Multicast

This chapter contains the following sections:

Multicast Properties

Multicast forwarding enables one-to-many information dissemination. Multicast applications are useful for dissemination of information to multiple clients, where clients do not require reception of the entire content. A typical application is a cable-TV-like service, where clients can join a channel in the middle of a transmission, and leave before it ends.

The data is sent only to relevant ports. Forwarding the data only to the relevant ports conserves bandwidth and host resources on links. By default, all Multicast frames are flooded to all ports of the VLAN. It is possible to selectively forward only to relevant ports and filter (drop) the Multicast on the rest of the ports by enabling the Bridge Multicast filtering status in this section.

Multicast addresses have the following properties

- Each IPv4 Multicast address is in the address range 224.0.0.0 to239.255.255.255.
- The IPv6 Multicast address isFF00:/8.
- To map an IP Multicast group address to an Layer 2 Multicast address:

For IPv4, this is mapped by taking the 23 low-order bits from the IPv4 address, and adding them to the 01:00:5e prefix. By standard, the upper nine bits of the IP address are ignored, and any IP addresses that only differ in the value of these upper bits are mapped to the same Layer 2 address, since the lower 23 bits that are used are identical. For example, 234.129.2.3 is mapped to a MAC Multicast group address 01:00:5e:01:02:03. Up to 32 IP Multicast group addresses can be mapped to the same Layer 2 address.

For IPv6, this is mapped by taking the 32 low-order bits of the Multicast address, and adding the prefix of 33:33. For example, the IPv6 Multicast address FF00::1122:3344 is mapped to Layer 2 Multicast 33:33:11:22:33:44.

To configure Multicast properties, follow these steps:

Step 1 Click **Multicast** > **Properties**.

Step 2 Enter the parameters.

IGMP Snooping	Enable or disable IGMP Snooping globally on the switch (enabled by default). When enabling IGMP Snooping, the devices that monitor network flow will determine which hosts have requested to receive multicast traffic, and the switch only executes IGMP Snooping.
MLD Snooping	Enable or disable MLD Snooping globally on the switch (disabled by default).
Unknown Multicast Action	Choose how to deal with unknown Multicast frames. The possible options are: • Drop—Drops unknown Multicast frames. • Flood—Floods unknown Multicast frames. • Forward to Router Port—Forwards unknown Multicast frames to Mrouter port.

Step 3 Click **Apply**. The Running Configuration file is updated.

IP Multicast Group Address

The IP Multicast Group Address page is similar to the MAC Group Address page except that Multicast groups are identified by IP addresses. The IP Multicast Group Address page enables querying and adding IP Multicast groups.

To define and view IP Multicast groups, follow these steps:

Step 1 Click **Multicast** > **IP Multicast Group Address**.

The page contains all of the IP Multicast group addresses learned by snooping.

Step 2 Enter the parameters required for filtering.

- VLAN ID equals to—Define the VLAN ID of the group to be displayed.
- IP Version equals to—Select IPv6 or IPv4.
- IP Multicast Group Address equals to—Define the IP address of the Multicast group to be displayed. This is only relevant when the Forwarding mode is (S,G).

Step 3 Click **Go**. The results are displayed in the lower block.

Step 4 Click **Add** to add a static IP Multicast Group Address.

Step 5 Enter the parameters.

- VLAN ID—Defines the VLAN ID of the group to be added.
- IP Version—Select the IP address type.
- IP Multicast Group Address—Define the IP address of the new Multicast group.
- Source IP Address—Defines the source address to be included.

Step 6 For each port, select its association type. The options are:

- Static—Attaches the port to the Multicast group as a static member.
- None—Indicates that the port is not currently a member of this Multicast group on this VLAN.

Step 7 Click **Apply**. The Running Configuration file is updated.

IGMP Snooping

A multicast address is a single IP data packet set that represents a network host group. Multicast addresses are available to process datagrams or frames intended to be multicast to a designated network service. Multicast addressing is applied in the link layer (Layer 2 of the OSI Model) and the Internet layer (Layer 3 of the OSI Model) for IP versions 4 (IPv4) and 6 (IPv6).

