

13 Multicast

Multicast is a communication mode in which data is transmitted to multiple recipients at the same time.

[13.1 Introduction to Multicast](#)

[13.2 Basic Multicast Concepts](#)

[13.3 Multicast Model](#)

[13.4 Implementation Principles of Multicast](#)

[13.5 IPv6 Multicast](#)

[13.6 Configuring the Multicast Service](#)

The MA5800 supports multicast cascading for reducing the number of ports used on the convergence device, and also supports Multiple Spanning Tree Protocol (MSTP) network protection. With these two functions, the network structure is optimized and the multicast service reliability is improved.

[13.7 Multicast Maintenance and Diagnosis](#)

[13.8 Multicast Standards and Protocols Compliance](#)

[13.9 Multicast Feature Updates](#)

13.1 Introduction to Multicast

Why Is Multicast Required

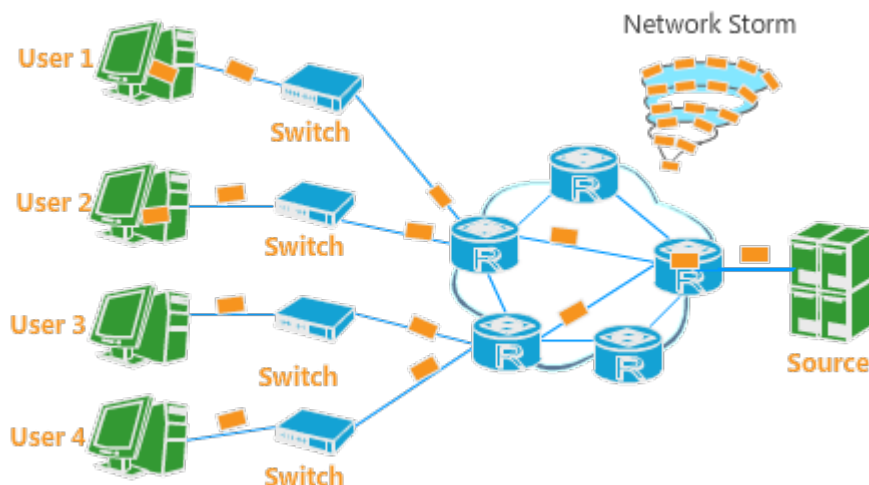
Traditional IP communications are implemented in unicast or broadcast mode.

- Unicast: a P2P transmission mechanism. Unicast involves only one information sender and one information recipient.
- Broadcast: a point-to-all-point transmission mechanism. Broadcast involves only one information sender and all the reachable information recipients in a LAN.

In broadcast IP communications, the source sends only one copy of packets to the broadcast address of the network. Then, the network copies these packets and sends them to all network segments for all routers and users, regardless of

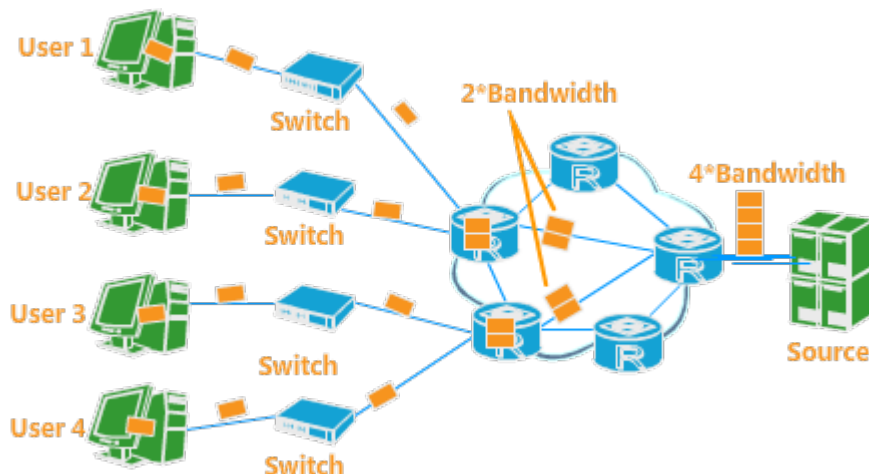
whether these routers and users require such data. In broadcast mode, if only a few users require such packets, network utilization is low and bandwidths are unnecessarily used. The users who do not require such data are adversely affected. In addition, a severe broadcast storm may occur due to routing loopback.

Figure 13-1 Diagram of broadcast implementation



In unicast IP communications, the source sends a separate copy of packets to each recipient. Therefore, each recipient requires a separate data channel. In unicast mode, the amount of data that needs to be transmitted on the network is determined based on the number of users requiring such data. If the number of users requiring the same data is large, multiple same data flows must be set up on the network. In this case, network bandwidth may become insufficient, degrading network transmission quality. Therefore, the unicast mode cannot be used for transmitting large amount of data for a large number of users.

Figure 13-2 Diagram of unicast implementation

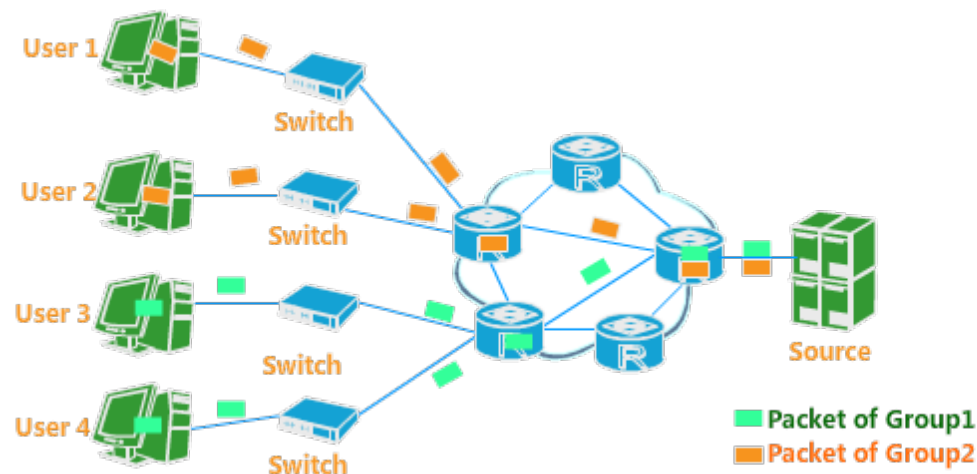


Traditional unicast and broadcast communications cannot meet P2MP service requirements. The IP network development supports more network applications. In addition, some large amount of data needs to be sent in P2MP mode. In this case, multicast is introduced to meet these service requirements.

What Is Multicast

Multicast is a communication mode in which one information sender sends one copy of IP data package to a group of information recipients on an IP network. Other hosts on the network cannot receive this data package.

Figure 13-3 Diagram of multicast implementation



Comparison between multicast and unicast, and multicast and broadcast:

- In the multicast mode, a single data stream is sent to a group of users at the same time. Only one copy of the same multicast data stream exists on each link. Compared with the unicast mode, in the multicast mode, the increase of users does not immediately increase the load of the network. Therefore, the server and the CPU can deal with a lighter load, reducing desired network bandwidths.
- Multicast messages can be sent across different network segments and will not be received by users who are not interested in the messages. Compared with the broadcast mode, the multicast mode achieves a longer information transmission distance and ensures that information is transmitted to only interested recipients. Hence, information security can be guaranteed.

The preceding comparisons show that multicast effectively resolves the problem of P2MP transmission and implements efficient P2MP data transmission in IP networks.

Multicast Applications

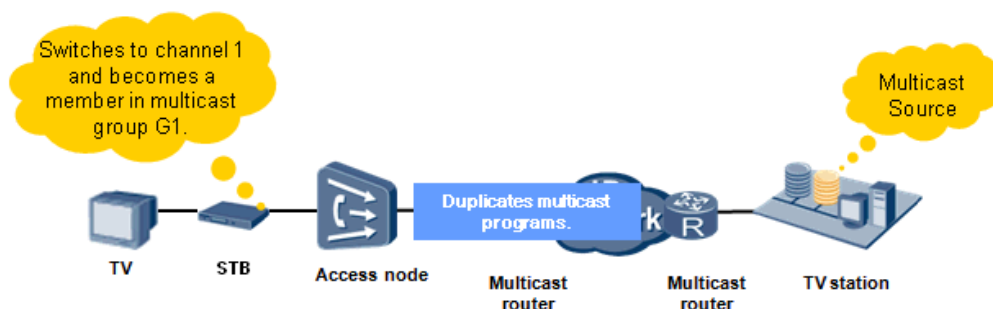
The multicast technology enables the device to provide value-added services, including live broadcast, IPTV, distance learning, TeleMedicine, network radio, live radio conference, and online game.

13.2 Basic Multicast Concepts

Basic Concepts

The following section provides an example of watching the program of a TV channel to aid the understanding of relevant concepts of IP multicast.

- The multicast group is an agreement between the sender and the recipient. For example, a TV channel can be regarded as a multicast group.
- The TV station is the multicast source and it sends data to a certain TV channel.
- The STB is a receiving host. When the user chooses to watch the program of a channel, this action can be regarded as the host joining a multicast group. Then, the TV set displays the program of the TV channel to the user, which means that the host has received the data sent to this multicast group.
- The user can turn on or turn off the STB or switch between channels any time, which means that the host can join or leave a multicast group dynamically.

Figure 13-4 Multicast concept diagram**Table 13-1** Table of Basic Concepts

Concept	Description
Multicast group	A multicast group is identified by a multicast IP address. Any host (or any other receiving device) joining a multicast group becomes a member of the group. The group member can identify and receive the IP messages destined to the multicast IP address.
Multicast source	A signal source sending IP messages destined to a multicast address is called a multicast source. • A multicast source can send data to multiple multicast groups at the same time. • Multiple multicast sources can send data to a multicast group at the same time.
Multicast group member	The members of a multicast group are dynamic. Hosts in a network can join or leave a multicast group any time. Multicast group members may be widely dispersed across the network. A multicast source is usually not a data recipient at the same time and is not the member of a multicast group.

Concept	Description
Multicast duplication	Multicast duplication is a capability with which the network device duplicates a multicast message from an ingress port into multiple copies and sends them to multiple egress ports. To ensure effective transmission of multitudes of data, this function can be implemented only by hardware.

Concept	Description
Multicast address	To enable the communication between a multicast source and its members, a network-layer multicast address must be available, which is the multicast IP address. In addition, a technology must also be available for mapping the multicast IP address to a link-layer multicast MAC address. The following part of this section will describe the two types of multicast address. • Multicast IP address As specified by Internet Assigned Numbers Authority (IANA), multicast messages use class-D IP addresses (224.0.0.0-239.255.255.255) as their destination addresses, and the class-D IP addresses must not appear in the source IP address field of the IP messages. For details of the MAC address range and description, see Table 13-2. Multicast addresses are not allocated to the receiving device or the multicast source device for identifying their network location. In the case of the multicast source device, the allocated multicast address is used for generating and carrying multicast data; in the case of the receiving device, the multicast address is used for distinguishing multicast data. In an actual multicast application, the multicast address does not need to be manually input. For example, in the live TV service, which is a common application, a menu interface is provided. When the user orders a program using a remote controller, the application software will automatically obtain the multicast IP address corresponding to the program. • Ethernet multicast MAC address When IP messages are unicast over an Ethernet, the destination MAC addresses used are the MAC addresses of recipients. However, in the transmission of multicast messages, the transmission destination is no longer a specific recipient. Instead, it is a group with uncertain members. In this case, the multicast MAC address is used. Specified by IANA, the most significant 25 bits of a multicast MAC address are 0x01005e, and the least significant 23 bits of the MAC address are the least significant 23 bits of the multicast IP address. The following figure shows the mapping.

Concept	Description
	Figure 13-5 Mapping between multicast MAC address and multicast IP address The first four bits of the multicast IP address are 1110, which stands for the multicast ID, and in the last 28 bits, only 23 bits are mapped to the MAC address. Therefore, five bits of information in the IP address is lost. The direct result is that 32 multicast IP addresses are mapped to the same MAC address.
Multicast router	Multicast routers support multicast. A multicast router supports the following functions: • Manages group members in the network segment close to user hosts. • Supports multicast routing for forwarding multicast packets. • Functions as a group member.

Table 13-2 Multicast addresses and meanings

Multicast Address Range	Description
224.0.0.0-224.0.0.255	Permanent group addresses reserved for routing protocols
224.0.1.0-238.255.255.255	User multicast addresses
239.0.0.0-239.255.255.255	Local management group addresses (private addresses) NOTE This address range limits multicast to be implemented within a specified multicast domain so that the MAC addresses in different domains can be duplicated.

Basic Managed Objects

Table 13-3 Basic managed objects

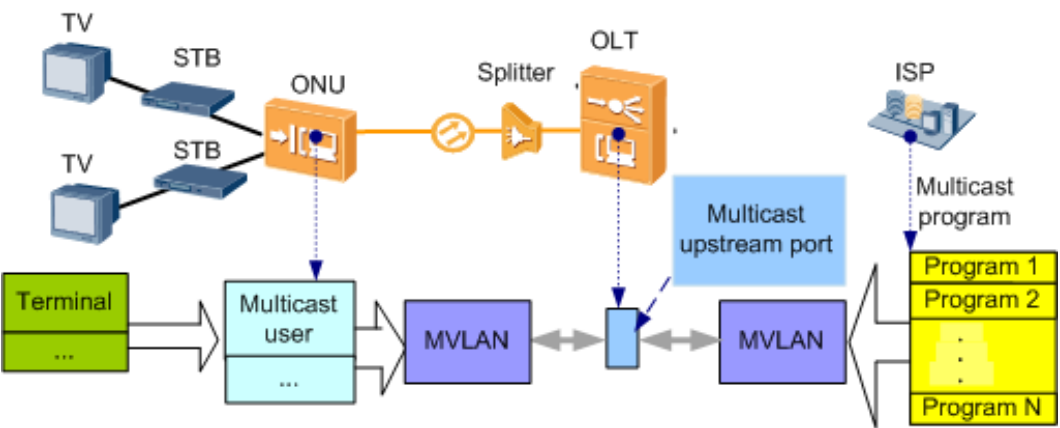
Managed Object	Description
Multicast VLAN	A multicast VLAN (also called an MVLAN) refers to the VLAN tag carried by multicast data. MVLANs are usually divided based on ISP. By the implementation of the forwarding plane, control plane, and management plane based on VLAN instance, multicast services are provisioned to the users of the same device, allowing the users not to be interfered by each other. Except the super VLAN, the VLAN of any attribute or any type configured on the device can serve as an MVLAN. For details on the MVLAN, see "13.4.5.6 Multi-instance Multicast".
Multicast program	A multicast program can be regarded as a multicast group. Its basic attribute is the multicast IP address. The device can manage a multicast program at a finer grain, such as by rights control and CAC. According to whether the attributes (such as the multicast IP address) of each program are configured before the service is provisioned, multicast programs can be classified into two types: pre-configured programs and dynamic programs. Determine whether to support the programs of the two types based on the configured MVLAN program mapping mode. Table 13-4 shows the supporting status for pre-configured programs and dynamic programs. For details about dynamic programs, see Dynamic Programs.
Multicast uplink port	A multicast uplink port is one through which a multicast source connects to the device, and is also a port through which an upper-layer multicast router connects to the device. According to their dependency on the link-layer loop protocol, multicast uplink ports can be classified into two types: manually configured (static) uplink ports and dynamic uplink ports. For details on dynamic uplink ports, see 13.4.4.2 Ring Network of Uplink Ports.
Multicast user	A multicast user is a multicast data recipient. A service stream must be configured for the multicast user for carrying multicast control messages in the upstream direction (the device can distinguish the user by traffic classification). Therefore, a multicast user corresponds to a unique terminal or service subscriber. In addition, an MVLAN must be specified for the multicast user to indicate to which ISP the service subscriber belongs.

Table 13-4 Program type

Program Type	Description
Pre-configured programs	Configure the program list before users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.
Dynamic programs	A program list is dynamically generated according to the programs requested by users. In this mode, the program list does not need to be configured or maintained; however, the functions such as program management, user multicast bandwidth management, program preview, and program prejoin are not supported.

The following figure shows the relationships between the basic managed objects.

Figure 13-6 Multicast managed objects



NOTE

- As a device placed at users' home, an ONT does not support multiple multicast users. Although the ONT is for only one multicast user, it can still connect to multiple STBs.
- Traffic streams with the QinQ attribute do not support multicast users.
- Traffic streams that classify traffic by double VLANs do not support multicast users.

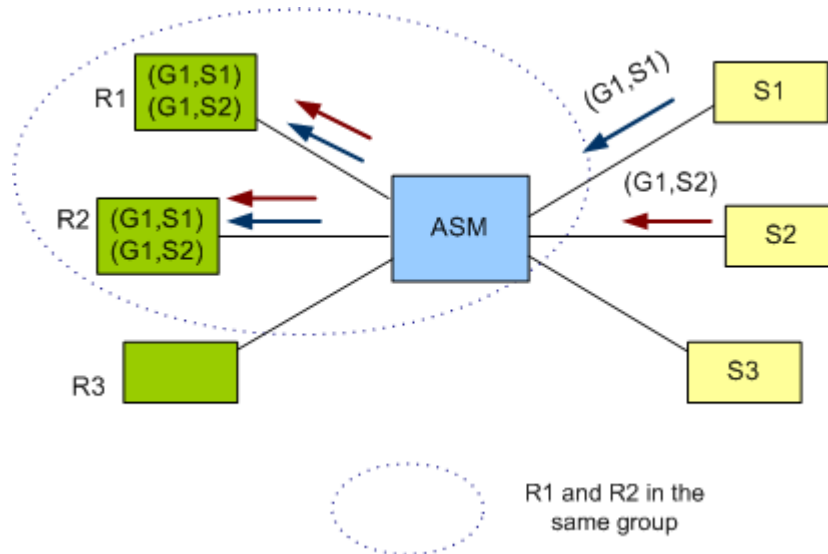
13.3 Multicast Model

According to the multicast source control level, multicast has three models:

ASM

Any-source multicast (ASM) is defined in RFC 1112. In this model, a recipient, by joining a group identified by the multicast address, can receive data sent to the group. A recipient can join or leave a group at any time, and the recipient location or quantity is not limited. In addition, any sender can serve as the multicast source to send data to the group. Therefore, this model is applicable to the multipoint-to-multipoint (MP2MP) multicast application.

Figure 13-7 ASM network model



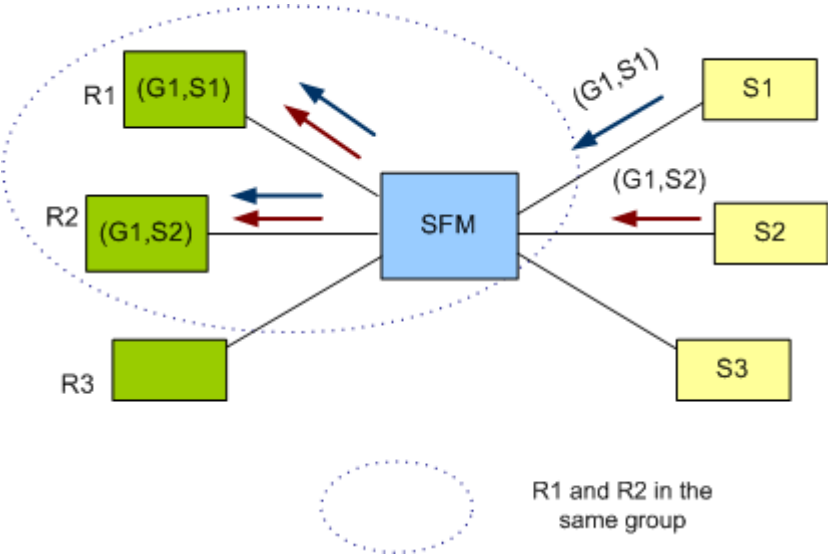
SFM

As an extension of ASM, source-filtered multicast (SFM) extends the source filtering function of the upper-layer protocol module. That is, in the SFM model, whether the multicast data of specified multicast source(s) is allowed to pass can be controlled. Viewed from recipients, SFM and ASM are different; but viewed from senders, they are the same. Therefore, SFM is the same as ASM in terms of network interoperability.

NOTE

The SFM is basically an ASM with a multicast source filtering policy. The basic principles and configurations of ASM and SFM are the same. In this manual, both SFM and ASM are called ASM.

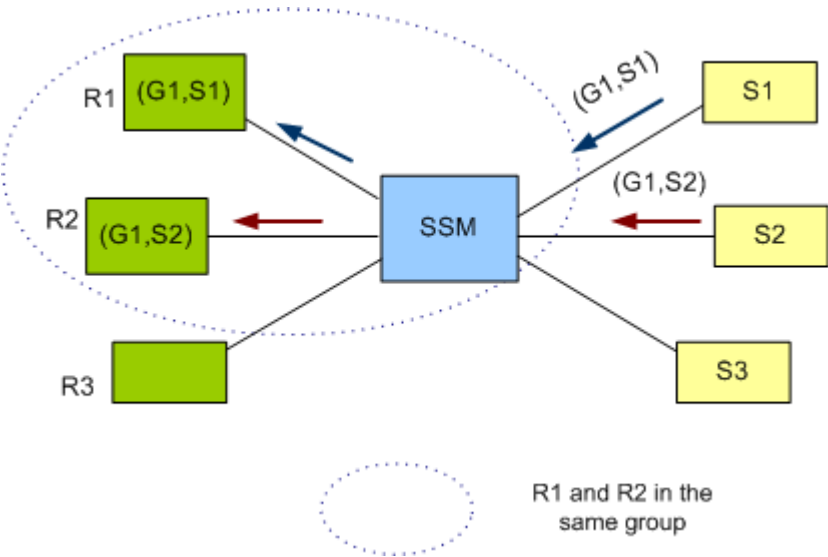
Figure 13-8 SFM network model



SSM

Source-specific multicast (SSM) is defined in RFC 4607. In this model, a recipient joins a channel by specifying the multicast source and group and receives data sent to the group from a specific multicast source. The recipient quantity is not limited. In addition, only the specific sender can serve as the multicast source to send data to the channel. Therefore, this model is applicable to the point-to-multipoint (P2MP) multicast application.

Figure 13-9 SSM network model



The following table lists the protocols that support ASM/SSM.

Multicast Model	Typical Protocol Combination of Devices in the Network			
	STB	AN	Router	Inter-domain router
ASM	IGMPv2	IGMPv2	PIM-SM	MSDP/MBGP
SSM	IGMPv3	IGMPv3	PIM-SSM	MBGP

Based on the preceding multicast models, the OLT supports three group filtering modes: ASMSSM, ASM ONLY, and SSM ONLY.

NOTE

Only the OLT supports group filtering mode.

In different group filter modes, for the differences in management plane and control plane, see [Multi-instance Multicast](#); for the differences in the forwarding plane, see [Forwarding Framework on the Device](#).

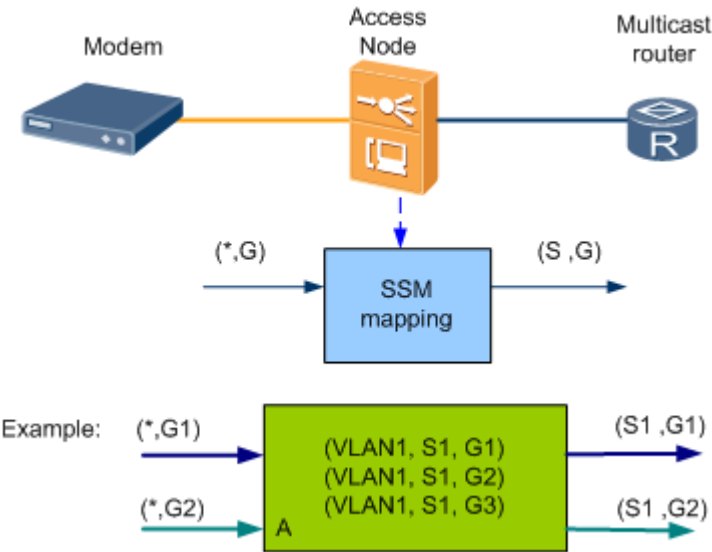
Follow the rules below to select a proper filter mode:

- For compatibility with the original VLAN+GMAC, select ASMSSM.
- For strict ASM or SSM message filtering, select ASM ONLY or SSM ONLY.
- For maximum compatibility of various STBs in a home network, select ASMSSM.
- For SIP+GIP forwarding (that is, posing no restrictions on SIP and GIP planning among different ISPs), select SSM ONLY. However, the entire network needs to support IGMPv3 for implementing SSM ONLY.

