Configuring Dynamic and Static Routing

The Routing feature lets you specify static route, RIP, proxy ARP, OSPF, and BGP configuration parameters.

For more information about configuring routing on the FWSM, see the following:

- ASR Group, page 14-1
- Dynamic Routing, page 14-2
- Static Route, page 14-27
- Proxy ARPs, page 14-29

ASR Group

Use the ASR Group pane to assign asynchronous routing group ID numbers to interfaces.

In some situations, return traffic for a session may be routed through a different interface than it originated from. In failover configurations, return traffic for a connection that originated on one unit may return through the peer unit. This most commonly occurs when two interfaces on a single FWSM, or two FWSMs in a failover pair, are connected to different service providers and the outbound connection does not use a NAT address. By default, the FWSM drops the return traffic because there is no connection information for the traffic.

You can prevent the return traffic from being dropped using an ASR Group on interfaces where this is likely to occur. When an interface configured with an ASR Group receives a packet for which it has no session information, it checks the session information for the other interfaces that are in the same group.

**Note**

In failover configurations, you must enable Stateful Failover for session information to be passed from the standby failover group to the active failover group.

If it does not find a match, the packet is dropped. If it finds a match, then one of the following actions occurs:

- If the incoming traffic originated on a peer unit in a failover configuration, some or all of the layer 2 header is rewritten and the packet is redirected to the other unit. This redirection continues as long as the session is active.
- If the incoming traffic originated on a different interface on the same unit, some or all of the layer 2 header is rewritten and the packet is reinjected into the stream.
Fields
The ASR Group table displays the following information for each interface on the FWSM:

- **Interface**—Displays the name of the interface on the FWSM.
- **ASR Group ID**—Displays the number of the ASR Group the interface belongs to. If the interface has not been assigned an ASR Group number, this column displays “-- None --”. Valid values are from 1 to 32.

To assign an ASR Group number to an interface, click the **ASR Group ID** cell in the row of the desired interface. A list of valid ASR Group number appears. Select the desired ASR Group number from the list. You can assign a maximum of 8 interfaces to a single ASR Group.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Dynamic Routing
The Dynamic Routing area lets you edit a static route or configure OSPF or RIP parameters. See the following topics for more information:

- **BGP Stub Routing**
- **OSPF**
- **RIP**

BGP Stub Routing
The FWSM supports BGP stub routing. The BGP stub routing process advertises static and directly connected routes. See the following topics for more information:

- **BGP Stub Routing Limitations**, page 14-2
- **Configuring BGP Stub Routing**, page 14-3
- **BGP (field information)**, page 14-4

For information about monitoring the BGP routing process, see the “Monitoring BGP” section on page 28-1.

BGP Stub Routing Limitations
The following limitations apply to configuring BGP stub routing on the FWSM:

- You can only configure one BGP routing process, even in multiple context mode.
- You can only configure one BGP neighbor.
• The FWSM does not process UPDATE messages received from the BGP neighbor. It can only send routing updates to the BGP neighbor.
• You cannot redistribute routes discovered by other routing processes into the BGP routing process.
• BGP stub does not support IPv6, VPN, or NLRI multicast.
• Only iBGP is supported; eBGP is not supported.

Configuring BGP Stub Routing

Before configuring BGP stub routing on the FWSM:

• You must enable route reflector on the BGP neighbor. Refer to the documentation of the BGP neighbor for more information about configuring this option.
• If the FWSM is in multiple context mode, you must be in the admin context to configure BGP stub routing. Additionally, the admin context must be in routed mode.

To enable and configure a BGP routing process, perform the following steps:

---

**Step 1** Navigate to **Configuration > Routing > Dynamic Routing > BGP**. If you are in multiple context mode, you must be in the admin context to configure BGP stub routing.

**Step 2** Enable the BGP routing process by checking the **Enable BGP Routing** check box.

**Step 3** Assign an autonomous system number to the FWSM in the **Router AS** field. The autonomous system number must be the same as the AS number of the BGP peer. Valid values are from 1 to 65535.

**Step 4** (Optional) Enter a router ID for the FWSM in the **Router ID** field. The router ID can be any IP address, including an IP address that is not configured on the FWSM. If you do not enter a router ID, the highest IP address configured on the FWSM is used.

**Step 5** Specify the BGP neighbor that BGP updates are sent to by performing the following steps:

a. Enter the IP address of the BGP neighbor in the **Neighbor Address** field.

b. Enter the autonomous system number of the BGP neighbor in the **Remote AS** field. Valid values are from 1 to 65535.

c. (Optional) Enter a password used to authenticate the BGP message to the neighbor in the **Password** field. Reenter the same password in the **Confirm Password** field.

   This password must be set on both the neighbor and the FWSM before BGP messages can be exchanged. The password can contains numbers, letters, and any of the following symbols:
   `~ ! @ # $ % ^ & * ( ) - _ = + | } \ { ] [ " ` : ; / > < , . ?``

   The password cannot contain spaces.

**Step 6** (Optional) Select the authentication mode from the **Mode** list. If you select a mode, the BGP neighbor must support the mode option and have it set to the same value.

**Step 7** Specify which of the static and directly-connected networks that the BGP routing process advertises. Perform the following steps for each network you want to advertise. You can configure up to 200 networks on the FWSM.

a. Type the network address in the **IP Network** field.

b. Type or select the network mask from the **Netmask** field.

c. Click **Add** to add the network to the BGP Networks list.

d. (Optional) To remove a configured network from the BGP Networks list, select the network and click **Delete**.
Dynamic Routing

Chapter 14 Configuring Dynamic and Static Routing

Step 8 Click **Apply** to save your changes to the FWSM.

---

**BGP (field information)**

The BGP pane lets you enable and configure a BGP routing process. You can only enable a single BGP routing process on the device at a time.

**Fields**

**BGP Routing Parameters**

- **Enable BGP Routing**—Check this check box to enable the BGP routing process. Uncheck this check box to disable the BGP routing process.
- **Router AS**—The autonomous system number of the FWSM.
- **Router ID**—The router ID of the FWSM. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the FWSM. If not entered, the router ID is set to the highest IP address configured on the FWSM.

