

## Configuring Bridge Domains Properties (NSM Procedure)

---

You can configure the bridge domain properties using the following options. See the following topics:

- Configuring a Bridge Domain (NSM Procedure) on page 1
- Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain (NSM Procedure) on page 2
- Configuring Forwarding Options (NSM Procedure) on page 3
- Configuring Logical Interfaces (NSM Procedure) on page 5
- Configuring Multicast Snooping Options (NSM Procedure) on page 6
- Configuring IGMP Snooping (NSM Procedure) on page 8
- Configuring VLAN ID (NSM Procedure) on page 13

### Configuring a Bridge Domain (NSM Procedure)

A bridge domain must include a set of logical interfaces that participate in Layer 2 learning and forwarding. You can optionally configure a VLAN identifier and a routing interface for the bridge domain to also support Layer 3 IP routing.

To configure bridge domain in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 1.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 1: Bridge Domain Configuration Details**

Task	Your Action
Configure bridge domain.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Domain.</li><li>2. Click <b>domain</b>.</li><li>3. In the <b>Name</b> box, enter the name of the bridge domain.</li><li>4. In the <b>Comment</b> box, enter the comment.</li><li>5. In the <b>Description</b> box, enter the text to describe the bridge domain.</li><li>6. From the <b>Domain Type</b> list, select the type of domain for a Layer 2 bridge domain.</li><li>7. Select the <b>No Local Switching</b> check box to enable or disable local switching within customer edge(ce)-facing interfaces.</li><li>8. In the <b>Routing Interface</b> box, enter the interface name.</li></ol>

## Configuring Layer 2 Learning and Forwarding Properties for a Bridge Domain (NSM Procedure)

When you configure a bridge domain, Layer 2 address learning is enabled by default. The bridge domain learns unicast media access control (MAC) addresses to avoid flooding the packets to all the ports in the bridge domain. Each bridge domain creates a source MAC entry in its source and destination MAC tables for each source MAC address learned from packets received on the ports that belong to the bridge domain.

To configure bridge options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 2.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 2: Bridge Options Configuration Details**

Task	Your Action
Configure bridge domain.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Domain.</li><li>2. Click <b>Bridge Options</b>.</li><li>3. Expand <b>Bridge Options</b>.</li><li>4. In the <b>Comment</b> box, enter the comment.</li><li>5. In the <b>Mac Table Aging Time</b> list, select the timeout interval for entries in the MAC table.</li><li>6. Select the <b>No Mac Learning</b> check box to disable MAC learning.</li><li>7. Select the <b>Mac Statistics</b> check box to enable MAC accounting either for a specific bridge domain, or for a set of bridge domains associated with a Layer 2 trunk port.</li><li>8. In the <b>Routing Interface</b> box, enter the interface name.</li></ol>

**Table 2: Bridge Options Configuration Details** (continued)

Task	Your Action
Specify the logical interfaces to include in the bridge domain.	<ol style="list-style-type: none"> <li>1. Click <b>Interface</b> next to Bridge Options.</li> <li>2. Click <b>Add new entry</b> next to Interface.</li> <li>3. In the <b>Name</b> box, enter the interface name.</li> <li>4. In the <b>Comment</b> box, enter the comment.</li> <li>5. From the <b>Remote Site Id</b> list, select the remote site ID.</li> <li>6. Select the <b>No Mac Learning</b> check box to disable MAC learning.</li> <li>7. In the <b>Description</b> box, enter the description.</li> <li>8. Click <b>Interface Mac Limit</b> next to interface.</li> <li>9. In the <b>Comment</b> box, enter the comment.</li> <li>10. From the <b>Limit</b> list, select the maximum number of MAC addresses learned from an interface. Range: 1 through 131,071 MAC addresses per interface</li> <li>11. From the <b>Packet Action</b> list, select the packet action for the packets for new source MAC addresses.</li> <li>12. Click <b>Static Mac</b> next to interface.</li> <li>13. Click <b>Add new entry</b> next to Static Mac.</li> <li>14. In the <b>Name</b> box, enter the interface name.</li> <li>15. In the <b>Comment</b> box, enter the comment.</li> <li>16. Click <b>Vlan Id</b> next to static-mac.</li> <li>17. Click <b>Add new entry</b> next to Vlan ID.</li> <li>18. From the <b>Name</b> list, select the VLAN identifier to associate with the static MAC address. Range: 1 to 4094</li> <li>19. In the <b>Comment</b> box, enter the comment.</li> </ol>
Configure a limit to the number of MAC addresses that can be learned from a bridge domain, virtual switch, or set of bridge domains.	<ol style="list-style-type: none"> <li>1. Click <b>Interface Mac Limit</b> next to Bridge Options.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the <b>Limit</b> list, select the maximum number of MAC addresses learned from an interface. Range: 1 through 131,071 MAC addresses per interface</li> </ol>
Modify the size of the MAC address table for the bridge domain, a set of bridge domains associated with a trunk port, or a virtual switch.	<ol style="list-style-type: none"> <li>1. Click <b>Mac Table Size</b> next to Bridge Options.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the <b>Limit</b> list, select the maximum number of addresses in the MAC address table. Range: 16 through 1,048,575 MAC addresses Default: 5120 MAC addresses</li> </ol>

