Setting Up Virtual Routers

You can configure a managed device in a Layer 3 deployment so that it routes traffic between two or more interfaces. You must assign an IP address to each interface and assign the interfaces to a virtual router to route traffic. On Series 3 managed devices, you can group multiple physical interfaces into a single logical routed interface called a link aggregation group (LAG). This single aggregate logical link provides higher bandwidth, redundancy, and load-balancing between two endpoints.

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.

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

**Caution**
Adding a virtual router restarts the Snort process when you apply your changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 for more information.

See the following sections for more information about configuring a Layer 3 deployment:

- Configuring Routed Interfaces, page 7-1
- Configuring Virtual Routers, page 7-9
- Configuring LAGs, page 8-1

Configuring Routed Interfaces

**License:** Control

**Supported Devices:** Series 3

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. If the system receives a packet with no VLAN tag and you have not configured a physical routed interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical routed interface, it also drops the packet.

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.

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

See the following sections for more information:

- Configuring Physical Routed Interfaces, page 7-2
- Adding Logical Routed Interfaces, page 7-4
- Deleting Logical Routed Interfaces, page 7-7
- Configuring SFRP, page 7-7

## Configuring Physical Routed Interfaces

**License:** Control

**Supported Devices:** Series 3

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 Series 3 device restarts the Snort process when you apply your changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 for more information.

---

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 routed interfaces does not prevent ICMP responses in all scenarios. You can add rules to an access control policy to drop packets where the destination IP is the routed interface’s IP and the protocol is ICMP; see Controlling Traffic with Network-Based Rules, page 15-1.

If you have enabled the **Inspect Local Router Traffic** option on the managed device, it drops the packets before they reach the host, thereby preventing any response. For more information about inspecting local router traffic, see Understanding Advanced Device Settings, page 4-54.
Changing any (Series 2) or the highest (Series 3) MTU value for a sensing interface or inline set temporarily interrupts traffic inspection on all sensing interfaces on the device, not just the interface you changed, when you apply your changes. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and the interface type. See How Snort Restarts Affect Traffic, page 1-9.

To configure a physical routed interface:

**Access:** Admin/Network Admin

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

The Device Management page appears.

**Step 2** Next to the device where you want to configure the routed interface, click the edit icon (✏).

The Interfaces tab for that device appears.

**Step 3** Next to the interface you want to configure as a routed interface, click the edit icon (✏).

The Edit Interface pop-up window appears.

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

**Step 5** Optionally, from the Security Zone drop-down list, select an existing security zone or select New to add a new security zone.

**Step 6** Optionally, from the Virtual Router drop-down list, select an existing virtual router or select New to add a new virtual router.

Note that if you add a new virtual router, you must configure it on the Virtual Routers tab of the Device Management page (Devices > Device Management > Virtual Routers) after you set up the routed interface. See Adding Virtual Routers, page 7-10.

**Step 7** Select 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, select an option to designate the link mode or select Autonegotiation to specify that the interface is configured to auto negotiate speed and duplex settings. Note that mode settings are available only for copper interfaces.

**Note** Interfaces on 8000 Series appliances do not support half-duplex options.

**Step 9** From the MDI/MDIX drop-down list, select an option to designate whether the interface is configured for MDI (medium dependent interface), MDIX (medium dependent interface crossover), or Auto-MDIX. Note that MDI/MDIX settings are available only for copper interfaces.

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

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

The range within which you can set the MTU can vary depending on the FireSIGHT System device model and the interface type. See MTU Ranges for Managed Devices, page 4-64 for more information.

**Step 11** Next to ICMP, select the Enable Responses check box to allow the interface to respond to ICMP traffic such as pings and traceroute.
Chapter 7  Setting Up Virtual Routers

Configuring Routed Interfaces

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

Step 13  To add an IP address, click Add.

The Add IP Address pop-up window appears.

Step 14  In the Address field, type 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  Optionally, if your organization uses IPv6 addresses, next to the IPv6 field, select the Address Autoconfiguration check box to set the IP address of the interface automatically.

Step 16  For Type, select either Normal or SFRP.

For SFRP options, see Configuring SFRP, page 7-7 for more information.

Step 17  Click OK.

The IP address is added.

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

- Note  When adding an IP address to a routed interface of a clustered device, you must add a corresponding IP address to the routed interface on the cluster peer.

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

The Add Static ARP Entry pop-up window appears.

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

Step 20  In the MAC Address field, type a MAC address to associate with the IP address. Enter the address using the standard 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.

- Tip  To edit a static ARP entry, click the edit icon ( ). To delete a static ARP entry, click the delete icon ( ).