When the group filter mode is ASMSSM, even if the user side does not support IGMPv3, carriers can implement SSM network on the network side. The device, with its SSM mapping function (can be supported automatically), can help implement the SSM networking on the network side even if the user-side device does not support IGMPv3. With the SSM mapping function, the device maps the received (*, G) message to an (S, G) message according to the unique multicast program triplet, as shown in the following figure.

- A multicast user cannot belong to multiple MVLANs at the same time.
- Dynamic programs do not support SSM mapping.

Figure 13-10 SSM mapping



The following table describes whether the devices support the SSM and ASM modes.

User Side	Network Side	Supported or Not
SSM	SSM	Supported
ASM	ASM	Supported
ASM	SSM	Supported
SSM	ASM	Not supported

When the group filter mode is ASM ONLY, SSM mapping is not supported because ASM packets are dropped on the user side. For SSM ONLY, it is unnecessary to support SSM mapping.

13.4 Implementation Principles of Multicast

13.4.1 IGMP

13.4.1.1 IGMP Protocol

Internet Group Management Protocol (IGMP) is used to set up and maintain relationships between multicast members in a multicast group between hosts and the router connected to these hosts.

- Multicast members dynamically add to or leave a multicast group on the host.

- The relationships between group members are maintained and managed on the router. In addition, the IGMP protocol supports data exchanging with the upper-layer multicast routing protocol.

IGMP involves three versions: IGMPv1, IGMPv2, and IGMPv3. A new IGMP version is compatible with an earlier version. IGMPv1 is rarely supported. Therefore, according to TR101 requirements, Huawei hosts do not support IGMPv1 and simply discard IGMPv1 packets.

IGMPv1

IGMPv1 is defined in RFC 1112, defining the basic process of group member query and report. IGMPv1 is seldom used. Therefore, IGMPv1 is not described in the remainder of this document.

IGMPv2

IGMPv2 is defined in RFC 2236, supporting quick leave of group members compared with IGMPv1.

Table 13-5 IGMP packet

Role	Message Type	Description
Router	General query	A router periodically sends this message to maintain the requirements posed by all hosts connected to the router in all multicast groups. The router detects an accidentally offline host by an aging mechanism.
	Group-specific query	A router sends this message to check whether a multicast group is still required by any host. The router usually sends this message when receiving a leave message.
Host	Report	The report message is used by a host for actively joining a multicast group or for responding to a general query or a group-specific query.
	Leave	The leave message is used by a host for actively informing a router that the host no longer needs a multicast group.

Group Member Relationship Maintenance

Prerequisite: If a network segment contains multiple multicast routers, IGMPv2 enables the routers to use a querier election mechanism to elect a querier.

1. The querier periodically sends general query messages to group members to query group member relationships.
2. The hosts in the network segment make different responses to the querier after receiving the general query messages.

- The hosts out of the multicast group do not respond to the querier.
- Group members locally start a timer.
 - If a group member does not monitor a report message responded by other group members when the timer times out, this group member sends a report packet to respond to the querier.
 - If a group member monitors a report message responded by other group members before the timer times out, this group member does not send a report packet to respond to the querier (suppresses its response packet).
- 3. After receiving the report messages, the querier determines that this network segment contains group members and generates a multicast forwarding entry. When receiving data for the multicast group, the router forwards the data to the group members.

Group Member Join-in

1. If host A added to multicast group G1 monitors no data for G1 in the network segment, host A immediately sends a report message of G1 to the querier, without waiting for the receiving of a general query message sent by the querier.
2. After receiving the report message, the router in the network segment determines that this network segment contains G1 group members and adds the downlink port for G1 to multicast routing entry (*,G1). When receiving data for G1, the router forwards the data to the group members.

Group Member Leaving

1. When host A exits from G1, it sends a leave message to the querier.
2. After receiving the leave message, the querier sends a group-specific query message to group members to check whether all group members in G1 have left this group.
 - If a group member sends a report message to the querier, this network segment still contains G1 group members. Therefore, the querier does not delete the downlink port from multicast entry (*,G1).
 - If no group member sends a report message to the querier, the querier deletes the downlink port from multicast entry (*,G1).

IGMPv3

IGMPv3 is defined in RFC 3376. Compared with IGMPv2 (RFC 2236), IGMPv3 has the following improvements:

- Batch report. The destination IP address of report messages is always filled in as 224.0.0.22. In addition, the IGMP payload can carry multiple group records, reducing the number of report messages between devices. As shown in the following figure, the IGMP message carries the information about two groups 232.1.1.1 and 232.1.1.2. With IGMPv2 messages, the destination IP address must be filled in as the corresponding group IP address. Hence, one IGMPv2 message cannot carry the information about multiple groups.

Figure 13-11 Example of an IGMPv3 report message

```
* Internet Protocol, Src: 192.168.5.64 (192.168.5.64), Dst: 224.0.0.22
* Internet Group Management Protocol
  IGMP Version: 3
  Type: Membership Report (0x22)
  Header checksum: 0x2bd3 [correct]
  Num Group Records: 2
  * Group Record : 232.1.1.1 Mode Is Include
    Record Type: Mode Is Include (1)
    Aux Data Len: 0
    Num Src: 1
    Multicast Address: 232.1.1.1 (232.1.1.1)
    Source Address: 10.10.10.10 (10.10.10.10)
  * Group Record : 232.1.1.2 Mode Is Include
    Record Type: Mode Is Include (1)
    Aux Data Len: 0
    Num Src: 1
    Multicast Address: 232.1.1.2 (232.1.1.2)
    Source Address: 10.10.10.10 (10.10.10.10)
```

- Longer maximum response time for a query message. In IGMPv3, the maximum response time for the query message is extended from 25.5s (IGMPv2) to 3174.4s. Therefore, IGMPv3 is applicable to large-scale networks.
- Source filtering. With the source filter function, the host can receive or not receive the multicast data carrying the IP address of a specified multicast source. This function enables the device to better implement SSM and support the multiple-ISP scenario. IGMPv2 supports only ASM. The following uses different types of messages to explain the implementation of source filter.
 - Query messages

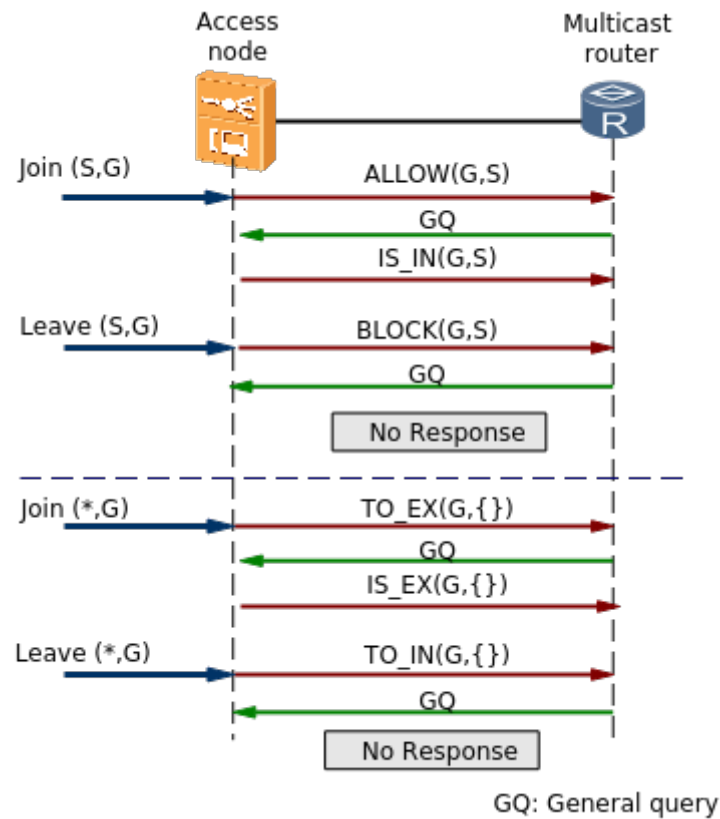
Message Type	Implementation of Source Filter
General query	The device sends this message to learn the reception status of an interface to "all" multicast groups. This is similar to the general query of IGMPv2.
Group-specific query	The device sends this message to learn the reception status of an interface to the multicast group with a specific address. This is similar to the group-specific query of IGMPv2.
Group-and-source-specific query	The device sends this message to learn the reception status of an interface to the multicast group with a specific group address and source address. This is a new message of IGMPv3.

- Report messages

Message Type	Implementation of Source Filter
IS_IN(G, S)	Reports the status. Indicates that the current mode of the group is the INCLUDE mode. This message is triggered when the device receives a query message. The source address list contains the source address S of the group.
TO_IN(G, S)	Changes the filter mode of the multicast group to the INCLUDE mode. The source address list contains a new source address S. TO_IN(G, {}) indicates leaving all sources of G and this message in this case is the same as the IGMPv2 leave message.
ALLOW(G, S)	Changes the source address list. This message is triggered when the source address changes. The source address contained in the record is the source address S that the system wishes to join.
BLOCK(G, S)	Changes the source address list. This message is triggered when the source address changes. The source address contained in the record is the source address S that the system does not wish to join.
IS_EX(G, S)	Reports the status. Indicates that the current mode of the group is the EXCLUDE mode. This message is triggered when the device receives a query message. The source address list contains the source address S that the group does not wish to join. IS_EX(G, {}) indicates that the device is interested in all sources of G and this message in this case is the same as the IGMPv2 join message. The device does not support the IS_EX message that contains an empty S.
TO_EX(G, S)	Changes the filter mode of the multicast group to the EXCLUDE mode. The source address list contains a new source address S that the device does not wish to join. TO_EX(G, {}) indicates joining all sources of G and this message in this case is the same as the IGMPv2 join message. The device supports the TO_EX message that contains an empty S.

The following figure shows an example of the report message application.

Figure 13-12 Program ordering behavior converted into IGMPv3 messages



IGMP Version Compatibility

The compatibility policies of the IGMP version on access devices distinguish between the network side and the user side.

The IGMP version on the network side is configured based on MVLAN. As shown in the following table, according to the IGMP version on the multicast router, the IGMP version on the device should be set to the recommended version to avoid incompatibility. Incompatibility may cause packet loss.

Multi cast Route r	MVLAN on Access Device	Interoperation Result
v1	v2/v3	Incompatible
v2	v2 (recommend ed)	Normal
v3	v2 (recommend ed)	Normal. The device can response the IGMPv3 query messages, and the multicast router can process the IGMPv2 join and leave messages.

Multi cast Route r	MVLAN on Access Device	Interoperation Result
v2	v3	The multicast router does not process IGMPv3 messages. Interoperation is normal only after the IGMP version on the device is downgraded to v2. Before the downgrade, packet loss may occur.
v3	v3 (recommend ed)	Normal

The IGMP version on the user side can be configured based on multicast users. As shown in the following table, according to the IGMP version on the terminal, the IGMP version on the device should be set to the recommended version to avoid incompatibility. Incompatibility may cause packet loss.

Termi nal	Multicast User on Access Device	Interoperation Result
v1	v2/v3/v3- forced	Incompatible
v2	v2 (recommend ed)	Normal
v3	v2	The device does not process IGMPv3 messages. Interoperation is normal only after the IGMP version on the terminal is downgraded to v2 (the terminal can be downgraded by enabling the function of periodically sending query messages to offline users). Before the downgrade, packet loss may occur.
v2	v3 (recommend ed)	The terminal does not process IGMPv3 messages. Interoperation is normal only after the IGMP version on the device is downgraded to v2. Even after downgraded to IGMPv2, the device can still identify the IGMPv3 messages sent from other terminals. This ensures greater compatibility of the device. In normal application scenarios, the terminal is usually the active initiating party. The IGMP version on the device can be seamlessly downgraded without packet loss.

Terminal	Multicast User on Access Device	Interoperation Result
v3	v3 (recommended)	Normal
v2	v3-forced	Incompatible
v3	v3-forced	The device drops IGMPv2 messages without processing them. Therefore, the device will not be downgraded to v2 but stays in v3.

13.4.1.2 IGMP Mode

MVLAN-based IGMP modes include IGMP proxy and IGMP snooping.

IGMP Proxy

IGMP proxy is a mode in which the device in a tree topology does not set up a route to forward multicast messages, but only acts as a proxy for multicast protocol messages. Details are as follows:

- From the perspective of a terminal, the device serves as a multicast router that implements the functions of the router in the IGMP protocol. Specifically, the device consistently functions as an IGMP querier (not supporting querier election for security concerns) on the user-side network. The device receives and terminates the join and leave messages of all multicast users, and duplicates the multicast program to only the interested multicast users according to the maintained group membership table.

Table 13-6 Structure of the group membership table OLT

Group Filter Mode	Index	Online Member
ASMSSM ASM ONLY	VLAN+GIP	Multicast user list (such as multicast user 1 and multicast user 2)
SSM ONLY	VLAN+GIP+SIP	Multicast user list (such as multicast user 1 and multicast user 2)

- From the perspective of a multicast router, the device serves as a multicast group member that implements the functions of the host in the IGMP protocol. According to the changes (addition or deletion) of the record in the group membership table, the device sends the join message or leave message of a program to the upper layer through the multicast uplink port. In addition, the device responds to the queries of the multicast router according to the status of the group membership table.

IGMP proxy effectively reduces the quantity of IGMP messages exchanged on the network side and therefore lessens the load of multicast routers. It is configurable on the device whether to send the IGMP general query to all multicast users or to only interested multicast users.

NOTE

After a multicast user orders a program for the first time, the system generates a value, indicating the random interval. The value ranges from 0 to the difference between the interval for the general query and maximum response time to the general query. After the random interval, the system sends the first general query message to the multicast user.

IGMP Snooping

IGMP snooping enables the device to listen to the multicast protocol packets transmitted between the router and hosts and set up a Layer 2 forwarding table for multicast data packets. This manages and controls multicast data packet forwarding so that the multicast data packets can be sent only to specified recipients. IGMP snooping features:

- Low bandwidth requirements, facilitating separate host charging.
- Separate data forwarding for each VLAN, improving data security.

IGMP snooping has two types:

- IGMP transparent snooping

It is a snooping function without proxy. The device selects the proxy, snooping, or snooping with proxy function based on MVLANS.

Before enabling IGMP transparent snooping, run the **igmp query-proxy**, **igmp report-proxy**, and **igmp leave-proxy** commands to disable proxy for query, report, and leave packets, respectively.

IGMP transparent snooping enables the device to process IGMP messages as follows:

- Query message

After receiving the general query message and group-specific query message from the multicast uplink port, the device forwards the network-side query message to the user.

NOTE

- To ensure that the multicast user responds to the query in a timely manner, the maximum response time configured on the device must be shorter than that configured on the upper-layer multicast router.
 - The network-side IGMP version of the device is not affected by the multicast router.
- Join/Leave message

The device transparently transmits all the join/leave message received from the multicast user to the MVLANS.

NOTE

The IGMPv3 message may contain multiple group records that match different MVLANS. In this case, the device segments the message and transparently transmits the segmented messages to the corresponding MVLANS.

- IGMP snooping with proxy

In IGMP upstream transmission, IGMP snooping with proxy is the same as IGMP proxy; in IGMP downstream transmission, however, IGMP snooping with proxy does not suppress the query message as IGMP proxy does.

IGMP snooping with proxy enables the device to process IGMP messages as follows:

- Query message

After receiving the query message from the multicast uplink port, the device reconstructs and sends the query message to the user (default mode, query proxy enabled based on MVLANS) or forwards the query message (disabling query proxy based on MVLANS). It also responds to the multicast router's query according to its multicast group membership table.

 NOTE

- Like IGMP proxy, the network-side IGMP version of the device is affected by the multicast router.
- Determine whether to enable query proxy. For details, see the "Usage Guidelines" of the **igmp query-proxy** command.

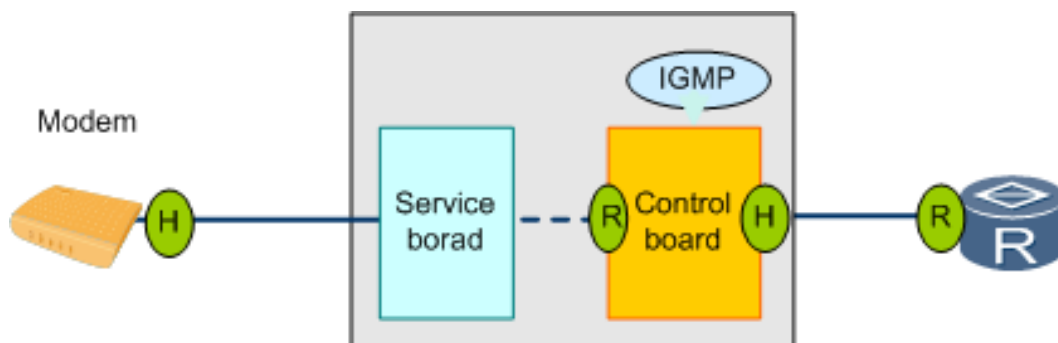
- Join/Leave message

The device sends only the first join message from the multicast users to the MVLAN. The device sends only the last leave message from the multicast users to the MVLAN.

13.4.1.3 IGMP Framework on the Device

Architecture of the IGMP Protocol Stack

Figure 13-13 Architecture of the IGMP protocol stack



R represents the router functions of the IGMP protocol, and H represents the host functions of the IGMP protocol.

In the architecture of the IGMP protocol stack, the operation on the control board and the network side is based on MVLAN, and the operation on the user side is based on multicast user (to ensure that the control planes of the users do not interfere with each other).

13.4.2 PIM

13.4.2.1 Introduction

Purpose

A multicast network requires multicast protocols to replicate and forward multicast data. PIM is a widely used intra-domain multicast protocol that builds MDTs to transmit multicast data between routers in the same domain.

PIM can create multicast routing entries on demand, forward packets based on multicast routing entries, and dynamically respond to network topology changes.

Definition

PIM is a multicast routing protocol that uses unicast routing protocols to forward data, but PIM is independent of any specific unicast routing protocols.

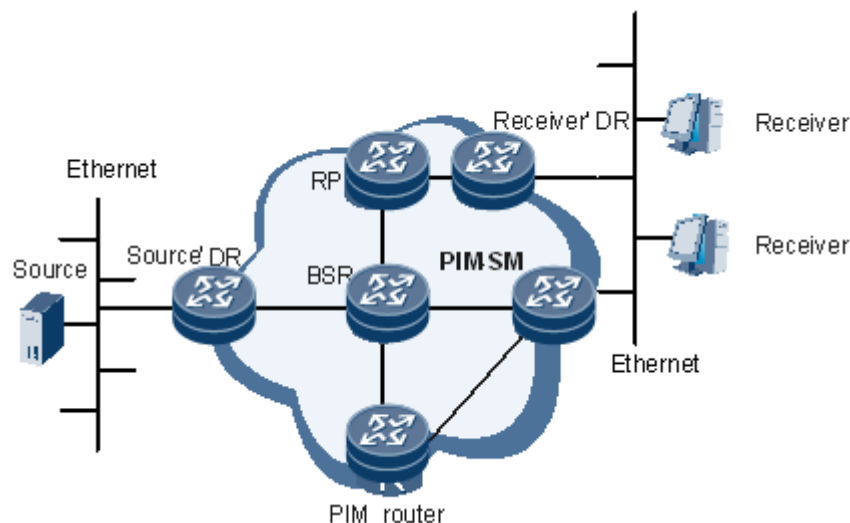
Concurrently, the MA5800 supports PIM-SM (used in an IPv4 network) and PIM-SSM (used in IPv4 and IPv6 networks).

Table 13-7 PIM implementation modes

Protocol	Full Name	Model	Deployment Scenario
PIM-SM	Protocol Independent Multicast-Sparse Mode	ASM model	Large-scale networks on which multicast data receivers are sparsely distributed.
PIM-SSM	Protocol Independent Multicast-Source-Specific Multicast	SSM model	Networks on which multicast data receivers can learn source locations before they join multicast groups and require multicast data from specific multicast sources.

Concepts

This section provides basic PIM concepts. [Figure 13-14](#) shows a typical PIM network.

Figure 13-14 PIM network

- **PIM device**

A router that runs PIM is called a PIM device. A router interface on which PIM is enabled is called a PIM interface.

- **Designated router**

A designated router (DR) can be a multicast source's DR or a receiver's DR.

- A multicast source's DR is a PIM device directly connected to a multicast source and is responsible for sending Register messages to an RP.
- A receiver's DR is a PIM device directly connected to receiver's hosts and is responsible for sending Join messages to an RP and forwarding multicast data to receiver's hosts.

 NOTE

The MA5800 can only be the receiver's DR and cannot be the multicast source's DR.

- **RP**

An RP is the forwarding core in a PIM-SM domain, used to process hosts' join requests and multicast source's registration requests. An RP constructs an MDT with the RP at the root and creates (S, G) entries to transmit multicast data to hosts. All routers in the PIM-SM domain need to know the RP's location. RP contains static and dynamic RPs.

Table 13-8 RP classifications

RP Type	Implementation	Deployment Scenario	Precautions
Static RP	A static RP is manually configured. If a static RP is used, the same RP address must be configured on all PIM devices in the same domain as the RP.	Static RPs are recommended on small-/medium-sized networks because a small-/medium-sized network is stable and has low forwarding requirements for an RP.	To use a static RP, ensure that all PIM devices, including the RP, have the same RP and multicast group address range information.
Dynamic RP	A dynamic RP is elected among C-RPs in the same PIM domain. The BSR sends Bootstrap messages to collect all C-RP information as an RP-Set, and advertises the RP-Set information to all PIM devices in the domain. Then, all the PIM devices use the same RP-Set information and follow the same rules to elect an RP. After the elected RP fails, the other C-RPs start an election process again to elect a new RP.	Dynamic RPs can be used on large-scale networks to improve network reliability and maintainability. • If multiple multicast sources are densely distributed on the network, configuring core devices close to the multicast sources as C-RPs is recommended. • If multiple users are densely distributed on the network, configuring core devices close to the users as C-RPs is recommended.	To use a dynamic RP, you must configure a BSR that dynamically advertises group-to-RP mapping information.

 NOTE

The MA5800 supports only static RPs and does not support dynamic RPs or BSR.

- **BSR**

A BSR on a PIM-SM network collects RP information, summarizes that information into an RP-Set (group-RP mapping database), and advertises the RP-Set to the entire PIM-SM network.

A network can have only one BSR but can have multiple C-BSRs. If a BSR fails, a new BSR is elected from the C-BSRs.

- **RPT**

An RPT is an MDT with an RP at the root and group members at the leaves.

- **SPT**

An SPT is an MDT with the multicast source at the root and group members at the leaves.

13.4.2.2 PIM-SM

PIM-SM implements P2MP data transmission on large-scale networks on which multicast data receivers are sparsely distributed. PIM-SM forwards multicast data only to network segments with active receivers that have required the data.

PIM-SM assumes that no host wants to receive multicast data, so PIM-SM sets up an MDT only after a host requests multicast data and then sends the data to the host along the MDT.

Concepts

For details about PIM-SSM, see [Concepts](#).

Implementation

The multicast data forwarding process in a PIM-SM domain is as follows:

1. Neighbor discovery

Each PIM device in a PIM-SM domain periodically sends Hello messages to all other PIM devices in the domain to discover PIM neighbors and maintain PIM neighbor relationships.

By default, a PIM device permits other PIM control messages or multicast messages from a neighbor, irrespective of whether the PIM device has received Hello messages from the neighbor. However, if a PIM device has the neighbor check function, the PIM device permits other PIM control messages or multicast messages from a neighbor only after the PIM device has received Hello messages from the neighbor.

2. DR election

PIM devices exchange Hello messages to elect a DR on a shared network segment. The receiver's DR is the only multicast data forwarder on a shared network segment. The source's DR is responsible for forwarding multicast data received from the multicast source along an MDT.

 NOTE

The MA5800 does not support DR election. It supports DR by default.

3. RP discovery

An RP is the forwarding core in a PIM-SM domain. An RP forwards multicast data over the entire network.

 NOTE

The MA5800 supports only static RPs. It is specified by configuring the same RP address on all PIM devices in a network and therefore it does not need election.

4. RPT setup

PIM-SM assumes that no hosts want to receive multicast data, so PIM-SM sets up an RPT only after a host requests multicast data, and then sends the data from the RP to the host along the RPT.

5. SPT switchover

A multicast group in a PIM-SM domain is associated with only one RP and one RPT. All multicast data packets are forwarded by the RP. The path along which the RP forwards multicast data may not be the shortest path from the multicast source to receivers. The load of the RP increases when the multicast traffic volume increases. If the multicast data forwarding rate exceeds a configured threshold, an RPT-to-SPT switchover can be implemented to reduce the burden on the RP.

NOTE

The MA5800 supports packet forwarding upon receiving the first packet (equivalent to threshold 0), and does not support threshold-crossing switchover (switchover is performed when the traffic reaches an extent).

If a network problem occurs, the Assert mechanism can be used to guarantee that multicast data is transmitted properly. If multiple multicast data forwarders exist on a network segment, each multicast packet is repeatedly sent across the network segment, generating redundant multicast data. To resolve this issue, the Assert mechanism can be used to select a unique multicast data forwarder on a network segment.

The detailed PIM-SM implementation process is as follows:

Neighbor Discovery

Each PIM-enabled interface on a PIM device sends Hello messages. A multicast packet that carries a Hello messages has the following features:

- The destination address is 224.0.0.13, indicating that this packet is destined for all PIM devices on the same network segment as the interface that sends this packet.
- The source address is an interface address.
- The TTL value is 1, indicating that the packet is sent only to neighbor interfaces.

Hello messages are used to discover neighbors, adjust protocol parameters, and maintain neighbor relationships.

- Discovering PIM neighbors

All PIM devices on the same network segment must receive multicast packets with the destination address 224.0.0.13. Directly connected multicast devices can then learn neighbor information from the received Hello messages.

- Adjusting protocol parameters

A Hello message carries the following protocol parameters:

- DR_Priority: priority used by each device to elect a DR. The higher a device's priority is, the higher the probability that the device will be elected as the DR.
- Holdtime: timeout period during which the neighbor remains in the reachable state.
- LAN_Delay: delay for transmitting a Prune message on the shared network segment.
- Override-Interval: interval carried in a Hello message for overriding a Prune message.

- Maintaining neighbor relationships

PIM devices periodically exchange Hello messages. If a PIM device does not receive a new Hello messages from its PIM neighbor within the Holdtime, the device considers the neighbor unreachable and deletes the neighbor from its neighbor list.

PIM neighbor relationship changes cause the multicast topology to change. If an upstream or a downstream neighbor is unreachable, multicast routes re-converge, and the MDT is transferred.

RPT Setup

Figure 13-15 RPT setup and data forwarding processes

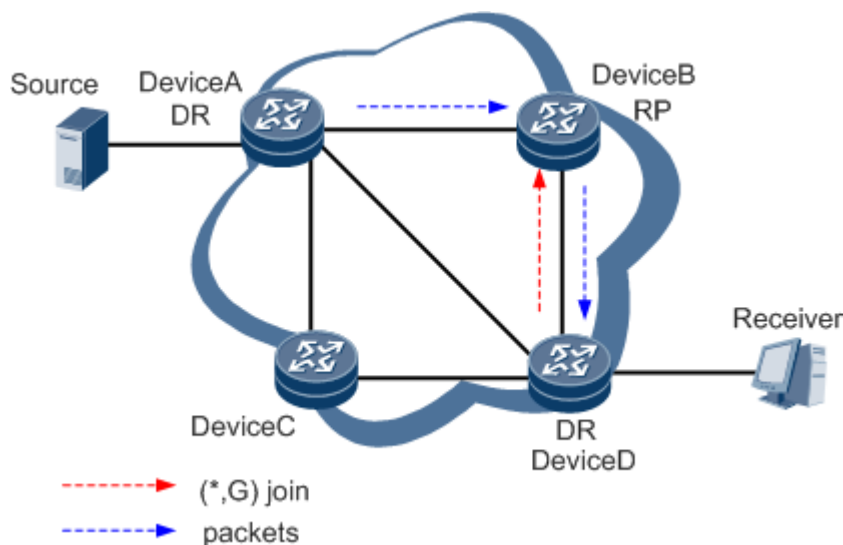


Figure 13-15 shows the RPT setup and data forwarding processes.

- When a multicast source sends the first multicast packet of a multicast group to its DR, the source's DR encapsulates the multicast packet in a Register message and unicasts the Register message to the RP. The RP creates an (S, G) entry to register the multicast source information.
- When a receiver joins a multicast group through IGMP, the receiver's DR sends a Join message to the RP. A (*, G) entry is then created on each hop, and an RPT is created.
- When a receiver joins a multicast group and a multicast source becomes active simultaneously, the multicast source's DR encapsulates the multicast packet in a Register message and unicasts the Register message to the RP. The RP then forwards the multicast data along the RPT to group members.

The RPT implements on-demand multicast data forwarding, which reduces bandwidth usage by preventing unrequested data transmission.

NOTE

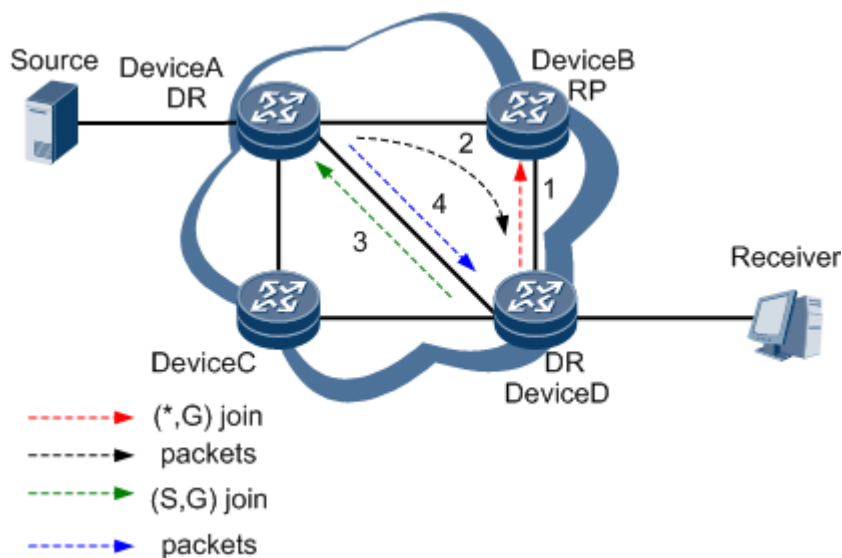
To reduce the RPT forwarding loads and improve multicast data forwarding efficiency, PIM-SM supports SPT switchover, allowing a multicast network to set up an SPT with the multicast source at the root. Then, the multicast source can send multicast data directly to receivers along the SPT.

SPT Switchover

In a PIM SM domain, a multicast group interacts with only one RP, and only one RPT is set up. If SPT switchover is not enabled, all multicast packets must be encapsulated in Register messages and then sent to the RP. After receiving the packets, the RP de-encapsulates them and forwards them along the RPT.

Since all multicast packets forwarded along the RPT are transferred by the RP, the RP may be overloaded when multicast traffic is heavy. To resolve this problem, PIM-SM allows the RP or the receiver's DR to trigger an SPT switchover.

Figure 13-16 SPT switchover triggered by the receiver's DR



An SPT switchover can be triggered by the RP or by the receiver's DR:

- SPT switchover triggered by the RP
Register messages sent from the source's DR are decapsulated by the RP, which then forwards multicast data along the RPT to group members. At the same time, the RP sends SPT Join messages to the source's DR to set up an SPT from the RP to the source.
After the SPT is set up and starts carrying multicast data packets, the RP stops processing Register messages. This frees the source's DR and RP from encapsulating and decapsulating packets. Multicast data is sent from the device directly connected to the multicast source to the RP along the SPT and then forwarded to group members along the RPT.
- SPT switchover triggered by the receiver's DR

- a. As shown in [Figure 13-16](#), multicast data is transmitted along the RPT. The receiver's DR (Device D) sends (*, G) Join messages to the RP. Multicast data is sent to receivers along the path source's DR (Device A) -> RP (Device B) -> receiver's DR (Device D).
- b. The receiver's DR periodically checks the forwarding rate of multicast packets. If the receiver's DR finds that the forwarding rate is greater than the configured threshold, the DR triggers an SPT switchover.
- c. The receiver's DR sends (S, G) Join messages to the source's DR. After receiving multicast data along the SPT, the receiver's DR discards multicast data received along the RPT and sends a Prune message to the RP to delete the receiver from the RPT. The switchover from the RPT to the SPT is complete.
- d. Multicast data is forwarded along the SPT. Specifically, multicast data is transmitted to receivers along the path multicast source's DR (Device A) -> receiver's DR (Device D).

An SPT is set up from the source to group members, and therefore subsequent packets may bypass the RP. The RPT may not be an SPT. After an SPT switchover is performed, delays in transmitting multicast data on the network are reduced.

If one source sends packets to multiple groups simultaneously and an SPT switchover policy is specified for a specified group range:

- Before an SPT switchover, these packets reach the receiver's DR along the RPT.
- After an SPT switchover, only the packets sent to the groups within the range specified in the SPT switchover policy are forwarded along the SPT. Packets sent to other groups are still forwarded along the RPT.

NOTE

By default, the RP performs an SPT switchover immediately after receiving the first Register message, and the receiver's DR performs an SPT switchover immediately after receiving the first multicast packet.

Assert

Either of the following conditions indicates other multicast forwarders are present on the network segment:

- A multicast packet fails the RPF check.
- The interface that receives the multicast packet is a downstream interface in the (S, G) entry on the local device.

If other multicast forwarders are present on the network segment, the PIM device starts the Assert mechanism.

The device sends an Assert message through the downstream interface. The downstream interface also receives an Assert message from a different multicast forwarder on the network segment. The destination address of the multicast packet in which the Assert message is encapsulated is 224.0.0.13. The source address of the packet is the downstream interface address. The TTL value of the packet is 1. The Assert message carries the route cost from the PIM device to the source or RP, priority of the used unicast routing protocol, and the group address.

The PIM device compares its information with the information contained in the message sent by its neighbor. This is called Assert election. The election rules are as follows:

1. The device that runs a higher priority unicast routing protocol wins.
2. If the devices have the same unicast routing protocol priority, the device with the smaller route cost to the source wins.
3. If the devices have the same priority and route cost, the device with the highest IP address for the downstream interface wins.

The device performs the following operations based on the Assert election result:

- If the device wins the election, the downstream interface of the device is responsible for forwarding multicast packets on the network segment. The downstream interface is called an Assert winner.
- If the device does not win the election, the downstream interface is prohibited from forwarding multicast packets and is deleted from the downstream interface list of the (S, G) entry. The downstream interface is called an Assert loser.

After Assert election is complete, only one upstream device that has a downstream interface exists on the network segment, and the downstream interface transmits only one copy of each multicast packet. The Assert winner then periodically sends Assert messages to maintain its status as the Assert winner. If the Assert loser does not receive any Assert messages from the Assert winner after the timer of the Assert loser expires, the loser re-adds downstream interfaces for multicast data forwarding.

13.4.2.3 PIM-SSM

Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) enables a user host to rapidly join a multicast group if the user knows a multicast source address. PIM-SSM sets up a shortest path tree (SPT) from a multicast source to a multicast group, while PIM-SM uses rendezvous points (RPs) to set rendezvous point trees (RPTs). Therefore, PIM-SSM implements a more rapid join function than PIM-SM.

Different from the any-source multicast (ASM) model, the SSM model does not need to maintain an RP, construct an RPT, or register a multicast source.

The SSM model is based on PIM-SM and IGMPv3. The procedure for setting up a multicast forwarding tree on a PIM-SSM network is similar to the procedure for setting up an SPT on a PIM-SM network. The receiver's DR, which knows the multicast source address, sends Join messages directly to the source so that multicast data streams can be sent to the receiver's designated router (DR).

Related Concepts

For details about PIM-SSM, see [Concepts](#).

Implementation

The process for forwarding multicast data in a PIM-SSM domain is as follows:

1. Neighbor Discovery

Each PIM device in a PIM-SSM domain periodically sends Hello messages to all other PIM devices in the domain to discover PIM neighbors and maintain PIM neighbor relationships.

By default, a PIM device permits other PIM control messages or multicast messages from a neighbor, irrespective of whether the PIM device has received Hello messages from the neighbor. However, if a PIM device has the neighbor check function, the PIM device permits other PIM control messages or multicast messages from a neighbor only after the PIM device has received Hello messages from the neighbor.

2. DR Election

PIM devices exchange Hello messages to elect a DR on a shared network segment. The receiver's DR is the only multicast data forwarder on the segment.

NOTE

The MA5800 does not support DR election. It supports DR by default.

3. SPT setup

Users on a PIM-SSM network can know the multicast source address and can, therefore, specify the source when joining a multicast group. After receiving a Report message from a user, the receiver's DR sends a Join message towards the multicast source to establish an SPT between the source and the user. Multicast data is then sent by the multicast source to the user along the SPT.

SPT establishment can be triggered by user join requests (both dynamic and static) and SSM-mapping.

The DR in an SSM scenario is valid only in the shared network segment connected to group members. The DR on the group member side sends Join messages to the multicast source, creates the (S, G) entry hop by hop, and then sets up an SPT.

If a network problem occurs, the Assert mechanism can be used to guarantee that multicast data is transmitted properly. If multiple multicast data forwarders exist on a network segment, each multicast packet is repeatedly sent across the network segment, generating redundant multicast data. To resolve this issue, the Assert mechanism can be used to select a unique multicast data forwarder on a network segment.

The detailed PIM-SSM implementation process is as follows:

Neighbor Discovery

Each PIM-enabled interface on a PIM device sends Hello messages. A multicast packet that carries a Hello messages has the following features:

- The destination address is 224.0.0.13, indicating that this packet is destined for all PIM devices on the same network segment as the interface that sends this packet.
- The source address is an interface address.
- The TTL value is 1, indicating that the packet is sent only to neighbor interfaces.

Hello messages are used to discover neighbors, adjust protocol parameters, and maintain neighbor relationships.

- Discovering PIM neighbors
All PIM devices on the same network segment must receive multicast packets with the destination address 224.0.0.13. Directly connected multicast devices can then learn neighbor information from the received Hello messages.
- Adjusting protocol parameters
A Hello message carries the following protocol parameters:
 - DR_Priority: priority used by each device to elect a DR. The higher a device's priority is, the higher the probability that the device will be elected as the DR.
 - Holdtime: timeout period during which the neighbor remains in the reachable state.
 - LAN_Delay: delay for transmitting a Prune message on the shared network segment.
 - Override-Interval: interval carried in a Hello message for overriding a Prune message.
- Maintaining neighbor relationships
PIM devices periodically exchange Hello messages. If a PIM device does not receive a new Hello messages from its PIM neighbor within the Holdtime, the device considers the neighbor unreachable and deletes the neighbor from its neighbor list.

PIM neighbor relationship changes cause the multicast topology to change. If an upstream or a downstream neighbor is unreachable, multicast routes re-converge, and the MDT is transferred.

Assert

Either of the following conditions indicates other multicast forwarders are present on the network segment:

- A multicast packet fails the RPF check.
- The interface that receives the multicast packet is a downstream interface in the (S, G) entry on the local device.

If other multicast forwarders are present on the network segment, the PIM device starts the Assert mechanism.

The device sends an Assert message through the downstream interface. The downstream interface also receives an Assert message from a different multicast forwarder on the network segment. The destination address of the multicast packet in which the Assert message is encapsulated is 224.0.0.13. The source address of the packet is the downstream interface address. The TTL value of the packet is 1. The Assert message carries the route cost from the PIM device to the source or RP, priority of the used unicast routing protocol, and the group address.

The PIM device compares its information with the information contained in the message sent by its neighbor. This is called Assert election. The election rules are as follows:

1. The device that runs a higher priority unicast routing protocol wins.

2. If the devices have the same unicast routing protocol priority, the device with the smaller route cost to the source wins.
3. If the devices have the same priority and route cost, the device with the highest IP address for the downstream interface wins.

The device performs the following operations based on the Assert election result:

- If the device wins the election, the downstream interface of the device is responsible for forwarding multicast packets on the network segment. The downstream interface is called an Assert winner.
- If the device does not win the election, the downstream interface is prohibited from forwarding multicast packets and is deleted from the downstream interface list of the (S, G) entry. The downstream interface is called an Assert loser.

After Assert election is complete, only one upstream device that has a downstream interface exists on the network segment, and the downstream interface transmits only one copy of each multicast packet. The Assert winner then periodically sends Assert messages to maintain its status as the Assert winner. If the Assert loser does not receive any Assert messages from the Assert winner after the timer of the Assert loser expires, the loser re-adds downstream interfaces for multicast data forwarding.

13.4.2.4 PIM Control Messages

PIM devices exchange control messages to implement multicast routing. A PIM control message is encapsulated in an IP packet, as shown in [Figure 13-17](#).

Figure 13-17 Encapsulation format of a PIM control message



- The protocol type field is 103.
- The destination address identifies a receiver. The destination address can be either a unicast address or a multicast address.

PIM Control Message Types

All PIM control messages use the same header format, as shown in [Figure 13-18](#).

Figure 13-18 Header format of a PIM protocol message



Table 13-9 Fields in a PIM control message

Field	Description
Version	PIM version The value is 2.
Type	Message type: • 0: Hello • 1: Register • 2: Register-Stop • 3: Join/Prune • 5: Assert
Reserved	Reserved
Checksum	Checksum

Hello Messages

PIM devices periodically send Hello messages through all PIM interfaces to discover neighbors and maintain neighbor relationships.

In an IP packet that carries a Hello message, the source address is a local interface's address, the destination address is 224.0.0.13, and the TTL value is 1. The IP packet is transmitted in multicast mode.

Figure 13-19 Hello message format

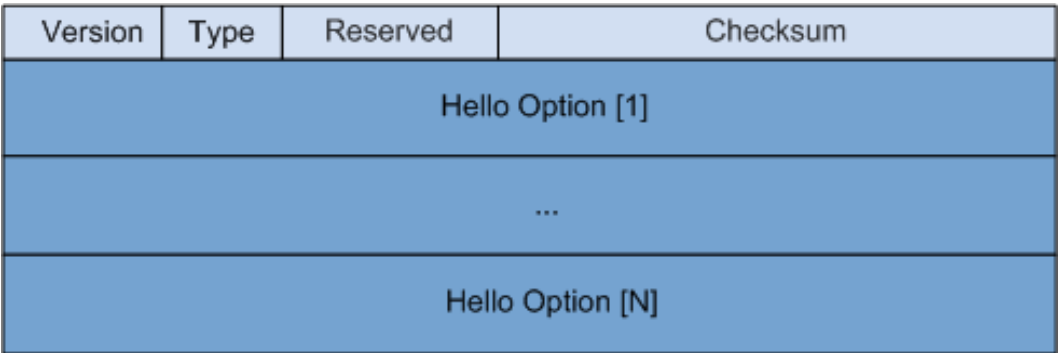


Figure 13-20 Hello Option field format

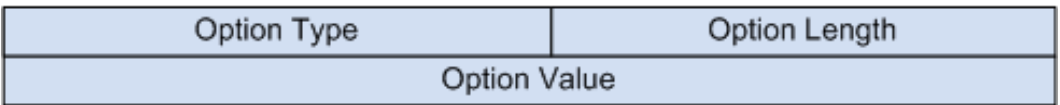


Table 13-10 Fields in a Hello message

Field	Description
Type	Message type The value is 0.
Reserved	Reserved The field is set to 0 when the message is sent and is ignored when the message is received.
Checksum	Checksum
Option Type	Parameter type Valid values of this field are listed in Table 1-13.
Option Length	Length of the Option Value field
Option Value	Parameter value

Table 13-11 Valid values of the Option Type field

Option Type	Option Value
1	Holdtime: timeout period during which a neighbor remains in the reachable state If a device does not receive any Hello message during the timeout period, the device considers its neighbor unreachable.
2	The field consists of the following parts: • LAN Prune Delay: delay before transmitting Prune messages on a shared network segment • Interval: interval for overriding a Prune message • T: capability of suppressing Join messages
19	DR Priority: priority of a device interface, used to elect a designated router (DR) The higher a device interface's priority, the higher the probability the device interface becomes a DR.
20	Generation ID: a random number, indicating neighbor status If the neighbor status changes, the random number is updated. When a device detects that the Hello messages received from an upstream device contain different Generation ID values, the device considers the upstream neighbor Down or the status of the upstream neighbor has changed.

Option Type	Option Value
21	State Refresh Capable: interval for refreshing neighbor status
22	Bidirectional Capable PIM-Hello: If a message sent by a device contains this parameter, this device is capable of Bidirectional Protocol Independent Multicast (BIDIR-PIM). The length of the Option Value field is 0.
24	Address List: secondary address list of PIM interfaces

Register Messages

 NOTE

Register messages are used only in PIM-SM.

When a multicast source becomes active on a PIM-SM network, the source's DR sends a Register message to register with the rendezvous point (RP).

In an IP packet that carries a Register message, the source address is the address of the source's DR, and the destination address is the RP's address. The message is transmitted in unicast mode.

Figure 13-21 Register message format

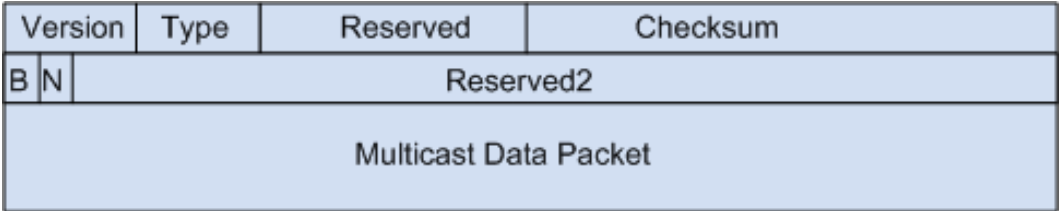


Table 13-12 Fields in a Register message

Field	Description
Type	Message type The value is 1.
Reserved	The field is set to 0 when the message is sent and is ignored when the message is received.
Checksum	Checksum
B	Border bit
N	Null-Register bit

Field	Description
Reserved2	Reserved. The field is set to 0 when the message is sent and is ignored when the message is received.
Multicast data packet	The source's DR encapsulates the received multicast data in a Register message and sends the message to the RP. After decapsulating the message, the RP learns the (S, G) information of the multicast data packet.

A multicast source can send data to multiple groups, and therefore a source's DR must send Register messages to the RP of each target multicast group. A Register message is encapsulated only in one multicast data packet, so the packet carries only one copy of (S, G) information.

In the register suppression period, a source's DR sends Null-Register messages to notify the RP of the source's active state. A Null-Register message contains only an IP header, including the source address and group address. After the register suppression times out, the source's DR encapsulates a Register message into a multicast data packet again.

Register-Stop Messages

 NOTE

Register-Stop messages are used only in PIM-SM.

On a PIM-SM network, an RP sends Register-Stop messages to a source's DR in the following conditions:

- Receivers stop requesting a multicast group's data from the RP.
- The RP stops serving a multicast group.
- Multicast data has been switched from a rendezvous point tree (RPT) to a shortest path tree (SPT).

After receiving a Register-Stop message, a source's DR stops using the Register message to encapsulate multicast data packets and enters the register suppressed state.

In an IP packet that carries a Register-Stop message, the source address is the RP's address, and the destination address is the source DR's address. The message is transmitted in unicast mode.

Figure 13-22 Register-Stop message format

Version	Type	-
Group Address		
Source Address		

Table 13-13 Fields in a Register-Stop message

Field	Description
Type	Message type The value is 2.
Group Address	Multicast group address
Source Address	Multicast source address

An RP can serve multiple groups, and a group can receive data from multiple sources. Therefore, an RP may simultaneously perform multiple (S, G) registrations.

A Register-Stop message carries only one copy of the (S, G) information. When an RP sends a Register-Stop message to a source's DR, the RP can terminate only one (S, G) registration.

After receiving the Register-Stop message carrying the (S, G) information, the source's DR stops encapsulating (S, G) packets. The source still uses Register messages to encapsulate packets and send the packets to other groups.

Join/Prune Messages

A Join/Prune message can contain both Join messages and Prune messages. A Join/Prune message that contains only a Join message is called a Join message. A Join/Prune message that contains only a Prune message is called a Prune message.

- When a PIM device is not required to send data to its downstream interfaces, the PIM device sends Prune messages through its upstream interfaces to instruct upstream devices to stop forwarding packets to the network segment on which the PIM device resides.
- When a receiver starts to require data from a PIM-SM network, the receiver's DR sends a Join message through the reverse path forwarding (RPF) interface towards the RP to instruct the upstream neighbor to forward packets to the receiver. The Join message is sent in the upstream direction hop by hop to set up an RPT.
- When an RP triggers an SPT switchover, the RP sends a Join message through the RPF interface connected to the source to instruct the upstream neighbor to forward packets to the network segment. The Join message is sent in the upstream direction hop by hop to set up an SPT.
- When a receiver's DR triggers an SPT switchover, the DR sends a Join message through the RPF interface connected to the source to instruct the upstream neighbor to forward packets to the network segment. The Join message is sent in the upstream direction hop by hop to set up an SPT.
- A PIM network segment may be connected to a downstream interface and multiple upstream interfaces. After an upstream interface sends a Prune message, if other upstream interfaces still require multicast packets, these

interfaces must send Join messages within the override-interval. Otherwise, the downstream interfaces responsible for forwarding packets on the network segment do not perform the prune action.

 NOTE

- If PIM is enabled on the interfaces of user-side routers, a receiver' DR is elected, and outbound interfaces are added to the PIM DR's outbound interface list. The PIM DR then sends Join messages to the RP.
- If PIM is not enabled on the interfaces of the user-side routers, no receiver' DR is elected, and outbound interfaces are added to the IGMP querier's outbound interface list. The IGMP sends Join messages to the RP.

In an IP packet that carries a Join/Prune message, the source address is a local interface's address, the destination address is 224.0.0.13, and the TTL value is 1. The message is transmitted in multicast mode.

Figure 13-23 Join/Prune messages on a PIM shared network segment

Version	Type	-	
Upstream Neighbor Address			
-	Number of Groups(N)	Holdtime	
Group J/P Record [1]			
...			
Group J/P Record [N]			

Figure 13-24 Format of the Group J/P Record field

Group Address [1]	
Number of Joined Sources (J)	Number of Pruned Sources (P)
Joined Source Address [1]	
...	
Joined Source Address [J]	
Pruned Source Address [1]	
...	
Pruned Source Address [P]	

Table 13-14 Fields in a Join/Prune message

Field	Description
Type	Message type The value is 3.
Upstream Neighbor Address	Upstream neighbor's address, that is, the address of the downstream interface that receives the Join/ Prune message and performs the Join or Prune action
Number of Groups	Number of groups contained in the message
Holdtime	Duration (in seconds) that an interface remains in the Join or Prune state
Group Address	Group address
Number of Joined Sources	Number of sources that the device joins
Number of Pruned Sources	Number of sources that the device prunes
Joined Source Address	Address of the source that the device joins
Pruned Source Address	Address of the source that the device prunes

Assert Messages

On a shared network segment, if a PIM device receives an (S, G) packet from the downstream interface of the (S, G) or (*, G) entry, it indicates that other forwarders exist on the network segment. The PIM device then sends an Assert message through the downstream interface to participate in the forwarder election. The device that fails in the forwarder election stops forwarding multicast packets through the downstream interface.

In an IP packet that carries an Assert message, the source address is a local interface's address, the destination address is 224.0.0.13, and the TTL value is 1. The packet is transmitted in multicast mode.

Figure 13-25 Assert message format

Version	Type	-
Group Address		
Source Address		
R	Metric Preference	
Metric		

Table 13-15 Fields in an Assert message

Field	Description
Type	Message type The value is 5.
Group Address	Group address
Source address	This field is a multicast source address if a unique forwarder is elected for (S, G) entries, and this field is 0 if a unique forwarder is elected for (*, G) entries.
R	RPT bit This field is 0 if a unique forwarder is elected for (S, G) entries, and this field is 1 if a unique forwarder is elected for (*, G) entries.
Metric Preference	Priority of the unicast path to the source address If the R field is 1, this field indicates the priority of the unicast path to the RP.
Metric	Cost of the unicast route to the source address If the R field is 1, this field indicates the cost of the unicast path to the RP.

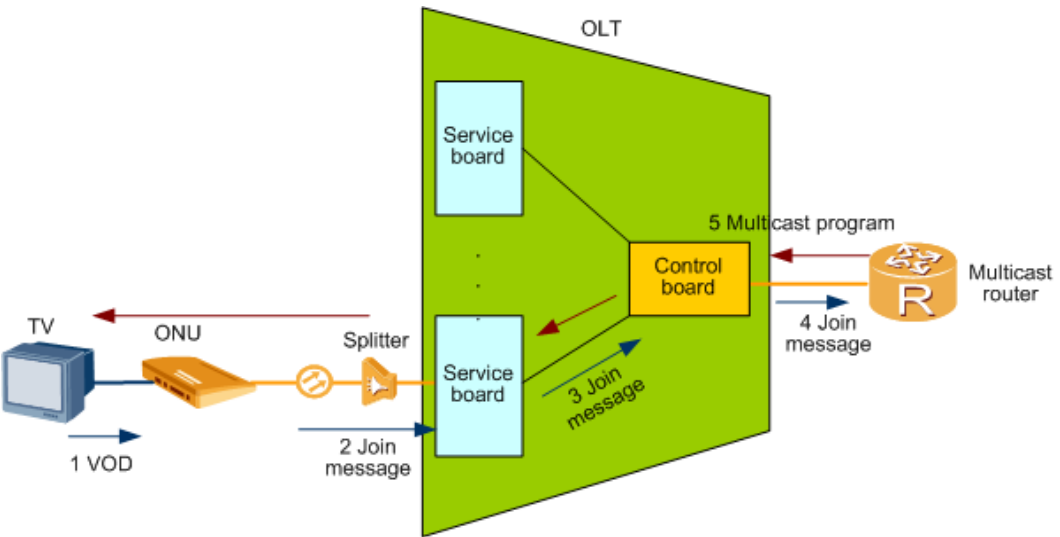
13.4.3 Multicast Forwarding

13.4.3.1 Join Flow

This section considers IGMPv2 proxy as an example to describe the join flow.

Join Flow

Figure 13-26 Join flow



1. The multicast user switches a channel and sends a join message for demanding a new program GIP1.
2. After receiving the join message, the control board enters the IGMP protocol stack of the multicast user. After multicast control is implemented (for details, see "[13.4.5.3 Multicast CAC](#)"), the following group membership table is generated on the control board.

Index	Online Member
MVLAN1+GIP1	Multicast user 1

At the same time, the following multicast forwarding tables are generated on the control board and the service board (for details on how to map GIP1 to GMAC1, see "[Basic Concepts](#)").

Table 13-16 Multicast forwarding table on the control board

Index	Duplication Destination
MVLAN1+ GMAC1	Corresponding port on service board 1

Table 13-17 Multicast forwarding table on the service board

Index	Duplication Destination
MVLAN1+ GMAC1	User port 1

3. According to MVLAN1 corresponding to the program, the service board serves as the proxy of multicast user 1 and sends a join message to the control board.
4. The control board then sends a join message to the multicast router through the multicast upstream port of MVLAN1.
5. After receiving the multicast stream, the device first duplicates the stream to service board 1 according to the multicast forwarding table of the control board, and then duplicates the stream to user port 1 according to the multicast forwarding table of the service board.

 NOTE

Though the SVLAN of a multicast user is different from the MVLAN, the device can still implement the mapping to the MVLAN according to the multicast member configuration relationship. In this way, cross-VLAN multicast is supported without requiring additional configuration.

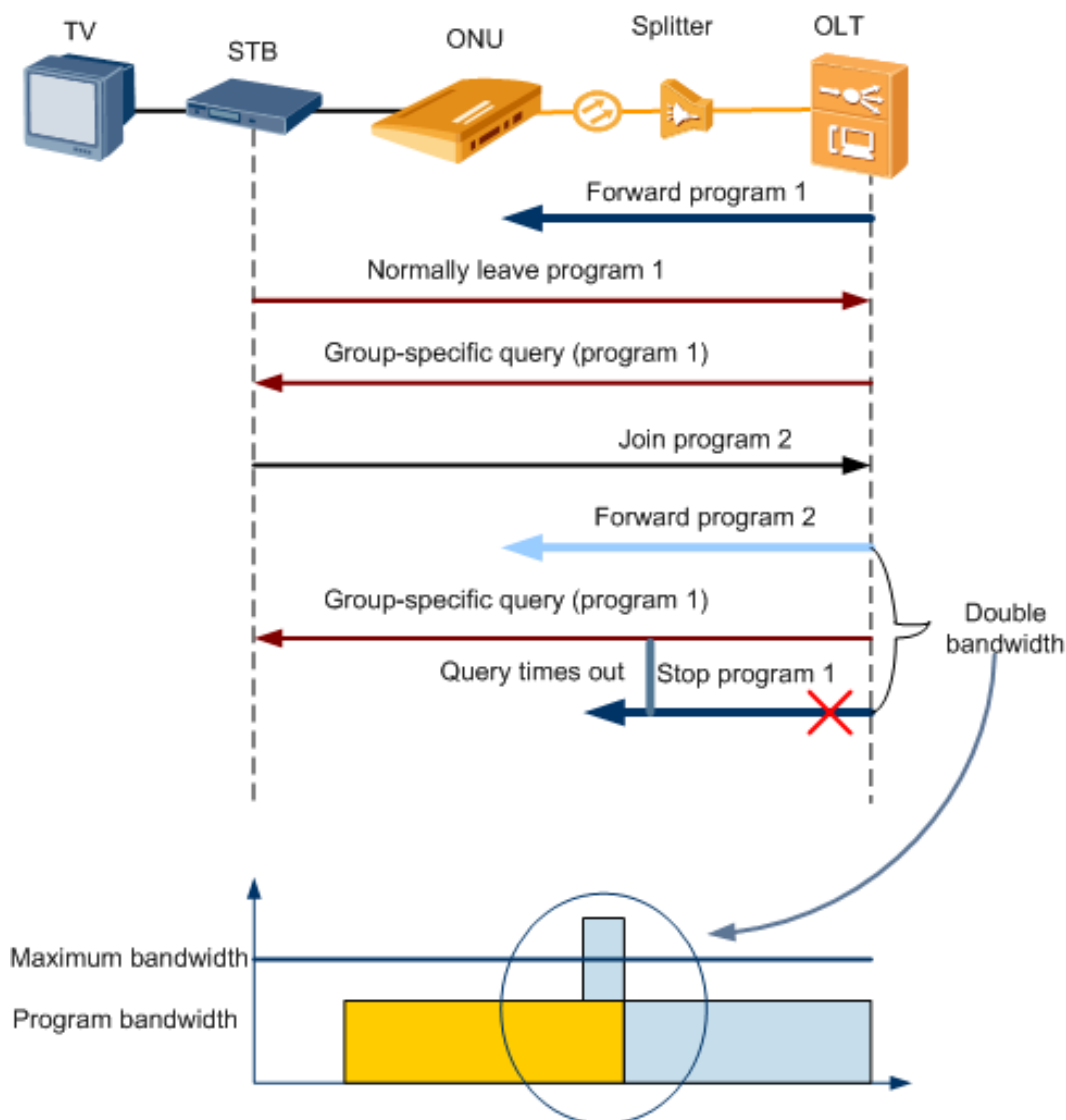
13.4.3.2 Leave Flow

Normal leave

As defined by IGMPv2, the router must send a group-specific query message after it receives the leave message from a host, and it considers that the host does not

need the data of the group until the query times out. The following figure illustrates the flow of a normal leave (the same to IGMPv3).

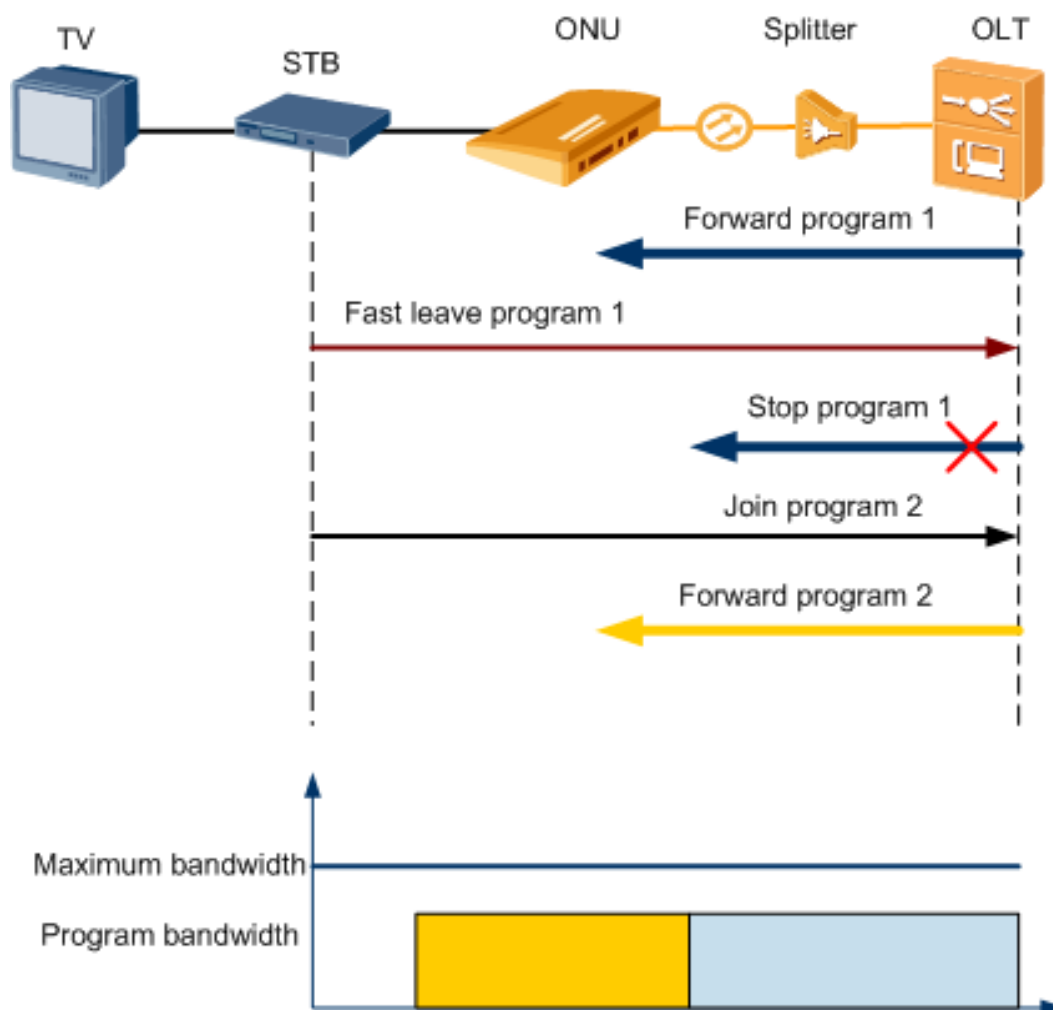
Figure 13-27 Flow of a normal leave



Two IGMP messages are transmitted in the case of a channel switching, one for leaving the original multicast group and one for joining the new multicast group. Therefore, traffic of two multicast groups exists on the subscriber line before the original multicast group is stopped. If the subscriber line does not reserve sufficient bandwidth for carrying the traffic of two multicast groups, traffic overflow (packet loss) will occur. For example, if video streams are carried, pixelation will occur.

Quick leave

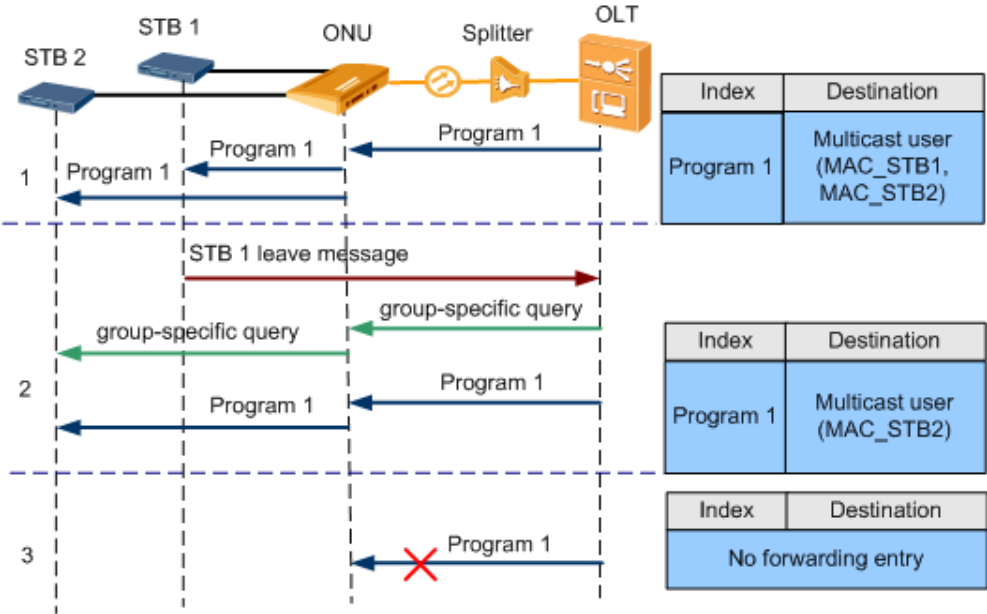
When the device receives the leave message from a multicast user, it immediately stops forwarding the messages of the user. The following figure illustrates the flow of a quick leave (the same to IGMPv3).

Figure 13-28 Flow of a quick leave

Quick leave based on the MAC address

When the device generates a multicast group membership table, it not only records the multicast user but also records the MAC addresses of the multicast group members of the multicast user. A maximum of eight MAC addresses are supported for each multicast user. When the device receives a leave message, it first deletes the MAC addresses in the multicast group membership table, and it stops forwarding the messages of the group only when all the MAC addresses of the multicast user are deleted. The following figure illustrates the flow of a quick leave based on the MAC address (the same to IGMPv3).

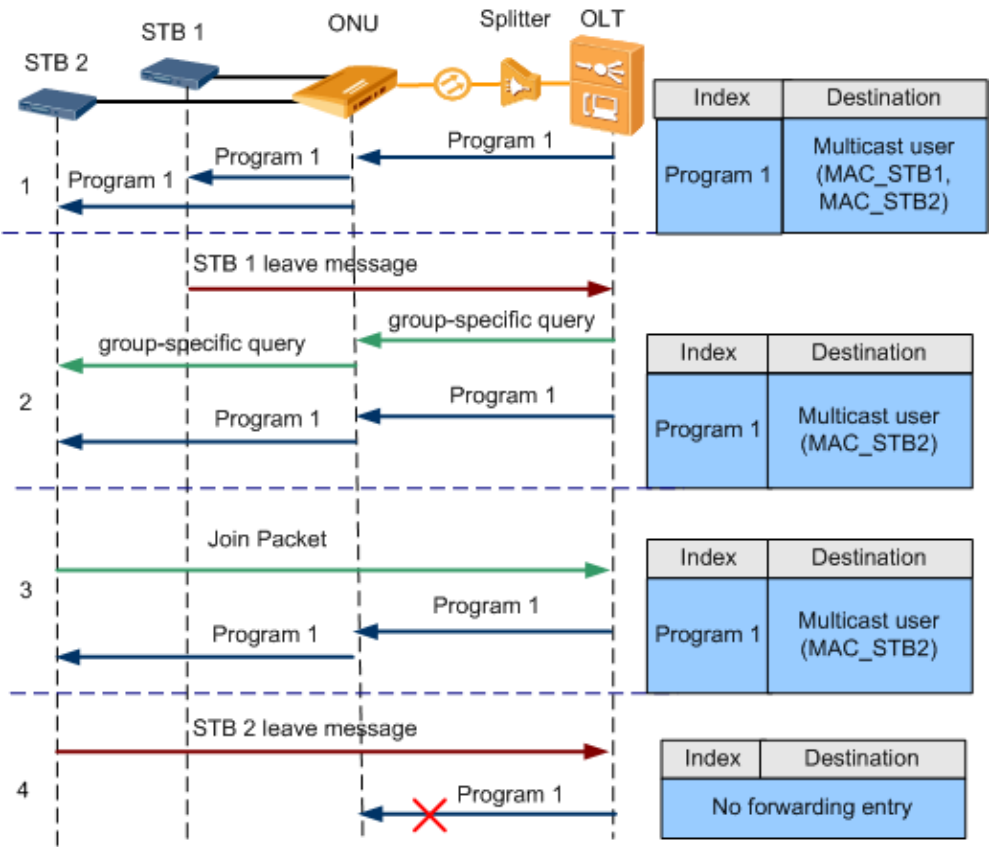
Figure 13-29 Flow of a quick leave based on the MAC address (STB2 has silently left.)



NOTE

The silent leaving of an STB indicates that the STB exceptionally leaves a program. For example, the STB is powered off or goes offline.

Figure 13-30 Flow of a quick leave based on the MAC address (STB2 is online.)



In summary, the three leave modes have their advantages and disadvantages. You can choose any of them according to actual needs and can set the leave mode for a multicast user.

Leave Mode	User-side Multi-STB Supported or Not	Bandwidth Occupation Time
Normal leave	Yes The STB quantity is not limited.	Aged upon reception of group-specific query
Quick leave	No	Released immediately
Quick leave based on the MAC address	Yes One multicast user supports a maximum of eight STBs at a time.	Released immediately

The following configurations are recommended and can be adopted by different users according to their home network topologies.

HG Function	STB Quantity	Reserved Bandwidth	Normal Leave	Quick Leave	Quick Leave Based on the MAC Address
No IGMP	One	Insufficient	-	√	√
		Sufficient	√	√	√
	Several	Insufficient	-	-	√ (Less than eight)
		Sufficient	√	-	√ (Less than eight)
IGMP snooping	One	Insufficient	-	√	√
		Sufficient	√	√	√
	Several	Insufficient	-	-	√ (Less than eight)
		Sufficient	√	-	√ (Less than eight)
IGMP proxy	One	Insufficient	-	√	√ (Not limited)
		Sufficient	√	√	√ (Not limited)
	Several	Insufficient	-	√	√ (Not limited)
		Sufficient	√	√	√ (Not limited)

Global Leave

As defined in TR101, the global leave message is an IGMP message with an all-zero group IP address, which indicates leaving all the groups.

- Network side

When the network topology changes, the device sends the global leave message to the upper-layer multicast router. After receiving the message, the upper-layer multicast router immediately sends the general query message, with the maximum response time set to the maximum time of responding to the group-specific query message. The device, after receiving the query message, responds to the upper-layer multicast router with the join message of the interested group. In this way, the multicast service can recover more quickly. Here, the network

topology change events include ring network switching, line up/down, and active/standby port switching in a protect group.

 NOTE

- If the device is interconnected with a network device that does not support the global leave message, multicast services may be interrupted during the network topology change. Therefore, it is recommended that the global leave function be manually disabled on the device.
- The device supports sending of the global leave message only in IGMPv2.
- User side

When the STB is powered on immediately after a sudden power-off, because the STB cannot remember the previously-watched program, the bandwidth of the previously-watched program and the program resources are released only after the general query ages.

If the STB supports the global leave function, the STB sends a global leave message after it is re-powered on. After receiving the message, the device sends a general query message, with the maximum response time set to the maximum time of responding to the group-specific query message. If the multicast user is a fast-leave or MAC-based fast-leave user, the device releases all program resources of this multicast user. If the user is a normal-leave user, the device sends a group-specific query message and releases the program resources after the group-specific query times out.

 NOTE

Only the IGMPv2 global leave messages can be processed.

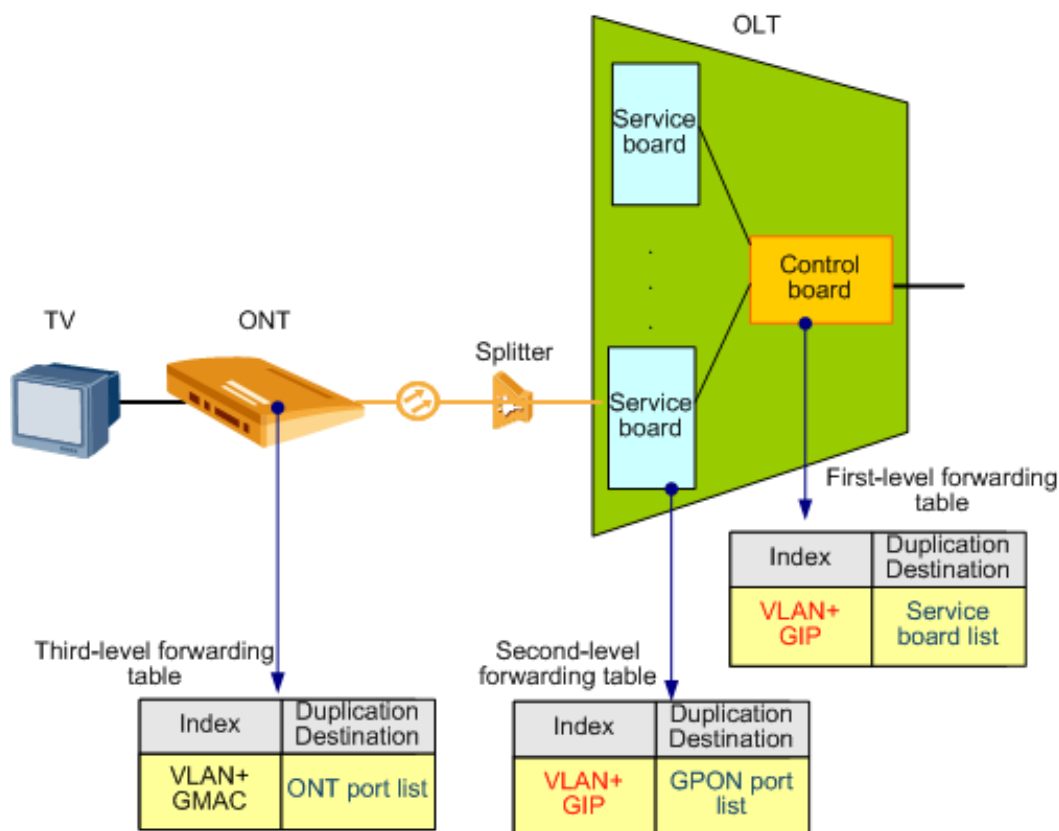
13.4.3.3 Forwarding Framework on the Device

 NOTE

The difference among the following forwarding tables is the first-level and second-level indexes. For example, the first-level and second-level index in the GPON multicast forwarding table (VLAN+GIP) is VLAN+GIP.

GPON Multicast Forwarding Table (VLAN+GIP) [OLT]

Figure 13-31 GPON multicast forwarding table (VLAN+GIP)



The OLT supports a distributed 2+1-level duplication architecture:

- The first-level duplication is implemented on the control board. By using the "VLAN+GIP" index, the control board duplicates multicast data to the service board interested in the multicast program in an as-per-requirement manner, effectively saving the backplane bandwidth.
- The second-level duplication is implemented on the service board. By using the "VLAN+GIP" index, the service board duplicates multicast data to the GPON port interested in the multicast program in an as-per-requirement manner, effectively saving the downstream bandwidth of the GPON port. Then the service board encapsulates and transmits the multicast data on the GPON port in the mode of multicast GEM port.
- The third-level duplication is implemented on the ONT. By using the "VLAN+GMAC" white list, the ONT filters out unneeded multicast data to avoid bandwidth overflow at the downstream ingress (ONT only supports that in olt-control mode). Then, by using the "VLAN+GMAC" index, the ONT duplicates the multicast data to the ONT ports in an as-per-requirement manner (only supports forwarding by using GMAC in snooping mode).

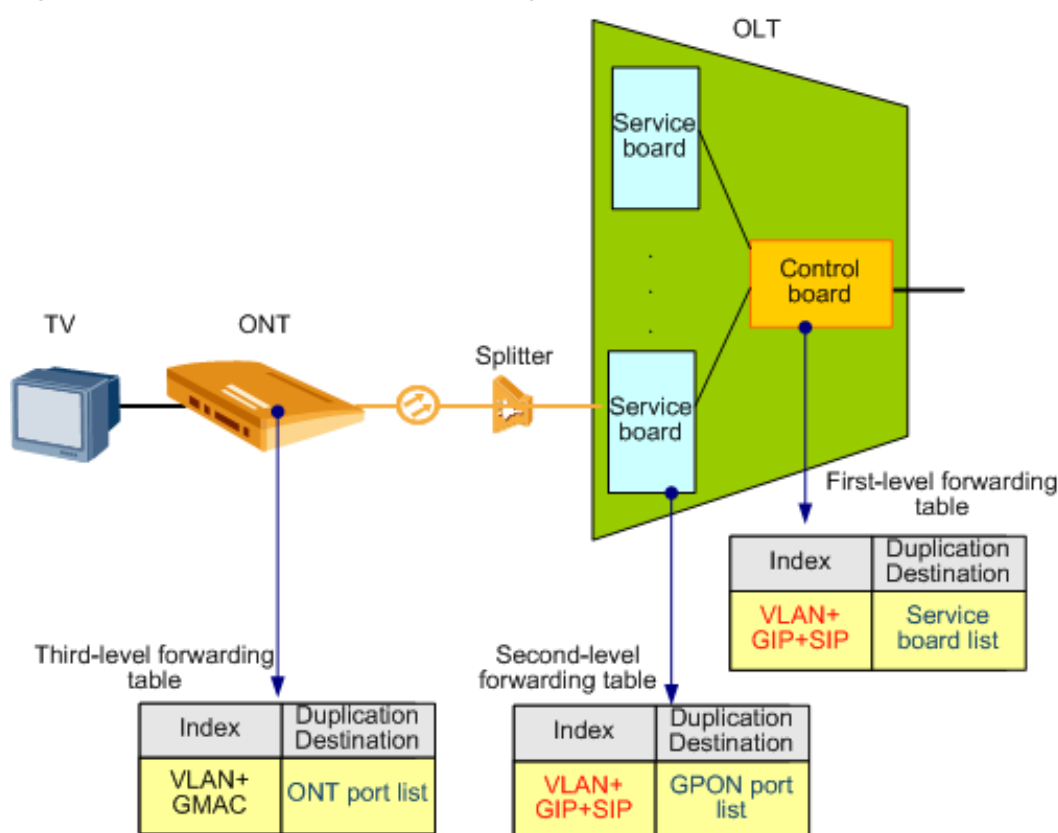
NOTE

1. This forwarding mode applies to ASMSSM and ASM ONLY group filter modes (for details, see "[group filtering mode](#)").
2. The ONT that implements the third-level duplication is recommended to use the chip that supports VLAN+GIP forwarding. If the ONT does not use such a chip, program GIP-to-GMAC mapping must be a one-to-one mapping. Without the one-to-one mapping on the same ONT, garbled images will occur.

This topic describes only the forwarding framework in the most common single-copy duplication mechanism. For the hardware forwarding framework in the multi-copy duplication mechanism, see "[GPON Multi-Copy Duplication](#)."

GPON Multicast Forwarding Table (VLAN+GIP+SIP) [OLT]

Figure 13-32 GPON multicast forwarding table (VLAN+GIP+SIP)



The OLT supports a distributed 2+1-level duplication architecture:

- The first-level duplication is implemented on the control board. By using the "VLAN+GIP+SIP" index, the control board duplicates multicast data to the service board interested in the multicast program in an as-per-requirement manner, effectively saving the backplane bandwidth.
- The second-level duplication is implemented on the service board. By using the "VLAN+GIP+SIP" index, the service board duplicates multicast data to the GPON port interested in the multicast program in an as-per-requirement manner, effectively saving the downstream bandwidth of the GPON port. Then the service board encapsulates and transmits the multicast data on the GPON port in the mode of multicast GEM port.

- The third-level duplication is implemented on the ONT. By using the "VLAN+GMAC" white list, the ONT filters out unneeded multicast data to avoid bandwidth overflow at the downstream ingress (ONT only supports that in olt-control mode). Then, by using the "VLAN+GMAC" index, the ONT duplicates the multicast data to the ONT ports in an as-per-requirement manner (only supports forwarding by using GMAC in snooping mode).

NOTE

1. This forwarding mode applies to the SSM ONLY group filter mode.
2. Due to hardware limitations, only the difference in the least significant 20 bits can be differentiated between source IP addresses (SIPs). For example, 1.1.1.1 and 2.1.1.1 are the same SIP for the device; 1.1.1.1 and 1.1.1.2 are different SIPs for the device.
3. The ONT that implements the third-level duplication is recommended to use the chip that supports VLAN+GIP forwarding. If the ONT does not use such a chip, program GIP-to-GMAC mapping must be a one-to-one mapping. Without the one-to-one mapping on the same ONT, garbled images will occur.

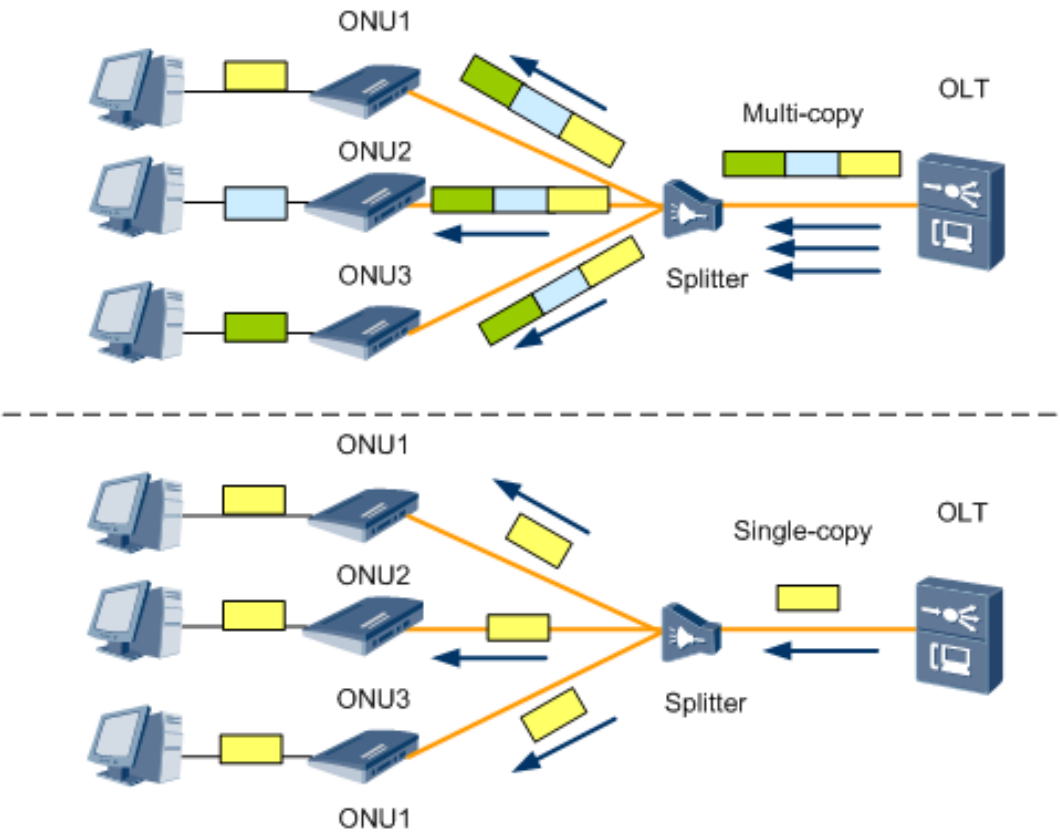
13.4.3.4 GPON Multicast Duplication

If the service board of the OLT is a GPON service board, the device has two multicast forwarding mechanisms and you can configure the forwarding mechanism based on MVLAN.

- Single-copy duplication
This is the most common duplication mode of GPON multicast (it also refers to the mode mentioned in this document unless otherwise stated). This mode makes the best of the GPON downstream WDM transmission principle and sends multicast data to all ONTs using the non-encrypted GEM port bearer channel. Each ONT receives the multicast data according to the multicast filtering table. For the corresponding hardware forwarding entry, see "[Multicast Forwarding Table](#)."
- Multi-copy duplication
The primary difference between single-copy duplication and multi-copy duplication is that, in multi-copy duplication, multicast data is duplicated to corresponding service ports according to user requirements, encapsulated in the encrypted unicast GEM port channel, and then sent to the ONT. The following table shows the multicast forwarding table at the GPON board level.

Index	Entry
VLAN+GMAC	Multicast user list

Figure 13-33 Single-copy duplication and multi-copy duplication



The following table lists the differences between single-copy duplication and multi-copy duplication.

Item	Single-copy Duplication	Multi-copy Duplication
Duplicati on granulari ty	Based on GPON port	Based on multicast user
Bandwid th	One GPON port has only one multicast stream.	One multicast user has only one multicast stream, but one GPON port may have multiple multicast streams.
Security	On the one hand, the security depends on the ONT filtering; on the other hand, the head end and STB encryption system are required.	This mode uses the GPON line AES128 encryption system and the real-time key conversion function, which provides better security than the common encryption system of the head end.

Item	Single-copy Duplication	Multi-copy Duplication
CAC of PON port	Supported	Not supported

13.4.4 Multicast Upstream Interoperation

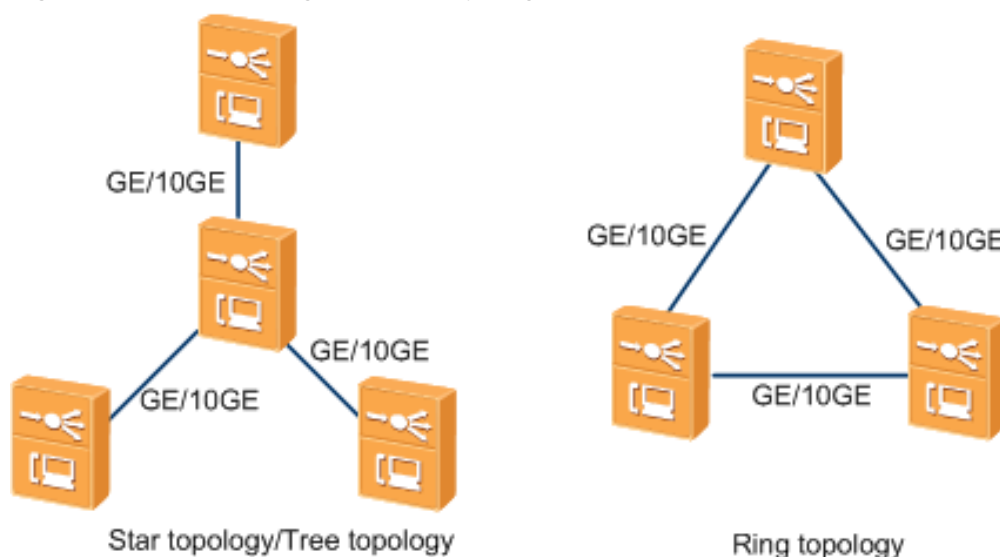
13.4.4.1 Multicast Cascading

- Ethernet cascading

Using Ethernet cascading on the access device, the number of ports on the convergence device and the optical cable routing cost can be reduced. In addition, capacity expansion for more users in the residential community access area can be easily implemented.

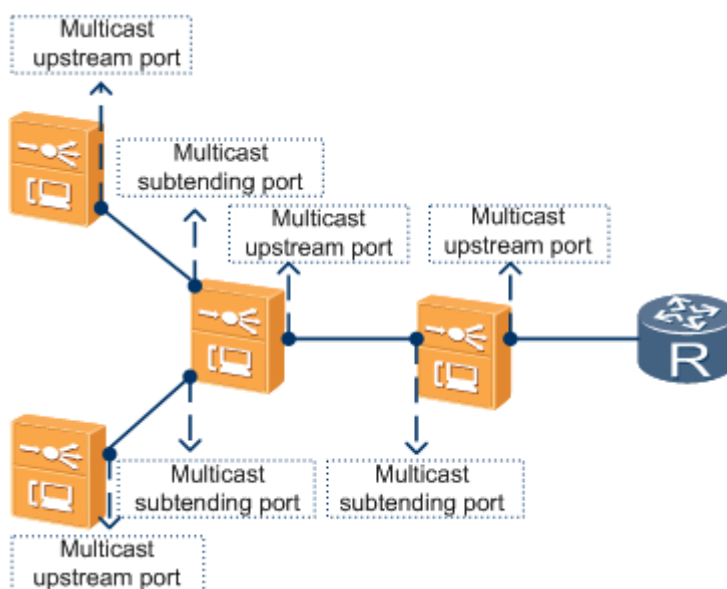
There are two common cascading network topologies, star (tree/chain) network and ring network, as shown in the following figure. Here, the star cascading network is used as an example. For details about the ring cascading network, see "[13.4.4.2 Ring Network of Uplink Ports](#)".

Figure 13-34 Cascading network topologies



- Multicast cascading port configuration

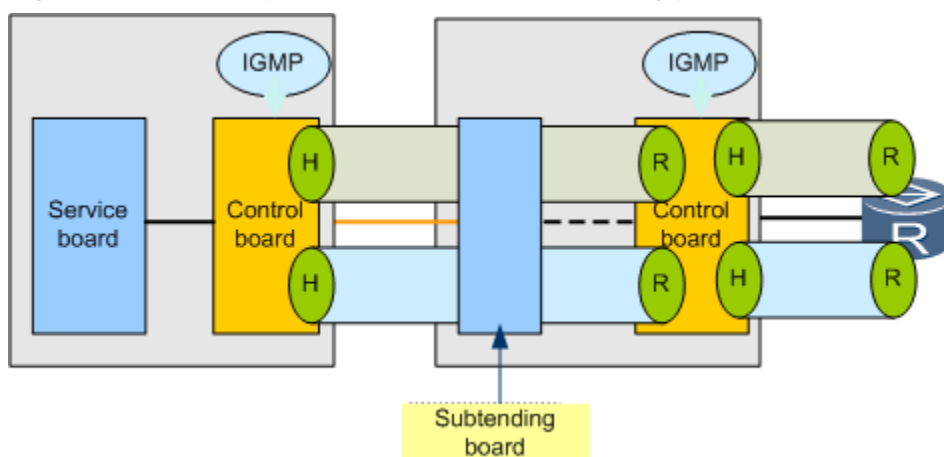
The device, through the Ethernet port of its cascading boards, can be physically connected to the lower-layer device. Multicast service is configured through the multicast cascading ports, and in this way the interoperation between the devices is managed. A multicast cascading port corresponds to a physical port (the channel for carrying services can be created through the port VLAN or service stream). The following figure shows the relationship between the multicast cascading port and the multicast upstream port.

Figure 13-35 Multicast cascading port and upstream port

- IGMP control message

In the multicast cascading scenario, the upper-layer device and the lower-layer device run the IGMP protocol stack separately. For a device, the cascading port (its lower-layer device) can be regarded as the multicast user. Multicast users are controlled by the lower-layer device and therefore the device does not support the following service functions for multicast users: rights management, multicast preview, multicast CAC, charging, and multicast service acceptance. The device supports the quick leave and normal leave functions.

On the cascading port, the IGMP protocol stack is based on different VLANs, as shown in the following figure.

Figure 13-36 IGMP protocol stack on the cascading port

NOTE

If an Ethernet port is not configured as the multicast cascading port, the Ethernet port discards the IGMP report message.

The (SIP, GIP) field of the IGMP message and the VLAN of the IGMP message are used for program matching. The policy of processing unmatched messages can be configured based on the cascading port.

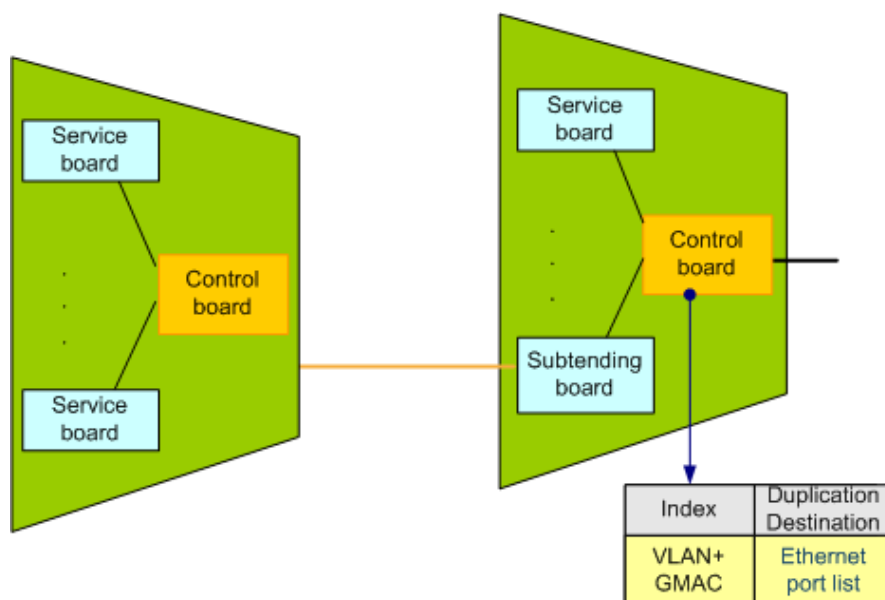
Considering the IGMP processing performance of the source node, it is recommended that all cascading devices adopt IGMP proxy instead of IGMP snooping.

– Multicast data forwarding

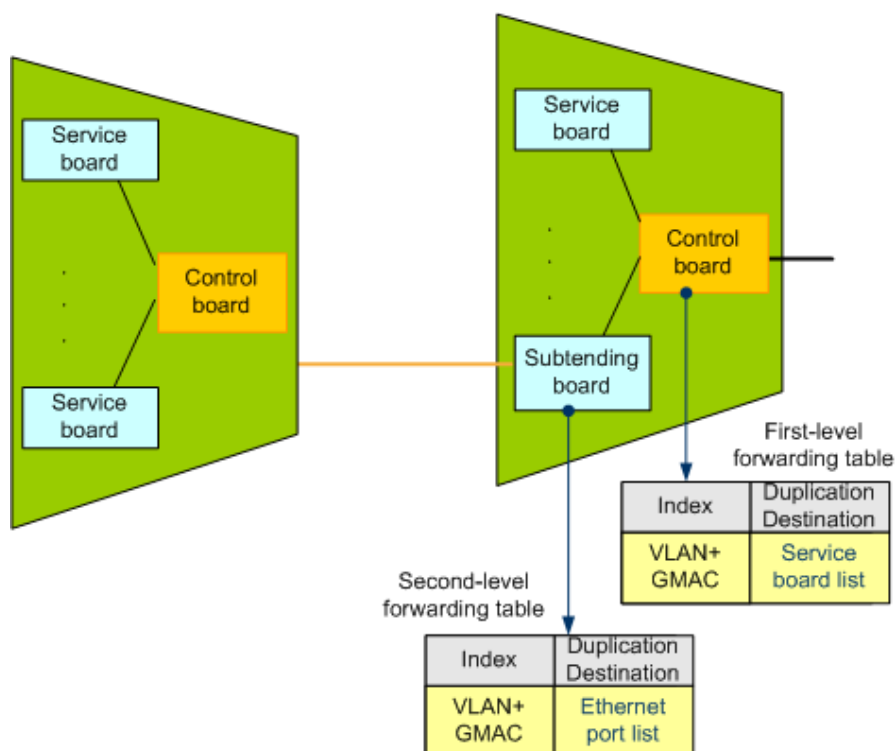
Multicast data can be forwarded only in a VLAN. According to different cascading boards, there are two forwarding architectures.

- One-level forwarding architecture: The following figure uses the control board as an example.

Figure 13-37 One-level forwarding architecture of multicast cascading



- Two-level forwarding architecture: The following figure uses the H901OXHD boards as an example.

Figure 13-38 Two-level forwarding architecture of multicast cascading

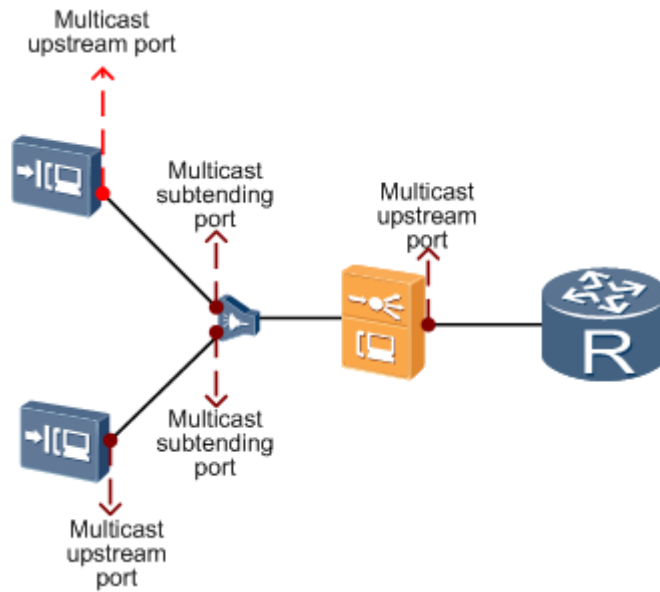
- xPON cascading

xPON cascading meets the requirements for multicast services in the FTTC/FTTB scenario.

- Multicast cascading port configuration

The device can implement the physical connection between the OLT and the MxU by using the PON line. Similar to Ethernet cascading mode, in xPON cascading mode, the interconnection between devices is also managed through the multicast cascading port object. One xPON cascading port corresponds to a logical interface (GEM port or LLID). The actual bearer channel can be created by using the service port. The following figure shows the relationship between the xPON cascading port and upstream port.

Figure 13-39 xPON cascading port and upstream port

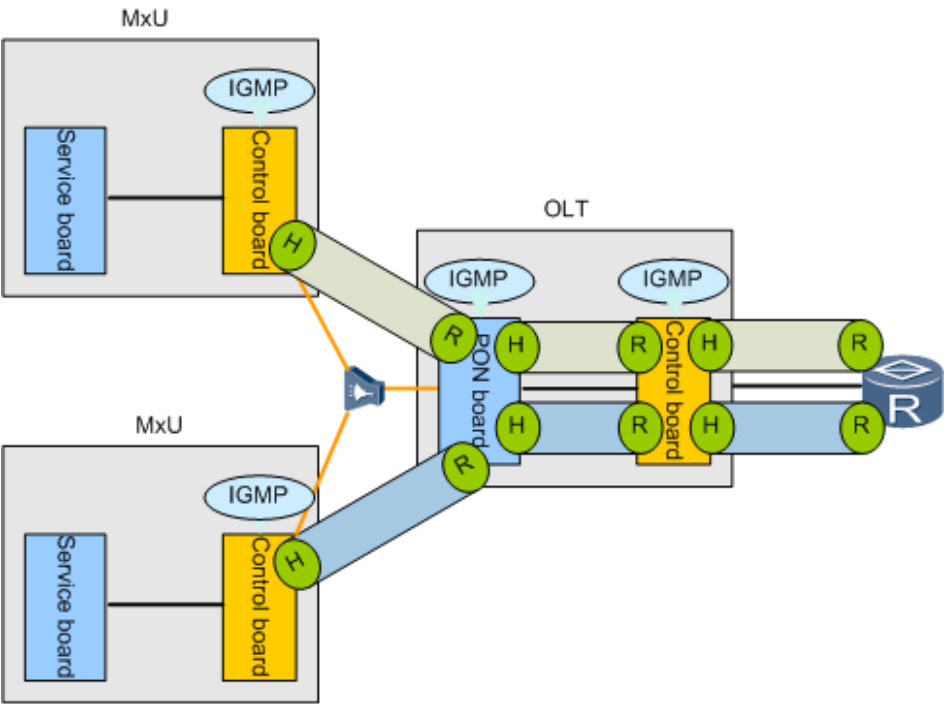


- IGMP control packet

In the xPON cascading scenario, the OLT and the MxU run the IGMP protocol stack separately. Like Ethernet cascading, xPON cascading supports normal leave and quick leave.

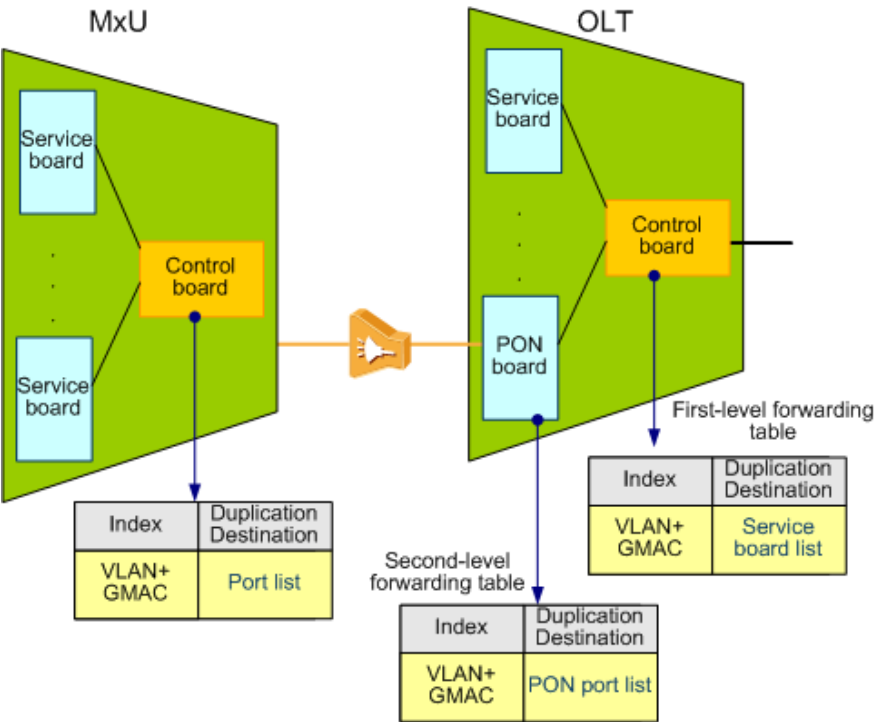
On the multicast cascading port, the IGMP protocol stack is based on different VLANs, as shown in the following figure. Different from Ethernet cascading, in xPON cascading, the bearer channel is limited by the maximum number of service ports that can be created on each GEM port or LLID, because the bearer channel is based on the service port. To support an MVLAN that is beyond the supported specifications, you can configure multiple GEM ports or LLIDs.

Figure 13-40 IGMP protocol stack of the xPON multicast cascading port



- Multicast data forwarding
xPON cascading supports forwarding in the same VLAN and does not support cross-VLAN forwarding.

Figure 13-41 xPON multicast forwarding architecture



 NOTE

Service ports that adopt traffic classification by two-tagged VLANs do not support multicast cascading ports.

13.4.4.2 Ring Network of Uplink Ports

In the ring network, access devices on the physical link are connected to form a ring. Devices on the ring maintain the ring status by running the Layer 2 link protocol.

The ring network of access devices has two advantages:

- Low network construction costs: In the ring network, an access device does not need to connect to the convergence switch, but connects to its nearest access device. This significantly saves optical cable resources. The switch provides only a few ports for the access device. In the ring network, however, deploying a small number of switches can meet the access requirements.
- High reliability: The Layer 2 link protocol provides the uplink backup protection. With this function, when the uplink of a single access device is faulty, the device can switch to the backup uplink.

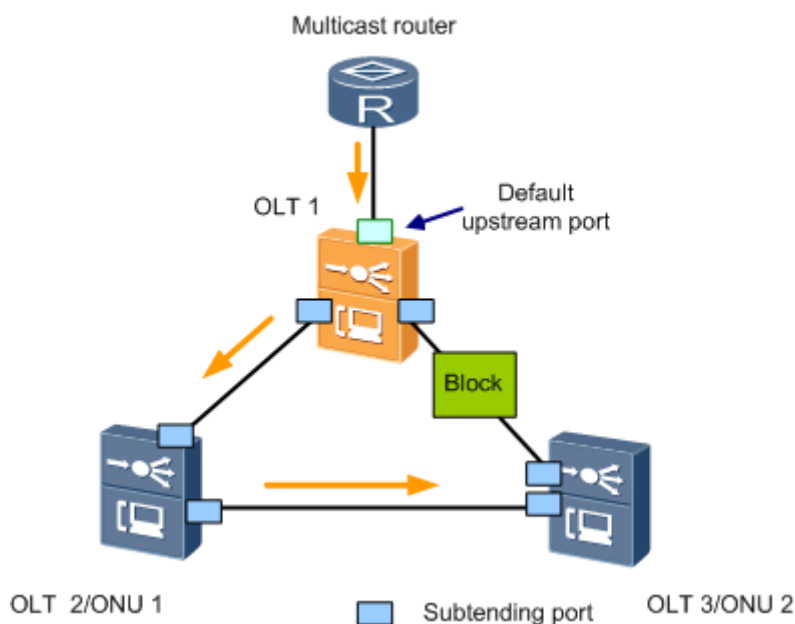
The multicast service supports the following ring networks on the network side.

- MSTP

The mode of the multicast uplink port needs to be set to MSTP by running the **igmp uplink-port-mode** command. In this case, the multicast uplink port of the device does not need to be configured; instead, the root port determined dynamically by MSTP serves as the multicast uplink port. If the access device is the MSTP root bridge (this device must be the injection point of the multicast data; using the MSTP priority configuration, ensure that this root bridge is not removed), the access device does not have the root port. Therefore, in the actual network, the multicast data injection port needs to be configured as the default multicast uplink port.

In addition, the device ports on the ring need to be configured as the multicast cascading ports. The actual multicast downlink ports are determined by IGMP according to the multicast group membership table. The following figure shows the configuration of each role.

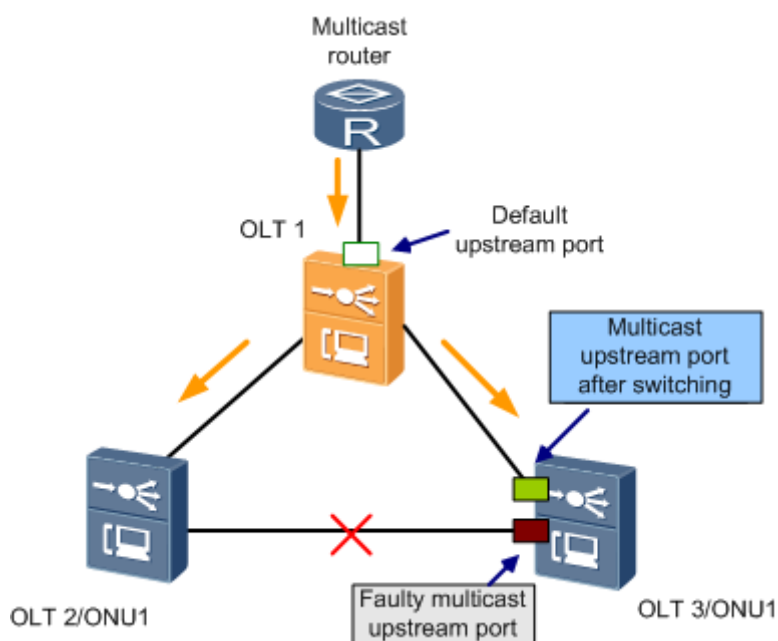
Figure 13-42 Multicast configuration in the MSTP ring network



NOTE

The root bridge must be the injection point of the multicast service. In the case of a link or device failure, after MSTP selects a backup link, the MVLAN-based IGMP protocol stack immediately sends the new root port (serving as the multicast uplink port) the join message targeting at the multicast group that the device is interested in. In this way, fast recovery of the multicast service can be ensured.

Figure 13-43 MSTP ring network fault



- ERPS

The mode of the multicast uplink port needs to be set to default by running the **igmp uplink-port-mode** command, and the multicast uplink port is configured as the video stream injection port. The master node of the ERPS ring must be planned in advance. The video stream injection node on the master node is the default uplink port. As shown in [Figure 13-44](#), OLT1 is the master node of the ERPS ring, and P1 is the default uplink port.

In addition, the node ports on the ring need to be configured as the uplink or cascading ports. The actual multicast downlink ports are determined by IGMP according to the multicast group membership table.

 NOTE

The two ports on the master node on the ERPS ring must be configured as cascading ports, and ports connected to cascading ports on the master node must be configured as uplink ports. Other ports on the ERPS ring can be configured as uplink and cascading ports at the same time. As shown in [Figure 13-44](#), P2 and P9 are cascading ports; P3 and P8 are uplink ports; other ports are mixed uplink and cascading ports.

Then, the RPL owner port of the ERPS ring needs to be configured. As shown in [Figure 13-44](#), P7 is the RPL owner port.

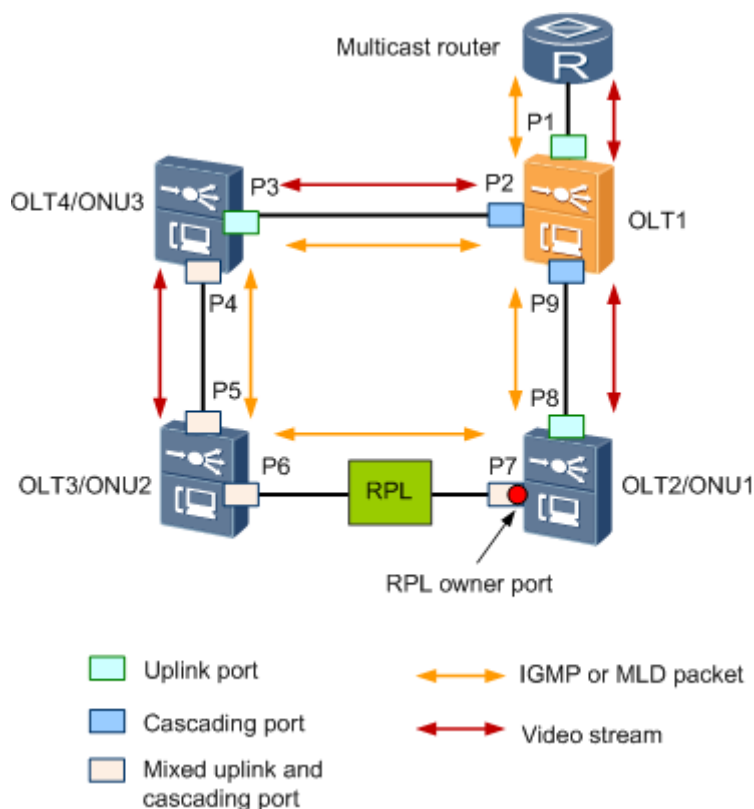
 NOTE

One ERPS ring has only one RPL owner port, which is configured by the user. The RPL owner port can be blocked to prevent loops on the ERPS ring. A blocked RPL owner port cannot forward data packets but can send ring automatic protection switching (R-APS) packets.

When the ERPS ring is carrying multicast services, you can run the **igmp ignore-block** command to set whether the RPL owner port of the ERPS ring can send IGMP or MLD packets. When the RPL owner port is enabled to send IGMP or MLD packets, dual back-up of multicast video data can be achieved. As shown in [Figure 13-44](#), video stream data injected from the uplink port P1 is transmitted in two different directions to P2 and P9. Because P7 is blocked, the video stream transmitted from access node 1 to access node 2 is terminated at P7 and the video stream transmitted from access node 1 through access node 4 to access node 3 is terminated at P6. This ensures that each access node does not repeatedly receive data of the same multicast video stream.

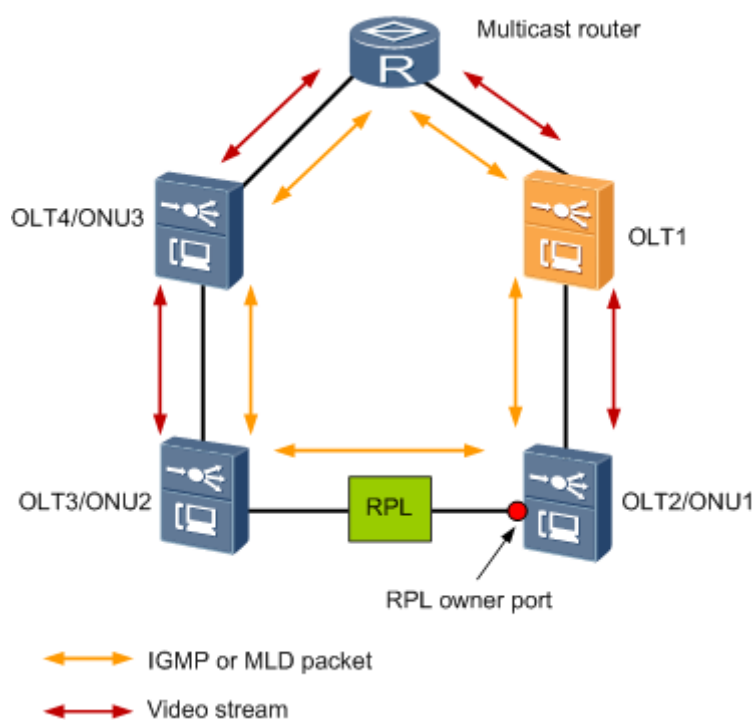
When link faults occur, the RPL owner port of the ERPS ring is switched to the forwarding status, and then the video stream on the RPL owner port is directly forwarded to the port that needs the video stream. If the RPL owner port is enabled to send IGMP or MLD packets, the status of the RPL owner port can be quickly switched during link faults.

Figure 13-44 Multicast configuration of the ERPS ring network



At present, the ERPS semi-ring network is frequently used, as shown in [Figure 13-45](#).

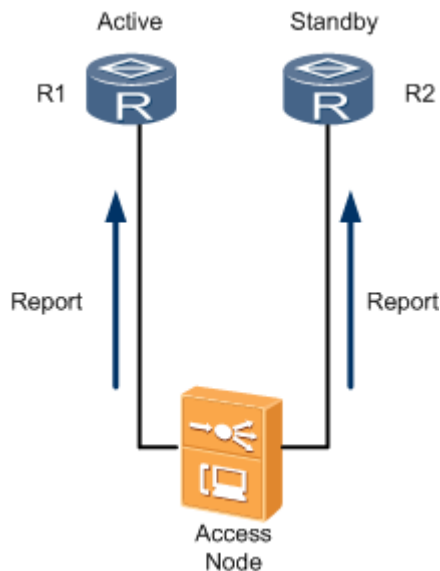
Figure 13-45 ERPS semi-ring network application



13.4.4.3 Dual-homing of Upstream Ports

Multicast routers 1 and 2 function as the active router and standby router respectively, as shown in the following figure. To ensure fast recovery of the multicast service after a switching, use the IGMP message broadcast function provided by the access node.

Figure 13-46 Upstream port broadcasting IGMP messages



First, set the two access node ports connected to routers 1 and 2 as the multicast upstream ports (the two ports must not be in the same aggregation group or protect group). After this setting, when the access node transmits IGMP messages to router 1, it transmits the same IGMP messages to router 2 at the same time. In this way, router 2 can maintain in real time the same multicast forwarding entry as that of router 1. Once a switching occurs, router 2 can directly obtain the multicast forwarding entry and can ensure fast recovery of multicast service in a shorter time.

Note: If the router supports transfer of the multicast forwarding entry using a proprietary protocol, this can substitute for the upstream port dual-homing function. In this case, add the two access node ports to one aggregation group. Such a function is more commonly used in actual applications.

13.4.5 Advanced Multicast Technologies

13.4.5.1 Multicast Program Management

Multicast programs can be static programs or dynamic program.

Static Programs

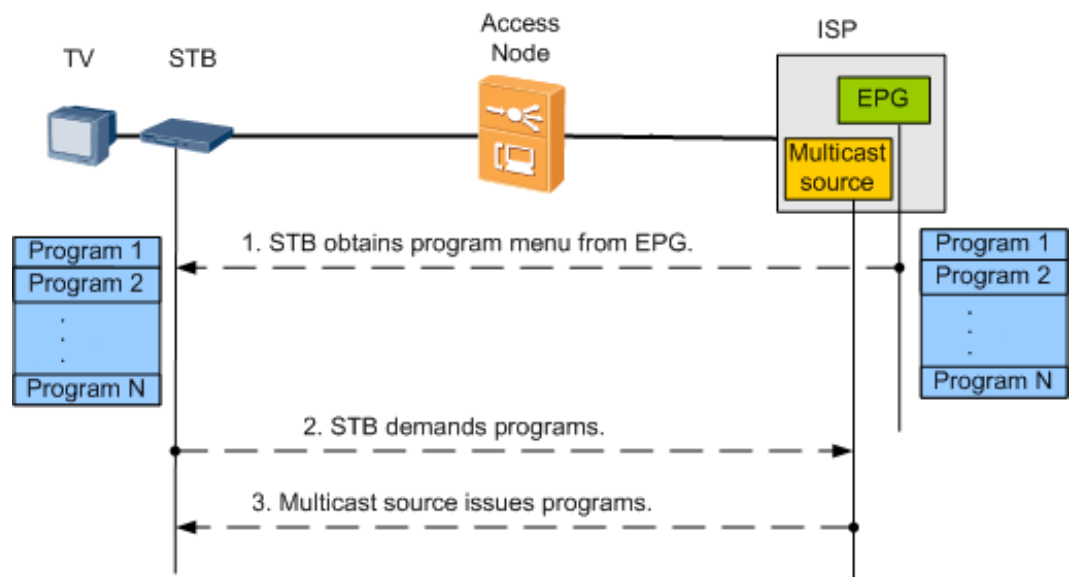
A program list is configured before users can watch these video programs. In this way, controllable multicast is implemented using a rights profile. However, the

program list and rights profile must be modified when the video service is modified. The device supports the program host, program prejoin, and multicast bandwidth management functions.

Dynamic Programs

In actual applications, if fine-grained management is not required on the device, dynamic programs can be applied. This avoids maintenance troubles brought by frequent program changes. In this case, program maintenance can be performed uniformly through the Electronic Program Guide (EPG) system.

Figure 13-47 Process of generating dynamic programs



1. After being started, the STB automatically obtains the program menu from the EPG server and provides the menu for the multicast user.
2. When the user orders a program, a corresponding IGMP message is generated and sent to the device. Hence, the program information on the device at this stage is not input by the administrator. Instead, it is dynamically generated in the MVLAN (to which the multicast user belongs) after the multicast group IP address and source IP address are extracted by the device from the real-time IGMP message of the multicast user.
3. The multicast program of the multicast source reaches the STB.

To prevent the user from using an inappropriate group IP address, a legal multicast address segment can be configured based on MVLAN on the device for dynamic programs. According to the configuration, a multicast program is generated only when the group IP address is within the legal address segment; otherwise, the IGMP message of the user is dropped. Apart from the restriction by the address segment, the number of programs that can be dynamically generated is also controlled by hardware specifications.

The fine-grained management that is not supported by dynamic programs on the device includes CAC, rights management, multicast preview, and pre-join.

Hot programs are added as static programs and other programs are ordered by users dynamically. This configuration speeds up hot program ordering and shortens channel switching time.

13.4.5.2 Multicast Rights Management

Rights Management

With the method of configuring different multicast programs on different profiles, package-based rights management can be implemented on the device.

- Rights profile

The rights to any multicast program can be specified in each rights profile, and each rights profile can be configured with a meaningful name. There are four types of rights:

Forbidden: It indicates that a multicast user is not allowed to watch or preview a multicast program.

Preview: It indicates that a multicast user can order a multicast program but is restricted in the watching duration and watching times.

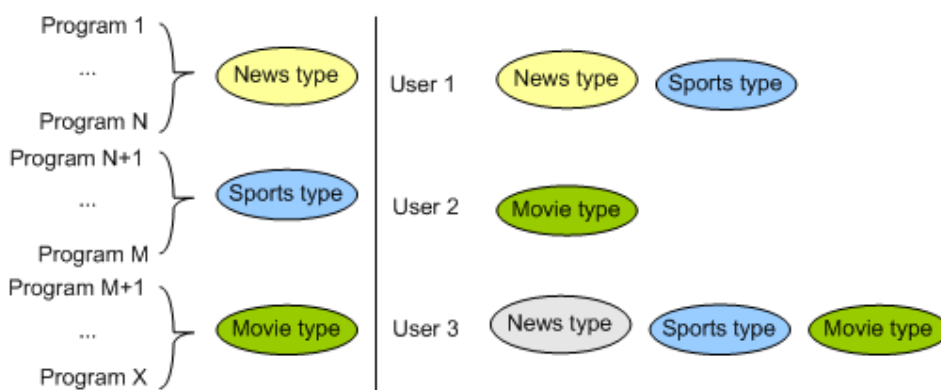
Watch: It indicates that a multicast user can order a multicast program normally without any restriction.

Idle: It indicates that a specific right is not assigned to a multicast program yet. It is the default value of the rights profile. The effect of "idle" equals that of "forbidden."

Carriers can plan the rights profiles according to user-defined rules. Usually, there are three modes of planning.

- The first one is planning by contents, such as planned as the news type, sports type, and movie type. In this case, one multicast program belongs to only one rights profile and the programs of different profiles do not overlap. Therefore, one user is usually bound to multiple profiles. See the following figure.

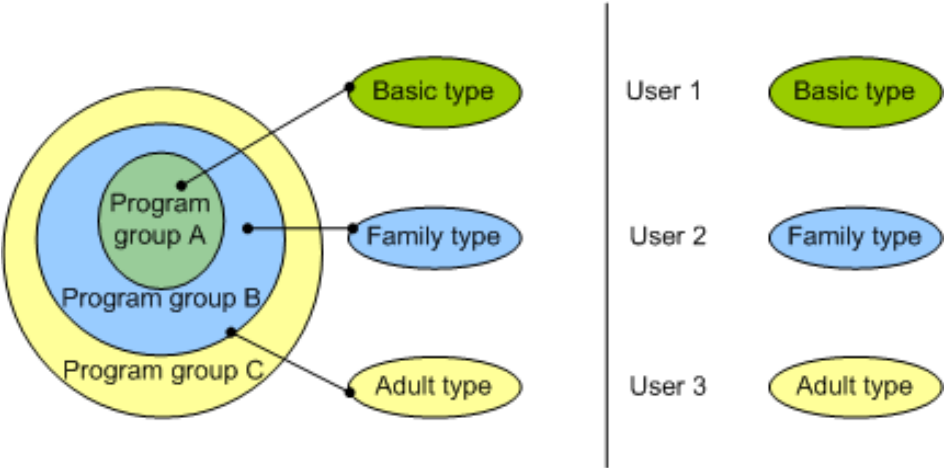
Figure 13-48 Planning rights profiles-mode 1



- The second one is planning different levels by content volumes, such as planned as the basic type, family type, and adult type. In this case, one multicast program may belong to multiple rights profiles and the

programs of different profiles may overlap. Therefore, one user is usually bound to only one profile. See the following figure.

Figure 13-49 Planning rights profiles-mode 2



- The third one is a hybrid of the first and second ones and is the most complicated as well as the most flexible mode. In this mode, the programs of different rights profiles may overlap and one user may be bound to multiple profiles. The same program may be configured with different rights in different rights profiles. To ensure that these rights profiles work as expected by the carrier when it comes to a specific program for a specific user, the rights of a program in the rights profiles must be prioritized. It is advised to plan the priorities before deployment to prevent any incorrect results. The following are examples.

Table 13-18 Priority of rights: forbidden > preview > watch > idle

Rights profile 1	Program 1: watch	User 1	Program 1: forbidden
Rights profile 2	Program 1: forbidden		

Table 13-19 Priority of rights: watch > preview > forbidden > idle

Rights profile 1	Program 1: watch	User 1	Program 1: watch
Rights profile 2	Program 1: forbidden		

- Rights control
The rights of each multicast user can be configured by the following two steps:

- a. Plan the rights profiles of all multicast programs.
- b. Bind a multicast user to the rights profiles required according to the contents subscribed to by the user.

The device provides open MIB interfaces to support such operations.

In addition, there is another method of implementing rights control: by configuring encryption on the head system and the STB. In this way, the carrier does not need to perform rights management on the device and only needs to enable or disable rights control at the system level or the multicast user level.

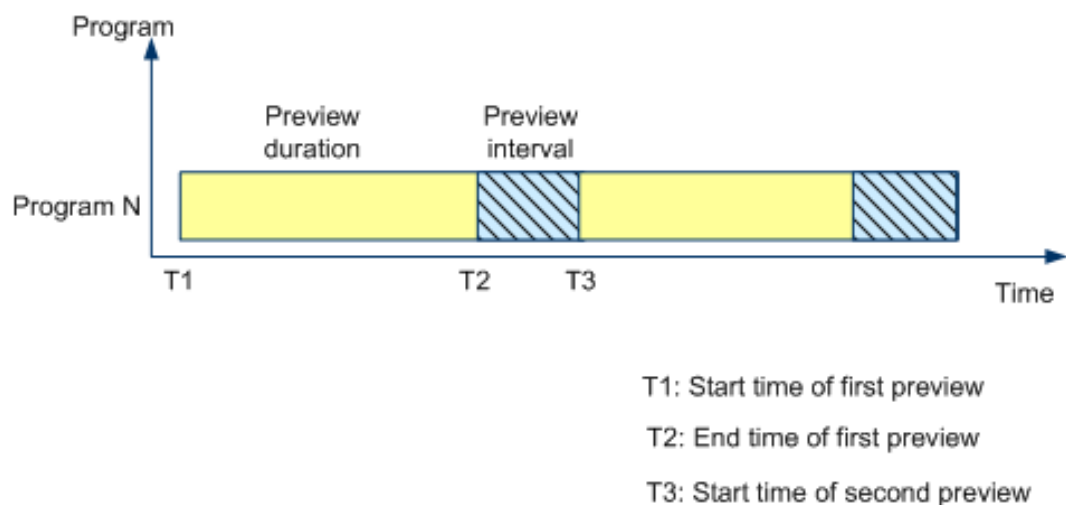
Multicast Preview

By providing the preview of certain special channels to multicast users, carriers may attract more users to subscribe to more programs with the watch right. Preview is usually used as an effective selling method.

The device manages the preview parameters of each multicast program by preview profiles. To be specific, each multicast program can be bound to a preview profile which is configured with preview parameters. Similar programs can be bound to the same preview profile to simplify management.

A preview profile contains three preview parameters.

Figure 13-50 Preview parameters



- Preview interval: It is the minimum interval between two previews. The interval is from the end time of the previous preview to the start time of the current preview (from T2 to T3 as shown in the preceding figure). If the interval between the two previews of a user does not reach the specified preview interval, the user is currently not allowed to preview the program. Such a mechanism guards against any "rogue" behavior of users. Without the restriction of the preview interval, a user may keep previewing the same program and is actually "watching" a program without having to pay for the "watch" right.
- Preview times: This parameter specifies how many times a multicast user is allowed to preview the same program during a day. Each time the user leaves

a previewed program, the counter increases by 1. When the counter exceeds the maximum value, the further orders of the user for the program will be rejected. In this case, the user's right to the program can be regarded as demoted to "forbidden." However, the preview right can recover the next day.

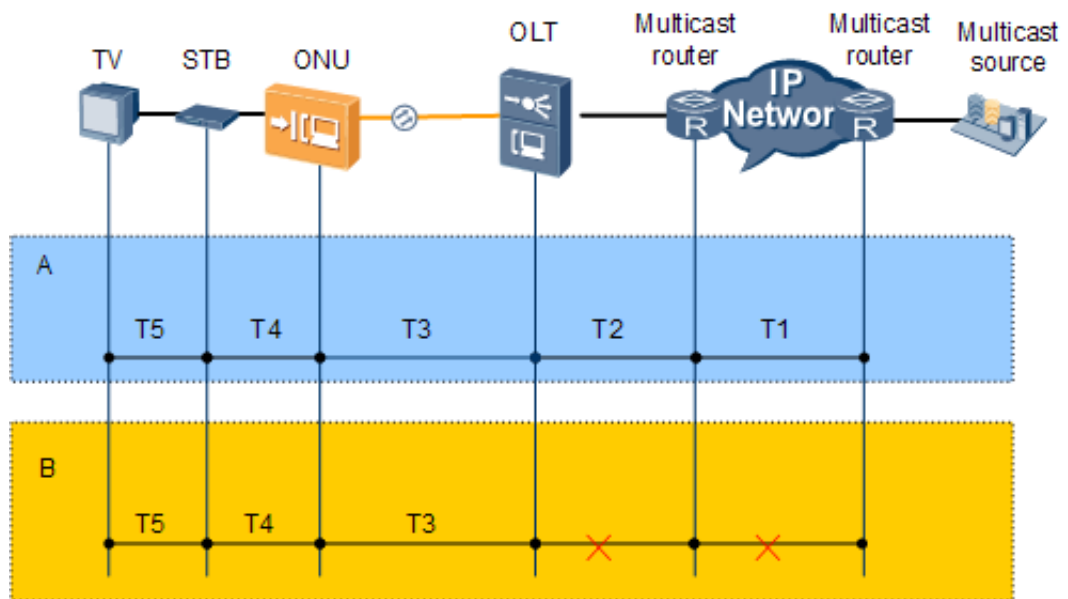
- Preview duration: This parameter specifies for how long a multicast user is allowed to watch the same program each time. The duration starts from the beginning of the order (from T1 to T2 as shown in the preceding figure). After the duration expires, the user will not be able to receive any data for the multicast program.

For details on how to control the preview of multicast users, see "[Rights Management](#)."

Prejoining a Program

The prejoin function is used to shorten the course of channel switching (reduce switching latency), so as to improve users' experience in channel switching. Switching latency comprises the processing consumption in each segment of a network, as shown in the following figure. With the prejoin function enabled, the network-side processing consumption (T1+T2) equals 0.

Figure 13-51 E2E multicast switching latency



A: Processing latency of non-prejoin program = $T1 + T2 + T3 + T4 + T5$

B: Processing latency of prejoin program = $T3 + T4 + T5$

The prejoin function applies to the IGMP proxy scenario. It equals that there is always online users for a program.

- The flow of prejoining a program is the same as the flow of joining a program normally. For details, see section 1.6.4. Once a multicast stream is successfully demanded, it is transmitted to the DSLAM.

- In the flow of leaving a prejoined program, compared with the flow of leaving a normally joined program, the DSLAM does not transmit the leave message to the multicast router even when the last multicast user leaves the program.
- In the flow of querying a prejoined program, compared with the flow of querying a normally joined program, the DSLAM responds to the multicast router's query as required by the protocol regardless of whether or not the multicast group membership table of the program contains a multicast user.

From above all, viewed from the router, there are always online users for a prejoined program.

The prejoin function can be set for a program. In general, set the prejoin function for the program that is most commonly demanded by users. A dynamic program does not support the prejoin function.

13.4.5.3 Multicast CAC

CAC is the short form for call admission control. Here, it means controlling the setup of IGMP sessions. If an IGMP session fails to be set up, a multicast user will fail to receive the multicast program ordered.

In a broad sense, implementing CAC requires implementing the first-level control in the system. Currently, system control includes the following:

- Anti-DoS attack. The rate of IGMP messages sent from the user side must not exceed the specified value in the system. Otherwise, the system will regard that a DoS attack occurs and drops the messages. Such a protection method applies not only to IGMP messages, but also to control packets such as DHCP and PPPoE packets. For details, see "Anti-DoS Attack."
- Anti-IP spoofing. When this function is enabled, the user must obtain a legal IP address through DHCP before ordering any program. Only the IGMP messages using the legal IP address as their source IP address will be accepted by the system; otherwise, the messages will be regarded as coming from unauthorized users and will be dropped by the system. For details, see "Anti-IP Spoofing."

NOTE

Only the centrally-controlled multicast supports this feature.

- Broadband message overload. When a service traffic burst occurs, the system resources may not be able to support all services. Then, the system will drop certain messages according to specified policies to ensure that the services with a higher priority are not affected. In this case, IGMP messages may be "sacrificed" to reduce the system load. For details, see "Broadband Message Overload."

After the first-level control in the system comes the multicast first-level control, which includes the following:

- Concurrent number of programs of a multicast user. This parameter specifies how many channels a multicast user is allowed to order at the same time. The parameter can be configured based on multicast user.
- Rights control. For details, see "[13.4.5.2 Multicast Rights Management](#)."
- Bandwidth check. Though the system supports QoS control on various types of traffic, packet loss (drop by priority or tail drop) may still occur when the

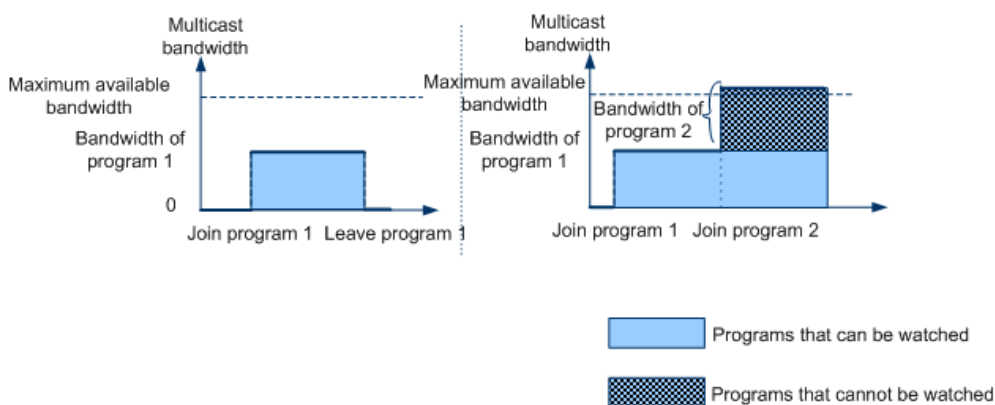
transmission bandwidth is overloaded. However, due to the real-time and non-retransmittable properties of multicast programs, postmortem QoS will directly cause pixelation to the programs with packet loss (not only to newly ordered programs). Hence, the requirements of IPTV for high-quality experience are not met. Bandwidth check enables the system to control a newly ordered program beforehand. In this way, the system can ensure that the programs that have been ordered enjoy sufficient bandwidth and will not be affected by the new program. With bandwidth check, only the newly ordered program is affected (if bandwidth is insufficient, the user will not be able to watch the newly ordered program).

CAC can be classified into the following types according to different control points and methods.

- Multicast user bandwidth CAC

First, each pre-configured program is configured with bandwidth. The bandwidth is configured with reference to the video bit streams, and the margin of packet encapsulation and network transmission jitter; if possible, actually tested network traffic can also be used, as a better reference. Then, each multicast user is configured with available bandwidth. The available bandwidth is configured with reference to the actual line bandwidth or the planning of service provisioning. Hence, when receiving the first IGMP join message of a program, the device subtracts the bandwidth occupied by the program from the available bandwidth of the user. If the remainder is smaller than 0, the device rejects the order request of the user. When receiving an IGMP leave message of a program, the device returns the bandwidth occupied by the program to the available bandwidth of the user. The time of returning is the time when the device stops forwarding multicast data. That is, the program is not ordered by any end user of the terminal.

Figure 13-52 Multicast user bandwidth CAC



Multicast user bandwidth CAC can be configured at the system level or at the multicast user level.

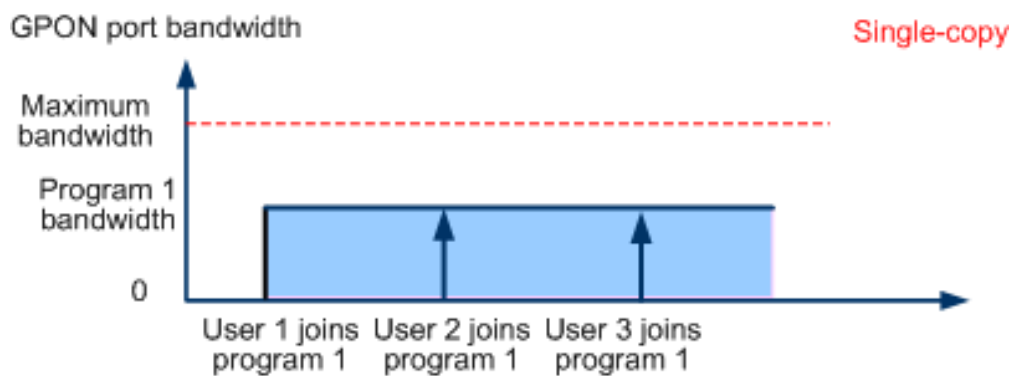
- GPON port bandwidth CAC

GPON single-copy duplication function (default configuration): Under the same GPON port, even if multiple multicast users order the same multicast program, the multicast data is duplicated only once and sent to corresponding multicast users through the downstream multicast channel. Therefore, this

function ensures that the downstream multicast bandwidth does not overflow the downstream line bandwidth of the GPON port.

To do so, the operator first needs to configure bandwidth for each pre-configured program (see "Multicast user bandwidth CAC"), and then allocates the available bandwidth for each GPON port (depending on the actual line bandwidth or the service provisioning plan). In this way, after receiving the first IGMP join message of the program, the device deducts the bandwidth of the corresponding program from the remaining bandwidth of the GPON port. If the deduction result is smaller than 0, the device rejects the order of the user. After receiving an IGMP leave message, the device returns the bandwidth of the corresponding program to the GPON port (the moment of returning is when the forwarding of multicast data is stopped, that is, no multicast user under the GPON port orders this program).

Figure 13-53 GPON port bandwidth CAC



This function can be configured at the system level or GPON port level. It can be used together with the multicast user bandwidth CAC.

13.4.5.4 Multicast QoS

This topic describes the quality of service (QoS) features dedicated to the multicast service. For more information about QoS (including traffic classification, traffic policing, ACL policy, and congestion avoidance and management), see the [QoS](#) feature.

Priority Processing of IGMP Packets

The device supports processing of only the 802.1p priority of IGMP packets.

Table 13-20 Priority processing in IGMP proxy/snooping

Cascading Mode	Upstream	Downstream
Multicast user/xPON cascading	Based on MVLAN.	Traffic classification methods: • VLAN: by the 802.1p priority specified in the traffic profile. • VLAN+encapsulation type: by the 802.1p priority specified in the traffic profile. • VLAN+802.1p priority: by the 802.1p priority specified by traffic classification.
Ethernet cascading	Based on MVLAN.	Based on MVLAN.

Priority Processing of Multicast Traffic Streams

The device supports processing of only the 802.1p priority (CoS) of the multicast traffic streams.

Table 13-21 Downstream multicast priority processing

Cascading Mode	Pre-configured Program	Dynamic Program
Multicast user/xPON cascading	Traffic classification methods: • VLAN: by the 802.1p priority specified in the traffic profile. • VLAN+encapsulation type: by the 802.1p priority specified in the traffic profile. • VLAN+802.1p priority: by the 802.1p priority specified by traffic classification.	
Ethernet cascading	Based on program.	The priority is not configurable. That is, the priority carried remains unchanged.

13.4.5.5 GPON ONT Multicast

The GPON end-to-end multicast service requires the cooperation of the ONT. The following points must be noted:

- VLAN translation

If the carrier plans the home gateway at the user's house, generally, the VLAN of the IPTV service (also called C-VLAN) needs to be planned. Because the OLT does not directly support translation of the MVLAN, the operator can configure VLAN translation on the ONT to meet the planning requirement

(the OLT provides the corresponding CLI and the configuration can be issued to the ONT through OMCI). The MVLAN can be translated in three ways: transparently transmitted, translated to untagged, and translated to a specified VLAN.

- Controllable multicast

In single-copy duplication, GPON downstream multicast programs are broadcast. Assume the following condition: After an authorized multicast user orders a program, all users under the GPON port can receive this program. Therefore, to implement complete rights control on the access device, the OLT must configure the ONT to work in the "dynamic controllable" mode. In this way, the multicast filtering table (white list) on the ONT is issued by the OLT after multicast control checking. If a downstream multicast program is not in the multicast filtering table, the ONT cannot receive this multicast program. If the ONT is configured to work in the "IGMP snooping" mode, the multicast filtering table on the ONT is completely maintained by the ONT. In this case, multicast program rights management is generally implemented by the encryption system of the IPTV platform.

13.4.5.6 Multi-instance Multicast

With the increased use of open networks, carriers' networks need to provide independent multicast domains for different multicast ISPs so that different ISPs do not interfere with each other. Independent multicast domains can be implemented on the management plane, control plane, and forwarding plane by planning different MVLANs on the device.