**BGP Neighbor**—The BGP Neighbor area lets you define the BGP neighbor that the BGP routing updates are sent to.

- **Neighbor Address**—The IP address of the BGP neighbor.
- **Remote AS**—The autonomous system number of the BGP neighbor.
- **Password**—Type a password used for MD5 authentication of the BGP messages. The BGP neighbor must be configured with the same password.
- **Mode**—Select the password mode from the list.
- **Confirm Password**—Re-type your password.

**BGP Networks**—The BGP Networks area lets you define the networks the BGP routing process can advertise.

- **BGP Networks**—Displays the networks that the BGP routing process can advertise.
- **IP Network**—Enter a network address.
- **Netmask**—The mask to apply to the IP Network. You can select a standard network mask from the list or type the mask in the field.
- **Add**—Click to add the defined network to the BGP Networks table.
- **Delete**—Click to delete the selected network from the BGP Networks table.

**Modes**

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
<th>Multiple Context</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
<td>Single</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*For More Information*

- BGP Stub Routing, page 14-2
OSPF

OSPF is an interior gateway routing protocol that uses link states rather than distance vectors for path selection. OSPF propagates link-state advertisements rather than routing table updates. Because only LSAs are exchanged, rather than entire routing tables, OSPF networks converge more quickly than RIP networks.

OSPF supports MD5 and clear text neighbor authentication. Authentication should be used with all routing protocols when possible because route redistribution between OSPF and other protocols (like RIP) can potentially be used by attackers to subvert routing information.

If NAT is used, if OSPF is operating on public and private areas, and if address filtering is required, then you need to run two OSPF processes—one process for the public areas and one for the private areas.

A router that has interfaces in multiple areas is called an Area Border Router (ABR). A router that acts as a gateway to redistribute traffic between routers using OSPF and routers using other routing protocols is called an Autonomous System Boundary Router (ASBR).

An ABR uses LSAs to send information about available routes to other OSPF routers. Using ABR type 3 LSA filtering, you can have separate private and public areas with the FWSM acting as an ABR. Type 3 LSAs (inter-area routes) can be filtered from one area to other. This lets you use NAT and OSPF together without advertising private networks.

Note

Only type 3 LSAs can be filtered. If you configure the FWSM as an ASBR in a private network, it will send type 5 LSAs describing private networks, which will get flooded to the entire AS including public areas.

If NAT is employed but OSPF is only running in public areas, then routes to public networks can be redistributed inside the private network, either as default or type 5 AS External LSAs. However, you need to configure static routes for the private networks protected by the FWSM. Also, you should not mix public and private networks on the same FWSM interface.

For more information about enabling and configuring OSPF, see the following:

- Setup
- Interface
- Static Neighbor
- Virtual Link
- Filtering
- Redistribution
- Summary Address

Setup

The Setup pane lets you enable OSPF processes, configure OSPF areas and networks, and define OSPF route summarization.

Note

You cannot enable OSPF if you have RIP enabled.
For more information about configuring these areas, see the following:

- Setup > Process Instances Tab
- Setup > Area/Networks Tab
- Setup > Route Summarization Tab

**Modes**

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

**Setup > Process Instances Tab**

You can enable up to two OSPF process instances. Each OSPF process has its own associated areas and networks.

**Fields**

- OSPF Process 1 and 2—Each group box contains the settings for a specific OSPF process.
- Enable this OSPF Process—Select the check box to enable an OSPF process. You cannot enable an OSPF process if you have RIP enabled on the FWSM. Clear this check box to remove the OSPF process.
- OSPF Process ID—Enter a unique numeric identifier for the OSPF process. This process ID is used internal and does not need to match the OSPF process ID on any other OSPF devices. Valid values are from 1 to 65535.
- Advanced—Opens the **Edit OSPF Process Advanced Properties** dialog box, where you can configure the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings.

**Modes**

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

**Edit OSPF Process Advanced Properties**

You can edit process-specific settings, such as the Router ID, Adjacency Changes, Administrative Route Distances, Timers, and Default Information Originate settings, in the Edit OSPF Process Advanced Properties dialog box.
**Fields**

- **OSPF Process**—Displays the OSPF process you are configuring. You cannot change this value.
- **Router ID**—To use a fixed router ID, enter a router ID in IP address format in the **Router ID** box.
  If you leave this value blank, the highest-level IP address on the FWSM is used as the router ID.
- **Ignore LSA MOSPF**—Select this check box to suppress the sending of syslog messages when the
  FWSM receives Type 6 (MOSPF) LSA packets. This setting is cleared by default.
- **RFC 1583 Compatible**—Select this check box to calculate summary route costs per RFC 1583. Clear
  this check box to calculate summary route costs per RFC 2328. To minimize the chance of routing
  loops, all OSPF devices in an OSPF routing domain should have RFC compatibility set
  identically. This setting is selected by default.
- **Adjacency Changes**—Contains settings that define the adjacency changes that cause syslog
  messages to be sent.
  - **Log Adjacency Changes**—Select this check box to cause the FWSM to send a syslog message
    whenever an OSPF neighbor goes up or down. This setting is selected by default.
  - **Log Adjacency Changes Detail**—Select this check box to cause the FWSM to send a syslog
    message whenever any state change occurs, not just when a neighbor goes up or down. This
    setting is cleared by default.
- **Administrative Route Distances**—Contains the settings for the administrative distances of routes
  based on the route type.
  - **Inter Area**—Sets the administrative distance for all routes from one area to another. Valid values
    range from 1 to 255. The default value is 100.
  - **Intra Area**—Sets the administrative distance for all routes within an area. Valid values range
    from 1 to 255. The default value is 100.
  - **External**—Sets the administrative distance for all routes from other routing domains that are
    learned through redistribution. Valid values range from 1 to 255. The default value is 100.
- **Timers**—Contains the settings used to configure LSA pacing and SPF calculation timers.
  - **SPF Delay Time**—Specifies the time between when OSPF receives a topology change and when
    the SPF calculation starts. Valid values range from 0 to 65535. The default value is 5.
  - **SPF Hold Time**—Specifies the hold time between consecutive SPF calculations. Valid values range
    from 1 to 65534. The default value is 10.
  - **LSA Group Pacing**—Specifies the interval at which LSAs are collected into a group and
    refreshed, checksummed, or aged. Valid values range from 10 to 1800. The default value is 240.
- **Default Information Originate**—Contains the settings used by an ASBR to generate a default
  external route into an OSPF routing domain.
  - **Enable Default Information Originate**—Select this check box to enable the generation of the
    default route into the OSPF routing domain.
  - **Always advertise the default route**—Select this check box to always advertise the default route.
    This option is cleared by default.
  - **Metric Value**—Specifies the OSPF default metric. Valid values range from 0 to 16777214. The
    default value is 1.
  - **Metric Type**—Specifies the external link type associated with the default route advertised into
    the OSPF routing domain. Valid values are 1 or 2, indicating a Type 1 or a Type 2 external route.
    The default value is 2.
Route Map—(Optional) The name of the route map to apply. The routing process generates the default route if the route map is satisfied.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