Step 22  Click Save.

The physical routed interface is configured. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Adding Logical Routed Interfaces

License: Control

Supported Devices: Series 3
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 a Series 3 device restarts the Snort process when you apply your changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See *How Snort Restarts Affect Traffic, page 1-9* for more information.

Note that disabling the **ICMP Enable Responses** option for routed interfaces does not prevent ICMP responses in all scenarios. You can add rules to an access control policy to drop packets where the destination IP is the routed interface’s IP and the protocol is ICMP; see *Controlling Traffic with Network-Based Rules, page 15-1*.

If you have enabled the **Inspect Local Router Traffic** option on the managed device, it drops the packets before they reach the host, thereby preventing any response. For more information about inspecting local router traffic, see *Understanding Advanced Device Settings, page 4-54*.

**Caution**

Changing any (Series 2) or the highest (Series 3) MTU value for a sensing interface or inline set temporarily interrupts traffic inspection on all sensing interfaces on the device, not just the interface you changed, when you apply your changes. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and the interface type. See *How Snort Restarts Affect Traffic, page 1-9*.

To edit an existing routed interface, click the edit icon (📝) next to the interface.

**To add a logical routed interface:**

**Access:** Admin/Network Admin

---

**Step 1**

Select **Devices > Device Management**.

The Device Management page appears.

**Step 2**

Next to the device where you want to add the routed interface, click the edit icon (📝).

The Interfaces tab for that device appears.

**Step 3**

Click **Add Interface**.

The Add Interface pop-up window appears.

**Step 4**

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

**Step 5**

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

**Step 6**

In the **VLAN Tag** field, type 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**

Optionally, from the **Security Zone** drop-down list, select an existing security zone or select **New** to add a new security zone.

**Step 8**

Optionally, from the **Virtual Router** drop-down list, select an existing virtual router or select **New** to add a new virtual router.
Note that if you add a new virtual router, you must configure it on the Device Management page (Devices > Device Management > Virtual Routers) after you finish setting up the routed interface. See Adding Virtual Routers, page 7-10.

**Step 9**
Select 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, type a maximum transmission unit (MTU), which designates the largest size packet allowed. Note that the MTU is the Layer 2 MTU/MRU and not the Layer 3 MTU.

The range within which you can set the MTU can vary depending on the FireSIGHT System device model and the interface type. See MTU Ranges for Managed Devices, page 4-64 for more information.

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

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

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

The Add IP Address pop-up window appears.

**Step 14**
In the **Address** field, type 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**
Optionally, if your organization uses IPv6 addresses, next to the **IPv6** field, select the **Address Autoconfiguration** check box to set the IP address of the interface automatically.

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

For SFRP options, see Configuring SFRP, page 7-7 for more information.

**Step 17**
Click **OK**.

The IP address is added.

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

**Note**
When you add an IP address to a routed interface of a clustered device, you must add a corresponding IP address to the routed interface on the cluster peer.

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

The Add Static ARP Entry pop-up window appears.

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

**Step 20**
In the **MAC Address** field, type a MAC address to associate with the IP address. Enter the address using the standard 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.
Chapter 7  Setting Up Virtual Routers

Tip
To edit a static ARP entry, click the edit icon ( ). To delete a static ARP entry, click the delete icon ( ).

Step 22
Click Save.

The logical routed interface is added. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Note
When a physical interface is disabled, the logical interface(s) associated with the physical interface is also disabled.

Deleting Logical Routed Interfaces

License: Control

Supported Devices: Series 3

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.

Caution
Adding a routed interface pair on a Series 3 device restarts the Snort process when you apply your changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. See How Snort Restarts Affect Traffic, page 1-9 for more information.

To delete a routed interface:

Access: Admin/Network Admin

Step 1
Select Devices > Device Management.
The Device Management page appears.

Step 2
Next to the device where you want to delete the routed interface, click the edit icon ( ).
The Interfaces tab for that device appears.

Step 3
Next to the logical routed interface you want to delete, click the delete icon ( ).

Step 4
When prompted, confirm that you want to delete the interface.
The interface is deleted. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Configuring SFRP

License: Control

Supported Devices: Series 3
You can configure Cisco Redundancy Protocol (SFRP) to achieve network redundancy for high availability on either a device cluster 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 master and an equal number as backup. The system supports only one master and one backup per IP address. If network connectivity is lost, the system automatically promotes the backup to master 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 master/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 at least one non-SFRP IP address.

For clustered devices, you designate the shared secret and the system copies it to the cluster peer along with the SFRP IP configuration. The shared secret authenticates peer data.

