

Configuration of Unregistered Multicast on 200/300 Series Managed Switches

Objective

Internet Group Management Protocol (IGMP) is a protocol designed for multicast purposes. With IGMP, you can establish group memberships between different users within a network. IGMP is mainly used for multimedia streaming, such as video-chat, between different users (one-to-many users or many-to-many users) in a network. Snooping, on the other hand, is the term used when a third party in a communication listens or observes the current connection data traffic. Therefore, IGMP Snooping is a process that listens specifically to multicast traffic. By default, the 300 Series Managed Switches forwards all multicast frames to all the ports that are assigned to a specific VLAN. This behavior is insecure and the multicast frames could end up in the wrong place. You can enable IGMP Snooping to forward multicast traffic to only already registered multicast clients on specific ports of the switch. This way, the multicast frames are only forwarded to a specific multicast client within a VLAN instead of to all the users in that VLAN.

The objective of this document is to show you how to configure IGMP Snooping on 200/300 Series Managed Switches.

Applicable Devices

- SF/SG 200 and SF/SG 300 Series Managed Switches

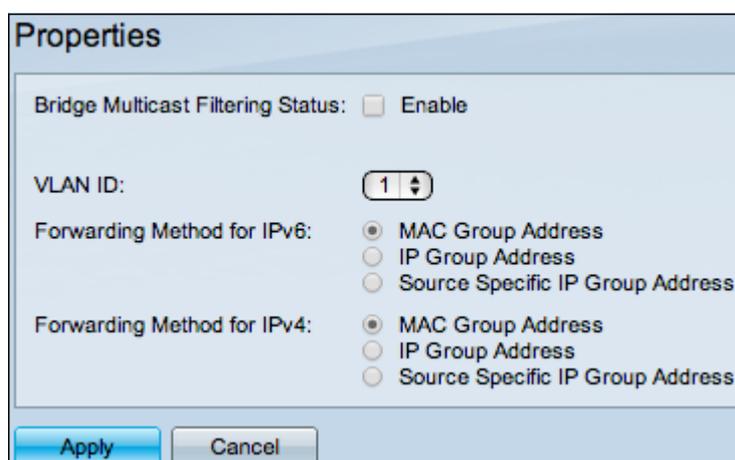
Software Version

- 1.3.0.62

Enable Bridge Multicast

In order for IGMP snooping to work, bridge multicast must be enabled.

Step 1. Log in to the web configuration utility and choose **Multicast > Properties**. The *Properties* page opens:



The screenshot shows a web configuration utility window titled "Properties". It contains the following settings:

- Bridge Multicast Filtering Status:** Enable
- VLAN ID:** 1 (with up/down arrows)
- Forwarding Method for IPv6:**
 - MAC Group Address
 - IP Group Address
 - Source Specific IP Group Address
- Forwarding Method for IPv4:**
 - MAC Group Address
 - IP Group Address
 - Source Specific IP Group Address

At the bottom of the window are two buttons: "Apply" and "Cancel".

Step 2. In the Bridge Multicast Filtering Status field, check the **Enable** check box.



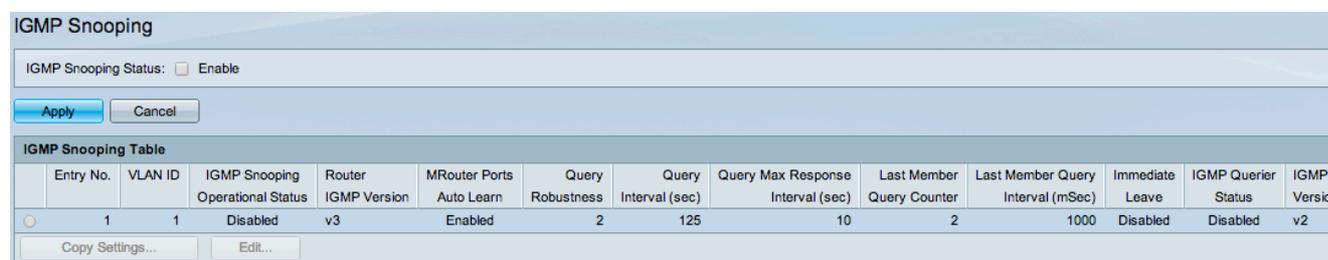
Step 3. Click **Apply**.