- Setup > Area/Networks Tab

The Area/Networks tab displays the areas, and the networks they contain, for each OSPF process on the FWSM.

Fields

- Area/Networks—Displays information about the areas and the area networks configured for each OSPF process. Double-clicking a row in the table opens the Add/Edit OSPF Area dialog box for the selected area.
  - OSPF Process—Displays the OSPF process the area applies to.
  - Area ID—Displays the area ID.
  - Area Type—Displays the area type. The area type is one of the following values: Normal, Stub, NSSA.
  - Networks—Displays the area networks.
  - Authentication—Displays the type of authentication set for the area. The authentication type is one of the following values: None, Password, MD5.
  - Options—Displays any options set for the area type.
  - Cost—Displays the default cost for the area.

- Add—Opens the Add/Edit OSPF Area dialog box. Use this button to add a new area configuration.
- Edit—Opens the Add/Edit OSPF Area dialog box. Use this button to change the parameters of the selected area.
- Delete—Removes the selected area from the configuration.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

-
Add/Edit OSPF Area

You define area parameters, the networks contained by the area, and the OSPF process associated with the area in the Add/Edit OSPF Area dialog box.

Fields

- **OSPF Process**—When adding a new area, select the OSPF process ID for the OSPF process for which the area is being. If there is only one OSPF process enabled on the FWSM, then that process is selected by default. When editing an existing area, you cannot change the OSPF process ID.

- **Area ID**—When adding a new area, enter the area ID. You can specify the area ID as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295. You cannot change the area ID when editing an existing area.

- **Area Type**—Contains the settings for the type of area being configured.
  - **Normal**—Select this option to make the area a standard OSPF area. This option is selected by default when you first create an area.
  - **Stub**—Selecting this option makes the area a stub area. Stub areas do not have any routers or areas beyond it. Stub areas prevent AS External LSAs (Type 5 LSAs) from being flooded into the stub area. When you create a stub area, you have the option of preventing summary LSAs (Type 3 and 4) from being flooded into the area by clearing the Summary check box.
  - **Summary**—When the area being defined is a stub area, clearing this check box prevents LSAs from being sent into the stub area. This check box is selected by default for stub areas.
  - **NSSA**—Select this option to make the area a not-so-stubby area. NSSAs accept Type 7 LSAs. When you create a NSSA, you have the option of preventing summary LSAs from being flooded into the area by clearing the Summary check box. You can also disable route redistribution by clearing the Redistribute check box and enabling Default Information Originate.
  - **Redistribute**—Clear this check box to prevent routes from being imported into the NSSA. This check box is selected by default.
  - **Summary**—When the area being defined is a NSSA, clearing this check box prevents LSAs from being sent into the stub area. This check box is selected by default for NSSAs.
  - **Default Information Originate**—Select this check box to generate a Type 7 default into the NSSA. This check box is cleared by default.
  - **Metric Value**—Specifies the OSPF metric value for the default route. Valid values range from 0 to 16777214. The default value is 1.
  - **Metric Type**—The OSPF metric type for the default route. The choices are 1 (Type 1) or 2 (Type 2). The default value is 2.

- **Area Networks**—Contains the settings for defining an OSPF area.
  - **Enter IP Address and Mask**—Contains the settings used to define the networks in the area.
    - **IP Address**—Enter the IP address of the network or host to be added to the area. Use 0.0.0.0 with a netmask of 0.0.0.0 to create the default area. You can only use 0.0.0.0 in one area.
    - **Netmask**—Select the network mask for the IP address or host to be added to the area. If adding a host, select the 255.255.255.255 mask.
  - **Add**—Adds the network defined in the Enter IP Address and Mask group box to the area. The added network appears in the Area Networks table.
  - **Delete**—Deletes the selected network from the Area Networks table.
  - **Area Networks**—Displays the networks defined for the area.
IP Address—Displays the IP address of the network.
Netmask—Displays the network mask for the network.

- Authentication—Contains the settings for OSPF area authentication.
  - None—Select this option to disable OSPF area authentication. This is the default setting.
  - Password—Select this option to use a clear text password for area authentication. This option is not recommended where security is a concern.
  - MD5—Select this option to use MD5 authentication.
- Default Cost—Specify a default cost for the area. Valid values range from 0 to 65535. The default value is 1.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Setup > Route Summarization Tab

In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range. To define summary address for external routes being redistributed into an OSPF area, see Summary Address.

Fields
- Route Summarization—Displays information about route summaries defined on the FWSM. Double-clicking a row in the table opens the Add/Edit Route Summarization dialog box for the selected route summary.
  - OSPF Process—Displays the OSPF process ID for the OSPF process associated with the route summary.
  - Area ID—Displays the area associated with the route summary.
  - IP Address—Displays the summary address.
  - Network Mask—Displays the summary mask.
  - Advertise—Displays “yes” when the route summaries are advertised when they match the address/mask pair or “no” when route summaries are suppressed when they match the address/mask pair.
- Add—Opens the Add/Edit Route Summarization dialog box. Use this button to define a new route summarization.
- Edit—Opens the Add/Edit Route Summarization dialog box. Use this button to change the parameters of the selected route summarization.
- Delete—Removes the selected route summarization from the configuration.
Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Add/Edit Route Summarization

Use the Add Route Summarization dialog box to add a new entry to the Route Summarization table. Use the Edit Route Summarization dialog box to change an existing entry.