**Note** Cisco does not recommend enabling more than one non-SFRP IP address on a clustered Series 3 device’s routed or hybrid interface where one SFRP IP address is already configured.

For more information about clustering devices, see Clustering Devices, page 4-29.

**To configure SFRP:**

**Access:** Admin/Network Admin

---

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

The Device Management page appears.

**Step 2** Next to the device where you want to configure SFRP, click the edit icon ( ).

The Interfaces tab for that device appears.

**Step 3** Next to the interface where you want to configure SFRP, click the edit icon ( ).

The Edit Interface pop-up window appears.

**Step 4** Select the type of interface where you want to configure SFRP:

- Click Routed to display the routed interface options.
- Click Hybrid to display the hybrid interface options.

**Step 5** You can configure SFRP while adding or editing an IP address:

- To add an IP address, click Add.
- To edit an IP address, click the edit icon ( ).

The Add IP Address or Edit IP Address pop-up window appears.

**Step 6** For Type, select SFRP to display the SFRP options.

**Step 7** In the Group ID field, enter a value that designates a group of master or backup interfaces configured for SFRP.

**Step 8** For Priority, select either Master or Backup to designate the preferred interface:
For individual devices, you must set one interface to master on one device and the other to backup on a second device.

For device clusters, when you set one interface as master, the other automatically becomes the backup.

**Step 9**  
In the **Shared Secret** field, type a shared secret.  
The Shared Secret field populates automatically for a group in a device cluster.

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

**Step 11**  
Click **OK**.  
The IP address is added or edited.

**Step 12**  
Click **Save**.  
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

---

### Configuring Virtual Routers

**License:** Control  
**Supported Devices:** Series 3

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.

See the following sections for more information about configuring virtual routers:

- **Viewing Virtual Routers**, page 7-9
- **Adding Virtual Routers**, page 7-10
- **Viewing Virtual Router Statistics**, page 7-32
- **Deleting Virtual Routers**, page 7-32

### Viewing Virtual Routers

**License:** Control  
**Supported Devices:** Series 3

The Virtual Routers tab of the Device Management page (Devices > Device Management > Virtual Routers) displays a list of all the virtual routers you have configured on a device. The table includes summary information about each router, as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the virtual router.</td>
</tr>
</tbody>
</table>
Adding Virtual Routers

License: Control

Supported Devices: Series 3

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.

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

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. Any changes you make to an existing virtual router may interrupt traffic on the device.

To edit an existing virtual router, click the edit icon (edit) next to the router.

You can configure virtual routers in several different ways beyond the general options. See the following sections for more information about these configurations:

- Setting Up DHCP Relay, page 7-11
- Setting Up Static Routes, page 7-13
- Setting Up Dynamic Routing, page 7-15
- Setting Up RIP Configuration, page 7-16
- Setting Up OSPF Configuration, page 7-21
- Setting Up Virtual Router Filters, page 7-28
• Adding Virtual Router Authentication Profiles, page 7-30

To add a virtual router:

Access: Admin/Network Admin

---

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

The Device Management page appears.

**Step 2**  
Next to the device where you want to add the virtual router, click the edit icon (📝).

The Interfaces tab for that device appears.

**Step 3**  
Click **Virtual Routers**.

The Virtual Routers tab appears.

---

**Tip**  
If your devices are in a clustered stack deployment, select the stack you want to modify from the **Selected Device** drop-down list.

---

**Step 4**  
Click **Add Virtual Router**.

The Add Virtual Router pop-up window appears.

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

**Step 6**  
To enable IPv6 static routing, OSPFv3, and RIPng on your virtual router, select the **IPv6 Support** check box. To disable these features, clear the check box.

**Step 7**  
Optionally, clear **Strict TCP Enforcement** if you do not want to enable strict TCP enforcement.

This option is enabled by default.

**Step 8**  
Under **Interfaces**, the **Available** list contains all enabled Layer 3 interfaces, routed and hybrid, on the device that you can assign to the virtual router. Select one or more interfaces to assign to the virtual router and click **Add**.

---

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

---

**Step 9**  
Click **Save**.

The virtual router is added. Note that your changes do not take effect until you apply the device configuration; see **Applying Changes to Devices**, page 4-25.

---

### Setting Up DHCP Relay

**License**: Control

**Supported Devices**: Series 3

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.