### Configuring Forwarding Options (NSM Procedure)

To configure forwarding options in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.

4. Select **Domain**.
5. Add or modify settings as specified in Table 3.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 3: Forwarding Options Configuration Details**

<b>Task</b>	<b>Your Action</b>
Configuring the extended DHCP relay agent.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Domain.</li> <li>2. Click <b>Forwarding Options</b>.</li> <li>3. Expand <b>Dhcp Relay</b>.</li> <li>4. Select <b>Authentication</b>.</li> <li>5. For Configuring Authentication Support for the DHCP Relay Agent, see Configuring Authentication Support for the DHCP Relay Agent (NSM Procedure).</li> </ol>
Configuring Group.	<ol style="list-style-type: none"> <li>1. Click <b>Group</b> next to Dhcp Relay.</li> <li>2. For configuring group, see Configuring Group (NSM Procedure).</li> </ol>
Overriding the default configuration settings for the extended DHCP relay agent.	<ol style="list-style-type: none"> <li>1. Click <b>Overrides</b> next to Dhcp Relay.</li> <li>2. For overriding the default configuration settings for the extended DHCP relay agent, see Overriding the Default Configuration Settings for the Extended DHCP Relay Agent (NSM Procedure).</li> </ol>
Configuring relay option 60 information for forwarding client traffic to specific DHCP servers.	<ol style="list-style-type: none"> <li>1. Click <b>Relay option 60</b> next to Dhcp Relay.</li> <li>2. For configuring relay option 60 information for forwarding client traffic to specific DHCP servers, see Configuring Relay Option 60 Information for Forwarding Client Traffic to Specific DHCP Servers (NSM Procedure).</li> </ol>
Configuring relay option 82 for a DHCP server.	<ol style="list-style-type: none"> <li>1. Click <b>Relay option 82</b> next to Dhcp Relay.</li> <li>2. For configuring relay option 82 for a DHCP server, see Configuring Relay Option 82 for a DHCP Server (NSM Procedure).</li> </ol>
Specifying the name of a group of DHCP server addresses for use by the extended DHCP relay agent.	<ol style="list-style-type: none"> <li>1. Click <b>Server Group</b> next to Dhcp Relay.</li> <li>2. For specifying the name of a group of DHCP server addresses for use by the extended DHCP relay agent, see Specifying the Name of a Group of DHCP Server Addresses for Use by the Extended DHCP Relay Agent (NSM Procedure)</li> </ol>
Configuring tracing operations for extended DHCP relay agent processes.	<ol style="list-style-type: none"> <li>1. Click <b>Traceoptions</b> next to Dhcp Relay.</li> <li>2. For configuring tracing operations for extended DHCP relay agent processes see Configuring Operations for Extended DHCP Relay Agent Processes (NSM Procedure)</li> </ol>
Apply a forwarding table filter at the ingress of a forwarding table.	<ol style="list-style-type: none"> <li>1. Click <b>Filter</b> next to Forwarding Options.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the <b>Input</b> list, select the name of the applied filter.</li> </ol>