Note: For information about how to configure multicast properties, refer to the article [Multicast Properties Configuration on 300 Series Managed Switches](#).

Configure IGMP Snooping on a VLAN

Configure IGMP Snooping on a Single VLAN

Step 1. Log in to the web configuration utility and choose **Multicast > IGMP Snooping**. The *IGMP Snooping* page opens:



Step 2. Check **Enable** to start IGMP Snooping globally.



Step 3. Click **Apply**.

Step 4. Click the radio button that corresponds to the VLAN on which you would like to apply IGMP Snooping.

Step 5. Click **Edit**.



The *Edit IGMP Snooping* window appears.

| | | | |
|---|--|--|-----------|
| VLAN ID: | <input type="text" value="1"/> | | |
| IGMP Snooping Status: | <input type="checkbox"/> Enable | Operational IGMP Snooping Status: | Disabled |
| MRouter Ports Auto Learn: | <input checked="" type="checkbox"/> Enable | | |
| Query Robustness: | <input type="text" value="5"/> (Range: 1 - 7, Default: 2) | Operational Query Robustness: | 2 |
| Query Interval: | <input type="text" value="250"/> sec (Range: 30 - 18000, Default: 125) | Operational Query Interval: | 125 (sec) |
| Query Max Response Interval: | <input type="text" value="15"/> sec (Range: 5 - 20, Default: 10) | Operational Query Max Response Interval: | 10 (sec) |
| Last Member Query Counter: | <input checked="" type="radio"/> Use Default <input type="radio"/> User Defined <input type="text" value=""/> (Range: 1 - 7, Default: 5 (Query Robustness)) | Operational Last Member Query Counter: | 2 |
| Last Member Query Interval: | <input type="text" value="2000"/> mS (Range: 100 - 25500, Default: 1000) | Operational Last Member Query Interval: | 1000 (mS) |
| Immediate leave: | <input type="checkbox"/> Enable | | |
| IGMP Querier Status: | <input type="checkbox"/> Enable | Operational Querier Source IP Address: | |
| Administrative Querier Source IP Address: | <input checked="" type="radio"/> Auto <input type="radio"/> User Defined <input type="text" value="192.168.1.254"/> | | |
| IGMP Querier Version: | <input checked="" type="radio"/> IGMPV2 <input type="radio"/> IGMPV3 | | |

Apply Close

Step 6. In the *IGMP Snooping Status* field, check the **Enable** check box. This option monitors the traffic to determine which hosts requested multicast traffic.

| | |
|-----------------------|--|
| VLAN ID: | <input type="text" value="1"/> |
| IGMP Snooping Status: | <input checked="" type="checkbox"/> Enable |

Step 7. In the *MRouter Ports Auto Learn* field, check the **Enable** check box. This option automatically learns to which the specific ports the MRouter is connected. An MRouter is a router designed to properly route multicast packets.

| | |
|---------------------------|--|
| MRouter Ports Auto Learn: | <input checked="" type="checkbox"/> Enable |
|---------------------------|--|

Step 8. In the *Query Robustness* field, enter the number queries the switch performs to connect to a host. If no response is received, the switch deletes the host information.

| | | | |
|------------------------------|--|--|-----------|
| Query Robustness: | <input type="text" value="5"/> (Range: 1 - 7, Default: 2) | Operational Query Robustness: | 2 |
| Query Interval: | <input type="text" value="250"/> sec (Range: 30 - 18000, Default: 125) | Operational Query Interval: | 125 (sec) |
| Query Max Response Interval: | <input type="text" value="15"/> sec (Range: 5 - 20, Default: 10) | Operational Query Max Response Interval: | 10 (sec) |
| Last Member Query Counter: | <input checked="" type="radio"/> Use Default <input type="radio"/> User Defined <input type="text" value=""/> (Range: 1 - 7, Default: 5 (Query Robustness)) | Operational Last Member Query Counter: | 2 |
| Last Member Query Interval: | <input type="text" value="2000"/> mS (Range: 100 - 25500, Default: 1000) | Operational Last Member Query Interval: | 1000 (mS) |

Step 9. In the *Query Interval* field, enter the time interval between sent query messages.

Step 10. In the *Query Max Response Interval* field, enter the time in seconds a host is given to respond a query.

Step 11. In the *Last Member Query Counter* field, click one of the following:

- Use Default — This option uses the default number of IGMP Group-Specific queries to be sent before the switch assumes there are not any more members in the group.
- User Defined — This option lets you enter a specific number of IGMP Group-Specific queries to be sent before the switch assumes there are not any more members in the group.