See the following sections for more information:

- Setting Up DHCPv4 Relay, page 7-12
- Setting Up DHCPv6 Relay, page 7-12

### Setting Up DHCPv4 Relay

**License:** Control  
**Supported Devices:** Series 3

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

**To set up DHCPv4 relay:**

**Access:** Admin/Network Admin

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Select <strong>Devices &gt; Device Management</strong>. The Device Management page appears.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Next to the device where you want to set up DHCP relay, click the edit icon ( ). The Interfaces tab for that device appears.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click <strong>Virtual Routers</strong>. The Virtual Routers tab appears.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Next to the virtual router where you want to set up DHCP relay, click the edit icon ( ). The Edit Virtual Router pop-up window appears.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>To set up DHCP relay for DHCPv4, select the <strong>DHCPv4</strong> check box.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Under the <strong>Servers</strong> field, type a server IP address.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click <strong>Add</strong>. The IP address is added to the <strong>Servers</strong> field. You can add up to four DHCP servers.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>To delete a DHCP server, click the delete icon ( ) next to the server IP address.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>In the <strong>Max Hops</strong> field, type the maximum number of hops from 1 to 255.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Click <strong>Save</strong>. Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see <strong>Applying Changes to Devices, page 4-25</strong>.</td>
</tr>
</tbody>
</table>

### Setting Up DHCPv6 Relay

**License:** Control  
**Supported Devices:** Series 3

The following procedure explains how to set up DHCPv6 relay on a virtual router.
### Setting Up Virtual Routers

#### Configuring Virtual Routers

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

**To set up DHCPv6 relay:**

- **Access:** Admin/Network Admin

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

The Device Management page appears.

**Step 2**
Next to the device where you want to set up DHCP relay, click the edit icon (✏️).

The Interfaces tab for that device appears.

**Step 3**
Click **Virtual Routers**.

The Virtual Routers tab appears.

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

The Edit Virtual Router pop-up window appears.

**Step 5**
To set up DHCP relay for DHCPv6, select the **DHCPv6** check box.

**Step 6**
In the **Interfaces** field, select 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 select whether the interface relays DHCP requests **Upstream**, **Downstream**, or **Both**.

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

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

**Step 9**
Click **Save**.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see **Applying Changes to Devices, page 4-25**.

### Setting Up Static Routes

**License:** Control

**Supported Devices:** Series 3

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.

See the following sections for more information:

- **Understanding the Static Routes Table View, page 7-14**
- **Adding Static Routes, page 7-14**
Understanding the Static Routes Table View

**License:** Control

**Supported Devices:** Series 3

The Static Routes tab of the Virtual Router editor displays a list of all the static routes you have configured on a virtual router. The table includes summary information about each route, as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Specifies whether this route is currently enabled or disabled.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the static route.</td>
</tr>
<tr>
<td>Destination</td>
<td>The destination network where traffic is routed.</td>
</tr>
</tbody>
</table>
| Type      | Specifies the action that is taken for this route, which will is 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. |

Adding Static Routes

**License:** Control

**Supported Devices:** Series 3

The following procedure explains how to add a static route.

To edit a static route, click the edit icon ( ). To delete a static route, click the delete icon ( ).

**To add a static route:**

**Access:** Admin/Network Admin

1. **Step 1** Select **Devices > Device Management**. The Device Management page appears.
2. **Step 2** Next to the device where you want to add the static route, click the edit icon ( ). The Interfaces tab for that device appears.
3. **Step 3** Click **Virtual Routers**. The Virtual Routers tab appears.
4. **Step 4** Next to the virtual router where you want to add the static route, click the edit icon ( ). The Edit Virtual Router pop-up window appears.
Step 5  Click **Static** to display the static route options.

Step 6  Click **Add Static Route**.

The Add Static Route pop-up window appears.

Step 7  In the **Route Name** field, type a name for the static route. You can use alphanumeric characters and spaces.

Step 8  For **Enabled**, select the check box to specify that the route is currently enabled.

Step 9  In the **Preference** field, type a numerical value between 1 and 65535 to determine the route selection. If you have multiple routes to the same destination, the system selects the route with the higher preference.

Step 10  From the **Type** drop-down list, select the type of static route you are configuring.

Step 11  In the **Destination** field, type the IP address for the destination network where traffic should be routed.

Step 12  In the **Gateway** field, you have two options:
- If you selected **IP** as the selected static route type, type an IP address.
- If you selected **Interface** as the selected static route type, select 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**.

The static route is added.

Step 14  Click **Save**.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

---

**Setting Up Dynamic Routing**

**License:** Control

**Supported Devices:** Series 3

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.

See the following sections for more information:
- Setting Up RIP Configuration, page 7-16
- Setting Up OSPF Configuration, page 7-21
Setting Up RIP Configuration

License: Control
Supported Devices: Series 3
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.