**Table 3: Forwarding Options Configuration Details** (continued)

Task	Your Action
Apply a forwarding table filter to a flood table.	<ol style="list-style-type: none"><li>1. Click <b>Flood</b> next to Forwarding Options.</li><li>2. In the <b>Comment</b> box, enter the comment.</li><li>3. From the <b>Input</b> list, select the name of the forwarding table filter.</li></ol>

### Configuring Logical Interfaces (NSM Procedure)

You can specify the logical interfaces to include in the bridge domain, VPLS instance, or virtual switch.

To configure logical interfaces in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 4.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 4: Logical Interface Configuration Details**

Task	Your Action
Configure logical interface to include in the bridge domain, VPLS instance, or virtual switch.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Domain.</li><li>2. Click <b>Interface</b>.</li><li>3. Click <b>Add new entry</b> next to Interface.</li><li>4. From the <b>Name</b> list, select the name of a logical interface.</li><li>5. In the <b>Comment</b> box, enter the comment.</li></ol>

## **Configuring Multicast Snooping Options (NSM Procedure)**

Multicast snooping is a way for a Layer 2 device to snoop at the Layer 3 packet content to determine which actions are to be taken to process or forward a frame. There are specific forms of snooping, such as IGMP snooping or PIM snooping. In all cases, snooping involves a device configured to function at Layer 2 having access to Layer 3 (packet) information. Snooping makes multicasting more efficient in these devices.

To configure Multicast Snooping:

1. In the navigation tree select **Device Manager > Devices**.
2. In the **Devices** list, double-click the device to select it.
3. In the **Configuration** tab, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify the settings as specified in Table 5.
6. Click one:
  - OK—saves the changes
  - Cancel—cancels the modifications

**Table 5: Multicast Snooping Options Configuration Details**

<b>Task</b>	<b>Your Action</b>
Establish multicast snooping option values.	<ol style="list-style-type: none"> <li>1. Click <b>Add new entry</b> next to Domain.</li> <li>2. Click <b>Multicast Snooping Options</b> next to domain.</li> </ol>
Establish a list of flood group addresses for multicast snooping.	<ol style="list-style-type: none"> <li>1. Click <b>Flood Groups</b> next to Multicast Snooping Options.</li> <li>2. Click <b>Add new entry</b> next to Flood Groups.</li> <li>3. In the dialog box, enter the IP addresses.</li> </ol>
Configure multicast forwarding cache properties.	<ol style="list-style-type: none"> <li>1. Click <b>Forwarding Cache</b> next to Multicast Snooping Options.</li> <li>2. In the <b>Comment</b> box, enter the comments.</li> <li>3. Expand <b>Forwarding Cache</b>.</li> <li>4. Click <b>Threshold</b> next to Forwarding Cache.</li> <li>5. In the <b>Comment</b> box, enter the comments.</li> <li>6. From the <b>Suppress</b> list, select the threshold value for a forwarding cache.  Range: 1 through 200,000</li> <li>7. From the <b>Reuse</b> list, select the reuse value for the threshold. The reuse value must be less than the suppression threshold value.  Range: 1 through 200,000</li> </ol>
Establish the graceful restart duration for multicast snooping.	<ol style="list-style-type: none"> <li>1. Click <b>Graceful Restart</b> next to Multicast Snooping Options.</li> <li>2. In the <b>Comment</b> box, enter the comments.</li> <li>3. From the <b>Restart Duration</b> list, select the duration for graceful restart. Range: 0 to 300 seconds  Default : 180 seconds</li> </ol>
Establish multicast snooping option values.	<ol style="list-style-type: none"> <li>1. Click <b>Option</b> next to Multicast Snooping Options.</li> <li>2. In the <b>Comment</b> box, enter the comments.</li> <li>3. Expand <b>Options</b>.</li> <li>4. Click <b>Syslog</b> next to Options.</li> <li>5. In the <b>Comment</b> box, enter the comments.</li> <li>6. From the <b>Upto</b> list, select the level up to which severity the messages are to be syslogged.</li> <li>7. From the <b>Mark</b> list, select the time interval in seconds to mark the trace file.  Range : -2147483647 seconds to 2147483647 Seconds  Default : 0</li> <li>8. Expand <b>Syslog</b>.</li> <li>9. Click <b>Level</b> next to Syslog.</li> <li>10. Select the Level of severity to be logged.</li> </ol>