Fields

- OSPF Process—Select the OSPF process the route summary applies to. You cannot change this value when editing an existing route summary entry.
- Area ID—Select the area ID the route summary applies to. You cannot change this value when editing an existing route summary entry.
- IP Address—Enter the network address for the routes being summarized.
- Network Mask—Select one of the common network masks from the list or type the mask in the box.
- Advertise—Select this check box to set the address range status to “advertise”. This causes Type 3 summary LSAs to be generated. Clear this check box to suppress the Type 3 summary LSA for the specified networks. This check box is selected by default.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Interface

The Interface pane lets you configure interface-specific OSPF authentication routing properties. For more information about configuring these properties, see the following:

- Interface > Authentication Tab
- Interface > Properties Tab

Modes

The following table shows the modes in which this feature is available:
Chapter 14  Configuring Dynamic and Static Routing

Dynamic Routing

Interface > Authentication Tab

The Authentication tab displays the OSPF authentication information for the FWSM interfaces.

**Fields**
- Authentication Properties—Displays the authentication information for the FWSM interfaces. Double-clicking a row in the table opens the Edit OSPF Interface Properties dialog box for the selected interface.
  - Interface—Displays the interface name.
  - Authentication Type—Displays the type of OSPF authentication enabled on the interface. The authentication type can be one of the following values:
    - None—OSPF authentication is disabled.
    - Password—Clear text password authentication is enabled.
    - MD5—MD5 authentication is enabled.
    - Area—The authentication type specified for the area is enabled on the interface. Area authentication is the default value for interfaces. However, area authentication is disabled by default. So, unless you previously specified an area authentication type, interfaces showing area authentication have authentication disabled.
- Edit—Opens the Edit OSPF Interface Properties dialog box for the selected interface.

**Modes**
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td>•</td>
<td>—</td>
</tr>
<tr>
<td>•</td>
<td>—</td>
</tr>
</tbody>
</table>

Edit OSPF Interface Authentication

The Edit OSPF Interface Authentication dialog box lets you configure the OSPF authentication type and parameters for the selected interface.

**Fields**
- Interface—Displays the name of the interface for which authentication is being configured. You cannot edit this field.
- Authentication—Contains the OSPF authentication options.
  - None—Select this option to disable OSPF authentication.
Dynamic Routing

- **Password**—Select this option to use clear text password authentication. This is not recommended where security is a concern.
- **MD5**—Select this option to use MD5 authentication (recommended).
- **Area**—(Default) Select this option to use the authentication type specified for the area (see Add/Edit OSPF Area for information about configuring area authentication). Area authentication is disabled by default. So, unless you have previously specified an area authentication type, interfaces set to area authentication have authentication disabled until you configure area authentication.

- **Authentication Password**—Contains the settings for entering the password when password authentication is enabled.
  - **Enter Password**—Enter a text string of up to 8 characters.
  - **Re-enter Password**—Reenter the password.

- **MD5 IDs and Keys**—Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID.
  - **Enter MD5 ID and Key**—Contains the settings for entering MD5 key information.
    - **Key ID**—Enter a numerical key identifier. Valid values range from 1 to 255.
    - **Key**—An alphanumeric character string of up to 16 bytes.
  - **Add**—Adds the specified MD5 key to the MD5 ID and Key table.
  - **Delete**—Removes the selected MD5 key and ID from the MD5 ID and Key table.
  - **MD5 ID and Key**—Displays the configured MD5 keys and key IDs.
    - **Key ID**—Displays the key ID for the selected key.
    - **Key**—Displays the key for the selected key ID.

**Modes**
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td>Multiple</td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

**Interface > Properties Tab**
The Properties tab displays the OSPF properties defined for each interface in a table format.

**Fields**
- **OSPF Interface Properties**—Displays interface-specific OSPF properties. Double-clicking a row in the table opens the Edit OSPF Interface Properties dialog box for the selected interface.
  - **Interface**—Displays the name of the interface that the OSPF configuration applies to.
  - **Broadcast**—Displays “No” if the interface is set to non-broadcast (point-to-point). Displays “Yes” if the interface is set to broadcast. “Yes” is the default setting for Ethernet interfaces.
  - **Cost**—Displays the cost of sending a packet through the interface.
Dynamic Routing

- Priority—Displays the OSPF priority assigned to the interface.
- MTU Ignore—Displays “No” if MTU mismatch detection is enabled. Displays “Yes” if the MTU mismatch detection is disabled.
- Database Filter—Displays “Yes” if outgoing LSAs are filtered during synchronization and flooding. Displays “No” if filtering is not enabled.

Edit—Opens the Edit OSPF Interface Properties dialog box for the selected interface.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Edit OSPF Interface Properties

Fields

- Interface—Displays the name of the interface for which you are configuring OSPF properties. You cannot edit this field.
- Broadcast—Select this check box to specify that the interface is a broadcast interface. This check box is selected by default for Ethernet interfaces. Clear this check box to designate the interface as a point-to-point, non-broadcast interface. Specifying an interface as point-to-point, non-broadcast lets you transmit OSPF routes over VPN tunnels.

When an interface is configured as point-to-point, non-broadcast, the following restrictions apply:
- You can define only one neighbor for the interface.
- You need to manually configure the neighbor (see Static Neighbor).
- You need to define a static route pointing to the crypto endpoint (see Static Route).
- If OSPF over the tunnel is running on the interface, regular OSPF with an upstream router cannot be run on the same interface.
- You should bind the crypto-map to the interface before specifying the OSPF neighbor to ensure that the OSPF updates are passed through the VPN tunnel. If you bind the crypto-map to the interface after specifying the OSPF neighbor, use the clear local-host all command to clear OSPF connections so the OSPF adjacencies can be established over the VPN tunnel.
- Cost—Specify the cost of sending a packet through the interface. The default value is 10.
- Priority—Specify the OSPF router priority. When two routers connect to a network, both attempt to become the designated router. The devices with the higher router priority becomes the designated router. If there is a tie, the router with the higher router ID becomes the designated router.

