

## Configuring Multicast (NSM Procedure)

---

You can configure generic multicast properties for routing instances. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The routing protocol parameters control the information in the routing tables.

To configure generic multicast properties for routing instance in NSM:

1. In the navigation tree, select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. Click the **Configuration** tab.
4. In the configuration tree, expand **Routing Options**.
5. Select **Multicast**.
6. Add or modify the parameters as specified in Table 1.
7. Click one:
  - **OK**—To save the changes.
  - **Cancel**—To cancel the modifications.
  - **Apply**—To apply the routing option settings.



**NOTE:** After you make changes to a device configuration, you must push that updated device configuration to the physical security device for those changes to take effect. You can update multiple devices at one time. See the *Updating Devices* section in the *Network and Security Manager Administration Guide* for more information.

---

**Table 1: Configuring Multicast Fields**

Option	Function	Your Action
Comment	Specifies the comment for the multicast configuration.	Enter the comment.
Backup Pe Group	Enables you to configure a backup provider edge (PE) group for ingress PE device redundancy when point-to-multipoint (P2MP) label-switched paths (LSPs) are used for multicast distribution.	<ol style="list-style-type: none"><li>1. Expand the <b>Multicast</b> tree and select <b>Backup Pe Group</b>.</li><li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li><li>3. Configure the PE group name, local address, and backup address.</li></ol>

---

**Table 1: Configuring Multicast Fields** (continued)

Option	Function	Your Action
Flow Map	<p>Enables you to set up multicast flow maps to manage a subset of multicast forwarding table entries. For example, you can specify that certain forwarding cache entries be permanent or have a different timeout value than those of other multicast flows that are not associated with this flow map .</p>	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Flow Map</b>.</li> <li>2. Click the <b>New</b> button or select a flow map and click the <b>Edit</b> button.</li> <li>3. Configure the following to create and define a flow map: <ul style="list-style-type: none"> <li>■ Enter the flow map name and comment.</li> <li>■ <b>Bandwidth</b>—Specify the bandwidth property of the multicast flow map.</li> <li>■ <b>Forwarding Cache</b>—Specify the forwarding cache properties of entries defined by a flow map. You can specify a timeout of never to make the forwarding entries permanent, or you can specify a timeout from 1 through 720 minutes.</li> <li>■ <b>Policy</b>—Specify the flow map policies.</li> <li>■ <b>Redundant Sources</b>—Specify the addresses for use as backup sources for multicast flows defined by a flow map.</li> </ul> </li> </ol>
Forwarding Cache	<p>Enables you to configure multicast forwarding cache properties. These properties include threshold suppression and reuse limits, and timeout values.</p> <p>You can specify a value for the threshold to suppress new multicast forwarding cache entries and an optional reuse value for the threshold at which the device begins to create new multicast forwarding cache entries. If you configure both reuse and suppression values, configure a reuse value that is less than the suppression value. The suppression value is mandatory. If you do not specify the optional reuse value, then the number of multicast forwarding cache entries is limited to the suppression value. A new entry is created as soon as the number of multicast forwarding cache entries falls below the suppression value. You can also specify a timeout value for all multicast forwarding cache entries.</p>	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Forwarding Cache</b>.</li> <li>2. Configure the timeout and threshold values.</li> </ol>

**Table 1: Configuring Multicast Fields** (continued)

Option	Function	Your Action
Interface	Enables you to configure the interfaces for multicast properties on which you plan to manage the maximum bandwidth.	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Interface</b>.</li> <li>2. Configure the interface and the bandwidth.</li> </ol>
Rpf Check Policy	<p>Multicast reverse path forwarding (RPF) checks are used to prevent multicast routing loops. Routing loops are particularly debilitating in multicast applications because packets are replicated with each pass around the routing loop.</p> <p>You can apply policies for disabling reverse-path forwarding (RPF) checks on arriving multicast packets.</p>	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Rpf Check Policy</b>.</li> <li>2. Click the <b>New</b> button or select a policy and click the <b>Edit</b> button.</li> <li>3. Enter the RPF check policy name.</li> </ol>
Scope	Enables you to configure multicast scoping to limit multicast traffic by configuring it to an administratively defined topological region. Multicast scoping controls the propagation of multicast messages—both multicast group joins upstream toward a source and data forwarding downstream. Scoping can relieve stress on scarce resources, such as bandwidth, and improve privacy or scaling properties.	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Scope</b>.</li> <li>2. Configure the scope and the interface for the multicast.</li> </ol>
Scope Policy	Enables you to configure multicast scoping policy. A multicast scope policy contains a set of device interfaces on which you are configuring scoping and the scope's address range configured as a series of device filters.	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Scope Policy</b>.</li> <li>2. Specify the scope policy for the multicast group.</li> </ol>
Ssm Groups	Enables you to configure source-specific multicast (SSM) groups. SSM is a service model that identifies session traffic by both source and group address. Using SSM, a client can receive multicast traffic directly from the source. To deploy SSM successfully, you need an end-to-end multicast-enabled network and applications that use an Internet Group Management Protocol version 3 (IGMPv3).	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Ssm Groups</b>.</li> <li>2. Click the <b>New</b> button or select a group and click the <b>Edit</b> button.</li> <li>3. Specify the address range of the SSM group.</li> </ol>
Ssm Map	SSM mapping translate IGMPv1 or IGMPv2 membership reports to an IGMPv3 report allowing you to support an SSM network without requiring all hosts to support IGMPv3.	<ol style="list-style-type: none"> <li>1. Expand the <b>Multicast</b> tree and select <b>Ssm Map</b>.</li> <li>2. Click the <b>New</b> button or select an SSM map and click the <b>Edit</b> button.</li> <li>3. Specify the SSM policy for the SSM map and the source address.</li> </ol>

**Table 1: Configuring Multicast Fields** *(continued)*

Option	Function	Your Action
Traceoptions	Defines tracing options for the multicast group. You can also set up the file management and access control parameters .	<ol style="list-style-type: none"><li data-bbox="1032 384 1414 447">1. Expand the <b>Multicast</b> tree and select the <b>Traceoptions</b> tab.</li><li data-bbox="1032 447 1414 489">2. Set up the file and flag parameters.</li></ol>

---

Published: 2009-08-23