**Table 5: Multicast Snooping Options Configuration Details** (continued)

Task	Your Action
Configure tracing options.	<ol style="list-style-type: none"><li>1. Click <b>Traceoptions</b> next to Multicast Snooping Options.</li><li>2. In the <b>Comment</b> box, enter the comments.</li><li>3. Expand <b>Traceoptions</b>.</li><li>4. Click <b>File</b> next to Trace Options.</li><li>5. In the <b>Comment</b> box, enter the comments.</li><li>6. In the <b>Filename</b> box, enter the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks.</li><li>7. In the <b>Size</b> box, enter the maximum size of each trace file in bytes.  Range : 10240 to 4294967295 bytes</li><li>8. From the <b>Files</b> list, select the maximum number of files.</li><li>9. Select one of the following:<ul style="list-style-type: none"><li>■ <b>world-readable</b>—To enable log file access to all users.</li><li>■ <b>no-world-readable</b>—To prevent all users from reading the log file.</li></ul></li><li>10. Click <b>Flag</b> next to Trace Options.</li><li>11. Click Add new entry next to flag.</li><li>12. From the <b>Name</b> list, select a tracing operation to perform.</li><li>13. In the <b>Comment</b> box, enter the comments.</li></ol>

### Configuring IGMP Snooping (NSM Procedure)

The Internet Group Management Protocol (IGMP) manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members. IGMP is also used as the transport for several related multicast protocols (for example, Distance Vector Multicast Routing Protocol [DVMRP] and Protocol Independent Multicast version 1 [PIMv1]). IGMP is an integral part of IP and must be enabled on all routers and hosts that need to receive IP multicast traffic.

To configure IGMP snooping in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 6.
6. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.

**Table 6: Igmp Snooping Configuration Details**

Task	Your Action
Configure IGMP snooping.	<ol style="list-style-type: none"><li>1. Click <b>Add new entry</b> next to Domain.</li><li>2. Click and expand <b>Protocol</b>.</li><li>3. Select <b>Igmp Snooping</b>.</li><li>4. In the <b>Comment</b> box, enter the comment.</li><li>5. From the <b>Query Interval</b> list, select the time interval the querier router sends general host-query messages. Range: 1 through 1024 Default: 125 seconds</li><li>6. In the <b>Query Response Interval</b> box, enter the time interval the querier router waits to receive a response to a host-query message from a host. This interval must be less than the interval between general host-query messages. Range: 1 through 1024 Default: 10 seconds</li><li>7. In the <b>Query Last Member Interval</b> box, enter the time interval the querier router sends group-specific query messages. Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024 Default: 1 second</li><li>8. From the <b>Robust Count</b> list, select the robustness variable used to calculate several IGMP message intervals. Range: 2 through 10 Default: 2</li><li>9. Select the <b>Immediate Leave</b> check box to enable immediate leave. When this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives a leave group membership message from a host associated with the interface, the router immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group. When this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives a report with the type BLOCK_OLD_SOURCES, the router suppresses the sending of group-and-source queries but relies on the host-tracking mechanism supported by the JUNOS Software to determine whether or not it removes a particular source group membership from the interface.</li></ol> <p><b>NOTE:</b> When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that properly remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.</p>

