

Multicast

This chapter contains the following sections:

- Multicast Properties, on page 1
- MAC Group Address, on page 3
- IP Multicast Group Address, on page 4
- IPv4 Multicast Configuration, on page 5
- IPv6 Multicast Configuration, on page 8
- IGMP/MLD Snooping IP Multicast Group, on page 10
- Multicast Router Port, on page 11
- Forward All, on page 12
- Unregistered Multicast, on page 13

Multicast Properties

Note This setting and its subsets are available in the Advanced View mode.

Multicast forwarding enables one-to-many information dissemination. Multicast applications are useful for dissemination of information to multiple clients, where clients don't 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's 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 to 239.255.255.255.
- The IPv6 Multicast address is FF00:/8.
- To map an IP Multicast group address to a 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 to 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 enable Multicast filtering, and select the forwarding method, follow these steps:

Procedure

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

Step 2 Enter the parameters.

Bridge Multicast Filtering Status	Select Enable to enable filtering.
VLAN ID	Select the VLAN ID to set its forwarding method.
Forwarding Method for IPv6	Set one of the following forwarding methods for IPv6 addresses: • MAC Group Address—Forward packets according to the MAC Multicast group address • IP Group Address—Forward packets according to the IPv6 Multicast group address • Source-Specific IP Group Address—Forward packets according to the source IPv6 and IPv6 Multicast group address. If an IPv6 address is configured on the VLAN, the operational forwarding methods for IPv6 Multicast are IP Group Address. **Note** For IPv6 IP Group and Source-Specific IP Group Address modes, the device checks a match only for 4 bytes of the destination Multicast and source address. For the destination Multicast address, the last 4 bytes of group ID are matched. For the source address, the last 3 bytes + the 5th from the last byte are matched.
Forwarding Method for IPv4	Set one of the following forwarding methods for IPv4 addresses: • MAC Group Address—Forward packets according to the MAC Multicast group address • IP Group Address—Forward packets according to the IPv4 Multicast group address • Source-Specific IP Group Address—Forward packets according to the source IPv4 and IPv4 Multicast group address If an IPv4 address is configured on the VLAN, the operational forwarding method for IPv4 Multicast is IP Group Address.

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

MAC Group Address

This setting is only visible in the Advanced Mode view.

The MAC Group Address page has the following functions:

- Query and view information from the Multicast Forwarding Data Base (MFDB), relating to a specific VLAN ID or a specific MAC address group This data is acquired either dynamically through IGMP/MLD snooping or statically by manual entry.
- Add or delete static entries to the MFDB that provide static forwarding information, based on MAC destination addresses.
- Displays all ports/LAGs that are members of each VLAN ID and MAC address group.

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

Procedure

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

Step 2 Enter the Filter parameters.

- VLAN ID equals to—Set the VLAN ID of the group to be displayed.
- MAC Group Address equals to—Set the MAC address of the Multicast group to be displayed. If no MAC Group Address is specified, the page contains all the MAC Group Addresses from the selected VLAN.

Step 3 Click **Go,** and the MAC Multicast group addresses are displayed in the lower block.

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

Step 5 Enter the parameters.

- VLAN ID—Defines the VLAN ID of the new Multicast group.
- MAC Group Address—Defines the MAC address of the new Multicast group.

Step 6 Click **Apply**, the MAC Multicast group is saved to the Running Configuration file.

To configure and display the registration for the interfaces within the group, select an address, and click **Details.**

The page displays:

- VLAN ID—The VLAN ID of the Multicast group.
- MAC Group Address—The MAC address of the group.

Step 7 Select either port or LAG from the Filter: Interface Type menu.

Step 8 Click **Go** to display the port or LAG membership of the VLAN.

Step 9 Select the way that each interface is associated with the Multicast group:

- Static—Attaches the interface to the Multicast group as a static member.
- Dynamic—Indicates that the interface was added to the Multicast group as a result of IGMP/MLD snooping.

- Forbidden—Specifies that this port isn't allowed to join this Multicast group on this VLAN.
- None—Specifies that the port isn't currently a member of this Multicast group on this VLAN.

Step 10 Click **Apply**, and the Running Configuration file is updated.

IP Multicast Group Address

Note This setting is only visible in the Advanced Mode view.