See the following sections for more information on configuring RIP:
- Adding Interfaces for RIP Configuration, page 7-16
- Configuring Authentication Settings for RIP Configuration, page 7-17
- Configuring Advanced Settings for RIP Configuration, page 7-18
- Adding Import Filters for RIP Configuration, page 7-19
- Adding Export Filters for RIP Configuration, page 7-20

Adding Interfaces for RIP Configuration

License: Control
Supported Devices: Series 3
While configuring RIP, you must select interfaces from those already included in the virtual router, where you want to configure RIP. Disabled interfaces are not available.

To edit a RIP interface, click the edit icon ( ). To delete a RIP interface, click the delete icon ( ).

To add an interface for RIP configuration:
Access: Admin/Network Admin

Step 1 Select Devices > Device Management.
The Device Management page appears.

Step 2 Next to the device where you want to add the RIP interface, click the edit icon ( ).
The Interfaces tab for that device appears.

Step 3 Click Virtual Routers.
The Virtual Routers tab appears.

Step 4 Next to the virtual router where you want to add the RIP interface, click the edit icon ( ).
The Edit Virtual Router pop-up window appears.

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 ( ).
The Add an Interface pop-up window appears.
Step 8 From the Name drop-down list, select the interface where you want to configure RIP.
Chapter 7  Setting Up Virtual Routers

Configuring Virtual Routers

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, type 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, select 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.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Configuring Authentication Settings for RIP Configuration

License: Control
Supported Devices: Series 3

RIP authentication uses one of the authentication profiles you configured on the virtual router. For more information about configuring authentication profiles, see Adding Virtual Router Authentication Profiles, page 7-30.

To configure authentication settings for RIP configuration:
Access: Admin/Network Admin

Step 1 Select Devices > Device Management.
The Device Management page appears.

Step 2 Next to the device where you want to add the RIP authentication profile, click the edit icon ( )
The Interfaces tab for that device appears.

Step 3 Click Virtual Routers.
The Virtual Routers tab appears.

Step 4 Next to the virtual router where you want to add the RIP authentication profile, click the edit icon ( )
The Edit Virtual Router pop-up window appears.

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

Step 6 Click RIP to display the RIP options.

Step 7 Under Authentication, use the Profile drop-down list to select an existing virtual router authentication profile or select None.

Step 8 Click Save.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

**Configuring Advanced Settings for RIP Configuration**

**License:** Control

**Supported Devices:** Series 3

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.

---

**To configure advanced settings for RIP configuration:**

**Access:** Admin/Network Admin

---

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

The Device Management page appears.

**Step 2** Next to the device where you want to edit the RIP advanced settings, click the edit icon (💾).

The Interfaces tab for that device appears.

**Step 3** Click **Virtual Routers**.

The Virtual Routers tab appears.

**Step 4** Next to the virtual router where you want to edit the RIP advanced settings, click the edit icon (🛠).

The Edit Virtual Router pop-up window appears.

**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, type 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, type the interval, in seconds, between periodic updates. A lower number determines faster convergence, but larger network load.

**Step 9** In the **Timeout Time** field, type a numerical value that specifies how old routes must be, in seconds, before being considered unreachable.

**Step 10** In the **Garbage Time** field, type a numerical value that specifies how old routes must be, in seconds, before being discarded.

**Step 11** In the **Infinity** field, type 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, select 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
Step 13 Click Save.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

## Adding Import Filters for RIP Configuration

**License:** Control

**Supported Devices:** Series 3

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. For more information about configuring filters, see Setting Up Virtual Router Filters, page 7-28.

**To add an import filter for RIP configuration:**

**Access:** Admin/Network Admin

---

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

The Device Management page appears.

**Step 2** Next to the device where you want to add the RIP virtual router filter, click the edit icon ( )

The Interfaces tab for that device appears.

**Step 3** Click Virtual Routers.

The Virtual Routers tab appears.

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

The Edit Virtual Router pop-up window appears.

**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 ( ).

The Add an Import Filter pop-up window appears.

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

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

**Step 10** Click OK.

The import filter is added.

**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**.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

---

### Adding Export Filters for RIP Configuration

**License:** Control  
**Supported Devices:** Series 3

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. For more information about configuring filters, see Setting Up Virtual Router Filters, page 7-28.

**To add an export filter for RIP configuration:**  
**Access:** Admin/Network Admin

---

**Step 1** Select **Devices > Device Management**.  
The Device Management page appears.

**Step 2** Next to the device where you want to add the RIP virtual router filter, click the edit icon ( ).  
The Interfaces tab for that device appears.