Multicast addresses in IPV4 are defined using leading address bits of 1110, which originate from the classful network design of the early Internet when this group of addresses was designated as Class D.

IPv4 multicast packets are delivered using the Ethernet MAC address range 01:00:5e:00:00:00–01:00:5e:7f:ff:ff. This range has 23 bits of available address space. The first octet (01) includes the broadcast/multicast bit. The lower 23 bits of the 28-bit multicast IP address are mapped into the 23 bits of available Ethernet address space. This means that there is ambiguity in delivering packets. If two hosts on the same subnet each subscribe to a different multicast group whose address differs only in the first 5 bits, Ethernet packets for both multicast groups will be delivered to both hosts, requiring the network software in the hosts to discard the unrequired packets.

To support selective IPv4 Multicast forwarding, bridge Multicast filtering must be enabled (in Multicast Properties, on page 1). The IGMP Snooping must be enabled globally and for each relevant VLAN in the IGMP Snooping page.

To enable IGMP Snooping and identify the device as an IGMP Snooping Querier on a VLAN, follow these steps:

Step 1 Click **Multicast** > **IGMP Snooping**.

Step 2 Enter the following information:

- IGMP Snooping Version—Select either IGMPv2 or IGMPv3.
- Report Suppression—Enable or disable IGMP report suppression. Disabling this feature will forward all IGMP reports to Multicast routers.

Note IGMP report suppression is supported only when the Multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per Multicast router query to Multicast devices. When IGMP report suppression is enabled, the switch sends the first IGMP report from all hosts for a group to all Multicast routers. The switch does not send the remaining IGMP reports for the group to the Multicast routers. This feature prevents duplicate reports from being sent to the Multicast devices.

The switch always forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all Multicast routers, regardless of the Multicast router query also includes requests for IGMPv3 reports.

Step 3 Click **Apply**.

Step 4 To configure IGMP on an interface, select a static VLAN and click **Edit**. Enter the following fields:

Option	Description
VLAN ID	Select The VLAN Id from the dropdown list.
IGMP Snooping Status	Select to enable IGMP Snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic.
Multicast Router Ports Auto Learn	Select to enable Auto Learn of the Multicast router.
Query Robustness	Enter the robustness variable value to be used if this switch is the elected querier.
Query Interval	Enter the interval between the general queries to be used if this switch is the elected. querier.
Query Max Response Interval	Enter the delay used to calculate the maximum response code inserted into the periodic general queries.
Last Member Query Counter	Number of IGMP group-specific queries sent before the device assumes that there are no more members for the group, if the device is the elected querier.
Last Member Query Interval	Enter the maximum response delay to be used if the switch cannot read maximum response time value from group specific queries sent by the elected querier.
Immediate Leave	Select to enable the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface. When an IGMP Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the IGMP queries from the Multicast router, it deletes entries periodically if it doesn't receive any IGMP membership reports from the Multicast clients. When enabled, this feature reduces the time it takes to block unnecessary IGMP traffic sent to a device port.
IGMP Querier Status	Select to enable this feature. This feature is required if there's no Multicast router.
IGMP Querier Version	Select the IGMP version to be used if the device becomes the elected querier. Select IGMPv3 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding. Otherwise, select IGMPv2.

Step 5 Click **Apply**. The Running Configuration file is updated.

Note Changes in IGMP Snooping timers configuration, such as: Query Robustness, Query Interval etc. don’t take effect on timers which already created.

MLD Snooping

To support selective IPv6 Multicast forwarding, bridge Multicast filtering must be enabled (in the Multicast Properties, on page 1), and MLD Snooping must be enabled globally and for each relevant VLAN in the MLD Snooping pages.

To enable MLD Snooping and configure it on a VLAN, complete the following:

Step 1 Click **Multicast** > **MLD Snooping**.