Note All options on this page are disabled unless you enable the Bridge Multicast Filtering from the Multicast Properties page.

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:

Procedure

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).
- Source IP Address equals to—Define the source IP address of the sending device. If the mode is (S,G), enter the sender S. This together with the IP Group Address is the Multicast group ID (S,G) to be displayed. If mode is (*.G), enter an * to indicate that the Multicast group is only defined by destination.

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 Specific—Indicates that the entry contains a specific source, and adds the address in the IP Source Address field. If not, the entry is added as a (*, G) entry, an IP group address from any IP source.
- Source IP Address—Defines the source address to be included.

Step 6 Click **Apply**. The IP Multicast group is added, and the device is updated.

Step 7 To configure and display the registration of an IP group address, select an address and click **Details**.

The VLAN ID, IP Version, IP Multicast Group Address, and Source IP Address selected are displayed as read only in the top of the window. You can select the filter type:

- Interface Type equals to—Select whether to display ports or LAGs.

Step 8 For each interface, select its association type. The options are as follows:

- Static—Attaches the interface to the Multicast group as a static member.
- Dynamic—Attaches the interface to the Multicast group as a dynamic member.
- Forbidden—Specifies that this port is forbidden from joining this group on this VLAN.
- None—Indicates that the port isn't currently a member of this Multicast group on this VLAN. This is selected by default until Static or Forbidden is selected.

Step 9 Click **Apply**. The Running Configuration file is updated.

IPv4 Multicast Configuration

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.

This section covers how to configure the IPv4 multicast.

IGMP Snooping

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:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP Snooping**.

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

Step 2 IGMP Snooping is only operational when Bridge Multicast Filtering is enabled. You can enable it here: Multicast Properties, on page 1.

Step 3 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.
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 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.
Last Member Query Counter	Number of MLD group-specific queries sent before the device assumes that 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.
IGMP Querier Status	Select to enable this feature. This feature is required if there's no Multicast router.
IGMP Querier Election	IGMP Querier Election—Whether the IGMP querier election is enabled or disabled. If the IGMP Querier election mechanism is enabled, the IGMP Snooping querier supports the standard IGMP Querier election mechanism specified in RFC3810.

Option	Description
	If the IGMP Querier election mechanism is disabled, the IGMP Snooping querier delays sending General Query messages for 60 seconds after it was enabled, and if there's no other querier, it starts sending General Query messages. It stops sending General Query messages when it detects another querier. The IGMP Snooping Querier resumes sending General Query messages if it does hear another querier for a Query Passive interval that equals: Robustness * (Query Interval) + 0.5 * Query Response Interval.
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.
Querier Source IP Address	The IP address of the device source interface to be used in messages sent. In MLD this address is selected automatically by the system. • Auto—The system takes the source IP address from the IP address defined on the outgoing interface. • User Defined—Enter a user-defined IP address.

Step 4 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.

IGMP VLAN Settings

Note This setting is only available in the Advanced View mode.

To configure IGMP on a specific VLAN, complete the following steps:

Procedure

Step 1 Click **Multicast** > **IPv4 Multicast Configuration** > **IGMP VLAN Settings**.

The following fields are displayed for each VLAN on which IGMP is enabled:

- Interface Name—VLAN on which IGMP snooping is defined.
- Query Robustness—Enter the number of expected packet losses on a link.
- Query Interval (sec)—Interval between the General Queries to be used if this device is the elected querier.

- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- Last Member Query Interval (msec)—Enter the Maximum Response Delay to be used if the device can't read a Max Response Time value from group-specific queries sent by the elected querier.

Step 2 Select an interface, and click **Edit**. Enter the values of the fields described above.

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

IPv6 Multicast Configuration



Note This setting and its subsets are available in the Advanced View mode.

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It's the IP-specific form of multicast and is used for streaming media and other network applications. It uses specially reserved multicast address blocks in IPv4 and IPv6.

Unicast packets are delivered to a specific recipient on an Ethernet or IEEE 802.3 subnet by setting a specific layer 2 MAC address on the Ethernet packet address. Broadcast packets use a broadcast MAC address (FF:FF:FF:FF:FF:FF). For IPv6 multicast addresses, the Ethernet MAC is derived by the four low-order octets OR'ed with the MAC 33:33:00:00:00:00.

This section covers how to configure the IPv6 multicast.