**Step 3** Click **Virtual Routers**.  
The Virtual Routers tab appears.

**Step 4** Next to the virtual router where you want to add the RIP virtual router filter, click the edit icon ( ).  
The Edit Virtual Router pop-up window appears.

**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 ( ).  
The Add an Export Filter pop-up window appears.

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

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

**Step 10** Click **OK**.  
The export filter is added.

---

**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**.  
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.
Setting Up OSPF Configuration

**License:** Control  
**Supported Devices:** Series 3

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.

See the following sections for more information:
- Setting Up OSPF Routing Areas, page 7-21
- Adding Import Filters for OSPF Configuration, page 7-27
- Adding Export Filters for OSPF Configuration, page 7-27

Setting Up OSPF Routing Areas

**License:** Control  
**Supported Devices:** Series 3

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.

See the following sections for more information on setting up OSPF areas:
- Adding OSPF Areas, page 7-21
- Adding OSPF Area Interfaces, page 7-23
- Adding OSPF Area Vlinks, page 7-25

Adding OSPF Areas

**License:** Control  
**Supported Devices:** Series 3

The following procedure explains how to add an OSPF area and configure general settings.

**To add an OSPF area:**
**Access:** Admin/Network Admin

1. **Step 1** Select Devices > Device Management.  
The Device Management page appears.
2. **Step 2** Next to the device where you want to edit the OSPF general options, click the edit icon (✏️).
Chapter 7  Setting Up Virtual Routers

Configuring Virtual Routers

The Interfaces tab for that device appears.

Step 3  Click **Virtual Routers**.

The Virtual Routers tab appears.

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

The Edit Virtual Router pop-up window appears.

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 ( ).

The Add OSPF Area pop-up window appears.

Step 8  In the **Area Id** field, type a numerical value for the area. This value can be either an integer or an IPv4 address.

Step 9  Optionally, select 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.

The Default cost field and Stubnet field appear.

Step 10  In the **Default cost** field, type 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, type an IP address in CIDR notation.

Step 13  Select the **Hidden** check box to indicate that the stubnet is hidden. Hidden stubnets are not propagated into other areas.

Step 14  Select the **Summary** check box to designate that default stubnets that are subnetworks of this stubnet are suppressed.

Step 15  In the **Stub cost** field, type a value that defines the cost associated with routing to this stub network.

Step 16  Click **OK**.

The stubnet is added.

**Tip**

To edit a stubnet, click the edit icon ( ). To delete a stubnet, click the delete icon ( ).

Step 17  Optionally, under **Networks**, click the add icon ( ).

Step 18  In the **IP Address** field, type an IP address in CIDR notation for the network.

Step 19  Select the **Hidden** check box to indicate that the network is hidden. Hidden networks are not propagated into other areas.

Step 20  Click **OK**.

The network is added.

**Tip**

To edit a network, click the edit icon ( ). To delete a network, click the delete icon ( ).

Step 21  Click **Save**.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Adding OSPF Area Interfaces

License: Control

Supported Devices: Series 3

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, page 7-30.

**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.

---

*Note*
You can select only one interface for use in an OSPF area.

To add an OSPF area interface:
Access: Admin/Network Admin

**Step 1**
Select Devices > Device Management.
The Device Management page appears.

**Step 2**
Next to the device where you want to add the OSPF interface, click the edit icon ( ).
The Interfaces tab for that device appears.

**Step 3**
Click Virtual Routers.
The Virtual Routers tab appears.

**Step 4**  
Next to the virtual router where you want to add the OSPF interface, click the edit icon (✏).  
The Edit Virtual Router pop-up window appears.

**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 (➕).  
The Add OSPF Area pop-up window appears.

**Step 8**  
Click **Interfaces**.  
The Interfaces tab appears.

**Step 9**  
Click the add icon (➕).  
The Add OSPF Area Interface pop-up window appears.

**Step 10**  
Take any of the actions as described in **Adding OSPF Area Interfaces**, page 7-23.

**Step 11**  
Optionally under **Neighbors**, click the add icon (➕).

**Step 12**  
In the **IP address** field, type an IP address for the neighbor receiving hello messages on non-broadcast networks from this interface.

**Step 13**  
Select the **Eligible** check box to indicate that the neighbor is eligible to receive messages.

**Step 14**  
Click **OK**.  
The neighbor is added.

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

**Step 15**  
Click **OK**.  
The OSPF area interface is added.

**Step 16**  
Click **Save**.  
The OSPF area is saved.

**Step 17**  
Click **Save**.  
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see **Applying Changes to Devices**, page 4-25.