Note MLD Snooping is only operational when Bridge Multicast Filtering is enabled and can be enabled here Multicast Properties, on page 1.

Step 2 Enable or disable the following features:

- MLD Snooping Status—Select to enable MLD snooping globally on all interfaces.
- MLD Querier Status—Select to enable MLD querier globally on all interfaces.

Step 3 To configure MLD proxy on an interface, select a static VLAN and click **Edit**. Enter the following fields:

Option	Description
VLAN	Select the VLAN ID from the dropdown list.
MLD Snooping Status	Select to enable MLD Snooping on the VLAN. The device monitors network traffic to determine which hosts have asked to be sent Multicast traffic. The device performs MLD snooping only when MLD snooping and Bridge Multicast filtering are both enabled.
MRouter Ports Auto Learn	Select to enable Auto Learn of the Multicast router.
Immediate Leave	Select to enable the switch to remove an interface that sends a leave message from the forwarding table without first sending out MAC-based general queries to the interface. When an MLD Leave Group message is received from a host, the system removes the host port from the table entry. After it relays the MLD queries from the Multicast router, it deletes entries periodically if it does not receive any MLD membership reports from the Multicast clients. When enabled, this feature reduces the time it takes to block unnecessary MLD traffic sent to a device port.
Last Member Query Counter	Number of MLD group-specific queries sent before the device assumes there are no more members for the group, if the device is the elected querier. • Use Query Robustness (x)—The number in parentheses is the current query robustness value. • User Defined—Enter a user-defined value.

Step 4 Click **Apply**. The Running Configuration file is updated.

Note Changes in MLD Snooping timers configuration, such as: Query Robustness, Query Interval etc. do not take effect on timers which already created.

IGMP/MLD Snooping IP Multicast Group

The IGMP/MLD Snooping IP Multicast Group page displays the IPv4 and IPv6 group addresses learned from IGMP/MLD messages.

There might be a difference between information on this page and information on the MAC Group Address page. For example, assume that the system filters according to MAC-based groups and a port requested to join the following Multicast groups 224.1.1.1 and 225.1.1.1. Both are mapped to the same MAC Multicast address 01:00:5e:01:01:01. In this case, there's a single entry in the MAC Multicast page, but two entries on this page.

To query for an IP Multicast group, complete the following steps:

Step 1 Click **Multicast** > **IGMP/MLD Snooping IP Multicast Group**.

Step 2 Set the type of snooping group for which to search: IGMP or MLD.

Step 3 Enter some or all of following query filter criteria:

- VLAN ID equals to—Defines the VLAN ID to query.
- IP Version equals to—Select either Version 4 or Version 6.
- IP Multicast Group Address equals to—Enter the IP Multicast group address to query.

Step 4 Click **Go**. The following fields are displayed for each Multicast group:

- VLAN—The VLAN ID.
- IP Multicast Group Address—The Multicast group IP address.
- Member Ports—The list of ports to where the corresponding Multicast stream is forwarded.
- Type—The group type is static or dynamic.

Multicast Router Port

A Multicast router (Mrouter) port is a port that connects to a Multicast router. The device includes one or more Multicast router ports numbers when it forwards the Multicast streams and IGMP/MLD registration messages. This is required so that the Multicast routers can, forward the Multicast streams and propagate the registration messages to other subnets.

To statically configure or to view the dynamically detected ports connected to the Multicast router, follow these steps:

Step 1 Click **Multicast** > **Multicast Router Port**.

Step 2 Enter the query filter criteria:

- VLAN ID equals to—Select the VLAN ID for the router ports that are described.
- IP Version equals to—Select the IP version that the Multicast router supports.
- Interface Type equals to—Select whether to display ports or LAGs.

Step 3 Click **Go**. The interfaces matching the query criteria are displayed.