MLD Snooping



Note This setting is only visible in the Advanced Mode view.

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:

Procedure

Step 1 Click **Multicast** > **IPv6 Multicast Configuration** > **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 ID	Select the VLAN ID from the drop down 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.
MLD Querier Status	Select to enable this feature. This feature is required if there is no Multicast router.
MLD Querier Election	Whether the MLD querier election is enabled or disabled. If the MLD Querier election mechanism is enabled, the MLD Snooping querier supports the standard MLD Querier election mechanism specified in RFC3810. If the MLD Querier election mechanism is disabled, the MLD Snooping querier delays sending General Query messages for 60 seconds after it was enabled, and if there is no other querier, it starts sending General Query messages. It stops sending General Query messages when it detects another querier. The MLD Snooping Querier resumes sending General Query messages if it does hear another querier for a Query Passive interval that equals: Robustness * (Query Interval) + 0.5 * Query Response Interval.
MLD Querier Version	Select the MLD version to be used if the device becomes the elected querier. Select MLDv2 if there are switches and/or Multicast routers in the VLAN that perform source-specific IP Multicast forwarding. Otherwise, select MLDv1.

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.

MLD VLAN Settings

Note This setting is only visible in the Advanced Mode view.

To configure MLD on a specific VLAN, follow these steps:

Procedure

Step 1 Click **Multicast** > **IPv6 Multicast Configuration** > **MLD VLAN Settings**.

The following fields are displayed for each VLAN on which MLD is enabled:

- Interface Name—VLAN for which MLD information is being displayed.
- Query Robustness—Enter the number of expected packet losses on a link
- Query Interval (sec)—Interval between the General Queries to be used if this device is the elected querier.
- Query Max Response Interval (sec)—Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.
- Last Member Query Interval (msec)—Enter the Maximum Response Delay to be used if the device can't read Max Response Time value from group-specific queries sent by the elected querier.

Step 2 To configure a VLAN, select it and click **Edit**. Enter the fields described above.

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

IGMP/MLD Snooping IP Multicast Group

Note This setting is only available in the Advanced View mode.

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:

Procedure

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 following query filter criteria:

- Group Address equals to—Defines the Multicast group MAC address or IP address to the query.
- Source Address equals to—Defines the sender address to the query.
- VLAN ID equals to—Defines the VLAN ID to the query.

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

- VLAN—The VLAN ID.
- Group Address—The Multicast group MAC address or IP address.
- Source Address—The sender address for all of the specified group ports.
- Included Ports—The list of destination ports for the Multicast stream.
- Excluded Ports—The list of ports not included in the group.
- Compatibility Mode—The oldest IGMP/MLD version of registration from the hosts the device receives on the IP group address.

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:

Procedure

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

Step 2 Enter some or all of following 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. To enable the dynamic learning of Multicast router ports, go to IGMP/MLD Snooping IP Multicast Group, on page 10.
- 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

When Bridge Multicast Filtering is enabled, registered Multicast packets are forwarded to ports based on IGMP and MLD snooping. If Bridge Multicast Filtering is disabled, all Multicast packets are flooded to the corresponding VLAN.

The Forward All page configures the ports and/or LAGs that receive Multicast streams from a specific VLAN. This feature requires that the Bridge Multicast filtering is enabled in Multicast Properties, on page 1. If it is disabled, then all Multicast traffic is flooded to the ports on the device. 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:

Procedure

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.
- 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.

Unregistered Multicast

Note This setting is only available in the Advanced View mode.

This feature is used to ensure that the customer receives only the Multicast groups requested (registered).

Unregistered Multicast frames are forwarded to all ports on the VLAN. You can select a port to filter unregistered Multicast streams. The configuration is valid for any VLAN of which the port is a member.

To define unregistered Multicast settings, follow these steps:

Procedure

Step 1 Click **Multicast** > **Unregistered Multicast**.

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

Step 3 Click **Go**.

Step 4 Define the following:

- Port/LAG—Displays the port or LAG ID.
- Displays the forwarding status of the selected interface. The possible values are:
  - Forwarding—Enables forwarding of unregistered Multicast frames to the selected interface.
  - Filtering—Enables filtering (rejecting) of unregistered Multicast frames to the selected interface.

Step 5 Click **Apply**. The settings are saved, and the Running Configuration file is updated.