Valid values for this setting range from 0 to 255. The default value is 1. Entering 0 for this setting makes the router ineligible to become the designated router or backup designated router. This setting does not apply to interfaces that are configured as point-to-point non-broadcast interfaces.
Dynamic Routing

- MTU Ignore—OSPF checks whether neighbors are using the same MTU on a common interface. This check is performed when neighbors exchange DBD packets. If the receiving MTU in the DBD packet is higher than the IP MTU configured on the incoming interface, OSPF adjacency will not be established.

- Database Filter—Select this check box to filter outgoing LSA interface during synchronization and flooding. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. In a fully meshed topology, this can waste bandwidth and lead to excessive link and CPU usage. Selecting this check box prevents flooding OSPF LSA on the selected interface.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Edit OSPF Interface Advanced Properties

The Edit OSPF Interface Advanced Properties dialog box lets you change the values for the OSPF hello interval, retransmit interval, transmit delay, and dead interval. Typically, you only need to change these values from the defaults if you are experiencing OSPF problems on your network.

Fields

- Hello Interval—Specifies the interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.

- Retransmit Interval—Specifies the time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.

- Transmit Delay—Specifies the estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this box before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.

- Dead Interval—Specifies the interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this setting is four times the interval set by the Hello Interval box.

Modes

The following table shows the modes in which this feature is available:
Dynamic Routing

Static Neighbor

The Static Neighbor pane displays manually defined neighbors; it does not display discovered neighbors. You need to define a static neighbor for each point-to-point, non-broadcast interface. You also need to define a static route for each static neighbor in the Static Neighbor table.

Fields

- Static Neighbor—Displays information for the static neighbors defined for each OSPF process. Double-clicking a row in the table opens the Add/Edit OSPF Neighbor Entry dialog box.
  - OSPF Process—Displays the OSPF process associated with the static neighbor.
  - Neighbor—Displays the IP address of the static neighbor.
  - Interface—Displays the interface associated with the static neighbor.
- Add—Opens the Add/Edit OSPF Neighbor Entry dialog box. Use this button to define a new static neighbor.
- Edit—Opens the Add/Edit OSPF Neighbor Entry dialog box. Use this button to change the settings for a static neighbor.
- Delete—Removes the selected entry from the Static Neighbor table.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Add/Edit OSPF Neighbor Entry

The Add/Edit OSPF Neighbor Entry dialog box lets you define a new static neighbor or change information for an existing static neighbor.

You must define a static neighbor for each point-to-point, non-broadcast interface.

Restrictions

- You cannot define the same static neighbor for two different OSPF processes.
- You need to define a static route for each static neighbor (see Static Route).
Fields
- OSPF Process—Select the OSPF process associated with the static neighbor. If you are editing an existing static neighbor, you cannot change this value.
- Neighbor—Enter the IP address of the static neighbor.
- Interface—Select the interface associated with the static neighbor. If you are editing an existing static neighbor, you cannot change this value.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
</tbody>
</table>

Virtual Link
If you add an area to an OSPF network, and it is not possible to connect the area directly to the backbone area, you need to create a virtual link. A virtual link connects two OSPF devices that have a common area, called the transit area. One of the OSPF devices must be connected to the backbone area.

Fields
The Virtual Link table displays the following information. Doubling-clicking an entry in the table opens the Add/Edit Virtual Link dialog box for the selected entry.
- OSPF Process—Displays the OSPF process associated with the virtual link.
- Area ID—Displays the ID of the transit area.
- Peer Router ID—Displays the router ID of the virtual link neighbor.
- Authentication—Displays the type of authentication used by the virtual link:
  - None—No authentication is used.
  - Password—Clear text password authentication is used.
  - MD5—MD5 authentication is used.

You can perform the following actions on the entries in the Virtual Link table:
- Add—Opens the Add/Edit Virtual Link dialog box for adding a new entry to the Virtual Link table.
- Edit—Opens the Add/Edit Virtual Link dialog box for the selected entry.
- Delete—Removes the selected entry from the Virtual Link table.

Modes
The following table shows the modes in which this feature is available:
Dynamic Routing

Add/Edit Virtual Link

The Add/Edit Virtual Link dialog box lets you define new virtual links or change the properties of existing virtual links.

Fields

- OSPF Process—Select the OSPF process associated with the virtual link. If you are editing an existing virtual link, you cannot change this value.
- Area ID—Select the area shared by the neighbor OSPF devices. The selected area cannot be an NSSA or a Stub area. If you are editing an existing virtual link, you cannot change this value.
- Peer Router ID—Enter the router ID of the virtual link neighbor. If you are editing an existing virtual link, you cannot change this value.
- Advanced—Opens the Advanced OSPF Virtual Link Properties dialog box. You can configure the OSPF properties for the virtual link in this area. These properties include authentication and packet interval settings.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>—</td>
</tr>
</tbody>
</table>

Advanced OSPF Virtual Link Properties

The Advanced OSPF Virtual Link Properties dialog box lets you configure OSPF authentication and packet intervals.

Fields

- Authentication—Contains the OSPF authentication options.
  - None—Select this option to disable OSPF authentication.
  - Password—Select this option to use clear text password authentication. This is not recommended where security is a concern.
  - MD5—Select this option to use MD5 authentication (recommended).
- Authentication Password—Contains the settings for entering the password when password authentication is enabled.
  - Enter Password—Enter a text string of up to 8 characters.
- Re-enter Password—Reenter the password.

- MD5 IDs and Keys—Contains the settings for entering the MD5 keys and parameters when MD5 authentication is enabled. All devices on the interface using OSPF authentication must use the same MD5 key and ID.
  
  - Enter MD5 ID and Key—Contains the settings for entering MD5 key information.
    
    Key ID—Enter a numerical key identifier. Valid values range from 1 to 255.
    
    Key—An alphanumeric character string of up to 16 bytes.
  
