the default administrative distance of 5.

Step 11 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interface**.

The **Interface** pane shows the EIGRP interface configurations. The **Interface Parameters** table shows all of the interfaces on the ASA and lets you modify the settings on a per-interface basis. For more information about these settings, see Configure Interfaces for EIGRP, on page 7.

Step 2 Double-click an interface entry or choose the Interface entry and click **Edit** to configure the delay value in the EIGRP parameters for an interface.

The **Edit EIGRP Interface Entry** dialog box appears.

Step 3 In the **Delay** field, enter the delay time, which is in tens of microseconds. Valid values are from 1 to 16777215.

Step 4 Click **OK**.

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 In the man ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the autonomous system (AS) number for the EIGRP process. The AS number can range from 1 to 65535.

Step 4 Click the **Networks** tab.

Step 5 Click **Add** to add a new network entry.

The **Add EIGRP Network** dialog box appears. To remove a network entry, choose the entry in the table and click **Delete**.

Step 6 Choose the AS number of the EIGRP routing process from the drop-down list.

Step 7 In the **IP Address** field, enter the IP address of the networks to participate in the EIGRP routing process.

Note
To change a network entry, you must first remove the entry and then add a new one. You cannot edit existing entries.

Step 8 In the **Network Mask** field, choose or enter a network mask to apply to the IP address.

Step 9 Click **OK**.

Step 10 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interfaces**.

The **Interface** pane displays the EIGRP interface configurations. The **Interface Parameters** table displays all of the interfaces on the ASA and lets you modify the settings on a per-interface basis. For more information about these settings, see Configure Interfaces for EIGRP, on page 7.

Step 11 Check the **Enable MD5 Authentication** check box to enable MD5 authentication of EIGRP process messages. After you check this check box, provide one of the following:

- In the **Key** field, enter the key to authenticate EIGRP updates. The key can include up to 16 characters.
- In the **Key ID** field, enter the key identification value. Valid values range from 1 to 255.

Step 12 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the AS number for the EIGRP process. The AS number can range from 1 to 65535.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Static Neighbor**.

The **Static Neighbor** pane appears and displays the statically-defined EIGRP neighbors. An EIGRP neighbor sends EIGRP routing information to and receives EIGRP routing information from the ASA. Normally, neighbors are dynamically discovered through the neighbor discovery process. However, on point-to-point, nonbroadcast networks, you must statically define the neighbors.

Each row of the **Static Neighbor** table displays the EIGRP autonomous system number for the neighbor, the neighbor IP address, and the interface through which the neighbor is available.

From the **Static Neighbor** pane, you can add or edit a static neighbor.

Step 5 Click **Add** or **Edit** to add or edit a EIGRP static neighbor.

The **Add** or **Edit EIGRP Neighbor Entry** dialog box appears.

Step 6 Choose the **EIGRP AS** number from the drop-down list for the EIGRP process for which the neighbor is being configured.

Step 7 Choose the **Interface Name** from the **Interface Name** drop-down list, which is the interface through which the neighbor is available.

Step 8 Enter the IP address of the neighbor in the **Neighbor IP Address** field.

Step 9 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the AS number for the EIGRP process. The AS number can range from 1 to 65535.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Redistribution**.

The **Redistribution** pane displays the rules for redistributing routes from other routing protocols to the EIGRP routing process. When redistributing static and connected routes to the EIGRP routing process, metrics are not required to be configured, although this is recommended. Each row of the **Redistribution** pane table includes a route redistribution entry.

Step 5 Click **Add** to add a new redistribution rule. If you are editing an existing redistribution rule, go to Step 6.

The **Add EIGRP Redistribution Entry** dialog box appears.

Step 6 Choose the address in the table and click **Edit** to edit an existing EIGRP static neighbor, You can also double-click an entry in the table to edit that entry.

The **Edit EIGRP Redistribution Entry** dialog box appears.

Step 7 Choose the AS number of the EIGRP routing process to which the entry applies from the drop-down list.

Step 8 In the **Protocol** area, click the radio button next to one of the following protocols for the routing process:

- **Static** to redistribute static routes to the EIGRP routing process. Static routes that fall within the scope of a network statement are automatically redistributed into EIGRP; you do not need to define a redistribution rule for them.
- **Connected** to redistribute connected routes into the EIGRP routing process. Connected routes that fall within the scope of a network statement are automatically redistributed into EIGRP; you do not need to define a redistribution rule for them.
- **RIP** to redistributes routes discovered by the RIP routing process to EIGRP.
- **OSPF** to redistribute routes discovered by the OSPF routing process to EIGRP.