Step 4 For each port or LAG, select its association type. The options are as follows:

- Static—The port is statically configured as a Multicast router port.
- Dynamic—(Display only) The port is dynamically configured as a Multicast router port by a MLD/IGMP query.
- Forbidden—This port isn't to be configured as a Multicast router port, even if IGMP or MLD queries are received on this port. If Forbidden is enabled on a port, the MRouter isn't learned on this port (i.e. MRouter Ports Auto-Learn isn't enabled on this port).
- None—The port isn't currently a Multicast router port.

Step 5 Click **Apply** to update the device.

Forward All

The Forward All page configures the ports and/or LAGs that receive Multicast streams from a specific VLAN.

You can statically (manually) configure a port to Forward All, if the devices connecting to the port don't support IGMP and/or MLD. Multicast packets, excluding IGMP and MLD messages, are always forwarded to ports that are defined as Forward All. The configuration affects only the ports that are members of the selected VLAN.

To define Forward All Multicast, complete the following steps:

Step 1 Click **Multicast** > **Forward All**.

Step 2 Define the following:

- VLAN ID equals to—The VLAN ID the ports/LAGs are to be displayed.
- IP version – IPv4 or IPv6
- Interface Type equals to—Define whether to display ports or LAGs.

Step 3 Click **Go**. The status of all ports/LAGs are displayed.

Step 4 Select the port/LAG that is to be defined as Forward All by using the following methods:

- Static—The port receives all Multicast streams.
- Forbidden—Ports can't receive any Multicast streams, even if IGMP/MLD snooping designated the port to join a Multicast group.
- None—The port isn't currently a Forward All port.

Step 5 Click **Apply**. The Running Configuration file is updated.

Maximum Multicast Groups

Use the Maximum Multicast Groups page to configure the maximum number of Multicast groups that are allowed on each interface and specify the action when the limit reaches.

To define the maximum number of IGMP and MLD groups on an interface:

Step 1 Click **Multicast** > **Maximum Multicast Groups**.

Step 2 Select the interface type (Port and LAG), and click **Go.**

Step 3 Select an interface and click **Edit**:

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- IGMP Maximum Multicast Group—Enter the maximum number of IGMP groups that are allowed on the interface.
- IGMP Exceed Action—Denies or replaces the existing group with the new group for which the IGMP report was received when the limit is reached.
- MLD Maximum Multicast Group—Enter the maximum number of MLD groups that are allowed on the interface.
- MLD Exceed Action—Denies or replaces the existing group with the new group for which the MLD report was received when the limit is reached.

Step 5 Click **Apply**. The Running Configuration is updated.

Multicast Filtering

You can add a Multicast filter profile to permit or deny a range of Multicast groups be learned when the join groups match the profile IP group range, and assign the profile to an interface. The Multicast filter settings will be applied to the selected interface.

Multicast Filtering Profiles

A Multicast filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range.

To create a Multicast filter profile:

Step 1 Click **Multicast** > **Multicast Filtering** > **Profiles**.

Step 2 Select either Version 4 or Version 6 that the filter profile is applied to IPv4 or IPv6 Multicast traffic, and click Go.

Step 3 Click **Add**.

Step 4 Enter the following information:

- Profile Index—Enter the sequence number for the profile.
- IP Version—Select ether Version 4 or Version 6 to apply the filter profile to IPv4 or IPv6 Multicast traffic.
- Start Multicast Address—Enter the starting Multicast group address.
- End Multicast Address—Enter the ending Multicast group address.
- Action—Denies or permits Multicast frames when the join group matches.

Filter Settings

To assign a Multicast filter profile to an interface to deny or permit the Multicast group when the join group matches the filter profile:

Step 1 Click **Multicast** > **Multicast Filtering** > **Filter Settings**.

Step 2 Select the Interface Type equals to— To view either ports or LAGs.

Step 3 Select an interface and click **Edit**.

Step 4 Enter the following information:

- Interface—Select the port or LAG to be defined.
- Filter—Enable or disable filtering Multicast traffic on this interface.
- Filter Profile Index—If enabled, select the Multicast filter profile to be applied. The Multicast filter settings defined in the profile are applied to the interface.

Step 5 Click **Apply**. The Running Configuration file is updated.