  - Add—Adds the specified MD5 key to the MD5 and Key table.
  
  - Delete—Removes the selected MD5 key and ID from the MD5 and Key table.
  
  - MD5 ID and Key—Displays the configured MD5 keys and key IDs.
    
    Key ID—Displays the key ID for the selected key.
    
    Key—Displays the key for the selected key ID.

- Intervals—Contains the settings for modifying packet interval timing.
  
  - Hello Interval—Specifies the interval, in seconds, between hello packets sent on an interface. The smaller the hello interval, the faster topological changes are detected but the more traffic is sent on the interface. This value must be the same for all routers and access servers on a specific interface. Valid values range from 1 to 65535 seconds. The default value is 10 seconds.
  
  - Retransmit Interval—Specifies the time, in seconds, between LSA retransmissions for adjacencies belonging to the interface. When a router sends an LSA to its neighbor, it keeps the LSA until it receives the acknowledgement message. If the router receives no acknowledgement, it will resend the LSA. Be conservative when setting this value, or needless retransmission can result. The value should be larger for serial lines and virtual links. Valid values range from 1 to 65535 seconds. The default value is 5 seconds.
  
  - Transmit Delay—Specifies the estimated time, in seconds, required to send an LSA packet on the interface. LSAs in the update packet have their ages increased by the amount specified by this box before transmission. If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. The value assigned should take into account the transmission and propagation delays for the interface. This setting has more significance on very low-speed links. Valid values range from 1 to 65535 seconds. The default value is 1 second.
  
  - Dead Interval—Specifies the interval, in seconds, in which no hello packets are received, causing neighbors to declare a router down. Valid values range from 1 to 65535. The default value of this box is four times the interval set by the Hello Interval box.

**Modes**

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single Multiple</td>
</tr>
<tr>
<td></td>
<td>Context System</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
Filtering

The Filtering pane displays the ABR Type 3 LSA filters that have been configured for each OSPF process.

ABR Type 3 LSA filters allow only specified prefixes to be sent from one area to another area and restricts all other prefixes. This type of area filtering can be applied out of a specific OSPF area, into a specific OSPF area, or into and out of the same OSPF areas at the same time.

Benefits
OSPF ABR Type 3 LSA filtering improves your control of route distribution between OSPF areas.

Restrictions
Only Type 3 LSAs that originate from an ABR are filtered.

Fields
The Filtering table displays the following information. Double-clicking a table entry opens the Add/Edit Filtering Entry dialog box for the selected entry.

- OSPF Process—Displays the OSPF process associated with the filter entry.
- Area ID—Displays the ID of the area associated with the filter entry.
- Filtered Network—Displays the network address being filtered.
- Traffic Direction—Displays “Inbound” if the filter entry applies to LSAs coming in to an OSPF area or “Outbound” if it applies to LSAs coming out of an OSPF area.
- Sequence #—Displays the sequence number for the filter entry. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
- Action—Displays “Permit” if LSAs matching the filter are allowed or “Deny” if LSAs matching the filter are denied.
- Lower Range—Displays the minimum prefix length to be matched.
- Upper Range—Displays the maximum prefix length to be matched.

You can perform the following actions on entries in the Filtering table:

- Add—Opens the Add/Edit Filtering Entry dialog box for adding a new entry to the Filter table.
- Edit—Opens the Add/Edit Filtering Entry dialog box for modifying the selected filter.
- Delete—Removes the selected filter from the Filter table.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
<th>Multiple</th>
<th>Single</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
<td>Context</td>
<td>System</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Add/Edit Filtering Entry

The Add/Edit Filtering Entry dialog box lets you add new filters to the Filter table or to modify an existing filter. Some of the filter information cannot be changed when you edit an existing filter.

Fields
- **OSPF Process**—Select the OSPF process associated with the filter entry. If you are editing an existing filter entry, you cannot modify this setting.
- **Area ID**—Select the ID of the area associated with the filter entry. If you are editing an existing filter entry, you cannot modify this setting.
- **Filtered Network**—Enter the address and mask of the network being filtered using CIDR notation (a.b.c.d/m).
- **Traffic Direction**—Select the traffic direction being filtered. Select “Inbound” to filter LSAs coming into an OSPF area or “Outbound” to filter LSAs coming out of an OSPF area. If you are editing an existing filter entry, you cannot modify this setting.
- **Sequence #**—Enter a sequence number for the filter. Valid values range from 1 to 4294967294. When multiple filters apply to an LSA, the filter with the lowest sequence number is used.
- **Action**—Select “Permit” to allow the LSA traffic or “Deny” to block the LSA traffic.
- **Optional**—Contains the optional settings for the filter.
  - **Lower Range**—Specify the minimum prefix length to be matched. The value of this setting must be greater than the length of the network mask entered in the Filtered Network box and less than or equal to the value, if present, entered in the Upper Range box.
  - **Upper Range**—Enter the maximum prefix length to be matched. The value of this setting must be greater than or equal to the value, if present, entered in the Lower Range box, or, if the Lower Range box is left blank, greater than the length of the network mask length entered in the Filtered Network box.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Redistribution

The Redistribution pane displays the rules for redistributing routes from one routing domain to another.

Fields

The Redistribution table displays the following information. Double-clicking a table entry opens the Add/Edit OSPF Redistribution Entry dialog box for the selected entry.
- **OSPF Process**—Displays the OSPF process associated with the route redistribution entry.
- **Protocol**—Displays the source protocol the routes are being redistributed from. Valid entries are the following:
Dynamic Routing

- Static—The route is a static route.
- Connected—The route was established automatically by virtue of having IP enabled on the interface. These routes are redistributed as external to the AS.
- OSPF—The route is an OSPF route from another process.

- Match—Displays the conditions used for redistributing routes from one routing protocol to another.
- Subnets—Displays “Yes” if subnetted routes are redistributed. Does not display anything if only routes that are not subnetted are redistributed.
- Metric Value—Displays the metric that is used for the route. This column is blank for redistribution entries if the default metric is used.
- Metric Type—Displays “1” if the metric is a Type 1 external route, “2” if the metric is Type 2 external route.
- Tag Value—A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.
- Route Map—Displays the name of the route map to apply to the redistribution entry.