**Table 6: Igmp Snooping Configuration Details** (continued)

Task	Your Action
Enable IGMP on an interface and configure interface-specific properties.	<ol style="list-style-type: none"><li>1. Click <b>Interface</b> next to Igmp Snooping.</li><li>2. Click <b>Add new entry</b> next to Interface.</li><li>3. In the <b>Name</b> box, enter the interface name.</li><li>4. In the <b>Comment</b> box, enter the comment.</li><li>5. Select the <b>Multicast Router Interface</b> check box if the interface is a multicast router interface.</li><li>6. Select the <b>Immediate Leave</b> check box to enable immediate leave on a router.</li><li>7. Select the <b>Host Only Interface</b> check box if the interface is to be configured as a host-facing interface.</li><li>8. From the <b>Group Limit</b> list, select the limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the interface.</li><li>9. Click <b>Static</b> next to interface.</li><li>10. In the <b>Comment</b> box, enter the comment.</li><li>11. Expand <b>Static</b>.</li><li>12. Click <b>Group</b> next to Static.</li><li>13. Click <b>Add new entry</b> next to Group.</li><li>14. In the <b>Name</b> box, enter the IGMP multicast group address.</li><li>15. In the <b>Comment</b> box, enter the comment.</li><li>16. Click <b>Source</b> next to group.</li><li>17. Click <b>Add new entry</b> next to Source.</li><li>18. In the <b>Name</b> box, enter the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.</li><li>19. In the <b>Comment</b> box, enter the comment.</li></ol>
Configuring IGMP snooping proxy mode.	<ol style="list-style-type: none"><li>1. Click <b>Proxy</b> next to Igmp Snooping.</li><li>2. In the <b>Comment</b> box, enter the comment.</li><li>3. In the <b>Source Address</b> box, enter the IP address to use as the source for IGMP snooping reports in proxy mode.</li></ol>

**Table 6: Igmp Snooping Configuration Details** (continued)

<b>Task</b>	<b>Your Action</b>
Configure IGMP tracing options.	<ol style="list-style-type: none"><li>1. In the <b>Comment</b> box, enter the comment for the traceoptions.</li><li>2. Click <b>File</b> next to Traceoptions.</li><li>3. In the <b>Comment</b> box, enter the comment for the filename.</li><li>4. In the <b>Filename</b> box, enter the name of the file to receive the output of the tracing operation.</li><li>5. In the <b>Size</b> box, enter the maximum trace file size in bytes. Range : 10240 to 4294967295</li><li>6. From the <b>Files</b> list, select the maximum number of trace files. Range: 2 through 1000 files Default: 2 files</li><li>7. Select one of the following:<ul style="list-style-type: none"><li>■ <b>no-world-readable</b>—To restrict the file access to owner.</li><li>■ <b>world-readable</b>—To enable unrestricted access.</li></ul></li><li>8. Click <b>Flag</b> next to Traceoptions.</li><li>9. Click <b>Add new entry</b> next to Flag.</li><li>10. From the <b>Name</b> list, select the flag to perform the trace operation.</li><li>11. In the <b>Comment</b> box, enter the comment for the flag.</li><li>12. Select the corresponding flag modifier check box.</li></ol>

**Table 6: Igmp Snooping Configuration Details** (continued)

Task	Your Action
Configure IGMP snooping parameters for a particular VLAN.	<ol style="list-style-type: none"> <li>1. From the <b>Name</b> list, select the VLAN ID.</li> <li>2. In the <b>Comment</b> box, enter the comment.</li> <li>3. From the <b>Query Interval</b> list, select the time interval the querier router sends general host-query messages. Range: 1 through 1024 Default: 125 seconds</li> <li>4. In the <b>Query Response Interval</b> box, enter the time interval the querier router waits to receive a response to a host-query message from a host. This interval must be less than the interval between general host-query messages. Range: 1 through 1024 Default: 10 seconds</li> <li>5. In the <b>Query Last Member Interval</b> box, enter the time interval querier router sends group-specific query messages. Range: 0.1 through 0.9, then in 1-second intervals 1 through 1024 Default: 1 second</li> <li>6. From the <b>Robust Count</b> list, select the robustness variable used to calculate several IGMP message intervals. Range: 2 through 10 Default: 2</li> <li>7. Select the <b>Immediate Leave</b> check box to enable immediate leave. When this statement is enabled on a router running IGMP version 2 (IGMPv2), after the router receives a leave group membership message from a host associated with the interface, the router immediately removes the group membership from the interface and suppresses the sending of any group-specific queries for the multicast group. When this statement is enabled on a router running IGMP version 3 (IGMPv3), after the router receives a report with the type BLOCK_OLD_SOURCES, the router suppresses the sending of group-and-source queries but relies on the host-tracking mechanism supported by the JUNOS Software to determine whether or not it removes a particular source group membership from the interface.</li> </ol>
<p><b>NOTE:</b> When issuing this command on IGMPv2 interfaces, ensure that the IGMP interface has only one IGMP host connected. If more than one IGMPv2 host is connected to a LAN through the same interface, and one host sends a done message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that properly remain in the multicast group until they send join requests in response to the next general multicast listener query from the router.</p>	