---

**Adding OSPF Area Vlinks**

**License**: Control  
**Supported Devices**: Series 3  

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.
To add an OSPF area vlink:

Access: Admin/Network Admin

Step 1 Select Devices > Device Management.
The Device Management page appears.

Step 2 Next to the device where you want to add the OSPF vlink, click the edit icon ( ).
The Interfaces tab for that device appears.

Step 3 Click Virtual Routers.
The Virtual Routers tab appears.

Step 4 Next to the virtual router where you want to add the OSPF interface, click the edit icon ( )
The Edit Virtual Router pop-up window appears.

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 ( )
The Add OSPF Area pop-up window appears.

Step 8 Click Vlinks.
The Vlinks tab appears.

Step 9 Click the add icon ( )
The Add OSPF Area Vlink pop-up window appears.

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

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

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

Step 13 In the Retrans Interval field, type the interval, in seconds, between retransmissions of unacknowledged updates.

Step 14 In the Wait Time field, type the number of seconds that the router waits between starting election and building adjacency.

Step 15 In the Dead Interval field, 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.

Step 16 In the Dead Count field, 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.

Step 17 Click OK.
The OSPF area vlink is added.

Step 18 Click Save.
The OSPF area is saved.

Step 19 Click Save.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.
Adding Import Filters for OSPF Configuration

License: Control
Supported Devices: Series 3

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. For more information about configuring filters, see Setting Up Virtual Router Filters, page 7-28.

To add an import filter for OSPF configuration:

Access: Admin/Network Admin

Step 1 Select Devices > Device Management.
The Device Management page appears.

Step 2 Next to the device where you want to add the OSPF virtual router filter, click the edit icon ( ).
The Interfaces tab for that device appears.

Step 3 Click Virtual Routers.
The Virtual Routers tab appears.

Step 4 Next to the virtual router where you want to add the OSPF virtual router filter, click the edit icon ( ).
The Edit Virtual Router pop-up window appears.

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 ( ).
The Add Import Filter pop-up window appears.

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

Step 9 Next to Action, select Accept or Reject.

Step 10 Click OK.
The import filter is added.

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.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

Adding Export Filters for OSPF Configuration

License: Control
Supported Devices: Series 3
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. For more information about configuring filters, see Setting Up Virtual Router Filters, page 7-28.

**To add an export filter for OSPF configuration:**

**Access:** Admin/Network Admin

---

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

The Device Management page appears.

**Step 2** Next to the device where you want to add the OSPF virtual router filter, click the edit icon ( ).

The Interfaces tab for that device appears.

**Step 3** Click Virtual Routers.

The Virtual Routers tab appears.

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

The Edit Virtual Router pop-up window appears.

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

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

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

The Add an Export Filter pop-up window appears.

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

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

**Step 10** Click OK.

The export filter is added.

---

**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.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.

---

**Setting Up Virtual Router Filters**

**License:** Control

**Supported Devices:** Series 3

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.
### Tip

To edit a virtual router filter, click the edit icon (✏️). To delete a virtual router filter, click the delete icon (🗑️).

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, as described in the following table.

#### Table 7-3 Virtual Router Filters Table View Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the filter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol that the route originates from:</td>
</tr>
<tr>
<td></td>
<td>• Static — The route originates as a local static route.</td>
</tr>
<tr>
<td></td>
<td>• RIP — The route originates from a dynamic RIP configuration.</td>
</tr>
<tr>
<td></td>
<td>• OSPF — The route originates from a dynamic OSPF configuration.</td>
</tr>
<tr>
<td>From Router</td>
<td>The router IP addresses that this filter attempts to match in a router. You must enter this value for static and RIP filters.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next hop where packets using this route are forwarded. You must enter this value for static and RIP filters.</td>
</tr>
<tr>
<td>Destination Type</td>
<td>The type of destination where packets are sent:</td>
</tr>
<tr>
<td></td>
<td>• Router</td>
</tr>
<tr>
<td></td>
<td>• Device</td>
</tr>
<tr>
<td></td>
<td>• Discard</td>
</tr>
<tr>
<td>Destination Network</td>
<td>The networks that this filter attempts to match in a route.</td>
</tr>
<tr>
<td>OSPF Path Type</td>
<td>Applies only to OSPF protocol. The path type can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Ext-1</td>
</tr>
<tr>
<td></td>
<td>• Ext-2</td>
</tr>
<tr>
<td></td>
<td>• Inter Area</td>
</tr>
<tr>
<td></td>
<td>• Intra Area</td>
</tr>
<tr>
<td>OSPF Router ID</td>
<td>Applies only to OSPF protocol. The router ID of the router advertising that route/network.</td>
</tr>
</tbody>
</table>

#### To add a virtual router filter:

**Access:** Admin/Network Admin

---

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

The Device Management page appears.