You can perform the following actions on the Redistribution table entries:
- Add—Opens the Add/Edit OSPF Redistribution Entry dialog box for adding a new redistribution entry.
- Edit—Opens the Add/Edit OSPF Redistribution Entry dialog box for modifying the selected redistribution entry.
- Delete—Removes the selected redistribution entry from the Redistribution table.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Add/Edit OSPF Redistribution Entry

The Add/Edit OSPF Redistribution Entry dialog box lets you add a new redistribution rule to or edit an existing redistribution rule in the Redistribution table. Some of the redistribution rule information cannot be changed when you are editing an existing redistribution rule.

Fields

- OSPF Process—Select the OSPF process associated with the route redistribution entry. If you are editing an existing redistribution rule, you cannot change this setting.
- Protocol—Select the source protocol the routes are being redistributed from. You can select one of the following options:
  - Static—The route is a static route.
  - Connected—The route was established automatically by virtue of having IP enabled on the interface. Connected routes are redistributed as external to the AS.
OSPF—The route is an OSPF route from another process.

OSPF—Select the OSPF process ID for the route being redistributed.

- **Match**—Displays the conditions used for redistributing routes from one routing protocol to another. The routes must match the selected condition to be redistributed. You can select one or more of the following match conditions:
  - *Internal*—The route is internal to a specific AS.
  - *External 1*—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes.
  - *External 2*—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes.
  - *NSSA External 1*—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.
  - *NSSA External 2*—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 NSSA routes.

- **Metric Value**—Specify the metric value for the routes being redistributed. Valid values range from 1 to 16777214. When redistributing from one OSPF process to another OSPF process on the same device, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.

- **Metric Type**—Select “1” if the metric is a Type 1 external route, “2” if the metric is a Type 2 external route.

- **Tag Value**—The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.

- **Use Subnets**—Select this check box to enable the redistribution of subnetted routes. Clear this check box to cause only routes that are not subnetted to be redistributed.

- **Route Map**—Enter the name of the route map to apply to the redistribution entry.

### Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>

### Summary Address

The Summary Address pane displays information about the summary addresses configured for each OSPF routing process.

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. Summary routes help reduce the size of the routing table.
Using summary routes for OSPF causes an OSPF ASBR to advertise one external route as an aggregate for all redistributed routes that are covered by the address. Only routes from other routing protocols that are being redistributed into OSPF can be summarized.

**Fields**
The following information appears in the Summary Address table. Double-clicking an entry in the table opens the Add/Edit OSPF Summary Address Entry dialog box for the selected entry.

- OSPF Process—Displays the OSPF process associated with the summary address.
- IP Address—Displays the IP address of the summary address.
- Netmask—Displays the network mask of the summary address.
- Advertise—Displays “Yes” if the summary routes are advertised. Displays “No” if the summary route is not advertised.
- Tag—Displays a 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs.

You can perform the following actions on the entries in the Summary Address table:

- Add—Opens the Add/Edit OSPF Summary Address Entry dialog box for adding new summary address entries.
- Edit—Opens the Add/Edit OSPF Summary Address Entry dialog box for editing the selected entry.
- Delete—Removes the selected summary address entry from the Summary Address table.

**Modes**
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

*Add/Edit OSPF Summary Address Entry*

The Add/Edit OSPF Summary Address Entry dialog box lets you add new entries to or modify existing entries in the Summary Address table. Some of the summary address information cannot be changed when editing an existing entry.

**Fields**

- OSPF Process—Select the OSPF process associated with the summary address. You cannot change this information when editing an existing entry.
- IP Address—Enter the IP address of the summary address. You cannot change this information when editing an existing entry.
- Netmask—Type the network mask for the summary address, or select the network mask from the list of common masks. You cannot change this information when editing an existing entry.
- Advertise—Select this check box to advertise the summary route. Clear this check box to suppress routes that fall under the summary address. By default this check box is selected.
• Tag—(Optional) The tag value is a 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between ASBRs. Valid values range from 0 to 4294967295.

Modes

The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

RIP

RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. When RIP is enabled on an interface, the interface exchanges RIP broadcasts with neighboring devices to dynamically learn about and advertise routes.

The FWSM support both RIP version 1 and RIP version 2. RIP version 1 does not send the subnet mask with the routing update. RIP version 2 sends the subnet mask with the routing update and supports variable-length subnet masks. Additionally, RIP version 2 supports neighbor authentication when routing updates are exchanged. This authentication ensures that the FWSM receives reliable routing information from a trusted source.

Note

You cannot enable RIP if you have OSPF processes running.

Limitations

RIP has the following limitations:

• The FWSM cannot pass RIP updates between interfaces.
• RIP Version 1 does not support variable-length subnet masks.
• RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable.
• RIP convergence is relatively slow compared to other routing protocols.

RIP Version 2 Notes

The following information applies to RIP Version 2 only:

• If using neighbor authentication, the authentication key and key ID must be the same on all neighbor devices that provide RIP version 2 updates to the interface.
• With RIP version 2, the FWSM transmits and receives default route updates using the multicast address 224.0.0.9. In passive mode, it receives route updates at that address.
• When RIP version 2 is configured on an interface, the multicast address 224.0.0.9 is registered on that interface. When a RIP version 2 configuration is removed from an interface, that multicast address is unregistered.
Dynamic Routing