Step 12. In the *Last Member Query Interval* field, enter the Maximum Response Delay used in case the switch cannot read the Max Response Interval value from group-specific queries.

Step 13. In the *Immediate Leave* field, check the **Enable** check box to block a multicast stream faster that was sent to a member port in the case that an IGMP Group Leave message is received.

| | |
|------------------|--|
| Immediate leave: | <input checked="" type="checkbox"/> Enable |
|------------------|--|

Step 14. In the *IGMP Querier Status* field, check the **Enable** check box to enable IGMP Querier.

| | |
|---|---|
| IGMP Querier Status: | <input checked="" type="checkbox"/> Enable |
| Administrative Querier Source IP Address: | <input checked="" type="radio"/> Auto <input type="radio"/> User Defined 192.168.1.254 |
| IGMP Querier Version: | <input checked="" type="radio"/> IGMPV2 <input type="radio"/> IGMPV3 |

Step 15. In the *Administrative Querier Source IP Address* field, click one of the following radio buttons:

- Auto — This option chooses the management IP address.
- User Defined — This option lets you choose an IP address of your choice from the drop-down list.

Step 16. In the *IGMP Querier Version* field, click **IGMPV3** if in this VLAN there are switches or multicast routers that perform source-specific IP multicast forwarding; otherwise, click **IGMPV2**.

| | |
|-----------------------|---|
| IGMP Querier Version: | <input type="radio"/> IGMPV2 <input checked="" type="radio"/> IGMPV3 |
|-----------------------|---|

Note: The information on the right side of the *Edit IGMP Snooping* window displays the current IGMP configuration.

| | |
|--|-----------|
| Operational IGMP Snooping Status: | Disabled |
| Operational Query Robustness: | 2 |
| Operational Query Interval: | 125 (sec) |
| Operational Query Max Response Interval: | 10 (sec) |
| Operational Last Member Query Counter: | 2 |
| Operational Last Member Query Interval: | 1000 (mS) |
| Operational Querier Source IP Address: | |

The following information is displayed:

- Operational IGMP Status — Current IGMP status of the chosen VLAN.

- Operational Query Robustness — Current Query Robustness value of the chosen VLAN.
- Operational Query Interval — Current Query Interval value of the chosen VLAN.
- Operational Query Max Response Interval — Current Query Max Response Interval value of the chosen VLAN.
- Operational Last Member Response Interval — Last Member Response Interval value of the chosen VLAN.
- Operational Last Member Query Counter — Last Member Query Counter value of the chosen VLAN.
- Operational Last Member Query Interval — Last Member Query Interval value of the chosen VLAN.
- Operational Querier Source IP Address — Current Querier Source IP Address of the chosen VLAN.

Step 17. Click **Apply**.

Configure IGMP Snooping on Multiple VLANs

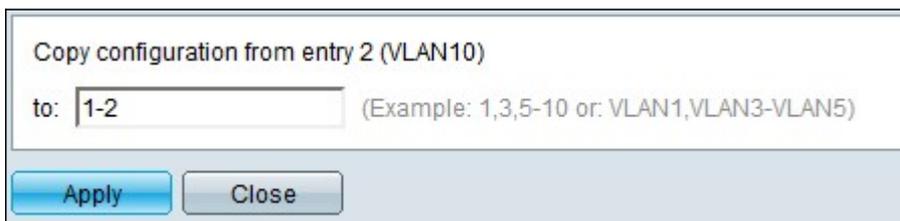
This section explains how to apply the IGMP snooping configuration of a specific VLAN, in multiple VLANs.

Step 1. Log in to the web configuration utility and choose **Multicast > IGMP Snooping**. The *IGMP Snooping* page opens:



Step 2. Click the VLAN with the IGMP snooping configuration that you want to apply on other VLANs.

Step 3. Click **Copy Settings**. The *Copy Settings* window appears.



Step 4. In the field provided, enter the VLANs to which you want to apply the IGMP snooping configuration of the previously chosen VLAN. You can enter each VLAN or a range of VLANs based on their entry number from the IGMP Snooping Table, such as 1, 2 or 1-2, or with their VLAN ID, such as VLAN1, VLAN2 or VLAN1-VLAN2.

Step 5. Click **Apply**.