Step 9 In the **Optional Metrics** area, choose one of the following metrics used for the redistributed route:

- **Bandwidth**, which is the EIGRP bandwidth metric in kilobits per second. Valid values range from 1 to 4294967295.
- **Delay**, which is the EIGRP delay metric, in 10-microsecond units. Valid values range from 0 to 4294967295.
- **Reliability**, which is the EIGRP reliability metric. Valid values range from 0 to 255; 255 indicates 100 percent reliability.
- **Loading**, which is the EIGRP effective bandwidth (loading) metric. Valid values range from 1 to 255; 255 indicates 100 percent loaded.
- **MTU**, which is the MTU of the path. Valid values range from 1 to 65535.

Step 10 Choose the route map from the **Route Map** drop-down list to define which routes are redistributed into the EIGRP routing process. For more details about how to configure a route map, see Route Maps.

Step 11 In the **Optional OSPF Redistribution** area, click one of the following OSPF radio buttons to further specify which OSPF routes are redistributed into the EIGRP routing process:

- **Match Internal** to match routes internal to the specified OSPF process.
- **Match External 1** to match type 1 routes external to the specified OSPF process.
- **Match External 2** to match type 2 routes external to the specified OSPF process.
- **Match NSSA-External 1** to match type 1 routes external to the specified OSPF NSSA.
- **Match NSSA-External 2** to match type 2 routes external to the specified OSPF NSSA.

Step 12 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 In the **EIGRP Process** field, enter the AS number for the EIGRP process. The AS number can range from 1 to 65535.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Filter Rules**.

The **Filter Rules** pane appears and displays the route filtering rules configured for the EIGRP routing process. Filter rules let you control which routes are accepted or advertised by the EIGRP routing process.

Each row of the **Filter Rule** table describes a filter rule for a specific interface or routing protocol. For example, a filter rule with a direction of in on the outside interface would apply filtering to any EIGRP updates received on the outside interface. A filter rule with a direction of out with OSPF 10 specified as the routing protocol would apply the filter rules to routes redistributed into the EIGRP routing process in outbound EIGRP updates.

Step 5 Click **Add** to add a filter rule. If you are editing an already existing filter rule, skip to Step 6.

The **Add Filter Rules** dialog box appears.

Step 6 To edit a filter rule, choose the filter rule in the table and click **Edit**.

The **Edit Filter Rules** dialog box appears. You can also double-click a filter rule to edit the rule. To remove a filter rule, choose the filter rule in the table and click **Delete**.

Step 7 Choose the AS number from the drop-down list of the EIGRP routing process to which the entry applies.

Step 8 Choose the direction of the filter routes from the drop-down list.

Choose **in** for rules that filter routes from incoming EIGRP routing updates. Choose **out** to filter routes from EIGRP routing updates that are sent by the ASA.

If you choose **out**, the **Routing** process field becomes active. Choose the type of route to be filtered. You can filter routes redistributed from static, connected, RIP, and OSPF routing processes. Filters that specify a routing process filter those routes from updates sent on all interfaces.

Step 9 Enter the OSPF process ID in the **ID** field.

Step 10 Click the **Interface** radio button and choose the interface to which the filter applies.

Step 11 Click **Add** or **Edit** to define an ACL for the filter rule. Clicking **Edit** opens the **Network Rule** dialog box for the selected network rule.

Step 12 In the **Action** drop-down list, choose **Permit** to allow the specified network to be advertised; choose **Deny** to prevent the specified network from being advertised.

Step 13 In the **IP Address** field, type IP address of the network being permitted or denied. To permit or deny all addresses, use the IP address **0.0.0.0** with a network mask of **0.0.0.0**.

Step 14 From the **Netmask** drop-down list, choose the network mask applied to the network IP address. You can type a network mask into this field or select one of the common masks from the list.

Step 15 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 Click **OK**.

Step 4 Choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interfaces**.

The **Interface** pane appears and displays all of the EIGRP interface configurations.

Step 5 Double-click an interface entry or choose the entry and click **Edit**.

The **Edit EIGRP Interface Entry** dialog box appears.

Step 6 Choose the EIGRP AS number from the drop-down list, which is populated from system numbers that were set up when you enabled the EIGRP routing process.

Step 7 In the **Hello Interval** field, enter the interval between EIGRP hello packets sent on an interface.

Valid values range from 1 to 65535 seconds. The default value is 5 seconds.

Step 8 In the **Hold Time** field, specify the hold time, in seconds.

Valid values range from 1 to 65535 seconds. The default value is 15 seconds.

Step 9 Click **OK**.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 Click the **Process Instance** tab.

Step 4 Click **Advanced**.

Step 5 In the **Summary** area, uncheck the **Auto-Summary** check box.

Note
This setting is enabled by default.

Step 6 Click **OK**.

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.

In ASDM, the Default Information pane displays a table of rules for controlling the sending and receiving of default route information in EIGRP updates. You can have one in and one out rule for each EIGRP routing process (only one process is currently supported).

By default, default routes are sent and accepted. To restrict or disable the sending and receiving of default route information, perform the following steps:

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The main **EIGRP Setup** pane appears.

Step 2 Check the **Enable EIGRP routing** check box.

Step 3 Click **OK**.

Step 4 Do one of the following:

- Click **Add** to create a new entry.
- To edit an entry, double-click the entry in the table or select an entry in the table and click **Edit**.

  The **Add Default Information** or **Edit Default Information** dialog box appears for that entry. The EIGRP AS number is automatically selected in the EIGRP field.

Step 5 In the **Direction** field, choose the direction for the rule from the following options:

- **in**—The rule filters default route information from incoming EIGRP updates.
- **out**—The rule filters default route information from outgoing EIGRP updates.

You can have one in rule and one out rule for each EIGRP process.

Step 6 Add network rules to the network rule table. The network rules define which networks are allowed and which are not when receiving or sending default route information. Repeat the following steps for each network rule you are adding to the default information filter rule.

a) Click **Add** to add a network rule. Double-click an existing network rule to edit the rule.
b) In the **Action** field, click **Permit** to allow the network or **Deny** to block the network.
c) Enter the IP address and network mask of the network being permitted or denied by the rule in the IP Address and Network Mask fields.

   To deny all default route information from being accepted or sent, enter **0.0.0.0** as the network address and choose **0.0.0.0** as the network mask.

d) Click **OK** to add the specified network rule to the default information filter rule.

Step 7 Click **OK** to accept the default information filter rule.

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 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Interface**.

The **Interface** pane appears and displays the EIGRP interface configurations.

Step 2 Double-click an interface entry or choose the entry and click **Edit**.

The **Edit EIGRP Interface Entry** dialog box appears.

Step 3 Choose the EIGRP Autonomous system (AS) number from the drop-down list, which is populated from system numbers that were set up when you enabled the EIGRP routing process.

Step 4 Uncheck the **Split Horizon** check box.

Step 5 Click **OK**.

Restart the EIGRP Process

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

Procedure

Step 1 In the main ASDM window, choose **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.

The **EIGRP Setup** pane appears.

Step 2 Click **Reset**.

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, perform the following steps:

Procedure

Step 1 In the main ASDM window, choose **Monitoring** > **Routing** > **EIGRP Neighbor**.

Each row represents one EIGRP neighbor. For each neighbor, the list includes its IP address, the interface to which the neighbor is connected, the holdtime, the uptime, the queue length, the sequence number, the smoothed round trip time, and the retransmission timeout. The list of possible state changes are the following:

- NEW ADJACENCY—A new neighbor has been established.
- PEER RESTARTED—The other neighbor initiates the reset of the neighbor relationship. The router getting the message is not the one resetting the neighbor.
- HOLD TIME EXPIRED—The router has not heard any EIGRP packets from the neighbor within the hold-time limit.
- RETRY LIMIT EXCEEDED—EIGRP did not receive the acknowledgment from the neighbor for EIGRP reliable packets, and EIGRP has already tried to retransmit the reliable packet 16 times without any success.
- ROUTE FILTER CHANGED—The EIGRP neighbor is resetting because there is a change in the route filter.
- INTERFACE DELAY CHANGED—The EIGRP neighbor is resetting because there is a manual configuration change in the delay parameter on the interface.
- INTERFACE BANDWIDTH CHANGED—The EIGRP neighbor is resetting because there is a manual configuration change in the interface bandwidth on the interface.
- STUCK IN ACTIVE—The EIGRP neighbor is resetting because EIGRP is stuck in active state. The neighbor getting reset is the result of the stuck-in-active state.

Step 2 Click the EIGRP neighbor that you want to monitor.

Step 3 To remove the current list of neighbors, click **Clear Neighbors**.

Step 4 To refresh the current list of neighbors, click **Refresh**.

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

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 screen:**Configuration** > **Device Setup** > **Routing** > **EIGRP** .
Dynamic Routing in Multiple Context Mode	9.0(1)	EIGRP routing is supported in multiple context mode. We modified the following screen: **Configuration** > **Device Setup** > **Routing** > **EIGRP** > **Setup**.
Clustering	9.0(1)	For EIGRP, bulk synchronization, route synchronization, and layer 2 load balancing are supported in the clustering environment.
EIGRP Auto-Summary	9.2(1)	For EIGRP, the Auto-Summary field is now disabled by default. We modified the following screen: Configuration > Device Setup > Routing > EIGRP > Setup > Edit EIGRP Process Advanced Properties.