Fields
- RIP—Displays RIP configuration information. Double-clicking a row in the RIP table opens the Add/Edit RIP Configuration dialog box, where you can change the parameters for the selected RIP configuration.
  - Interface—Displays the name of the interface on which RIP is enabled.
  - Action—Displays the action configured for RIP on the selected interface. This column displays “BCast default route” if the interface is configured to send RIP updates only, “Passive RIP” if the interface is configured to receive RIP updates only, or “BCast default route & Passive RIP” if the interface is configured to send and receive RIP updates.
  - Version—Displays which version of RIP is enabled on the interface.
  - Auth Type—Displays the type of authentication used for RIP version 2 authentication on the specified interface. This column contains “MD5” if MD5 authentication is enabled, “Text” if plaintext authentication is enabled, or is blank if authentication is not enabled.
  - Auth Key—Displays the authentication key used for RIP version 2 authentication on the specified interface. This column is blank if authentication is not enabled.
  - Key ID—Displays the identification number of the authentication key used in RIP version 2 authentication on the specified interface. This column is blank if authentication is not enabled.
- Add—Opens the Add/Edit RIP Configuration dialog box. Use this button to add a new RIP configuration to the FWSM.
- Edit—Opens the Add/Edit RIP Configuration dialog box. Use this button to change the parameters of the selected RIP configuration.
- Delete—Removes the selected RIP configuration. When you remove a RIP Version 2 configuration from an interface, the multicast address 224.0.0.9 is unregistered from that interface.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>—</td>
</tr>
</tbody>
</table>

Add/Edit RIP Configuration

The Add RIP Configuration dialog box lets you add a new RIP configuration to the FWSM. By adding a new RIP configuration, you enable RIP on the selected interface. The Edit RIP Configuration dialog box lets you make changes to an existing RIP configuration.

Fields
- Interface—Specifies the interface for the RIP configuration. You cannot specify two different RIP configurations for the same interface.
- Action options—Sets the behavior of RIP updates on the selected interface. You can select from the following actions:
  - Broadcast/multicast default route—Sets the selected interface to send RIP routing updates.
- Passive RIP—Sets the selected interface to listen for RIP routing broadcasts and to use that information to populate its routing table but not to send RIP routing updates.
- BCast Default route & Passive RIP—Sets the selected interface to send and receive RIP routing updates.

- Version options—Selects the version of RIP that is enabled on the selected interface. You can select from the following versions:
  - RIP Version 1—Selecting this option enables RIP Version 1 on the interface.
  - RIP Version 2—Selecting this option enables RIP Version 2 on the interface. Configuring RIP Version 2 on an interface registers the multicast address 224.0.0.9 on the interface.

- Version 2 Authentication—Contains the settings that let you enable and select the type of authentication used in RIP Version 2.
  - Enable Authentication—Select this check box to enable RIP neighbor authentication. Clear this check box to disable RIP neighbor authentication.
  - MD5—(Recommended) Uses the MD5 hash algorithm for authentication.
  - Clear text—Uses clear text for authentication.
  - Key—The shared key used for authentication. This key must be shared with all other devices sending updates to and receiving updates from the FWSM. This box accepts up to 16 characters.
  - Key ID—The identification number of the authentication key. This number must be shared with all other devices sending updates to and receiving updates from the FWSM. Valid values range from 1 to 255.

**Modes**
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple</td>
</tr>
<tr>
<td></td>
<td>Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

**Static Route**
The Static Route pane lets you create static routes to ensure that the FWSM correctly forwards network packets destined to the host or network. You can also use a static route to override any dynamic routes that are discovered for this host or network by specifying a static route with a lower metric than the discovered dynamic routes. You can define up to three equal cost routes to the same destination per interface (ECMP). ECMP is not supported across multiple interfaces. With ECMP, the traffic is not necessarily divided evenly between the routes; traffic is distributed among the specified gateways based on an algorithm that hashes the source and destination IP addresses.

To enter a default route, set the IP address and mask to 0.0.0.0, or the shortened form of 0. You can define up to three equal cost default route entries per device. You can also define a separate default route for tunneled traffic in addition to the standard default routes.

If an IP address from one FWSM interface is used as the gateway IP address, the FWSM will ARP the designated IP address in the packet instead of ARPing the gateway IP address.
Fields
The Static Route pane shows the Static Route table:

- **Interface**—Lists the interface name for which the route will apply.
- **IP Address**—Lists the destination network IP address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 IP address can be abbreviated as 0.
- **Netmask**—Lists the network mask for the destination address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.
- **Gateway IP**—Lists the IP address of the next hop router for this route.
- **Metric**—Lists the administrative distance of the route. The default is 1 if a metric is not specified.

Modes
The following table shows the modes in which this feature is available:

<table>
<thead>
<tr>
<th>Firewall Mode</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routed</td>
<td>Transparent</td>
</tr>
<tr>
<td></td>
<td>Single</td>
</tr>
<tr>
<td></td>
<td>Multiple Context</td>
</tr>
<tr>
<td></td>
<td>System</td>
</tr>
</tbody>
</table>

Add/Edit Static Route

The Add/Edit Static Route dialog box lets you add or edit a static route.

Fields

- **Interface Name**—Specifies the interface name for which the route will apply.
- **IP Address**—Specifies the destination network IP address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 IP address can be abbreviated as 0.
- **Mask**—Specifies the network mask for the destination address. Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.
- **Gateway IP**—Specifies the IP address of the next hop router for this route.
- **Metric**—Specifies the administrative distance of the route. The default is 1 if a metric is not specified.

Administrative distance is a parameter used to compare routes among different routing protocols. The default administrative distance for static routes is 1, giving it precedence over routes discovered by dynamic routing protocols but not directly connect routes. The default administrative distance for routes discovered by OSPF is 110. If a static route has the same administrative distance as a dynamically discovered route, the static routes take precedence. Connected routes always take precedence over static or dynamically discovered routes.

Modes
The following table shows the modes in which this feature is available:
Proxy ARPs

In rare circumstances, you might want to disable proxy ARP for global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking “Who is this IP address?” The device owning the IP address replies, “I own that IP address; here is my MAC address.”

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The FWSM uses proxy ARP when you configure NAT and specify a global address that is on the same network as the FWSM interface. The only way traffic can reach the hosts is if the FWSM uses proxy ARP to claim that the FWSM MAC address is assigned to destination global addresses.

Fields
- Interface—Lists the interface names.
- Proxy ARP Enabled—Shows whether proxy ARP is enabled or disabled for NAT global addresses, Yes or No.
- Enable—Enables proxy ARP for the selected interface. By default, proxy ARP is enabled for all interfaces.
- Disable—Disables proxy ARP for the selected interface.

Modes
The following table shows the modes in which this feature is available: