



Setting Up Virtual Routers

The following topics describe how to set up virtual routers in the Firepower System:

- [Virtual Routers, on page 1](#)
- [Routed Interfaces, on page 2](#)
- [Configuring Physical Routed Interfaces, on page 3](#)
- [Adding Logical Routed Interfaces, on page 5](#)
- [Deleting Logical Routed Interfaces, on page 7](#)
- [Configuring SFRP, on page 7](#)
- [Virtual Router Configuration, on page 9](#)
- [Adding Virtual Routers, on page 10](#)
- [DHCP Relay, on page 11](#)
- [Static Routes, on page 13](#)
- [Dynamic Routing, on page 15](#)
- [Virtual Router Filters, on page 27](#)
- [Adding Virtual Router Authentication Profiles, on page 30](#)
- [Viewing Virtual Router Statistics, on page 30](#)
- [Deleting Virtual Routers, on page 31](#)

Virtual Routers

You can configure a managed device in a Layer 3 deployment so that it routes traffic between two or more interfaces. To route traffic, you must assign an IP address to each interface and assign the interfaces to the virtual router. The interfaces assigned to virtual routers can be physical, logical, or link aggregation group (LAG) interfaces.

You can configure the system to route packets by making packet forwarding decisions according to the destination address. Interfaces configured as routed interfaces receive and forward the Layer 3 traffic. Routers obtain the destination from the outgoing interface based on the forwarding criteria, and access control rules designate the security policies to be applied.

In Layer 3 deployments, you can define static routes. In addition, you can configure Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) dynamic routing protocols. You can also configure a combination of static routes and RIP or static routes and OSPF.

Note that you can only configure virtual routers, physical routed interfaces, or logical routed interfaces on a 7000 or 8000 Series device.



Caution If a Layer 3 deployment fails for any reason, the device no longer passes traffic.

Related Topics

[LAG Configuration](#)

Routed Interfaces

You can set up routed interfaces with either physical or logical configurations. You can configure physical routed interfaces for handling untagged VLAN traffic. You can also create logical routed interfaces for handling traffic with designated VLAN tags.

In a Layer 3 deployment, the system drops any traffic received on an external physical interface that does not have a routed interface waiting for it. The system drops a packet if:

- It receives a packet with no VLAN tag, and you have not configured a physical routed interface for that port.
- It receives a VLAN-tagged packet, and you have not configured a logical routed interface for that port.

The system handles traffic that has been received with VLAN tags on switched interfaces by stripping the outermost VLAN tag on ingress prior to any rules evaluation or forwarding decisions. Packets leaving the device through a VLAN-tagged logical routed interface are encapsulated with the associated VLAN tag on egress. The system drops any traffic received with a VLAN tag after the stripping process completes.

You can add static Address Resolution Protocol (ARP) entries to a routed interface. If an external host needs to know the MAC address of the destination IP address it needs to send traffic to on your local network, it sends an ARP request. When you configure static ARP entries, the virtual router responds with an IP address and associated MAC address.

Note that disabling the **ICMP Enable Responses** option for logical routed interfaces does not prevent ICMP responses in all scenarios. You can add network-based rules to an access control policy to drop packets where the destination IP is the routed interface's IP and the protocol is ICMP.

If you have enabled the **Inspect Local Router Traffic** option on the managed device, the system drops the packets before they reach the host, thereby preventing any response.

The range of MTU values can vary depending on the model of the managed device and the interface type.



Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

If you change the parent physical interface to inline or passive, the system deletes all the associated logical interfaces.

Related Topics

[Advanced Settings](#)

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)

Snort® Restart Scenarios

Configuring Physical Routed Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can configure one or more physical ports on a managed device as routed interfaces. You must assign a physical routed interface to a virtual router before it can route traffic.



Caution

Adding a routed interface pair on a 7000 or 8000 Series device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click **Edit** (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Next to the interface you want to modify, click **Edit** (✎).
- Step 4** Click **Routed** to display the routed interface options.
- Step 5** If you want to apply a security zone, do one of the following:
 - Choose an existing security zone from the **Security Zone** drop-down list.
 - Choose **New** to add a new security zone; see [Creating Security Zone and Interface Group Objects](#).
- Step 6** If you want to specify a virtual router, do one of the following:
 - Choose an existing virtual router from the **Virtual Router** drop-down list.
 - Choose **New** to add a new virtual router; [Adding Virtual Routers, on page 10](#).
- Step 7** Check the **Enabled** check box to allow the routed interface to handle traffic. If you clear the check box, the interface becomes disabled so that users cannot access it for security purposes.
- Step 8** From the **Mode** drop-down list, choose an option to designate the link mode, or choose **Autonegotiation** to specify that the interface is configured to auto negotiate speed and duplex settings.

Mode settings are available only for copper interfaces.

Interfaces on 8000 Series appliances do not support half-duplex options.
- Step 9** From the **MDI/MDIX** drop-down list, choose an option to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX.

Normally, MDI/MDIX is set to Auto-MDIX, which automatically handles switching between MDI and MDIX to attain link.

MDI/MDIX settings are available only for copper interfaces.

Step 10 In the **MTU** field, choose a maximum transmission unit (MTU), which designates the largest size packet allowed.

The MTU is the Layer 2 MTU/MRU and not the Layer 3 MTU.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

Step 11 Next to **ICMP**, check the **Enable Responses** check box to allow the interface to respond to ICMP traffic such as pings and traceroute.

Step 12 Next to **IPv6 NDP**, check the **Enable Router Advertisement** check box to enable the interface to broadcast router advertisements.

Step 13 To add an IP address, click **Add**.

Step 14 In the **Address** field, enter the routed interface's IP address and subnet mask using CIDR notation.

Note the following:

- You cannot add network and broadcast addresses, or the static MAC addresses 00:00:00:00:00:00 and FF:FF:FF:FF:FF:FF.
- You cannot add identical IP addresses, regardless of subnet mask, to interfaces in virtual routers.

Step 15 If your organization uses IPv6 addresses and you want to set the IP address of the interface automatically, check the **Address Autoconfiguration** check box next to the **IPv6** field.

Step 16 For **Type**, choose either **Normal** or **SFRP**.

For SFRP options, see [Configuring SFRP, on page 7](#) for more information.

Step 17 Click **OK**.

- To edit an IP address, click **Edit** (.

- To delete an IP address, click **Delete** (.

When adding an IP address to a routed interface of a 7000 or 8000 Series device in a high-availability pair, you must add a corresponding IP address to the routed interface on the high-availability pair peer.

Step 18 To add a static ARP entry, click **Add**.

Step 19 In the **IP Address** field, enter an IP address for the static ARP entry.

Step 20 In the **MAC Address** field, enter a MAC address to associate with the IP address. Use the standard address format of six groups of two hexadecimal digits separated by colons (for example, 01:23:45:67:89:AB).

Step 21 Click **OK**.

Step 22 Click **Save**.

What to do next

Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv](#)

[Snort® Restart Scenarios](#)

Adding Logical Routed Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
N/A	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

For each physical routed interface, you can add multiple logical routed interfaces. You must associate each logical interface with a VLAN tag to handle traffic received by the physical interface with that specific tag. You must assign a logical routed interface to a virtual router to route traffic.



Caution

Adding a routed interface pair on 7000 or 8000 Series devices restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Add Interface**.

Step 4 Click **Routed** to display the routed interface options.

Step 5 From the **Interface** drop-down list, choose the physical interface where you want to add the logical interface.

Step 6 In the **VLAN Tag** field, enter a tag value that gets assigned to inbound and outbound traffic on this interface. The value can be any integer from 1 to 4094.

Step 7 If you want to apply a security zone, do one of the following:

- Choose an existing security zone from the **Security Zone** drop-down list.
- Choose **New** to add a new security zone; see [Creating Security Zone and Interface Group Objects](#).

Step 8 If you want to specify a virtual router, do one of the following:

- Choose an existing virtual router from the **Virtual Router** drop-down list.
- Choose **New** to add a new virtual router; [Adding Virtual Routers, on page 10](#).

Step 9 Check the **Enabled** check box to allow the routed interface to handle traffic.

If you clear the check box, the interface becomes disabled and administratively taken down. If you disable a physical interface, you also disable all of the logical interfaces associated with it.

Step 10 In the **MTU** field, enter a maximum transmission unit (MTU), which designates the largest size packet allowed. The MTU is the Layer 2 MTU/MRU and not the Layer 3 MTU.

The range of MTU values can vary depending on the model of the managed device and the interface type.

Caution Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See [Snort® Restart Traffic Behavior](#) for more information.

Step 11 Next to **ICMP**, check the **Enable Responses** check box to communicate updates or error information to other routers, intermediary devices, or hosts.

Step 12 Next to **IPv6 NDP**, check the **Enable Router Advertisement** check box to enable the interface to broadcast router advertisements.

Step 13 To add an IP address, click **Add**.

Step 14 In the **Address** field, enter the IP address in CIDR notation.

Note the following:

- You cannot add network and broadcast addresses, or the static MAC addresses 00:00:00:00:00:00 and FF:FF:FF:FF:FF:FF.
- You cannot add identical IP addresses, regardless of subnet mask, to interfaces in virtual routers.

Step 15 If your organization uses IPv6 addresses and you want to set the IP address of the interface automatically, choose the **Address Autoconfiguration** check box next to the **IPv6** field.

Step 16 For **Type**, choose either **Normal** or **SFRP**.

For SFRP options, see [Configuring SFRP, on page 7](#) for more information.

Step 17 Click **OK**.

- To edit an IP address, click the edit icon (.
- To delete an IP address, click the delete icon (.

When you add an IP address to a routed interface of a 7000 or 8000 Series device in a high-availability pair, you must add a corresponding IP address to the routed interface on the high-availability pair peer.

Step 18 To add a static ARP entry, click **Add**.

Step 19 In the **IP Address** field, enter an IP address for the static ARP entry.

Step 20 In the **MAC Address** field, enter a MAC address to associate with the IP address. Use the standard address format of six groups of two hexadecimal digits separated by colons (for example, 01:23:45:67:89:AB).

Step 21 Click **OK**. The static ARP entry is added.

Step 22 Click **Save**.