**Table 6: Igmp Snooping Configuration Details** (continued)

Task	Your Action
Configure interface specific properties.	<ol style="list-style-type: none"> <li>1. Click <b>Interface</b> next to vlan.</li> <li>2. Click <b>Add new entry</b> next to Interface.</li> <li>3. In the <b>Name</b> box, enter the interface name.</li> <li>4. In the <b>Comment</b> box, enter the comment.</li> <li>5. Select the <b>Multicast Router Interface</b> check box if the interface is a multicast router interface.</li> <li>6. Select the <b>Immediate Leave</b> check box to enable immediate group leave on a router.</li> <li>7. Select the <b>Host Only Interface</b> check box if the interface is to be configured as a host-facing interface.</li> <li>8. From the <b>Group Limit</b> list, select the limit for the number of multicast groups (or [S,G] channels in IGMPv3) allowed on an interface. After this limit is reached, new reports will be ignored and all related flows are not flooded on the interface.</li> <li>9. Click <b>Static</b> next to interface.</li> <li>10. In the <b>Comment</b> box, enter the comment.</li> <li>11. Expand <b>Static</b>.</li> <li>12. Click <b>Group</b> next to Static.</li> <li>13. Click <b>Add new entry</b> next to Group.</li> <li>14. In the <b>Name</b> box, enter the IGMP multicast group address.</li> <li>15. In the <b>Comment</b> box, enter the comment.</li> <li>16. Click <b>Source</b> next to group.</li> <li>17. Click <b>Add new entry</b> next to Source.</li> <li>18. In the <b>Name</b> box, enter the IP version 4 (IPv4) unicast source address for the multicast group being statically configured on an interface.</li> <li>19. In the <b>Comment</b> box, enter the comment.</li> <li>20. Click <b>Proxy</b> next to vlan.</li> <li>21. In the <b>Comment</b> box, enter the comment.</li> <li>22. In the <b>Source Address</b> box, enter the IP address to use as the source for IGMP snooping reports in proxy mode.</li> </ol>

### Configuring VLAN ID (NSM Procedure)

You can configure VLAN IDs using the Vlan Id option.

To configure VLAN ID in NSM:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the device to select it.
3. Click the **Configuration** tab. In the configuration tree, expand **Bridge Domains**.
4. Select **Domain**.
5. Add or modify settings as specified in Table 7.
6. Click one:
  - OK—Saves the changes.
  - Cancel—Cancels the modifications.

**Table 7: VLAN ID Configuration Details**

Task	Your Action
Configure a VLAN ID	<ol style="list-style-type: none"><li data-bbox="467 373 883 394">1. Click <b>Add new entry</b> next to Domain.</li><li data-bbox="467 405 646 426">2. Click <b>Vlan Id</b>.</li><li data-bbox="467 436 883 457">3. Select <b>vlan-id</b> and enter the VLAN ID.</li><li data-bbox="467 468 1390 527">4. Select <b>vlan tag</b> to tag the VLAN interface so that it can be compared with the normalizing VLAN identifier.</li><li data-bbox="467 537 927 558">5. In the <b>Comment</b> box, enter the comment.</li><li data-bbox="467 569 935 590">6. In the <b>Inner</b> box, enter the VLAN identifier.</li><li data-bbox="467 600 935 621">7. In the <b>Outer</b> box, enter the VLAN identifier.</li></ol>

---

Published: 2009-08-23