**Step 2**
Next to the device where you want to add the virtual filter router, click the edit icon (✏️).

The Interfaces tab for that device appears.

**Step 3**
Click Virtual Routers.

The Virtual Routers tab appears.
Step 4  Next to the virtual router where you want to add the virtual filter router, click the edit icon ( ).
The Edit Virtual Router pop-up window appears.

Step 5  Click Filter to display the Filter options.

Step 6  Click Add Filter.
The Create Filter pop-up window appears.

Step 7  In the Name field, type a name for the filter. You can use alphanumeric characters only.

Step 8  Under Protocol, select All or select the protocol that applies to the filter.

Step 9  If you selected All, Static, or RIP as the Protocol, under From Router, type the router IP addresses that this
filter will attempt to match in a route.
Note that you can also enter a /32 CIDR block for IPv4 addresses and a /128 prefix length for IPv6
domains. All other address blocks are invalid for this field.

Step 10 Click Add.
The From Router field is populated.

Step 11 If you selected All, Static, or RIP as the Protocol, under Next Hop, type the IP addresses for the gateways
that this filter will attempt to match in a route.
Note that you can also enter a /32 CIDR block for IPv4 addresses and a /128 prefix length for IPv6
domains. All other address blocks are invalid for this field.

Step 12 Click Add.
The Next Hop field is populated.

Step 13 Under Destination Type, select the options that apply to the filter.

Step 14 Under Destination Network, type the IP address of the network that this filter will attempt to match in a
route.

Step 15 Click Add.
The Destination Network field is populated.

Step 16 If you selected All or OSPF as the Protocol, under Path Type, select the options that apply to the filter.
You must select at least one path type.

Step 17 If you selected OSPF as the Protocol, under Router ID, type the IP address that serves as the router ID of
the router advertising the route/network.

Step 18 Click Add.
The Router ID field is populated.

Step 19 Click OK.
The filter is added.

Step 20 Click Save.
Your changes are saved. Note that your changes do not take effect until you apply the device
configuration; see Applying Changes to Devices, page 4-25.

Adding Virtual Router Authentication Profiles

License: Control
Supported Devices: Series 3

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.

Tip
To edit an authentication profile, click the edit icon ( ). To delete an authentication profile, click the delete icon ( ).

To add a virtual router authentication profile:
Access: Admin/Network Admin

Step 1 Select Devices > Device Management.
The Device Management page appears.

Step 2 Next to the device where you want to add the virtual router authentication profile, click the edit icon ( ).
The Interfaces tab for that device appears.

Step 3 Click Virtual Routers.
The Virtual Routers tab appears.

Step 4 Next to the virtual router where you want to add the virtual router authentication profile, click the edit icon ( ).
The Edit Virtual Router pop-up window appears.

Step 5 Click Authentication Profile.
The Authentication Profile tab appears.

Step 6 Click Add Authentication Profile.
The Add Authentication Profile pop-up window appears.

Step 7 In the Authentication Profile Name field, type a name for the authentication profile.

Step 8 From the Authentication Type drop down list, select simple or cryptographic.

Step 9 In the Password field, type a secure password.

Step 10 In the Confirm Password field, type the password again to confirm it.

Step 11 Click OK.
The authentication profile is added.

Step 12 Click Save.
Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.
Viewing Virtual Router Statistics

License: Control
Supported Devices: Series 3

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.

To view virtual router statistics:
Access: Admin/Network Admin

Step 1  Select Devices > Device Management.
The Device Management page appears.
Step 2  Next to the device where you want to view the virtual router statistics, click the edit icon ( ).
The Interfaces tab for that device appears.
Step 3  Click Virtual Routers.
The Virtual Routers tab appears.
Step 4  Next to the virtual router where you want to view the router statistics, click the view icon ( ).
The Statistics pop-up window appears.
Step 5  Click OK to close the window.

Deleting Virtual Routers

License: Control
Supported Devices: Series 3

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

To delete a virtual router:
Access: Admin/Network Admin

Step 1  Select Devices > Device Management.
The Device Management page appears.
Step 2  Next to the device where you want to delete the virtual router, click the edit icon ( ).
The Interfaces tab for that device appears.
Step 3  Click Virtual Routers.
The Virtual Routers tab appears.
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.
The virtual router is deleted. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Devices, page 4-25.