What to do next

Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[MTU Ranges for 7000 and 8000 Series Devices and NGIPSv
Snort® Restart Scenarios](#)

Deleting Logical Routed Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

When you delete a logical routed interface, you remove it from the physical interface where it resides, as well as its assigned virtual router and security zone.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon **Edit** ()

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Next to the logical routed interface you want to delete, click **Delete** ()

Step 4 When prompted, confirm that you want to delete the interface.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Configuring SFRP

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can configure Cisco Redundancy Protocol (SFRP) to achieve network redundancy for high availability on either a 7000 or 8000 Series device high-availability pair or individual devices. SFRP provides gateway redundancy for both IPv4 and IPv6 addresses. You can configure SFRP on routed and hybrid interfaces.

If the interfaces are configured on individual devices, they must be in the same broadcast domain. You must designate at least one of the interfaces as primary and an equal number as backup. The system supports only one primary and one backup per IP address. If network connectivity is lost, the system automatically promotes the backup to primary to maintain connectivity.

The options you set for SFRP must be the same on all interfaces in a group of SFRP interfaces. Multiple IP addresses in a group must be in the same primary/backup state. Therefore, when you add or edit an IP address, the state you set for that address propagates to all the addresses in the group. For security purposes, you must enter values for **Group ID** and **Shared Secret** that are shared among the interfaces in the group.

To enable SFRP IP addresses on a virtual router, you must also configure one non-SFRP IP address. Note that only one non-SFRP address should be configured per interface.

As all SFRPs in a group failover together, all SFRPs on the same virtual router should be in the same SFRP group. In addition, you should also set up an HA link interface on each device in a high-availability pair when using NAT, HA state sharing, or VPN. For more information on HA link interfaces, see [Configuring HA Link Interfaces](#).

For 7000 or 8000 Series devices in a high-availability pair, you designate the shared secret and the system copies it to the high-availability pair peer along with the SFRP IP configuration. The shared secret authenticates peer data.



Note We do not recommend enabling more than one non-SFRP IP address on a 7000 or 8000 Series device high-availability pair's routed or hybrid interface where one SFRP IP address is already configured. The system does not perform NAT if a 7000 or 8000 Series device high-availability pair fails over while in standby mode.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click **Edit** (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Next to the interface where you want to configure SFRP, click **Edit** (✎).
- Step 4** Choose the type of interface where you want to configure SFRP, either **Routed** or **Hybrid**.
- Step 5** You can configure SFRP while adding or editing an IP address. Click **Add** to add an IP address. To edit an IP address, click **Edit** (✎).
- Step 6** For **Type**, choose **SFRP** to display the SFRP options.
- Step 7** In the **Group ID** field, enter a value that designates a group of primary or backup interfaces configured for SFRP.
- Step 8** For **Priority**, choose either primary or backup to designate the preferred interface:
 - For individual devices, you must set one interface to primary on one device and the other to backup on a second device.

- For 7000 or 8000 Series device high-availability pairs, when you set one interface as primary, the other automatically becomes the backup.

Step 9 In the **Shared Secret** field, enter a shared secret.

The Shared Secret field populates automatically for a group in a 7000 or 8000 Series device high-availability pair.

Step 10 In the **Adv. Interval (seconds)** field, enter an interval for route advertisements for Layer 3 traffic.

Step 11 Click **OK**.

Step 12 Click **Save**.

What to do next

Deploy configuration changes; see [Deploy Configuration Changes](#).

Related Topics

[About 7000 and 8000 Series Device High Availability](#)

Virtual Router Configuration



Caution

Adding a virtual router on a 7000 or 8000 Series device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Before you can use routed interfaces in a Layer 3 deployment, you must configure virtual routers and assign routed interfaces to them. A virtual router is a group of routed interfaces that route Layer 3 traffic.

You can assign only routed and hybrid interfaces to a virtual router.

To maximize TCP security, you can enable strict enforcement, which blocks connections where the three-way handshake was not completed. Strict enforcement also blocks:

- non-SYN TCP packets for connections where the three-way handshake was not completed
- non-SYN/RST packets from the initiator on a TCP connection before the responder sends the SYN-ACK
- non-SYN-ACK/RST packets from the responder on a TCP connection after the SYN but before the session is established
- SYN packets on an established TCP connection from either the initiator or the responder

Note that if you change the configuration of a Layer 3 interface to a non-Layer 3 interface or remove a Layer 3 interface from the virtual router, the router may fall into an invalid state. For example, if it is used in DHCPv6, it may cause an upstream and downstream mismatch.

Adding Virtual Routers

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can add virtual routers from the **Virtual Routers** tab of the device management page. You can also add routers as you configure routed interfaces.

If you want to create a virtual router before you configure the interfaces on your managed devices, you can create an empty virtual router and add interfaces to it later.



Caution

Adding a virtual router on a 7000 or 8000 Series device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort® Restart Traffic Behavior](#) for more information.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click **Edit** (.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Tip If your devices are in a stack in a high-availability pair, choose the stack you want to modify from the **Selected Device** drop-down list.

Step 4 Click **Add Virtual Router**.

Step 5 In the **Name** field, enter a name for the virtual router. You can use alphanumeric characters and spaces.

Step 6 Configure IPv6 static routing, OSPFv3, and RIPng on your virtual router by checking or clearing the **IPv6 Support** check box.

Step 7 If you do not want to enable strict TCP enforcement, clear the **Strict TCP Enforcement** check box. This option is enabled by default.

Step 8 Choose one or more interfaces from the **Available** list under **Interfaces**, and click **Add**.

The **Available** list contains all enabled Layer 3 interfaces, routed and hybrid, on the device that you can assign to the virtual router.

Tip

To remove a routed or hybrid interface from the virtual router, click **Delete** (). Disabling a configured interface from the Interfaces tab also removes it.

Step 9 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

DHCP Relay

DHCP provides configuration parameters to Internet hosts. A DHCP client that has not yet acquired an IP address cannot communicate directly with a DHCP server outside its broadcast domain. To allow DHCP clients to communicate with DHCP servers, you can configure DHCP relay instances to handle cases where the client is not on the same broadcast domain as the server.

You can set up DHCP relay for each virtual router you configure. By default, this feature is disabled. You can enable either DHCPv4 relay or DHCPv6 relay.



Note You cannot run a DHCPv6 Relay chain through two or more virtual routers running on the same device.

Setting Up DHCPv4 Relay

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

The following procedure explains how to set up DHCPv4 relay on a virtual router.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router you want to modify, click the edit icon (✎).
- Step 5** Check the **DHCPv4** check box.
- Step 6** Under the **Servers** field, enter a server IP address.
- Step 7** Click **Add**.
You can add up to four DHCP servers.
- Step 8** In the **Max Hops** field, enter the maximum number of hops from 1 to 255.

Step 9 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Setting Up DHCPv6 Relay

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You cannot run a DHCPv6 Relay chain through two or more virtual routers running on the same device.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router where you want to set up DHCP relay, click the edit icon (✎).

Step 5 Check the **DHCPv6** check box.

Step 6 In the **Interfaces** field, check the check boxes next to one or more interfaces that have been assigned to the virtual router.

Tip You cannot disable an interface from the **Interfaces** tab while it is configured for DHCPv6 Relay. You must first clear the DHCPv6 Relay interfaces check box and save the configuration.

Step 7 Next to a selected interface, click the drop-down icon and choose whether the interface relays DHCP requests **Upstream**, **Downstream**, or **Both**.

Note You must include at least one downstream interface and one upstream interface. Choosing both means that the interface is both downstream and upstream.

Step 8 In the **Max Hops** field, enter the maximum number of hops from 1 to 255

Step 9 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Static Routes

Static routing allows you to write rules about the IP addresses of traffic passing through a router. It is the simplest way of configuring path selection of a virtual router because there is no communication with other routers regarding the current topology of the network.

Do not configure routing to IP interfaces for DHCPv4 servers that the assigned virtual router cannot route packets to. Doing so will render previously specified routable DHCP4 servers unroutable.

The Static Routes table includes summary information about each route, as described in the following table.

Table 1: Static Routes Table View Fields

Field	Description
Enabled	Specifies whether this route is currently enabled or disabled.
Name	The name of the static route.
Destination	The destination network where traffic is routed.
Type	Specifies the action that is taken for this route, which will be one of the following: • IP — designates that the route forwards packets to the address of a neighboring router. • Interface — designates that the route forwards packets to an interface through which traffic is routed to hosts on a directly connected network. • Discard — designates that the static route drops packets.
Gateway	The target IP address if you selected IP as the static route type or the interface if you selected Interface as the static route type.
Preference	Determines the route selection. If you have multiple routes to the same destination, the system selects the route with the higher preference.

Viewing the Static Routes Table

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Any	Admin/Network Admin

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to view, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router where you want to view static routes, click the edit icon (✎).
If a view icon (🔍) appears instead, the configuration belongs to a descendant domain, or you do not have permission to modify the configuration.
- Step 5** Click the **Static** tab.
-

Adding Static Routes

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to add the static route, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router where you want to add the static route, click the edit icon (✎).
- Step 5** Click **Static** to display the static route options.
- Step 6** Click **Add Static Route**.
- Step 7** In the **Route Name** field, enter a name for the static route. You can use alphanumeric characters and spaces.
- Step 8** For **Enabled**, check the check box to specify that the route is currently enabled.
- Step 9** In the **Preference** field, enter a numerical value between 1 and 65535 to determine the route selection.
Note If you have multiple routes to the same destination, the system uses the route with the higher preference.
- Step 10** From the **Type** drop-down list, choose the type of static route you are configuring.
- Step 11** In the **Destination** field, enter the IP address for the destination network where traffic should be routed.
- Step 12** In the **Gateway** field, you have two options:

- If you chose **IP** as the selected static route type, choose an IP address.
- If you chose **Interface** as the selected static route type, choose an enabled interface from the drop-down list.

Tip Interfaces you have disabled from the **Interfaces** tab are not available; disabling an interface you have added removes it from the configuration.

Step 13 Click **OK**.

Step 14 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Dynamic Routing

Dynamic, or adaptive, routing uses a routing protocol to alter the path that a route takes in response to a change in network conditions. The adaptation is intended to allow as many routes as possible to remain valid, that is, have destinations that can be reached in response to the change. This allows the network to “route around” damage, such as loss of a node or a connection between nodes, so long as other path choices are available. You can configure a router with no dynamic routing, or you can configure the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) routing protocol.

RIP Configuration

Routing Information Protocol (RIP) is a dynamic routing protocol, designed for small IP networks, that relies on hop count to determine routes. The best routes use the fewest number of hops. The maximum number of hops allowed for RIP is 15. This hop limit also limits the size of the network that RIP can support.

Adding Interfaces for RIP Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

While configuring RIP, you must choose interfaces from those already included in the virtual router, where you want to configure RIP. Disabled interfaces are not available.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router you want to modify, click the edit icon (✎).

Step 5 Click **Dynamic Routing** to display the dynamic routing options.

Step 6 Click **RIP** to display the RIP options.

Step 7 Under **Interfaces**, click the add icon (+).

Step 8 From the **Name** drop-down list, choose the interface where you want to configure RIP.

Tip Interfaces you have disabled from the Interfaces tab are not available; disabling an interface you have added removes it from the configuration.

Step 9 In the **Metric** field, enter a metric for the interface. When routes from different RIP instances are available and all of them have the same preference, the route with the lowest metric becomes the preferred route.

Step 10 From the **Mode** drop-down list, choose one of the following options:

- **Multicast** — default mode where RIP multicasts the entire routing table to all adjacent routers at a specified address.
- **Broadcast** — forces RIP to use broadcast (for example, RIPv1) even though multicast mode is possible.
- **Quiet** — RIP will not transmit any periodic messages to this interface.
- **No Listen** — RIP will send to this interface but not listen to it.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Configuring Authentication Settings for RIP Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

RIP authentication uses one of the authentication profiles you configured on the virtual router.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router where you want to add the RIP authentication profile, click the edit icon (✎).

- Step 5** Click **Dynamic Routing** to display the dynamic routing options.
- Step 6** Click **RIP** to display the RIP options.
- Step 7** Under **Authentication**, choose an existing virtual router authentication profile from the **Profile** drop-down list, or choose **None**.
- Step 8** Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Configuring Advanced Settings for RIP Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can configure several advanced RIP settings pertaining to various timeout values and other features that affect the behavior of the protocol.



Caution

Changing any of the advanced RIP settings to incorrect values can prevent the router from communicating successfully with other RIP routers.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router you want to modify, click the edit icon (✎).
- Step 5** Click **Dynamic Routing** to display the dynamic routing options.
- Step 6** Click **RIP** to display the RIP options.
- Step 7** In the **Preference** field, enter a numerical value (higher is better) for the preference of the routing protocol. The system prefers routes learned through RIP over static routes.
- Step 8** In the **Period** field, enter the interval, in seconds, between periodic updates. A lower number determines faster convergence, but larger network load.
- Step 9** In the **Timeout Time** field, enter a numerical value that specifies how old routes must be, in seconds, before being considered unreachable.
- Step 10** In the **Garbage Time** field, enter a numerical value that specifies how old routes must be, in seconds, before being discarded.

- Step 11** In the **Infinity** field, enter a numerical value that specifies a value for infinity distance in convergence calculations. Larger values will make protocol convergence slower.
- Step 12** From the **Honor** drop-down list, choose one of the following options to designate when requests for dumping routing tables should be honored:
- **Always** — always honor requests
 - **Neighbor** — only honor requests sent from a host on a directly connected network
 - **Never** — never honor requests
- Step 13** Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding Import Filters for RIP Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can add an import filter to designate which routes are accepted or rejected from RIP into the route table. Import filters are applied in the order they appear in the table.

When adding an import filter, you use one of the filters you configured on the virtual router.



Tip To edit a RIP import filter, click the edit icon (✎). To delete a RIP import filter, click the delete icon (🗑).

Before you begin

- Add a virtual router as described in [Adding Virtual Routers, on page 10](#).
- Configure a filter on the virtual router as described in [Setting Up Virtual Router Filters, on page 28](#).

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router where you want to add the RIP virtual router filter, click the edit icon (✎).

Step 5 Click **Dynamic Routing** to display the dynamic routing options.

Step 6 Click **RIP** to display the RIP options.

Step 7 Under **Import Filters**, click the add icon (⊕).

Step 8 From the **Name** drop-down list, choose the filter you want to add as an import filter.

Step 9 Next to **Action**, choose **Accept** or **Reject**.

Step 10 Click **OK**.

Tip

To change the order of the import filters, click the move up (⬆) and move down (⬇) icons as needed. You can also drag the filters up or down in the list.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding Export Filters for RIP Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can add an export filter to define which routes will be accepted or rejected from the route table to RIP. Export filters are applied in the order they appear in the table.

When adding an export filter, you use one of the filters you configured on the virtual router.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router where you want to add the RIP virtual router filter, click the edit icon (✎).

Step 5 Click **Dynamic Routing** to display the dynamic routing options.

Step 6 Click **RIP** to display the RIP options.

Step 7 Under **Export Filters**, click the add icon (⊕).

Step 8 From the **Name** drop-down list, choose the filter you want to add as an export filter.

Step 9 Next to **Action**, choose **Accept** or **Reject**.

Step 10 Click **OK**.

Tip

To change the order of the export filters, click the move up () and move down () icons as needed. You can also drag the filters up or down in the list.

Step 11

Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

OSPF Configuration

Open Shortest Path First (OSPF) is an adaptive routing protocol that defines routes dynamically by obtaining information from other routers and advertising routes to other routers using link state advertisements. The router keeps information about the links between it and the destination to make routing decisions. OSPF assigns a cost to each routed interface, and considers the best routes to have the lowest costs.

OSPF Routing Areas

An OSPF network may be structured, or subdivided, into routing areas to simplify administration and optimize traffic and resource use. Areas are identified by 32-bit numbers, expressed either simply in decimal or often in octet-based dot-decimal notation.

By convention, area zero or 0.0.0.0 represents the core or backbone region of an OSPF network. You may choose to identify other areas. Often, administrators select the IP address of a main router in an area as the area's identification. Each additional area must have a direct or virtual connection to the backbone OSPF area. Such connections are maintained by an interconnecting router, known as the area border router (ABR). An ABR maintains separate link state databases for each area it serves and maintains summarized routes for all areas in the network.

Adding OSPF Areas

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure**Step 1**

Choose **Devices > Device Management**.

Step 2

Next to the device you want to modify, click the edit icon ().

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3

Click the **Virtual Routers** tab.

Step 4

Next to the virtual router you want to modify, click the edit icon ().

Step 5

Click **Dynamic Routing** to display the dynamic routing options.

- Step 6** Click **OSPF** to display the OSPF options.
- Step 7** Under **Areas**, click the add icon (+).
- Step 8** In the **Area Id** field, enter a numerical value for the area. This value can be either an integer or an IPv4 address.
- Step 9** Optionally, check the **Stubnet** check box to designate that the area does not receive router advertisements external to the autonomous system and routing from within the area is based entirely on a default route. If you clear the check box, the area becomes a backbone area or otherwise non-stub area.
- Step 10** In the **Default cost** field, enter a cost associated with the default route for the area.
- Step 11** Under **Stubnets**, click the add icon (+).
- Step 12** In the **IP Address** field, enter an IP address in CIDR notation.
- Step 13** Choose the **Hidden** check box to indicate that the stubnet is hidden.
Hidden stubnets are not propagated into other areas.
- Step 14** Choose the **Summary** check box to designate that default stubnets that are subnetworks of this stubnet are suppressed.
- Step 15** In the **Stub cost** field, enter a value that defines the cost associated with routing to this stub network.
- Step 16** Click **OK**.
- Step 17** If you want to add a network, click the add icon (+) under **Networks**.
- Step 18** In the **IP Address** field, enter an IP address in CIDR notation for the network.
- Step 19** Check the **Hidden** check box to indicate that the network is hidden. Hidden networks are not propagated into other areas.
- Step 20** Click **OK**.
- Step 21** Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

OSPF Area Interfaces

You can configure a subset of the interfaces assigned to the virtual router for OSPF. The following list describes the options you can specify on each interface.

Interfaces

Select the interface where you want to configure OSPF. Interfaces you have disabled from the Interfaces tab are not available.

Type

Select the type of OSPF interface from the following choices:

- **Broadcast** — On broadcast networks, flooding and hello messages are sent using multicasts, a single packet for all the neighbors. The option designates a router to be responsible for synchronizing the link state databases and originating network link state advertisements. This network type cannot be used on physically non-broadcast multiple-access (NBMP) networks and on unnumbered networks without proper IP prefixes.

- **Point-to-Point (PtP)** — Point-to-point networks connect just two routers together. No election is performed and no network link state advertisement is originated, which makes it simpler and faster to establish. This network type is useful not only for physically PtP interfaces, but also for broadcast networks used as PtP links. This network type cannot be used on physically NBMP networks.
- **Non-Broadcast** — On NBMP networks, the packets are sent to each neighbor separately because of the lack of multicast capabilities. Similar to broadcast networks, the option designates a router, which plays a central role in the propagation of link state advertisements. This network type cannot be used on unnumbered networks.
- **Autodetect** — The system determines the correct type based on the specified interface.

Cost

Specify the output cost of the interface.

Stub

Specify whether the interface should listen for OSPF traffic and transmit its own traffic.

Priority

Enter a numerical value that specifies the priority value used in designated router election. On every multiple access network, the system designates a router and backup router. These routers have some special functions in the flooding process. Higher priority increases preferences in this election. You cannot configure a router with a priority of 0.

Nonbroadcast

Specify whether hello packets are sent to any undefined neighbors. This switch is ignored on any NBMA network.

Authentication

Select the OSPF authentication profile that this interface uses from one of the authentication profiles you configured on the virtual router or select **None**. For more information about configuring authentication profiles, see [Adding Virtual Router Authentication Profiles, on page 30](#).

Hello Interval

Type the interval, in seconds, between the sending of hello messages.

Poll

Type the interval, in seconds, between the sending of hello messages for some neighbors on NBMA networks.

Retrans Interval

Type the interval, in seconds, between retransmissions of unacknowledged updates.

Retrans Delay

Type the estimated number of seconds it takes to transmit a link state update packet over the interface.

Wait Time

Type the number of seconds that the router waits between starting election and building adjacency.

Dead Interval

Type the number of seconds that the router waits before declaring a neighbor down when not receiving messages from it. If this value is defined, it overrides the value calculated from dead count.

Dead Count

Type a numerical value that when multiplied by the hello interval specifies the number of seconds that the router waits before declaring a neighbor down when not receiving messages from it.

To edit an OSPF area interface, click the edit icon (✎). To delete an OSPF area interface, click the delete icon (🗑). Disabling a configured interface from the Interfaces tab also deletes it.

Adding OSPF Area Interfaces

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can configure a subset of the interfaces assigned to the virtual router for OSPF.

You can choose only one interface for use in an OSPF area.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
 - Step 2** Next to the device where you want to add the OSPF interface, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
 - Step 3** Click the **Virtual Routers** tab.
 - Step 4** Next to the virtual router where you want to add the OSPF interface, click the edit icon (✎).
 - Step 5** Click **Dynamic Routing** to display the dynamic routing options.
 - Step 6** Click **OSPF** to display the OSPF options.
 - Step 7** Under **Areas**, click the add icon (+).
 - Step 8** Click **Interfaces**.
 - Step 9** Click the add icon (+).
 - Step 10** Take any of the actions as described in [OSPF Area Interfaces, on page 21](#).
 - Step 11** If you want to add a network, click the add icon (+) under **Networks**.
 - Step 12** In the **IP address** field, enter an IP address for the neighbor receiving hello messages on non-broadcast networks from this interface.
 - Step 13** Check the **Eligible** check box to indicate that the neighbor is eligible to receive messages.

Step 14 Click **OK**.

Tip To edit a neighbor, click the edit icon (). To delete a neighbor, click the delete icon (.

Step 15 Click **OK**.

Step 16 Click **Save**.

Step 17 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding OSPF Area Vlinks

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

All areas in an OSPF autonomous system must be physically connected to the backbone area. In some cases where this physical connection is not possible, you can use a vlink to connect to the backbone through a non-backbone area. Vlinks can also be used to connect two parts of a partitioned backbone through a non-backbone area.

You must add a minimum of two OSPF areas before you can add a vlink.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon (.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router you want to modify, click the edit icon (.

Step 5 Click **Dynamic Routing** to display the dynamic routing options.

Step 6 Click **OSPF** to display the OSPF options.

Step 7 Under **Areas**, click the add icon (.

Step 8 Click **Vlinks**.

Step 9 Click the add icon (.

Step 10 In the **Router ID** field, enter an IP address for the router.

Step 11 From the **Authentication** drop-down list, choose the authentication profile the vlink will use.

Step 12 In the **Hello Interval** field, enter the interval, in seconds, between sending of hello messages.

- Step 13** In the **Retrans Interval** field, enter the interval, in seconds, between retransmissions of unacknowledged updates.
- Step 14** In the **Wait Time** field, enter the number of seconds that the router waits between starting election and building adjacency.
- Step 15** In the **Dead Interval** field, enter the number of seconds that the router waits before declaring a neighbor down when not receiving messages from it. If this value is defined, it overrides the value calculated from dead count.
- Step 16** In the **Dead Count** field, enter a numerical value that when multiplied by the hello interval, specifies the number of seconds that the router waits before declaring a neighbor down when not receiving messages from it.
- Step 17** Click **OK**.
- Step 18** Click **Save**.
- Step 19** Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding Import Filters for OSPF Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can add an import filter to define which routes are accepted or rejected from OSPF into the route table. Import filters are applied in the order they appear in the table.

When adding an import filter, you use one of the filters you configured on the virtual router.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click **Virtual Routers**.
- Step 4** Next to the virtual router you want to modify, click the edit icon (✎).
- Step 5** Click **Dynamic Routing** to display the dynamic routing options.
- Step 6** Click **OSPF** to display the OSPF options.
- Step 7** Under **Import Filters**, click the add icon (+).
- Step 8** From the **Name** drop-down list, choose the filter you want to add as an import filter.
- Step 9** Next to **Action**, choose **Accept** or **Reject**.
- Step 10** Click **OK**.

Tip

To change the order of the import filters, click the move up () and move down () icons as needed. You can also drag the filters up or down in the list.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding Export Filters for OSPF Configuration

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can add an export filter to define which routes will be accepted or rejected from the route table to OSPF. Export filters are applied in the order they appear in the table.

When adding an export filter, you use one of the filters you configured on the virtual router.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click the edit icon ().

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the **Virtual Routers** tab.

Step 4 Next to the virtual router where you want to add the OSPF virtual router filter, click the edit icon ().

Step 5 Click the **Dynamic Routing** tab to display the dynamic routing options.

Step 6 Click **OSPF** to display the OSPF options.

Step 7 Under **Export Filters**, click the add icon ().

Step 8 From the **Name** drop-down list, choose the filter you want to add as an export filter.

Step 9 Next to **Action**, choose **Accept** or **Reject**.

Step 10 Click **OK**.

Tip

To change the order of the export filters, click the move up () and move down () icons as needed. You can also drag the filters up or down in the list.

Step 11 Click **Save**.

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Virtual Router Filters

Filters provide a way to match routes for importing into the virtual router's route table and for exporting routes to dynamic protocols. You can create and manage a list of filters. Each filter defines specific criteria to look for in routes that are defined statically or received from a dynamic protocol.

The Virtual Routers Filters table includes summary information about each filter you have configured on a virtual router, as described in the following table.

Table 2: Virtual Router Filters Table View Fields

Field	Description
Name	The name of the filter.
Protocol	The protocol that the route originates from: • Static — The route originates as a local static route. • RIP — The route originates from a dynamic RIP configuration. • OSPF — The route originates from a dynamic OSPF configuration.
From Router	The router IP addresses that this filter attempts to match in a router. You must enter this value for static and RIP filters.
Next Hop	The next hop where packets using this route are forwarded. You must enter this value for static and RIP filters.
Destination Type	The type of destination where packets are sent: • Router • Device • Discard
Destination Network	The networks that this filter attempts to match in a route.

Field	Description
OSPF Path Type	Applies only to OSPF protocol. The path type can be one of the following: • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	Applies only to OSPF protocol. The router ID of the router advertising that route/network.

Viewing Virtual Router Filters

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Any	Admin/Network Admin

The **Filter** tab of the virtual router editor displays a table listing of all the filters you have configured on a virtual router. The table includes summary information about each filter.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to view, click the edit icon (✎).
- In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router where you want to view the filters, click the edit icon (✎).
- Step 5** Click the **Filter** tab.
-

Setting Up Virtual Router Filters

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router you want to modify, click the edit icon (✎).
- Step 5** Click the **Filter** tab.
- Step 6** Click **Add Filter**.
- Step 7** In the **Name** field, enter a name for the filter. You can use alphanumeric characters only.
- Step 8** Under **Protocol**, choose **All** or choose the protocol that applies to the filter.
- Step 9** If you chose All, Static, or RIP as the **Protocol**, under **From Router**, enter the router IP addresses that this filter will attempt to match in a route.
- Note** You can also enter a /32 CIDR block for IPv4 addresses and a /128 prefix length for IPv6 addresses. All other address blocks are invalid for this field.
- Step 10** Click **Add**.
- Step 11** If you chose All, Static, or RIP as the **Protocol**, under **Next Hop**, enter the IP addresses for the gateways that this filter will attempt to match in a route.
- Note** You can also enter a /32 CIDR block for IPv4 addresses and a /128 prefix length for IPv6 addresses. All other address blocks are invalid for this field.
- Step 12** Click **Add**.
- Step 13** Under **Destination Type**, choose the options that apply to the filter.
- Step 14** Under **Destination Network**, enter the IP address of the network that this filter will attempt to match in a route.
- Step 15** Click **Add**.
- Step 16** If you chose All or OSPF as the **Protocol**, under **Path Type**, choose the options that apply to the filter. You must choose at least one path type.
- Step 17** If you chose OSPF as the **Protocol**, under **Router ID**, enter the IP address that serves as the router ID of the router advertising the route/network.
- Step 18** Click **Add**.
- Step 19** Click **OK**.
- Step 20** Click **Save**.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Adding Virtual Router Authentication Profiles

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

You can set up Authentication Profiles for use in RIP and OSPF configurations. You can configure a simple password or specify a shared cryptographic key. Simple passwords allow for every packet to carry eight bytes of the password. The system ignores received packets lacking this password. Cryptographic keys allow for validation, a 16-byte long digest generated from a password to be appended to every packet.

Note that for OSPF, each area can have a different authentication method. Therefore, you create authentication profiles that can be shared among many areas. You cannot add authentication for OSPFv3.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
 - Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
 - Step 3** Click the **Virtual Routers** tab.
 - Step 4** Next to the virtual router you want to modify, click the edit icon (✎).
 - Step 5** Click **Authentication Profile**.
 - Step 6** Click **Add Authentication Profile**.
 - Step 7** In the **Authentication Profile Name** field, enter a name for the authentication profile.
 - Step 8** From the **Authentication Type** drop down list, choose **simple** or **cryptographic**.
 - Step 9** In the **Password** field, enter a secure password.
 - Step 10** In the **Confirm Password** field, enter the password again to confirm it.
 - Step 11** Click **OK**.
 - Step 12** Click **Save**.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

Viewing Virtual Router Statistics

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Any	Admin/Network Admin

You can view runtime statistics for each virtual router. The statistics display unicast packets, packets dropped, and separate routing tables for IPv4 and IPv6 addresses.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to view statistics, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router where you want to view the router statistics, click the view icon (🔍).
-

Deleting Virtual Routers

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Control	7000 & 8000 Series	Leaf only	Admin/Network Admin

When you delete a virtual router, any routed interfaces assigned to the router become available for inclusion in another router.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click the edit icon (✎).
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click the **Virtual Routers** tab.
- Step 4** Next to the virtual router that you want to delete, click the delete icon (🗑).
- Step 5** When prompted, confirm that you want to delete the virtual router.
-

What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