- Management plane (ASMSSM or ASM ONLY)

Within each MVLAN, the multicast programs to be provisioned, and the multicast upstream ports and multicast users involved can be configured for each ISP. Here, the multicast programs need to be noted. To ensure that each ISP can plan multicast programs independently, the multicast program triplet (MVLAN, source IP address, and multicast IP address) needs to observe the following rules:

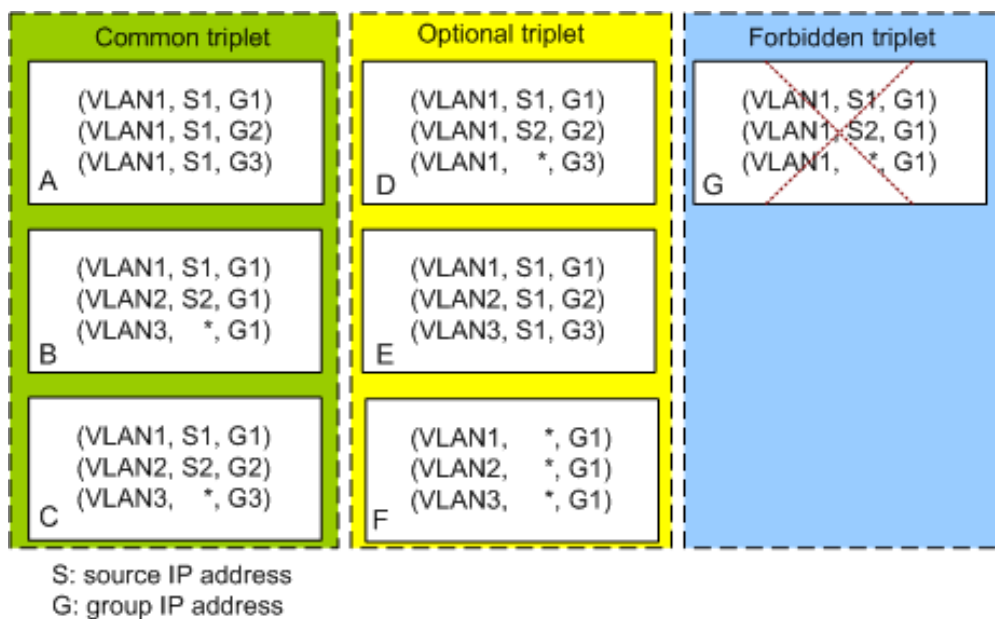
- If two GIPs are mapped to the same GMAC (for details on the mapping method, see "[Basic Concepts](#)"), the two GIPs are regarded as the same GIP.

 NOTE

If the device does not have boards that support only VLAN+GMAC forwarding chip, this rule may not be considered; otherwise, carriers need to follow this rule in planning.

- To ensure the uniqueness of a multicast forwarding entry on the forwarding plane, (MVLAN, multicast IP address) must be unique.
- Especially, in the case of an IGMPv2 message or an IGMPv3 message in the ASM mode, the multicast source IP address equals any value (usually represented as * or as any). In this case, only the second rule needs to be observed.

Use section G in the following figure as an example. According to the second rule, (MVLAN, multicast IP address) must be unique, but (VLAN1, G1) in section G is not unique. Therefore, configuring or generating the entries in section G is not allowed. The entries in the other sections in the following figure can also be judged by the rules described above.

Figure 13-54 Multicast program triplet (ASMSSM or ASM ONLY)

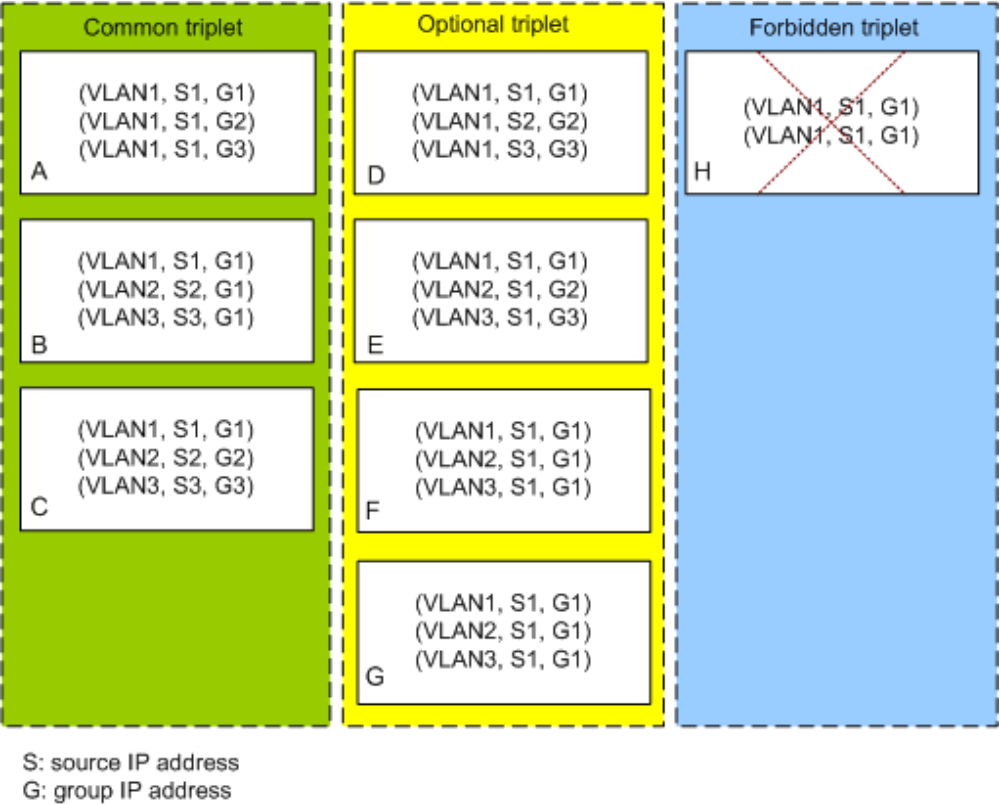
- Management plane (SSM ONLY)

Within each MVLAN, the multicast programs to be provisioned, and the multicast upstream ports and multicast users involved can be configured for each ISP. Here, the multicast programs need to be noted. To ensure that each ISP can plan multicast programs independently, the multicast program triplet (MVLAN, source IP address, and multicast IP address) needs to meet the following rules:

- If two source IP addresses have the same least significant 20 bits, these two source IP addresses are considered the same source IP address. Carriers need to have proper planning to avoid this.
- To ensure the uniqueness of a multicast forwarding entry on the forwarding plane, (MVLAN, multicast IP address, and source IP address) must be unique.

Use section H in the following figure as an example. According to the second rule, (MVLAN, multicast IP address, and source IP address) must be unique, but (VLAN1, G1, and S1) in section G is not unique. Therefore, the entries in section H are not allowed to be configured or generated. The entries in the other sections in the following figure can also be judged by the rules described above.

Figure 13-55 Multicast program triplet (SSM ONLY)



- Control plane
On the network side, each MVLAN has an independent IGMP protocol stack. Each ISP can select the protocol version, message priority, and IGMP proxy or IGMP snooping. On the user side, each multicast user has an independent IGMP protocol stack and is not affected by other multicast users. [Table 13-22](#) describes the IGMP message processing policies in different group filter modes.

Table 13-22 IGMP message processing policies

Group Filter Mode	IGMPv2	IGMPv3 Without Source	IGMPv3 with Source
ASMSSM	Processed	Processed	Processed
ASM ONLY	Processed	Processed	Dropped
SSM ONLY	Dropped	Dropped	Processed

- Forwarding plane
On the forwarding plane, multicast forwarding tables with the group filter mode use ASMSSM or ASM ONLY use the MVLAN and multicast IP address together as indexes (VLAN+GMAC as the index for boards that do not support VLAN+GIP). This ensures that different MVLANs do not interfere with each other. Multicast forwarding tables with the group filter mode SSM ONLY use

MVLAN, multicast IP address, and source IP address together as indexes. For details, see "[Multicast Forwarding Table](#)." For the control board, implementing QoS scheduling on the traffic of different MVLANs on the same port on the service board equals unicasting. For details, see "QoS".

NOTICE

1. In most situations, the MVLAN is different from the S-VLAN of the traffic stream to which the multicast user belongs. This S-VLAN can be used in the IPTV VoD service.
 2. VLANs in S-VLAN+C-VLAN forwarding mode are used for transmission over point-to-point channels and are not applicable to multicast duplication and forwarding. Therefore, the S-VLAN in S-VLAN+C-VLAN forwarding mode cannot be used as an MVLAN.
 3. When the group filter mode is ASMSSM, binding a multicast user to multiple MVLANs is not recommended. If a home has subscribed to multiple ISP programs, configure different multicast users for different MVLANs to ensure that one-to-one mapping between MVLANs and multicast users.
 4. When the group filter mode is ASM ONLY or SSM ONLY, binding a multicast user to multiple MVLANs is not supported.
-

13.4.5.7 Charging Mode

For multicast services, carriers or ISPs usually adopt two charging modes:

- Fixed charging. In this mode, programs are divided into different packages. The user needs to pay a fixed amount of fee for each package in a fixed period (such as by the year or by the month). This charging mode does not restrict the multicast user in the order count or the ordered volume of traffic.
- Pay per view (PPV): In this mode, the user is charged according to the order count of different programs.

In the first charging mode, since it is fixed charging, the charging does not relate to the behavior of the multicast user. Therefore, the first mode is supported by the device inherently and does not require additional functions from the device.

In the second mode, the device records the order behavior of each multicast user or each multicast terminal identified by the MAC address, and provides the behavior information in the form of a call detail record (CDR) to the accounting system for settling an account. The complete configuration of the CDR function consists of three steps:

1. Enabling the logging function. The function can be configured at the multicast user level, multicast program level (configurable for pre-configured programs, and defaulted to **enable** for dynamic programs), or system level. When a user finishes a complete watch behavior (from the program order starting to ending), or when the user fails to order a program because of failing to pass the multicast CAC, a log is generated.

 NOTE

When the logs reach the maximum capacity, new logs will overwrite old ones. Therefore, to prevent heavy consumption of log resources in the case where the user quickly browses through channels, the device supports a configurable flag time for generating logs. If the multicast user watches a channel for a duration shorter than the flag time, the device does not generate a log. On the contrary, to timely log the users who stay online for a long time, the device supports the configuration of another time value (if the value is 0, the log will not be generated). When a user stays online for longer than the preset value, the device automatically generates a log.

2. Configuring the file server. The operator needs to select a CDR transfer file. Available options are TFTP/FTP/SFTP. Also, the operator needs to set the IP addresses of the primary and secondary servers.

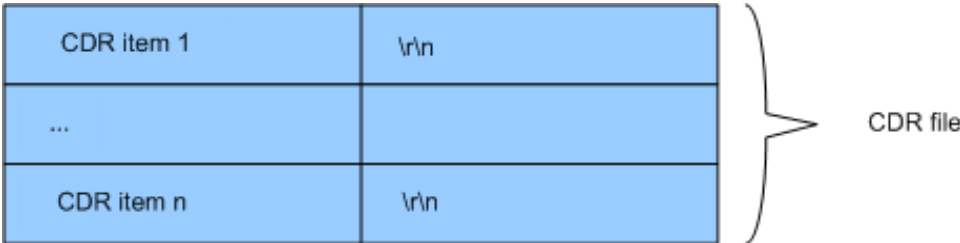
 NOTE

FTP and TFTP have security risks due to protocol restrictions. SFTP is recommended.

3. Enabling the CDR functions (at system level). After the CDR function is enabled, the device automatically integrates the logs that need to be reported into a text file and transfers the file to the server when either of the following conditions is met: when the reporting interval expires, or when the number of logs reaches the reporting threshold.

There are two types of CDR but they have the same format of the text file, as showed in [Figure 13-56](#). The format of the text file name is different from the detailed format of a CRD item.

Figure 13-56 Format of the text file



- Recording the order behavior of each multicast user

The format of the text file name is **HWCDR-host name-YYYYMMDDHHMMSS.txt**.

Table 13-23 Detailed format of a CDR item

ID	Field Name	Specificati on	Commentary
0	TAG	3 Bytes	Fixed as "Log". "Log" is the module name which generates syslog
1	SN	0..5 Bytes	Using a 16 bit variable to record. The maximum value is "65535" which occupies 5 bytes.

ID	Field Name	Specification	Commentary
2	FrameSlotPortG emport	5..13 Bytes	F/S/P/GemPort for GPON user
	FrameSlotPortFL ow	5..14 Bytes	F/S/P/FlowID for other type user
3	ProgramIP	0..15 Bytes	Sample: 239.1.1.1
4	OperMode	0..1 Bytes	0-Watch; 1-Preview; 2-No Right; Other is invalid
5	StartDate	0..18 Bytes	YYYY-MM-DD HH:MM:SS
6	EndDate	0..18 Bytes	YYYY-MM-DD HH:MM:SS
7	ProgramName	0..16 Bytes	Sample: cctv1. If the program does not exist, this parameter is "No-Name".
8	ProgramSrcIP	0..15 Bytes	Sample: 192.168.1.1. If the IP address is invalid, this parameter is "".
9	Reason	1..2 Bytes	Syslog generation reason: 11: User's online time is too long 0: User leave.

- Recording the order behavior of each multicast user or each multicast terminal identified by the MAC address

The format of the text file name is **BTVCDR-host name-X-YYYYMMDDHHMMSS***.txt**.

 NOTE

When the value of X is A, automatic reporting is enabled. When the value of X is M, manual reporting is required. *** indicates millisecond.

Table 13-24 Detailed format of a CDR item

ID	Field Name	Specification	Commentary
1	Record type	1..2 Bytes	• 0: Successful channel zap • 1: Channel timeout by general query or group-specific query • 2: Successful preview channel zap • 3: Preview channel timeout by general query or group-specific query • 4: It is automatically generated every N hours even when there is no channel (including preview channel) zap. • 5: Join a channel with no access right • 6: Join a channel with preview access right (but with preview limit exceeded)
2	System name	1..50 Bytes	The name of the OLT/DSLAM.
3	IGMP user	7..14 Bytes	Frame ID/Slot ID/Port ID/Service port Index Sample: 0/1/1/233
4	Terminal IP	7..15 Bytes	Zero-length string means IP is unknown. Sample: 192.168.0.1
5	Terminal MAC	17 Bytes	Zero-length string means MAC is unknown. Sample: 00-e0-fc-b4-0b-ee
6	Multicast VLAN	1..4 Bytes	Multicast VLAN of the program Sample: 200
7	Program Group IP	9..15 Bytes	Zero-length string means source IP of the program is not configured. Sample: 10.1.1.1
8	Program Source IP	0..15 Bytes	Sample: 192.168.1.1. If the IP address is invalid, this parameter is "".

ID	Field Name	Specification	Commentary
9	Start viewing time	19 Bytes	YYYY-MM-DD HH:MM:SS{+ -}hh:mm [DST]. Sample: 2011-08-27 09:30:20+08:00
10	Time of record generation	19 Bytes	YYYY-MM-DD HH:MM:SS{+ -}hh:mm [DST] Sample: 2011-08-27 10:30:20+08:00
11	Program Name	1..16 Bytes	Sample: cctv1
12	Duration viewed	1..n Bytes	Viewing duration in seconds. Sample: 30

13.4.5.8 Double-VLAN Tag Multicast

Double-tag multicast specially refers to the number of VLAN tags of packets carried by the network-side multicast of the access device. In actual multicast networks, generally only one VLAN tag is used for multicast. The reasons for using double-tag multicast are as follows:

- The unicast application is limited by VLAN number supported by device and more and more applications adopt the double-tag planning. In addition, because the convergence switches of some vendors interconnected with the access device do not support transmission of single-tag packets and double-tag packets on the same physical link, the multicast has to adopt the double-tag mode.
- To use the VLAN planning like that of unicast in a unified manner. For example, outer VLAN tags indicate different ISPs and inner VLAN tags indicate different services.

The device can be configured whether to use the double-tag multicast function.

- IGMP control message
Double-tag multicast and single-tag multicast have the same processing flow for IGMP control messages (see ["Join Flow"](#)). Difference between them: On the network side, the transmitted and received IGMP messages in single-tag multicast have one tag whereas the transmitted and received IGMP messages in double-tag multicast have two tags. The outer VLAN tag in double-tag multicast is the MVLAN to which the program belongs and the inner VLAN tag can be configured based on MVLAN (adopting the "easy in strict out" principle, the device does not check the inner tag and configuration consistency of received IGMP messages). The inner tag priority and outer tag priority of IGMP packets can be configured separately based on MVLAN, but the inner tag priority must be the same as the outer tag priority in the same MVLAN and cannot be configured separately. If interconnection with a device of non-0x8100 TPID is required, the MVLAN is configured to a stacking VLAN and then TPIDs of inner tag and outer tag are configured globally.

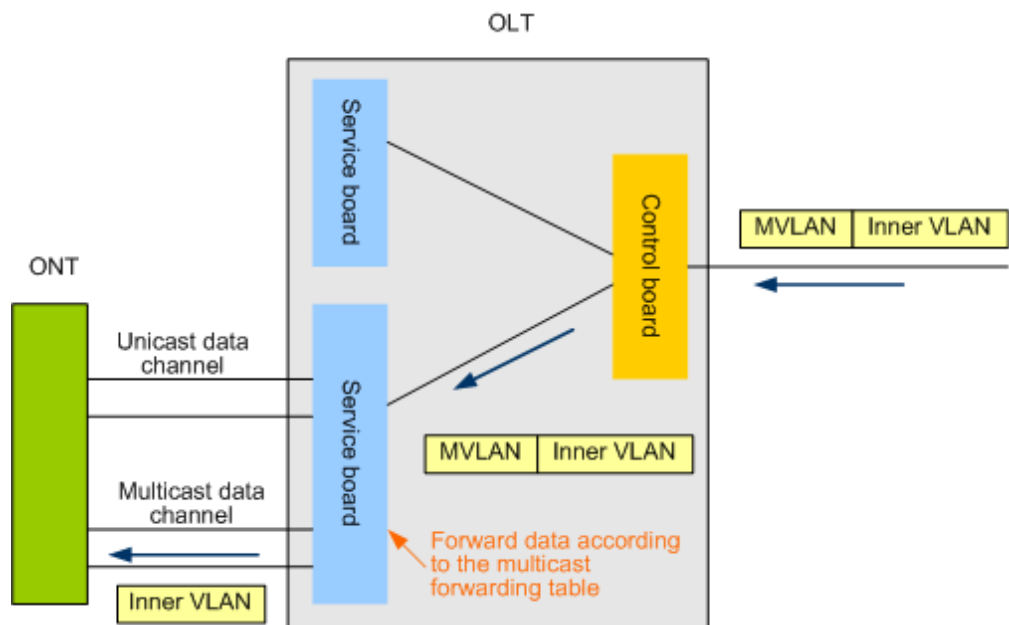
- Multicast data hardware forwarding

The data forwarding flow of double-tag multicast streams varies according to the GPON duplication mode. If the multicast duplication mode is multicast (single-copy duplication), multicast streams are forwarded on the control board and service board according to the multicast forwarding entry. The VLAN carried by the multicast streams forwarded to the ONT is the CVLAN. Because of the multicast duplication feature, in this scenario, the inner VLAN is often directly defined as the MVLAN (In addition, the device currently supports only this scenario).

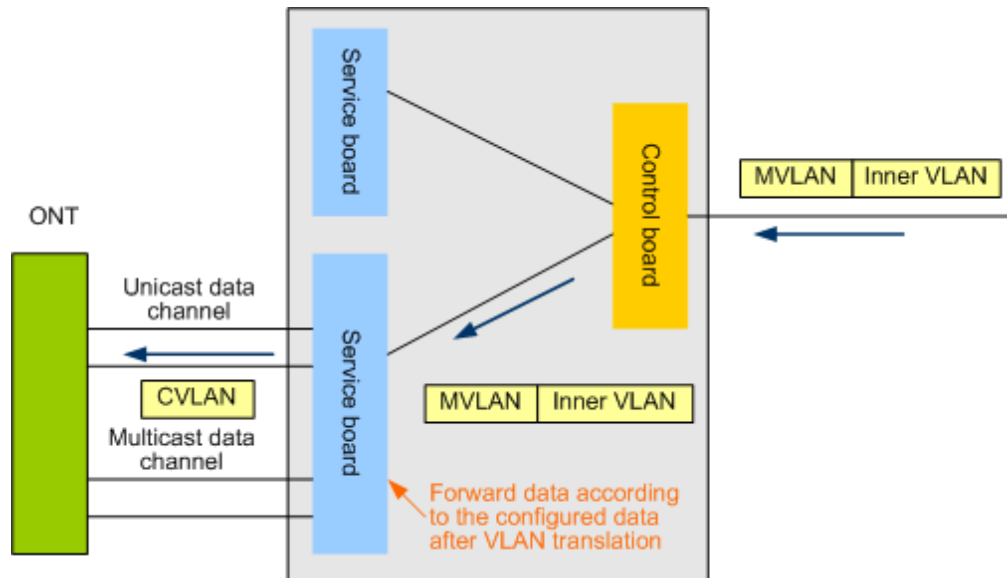
 NOTE

This scenario is applicable only when the TPID is 0x8100.

Figure 13-57 Double-tag multicast hardware forwarding (single-copy duplication)



If the multicast duplication mode is unicast (multi-copy duplication), multicast streams are forwarded on the control board according to the multicast forwarding entry and on the service board according to the configured service port. The VLAN carried by the multicast streams forwarded to the ONT is the CVLAN. In this scenario, the inner VLAN is often defined as the CVLAN.

Figure 13-58 Double-tag multicast hardware forwarding (multi-copy duplication)

13.4.5.9 Transparent Transmission of Multicast Data

- Transparent transmission of multicast data for private-line users
 - Transparent transmission of IGMP messages

In the upstream direction, the service board determines whether to transparently transmit the received IGMP messages according to the VLAN-level IGMP transparent transmission policy and service-port-level transparent transmission policy. If transparent transmission is allowed, IGMP messages are added with the SVLAN tag on the service board and then are transmitted to the control board. After arriving at the control board, IGMP messages are broadcast by the control board within the SVLAN. If transparent transmission is not allowed, IGMP messages are dropped.

In the downstream direction, the IGMP messages transmitted from the network side are broadcast by the control board within the SVLAN and after they arrive at the service board, the service board determines whether to transparently transmit them according to the VLAN-level IGMP transparent transmission policy and service-port-level transparent transmission policy. If transparent transmission is allowed, the service board translates the SVLAN tag to the CLAN tag according to the configuration of the traffic stream and then transmits the messages to users. If transparent transmission is not allowed, IGMP messages are dropped.

- Transparent transmission of unknown multicast data

In the upstream direction, the service board determines whether to transparently transmit the received unknown multicast data according to the VLAN-level IGMP transparent transmission policy and service-port-level transparent transmission policy. If transparent transmission is allowed, IGMP messages are added with the SVLAN tag on the service

board and then are transmitted to the control board. After arriving at the control board, IGMP messages are broadcast by the control board within the SVLAN. If transparent transmission is not allowed, IGMP messages are dropped.

In the downstream direction, the unknown multicast data transmitted from the network side is broadcast by the control board within the SVLAN and after the data arrives at the service board, the service board determines whether to transparently transmit the data according to the VLAN-level IGMP transparent transmission policy and service-port-level transparent transmission policy. If transparent transmission is allowed, the service board translates the SVLAN tag to the CLAN tag according to the configuration of the traffic stream and then transmits the data to users. If transparent transmission is not allowed, unknown multicast data is dropped.

NOTE

To prevent the multicast data of the multicast user provisioned with multicast service from being transmitted to the upstream unauthorized multicast sources, make sure that the policy of transmitting unknown multicast data is set to drop. The transparent transmission policies of unknown multicast traffic have the switches of two levels on a service board: the VLAN level and the service port level. When the two switches are both set to transparent transmission, the policy is transparent transmission. When either of the two switches is set to drop, the policy is drop. (Only transparent transmission is supported for connection-oriented traffic and the policy is not configurable in this case.)

- Co-existence of IPTV service and transparent transmission of multicast data
 - Multi-service-port solution

IPTV service and multicast transparent transmission service are carried on two service ports, and the SVLAN of the service port that carries multicast transparent transmission service must not be the MVLAN.

The service port that carries IPTV service processes the received IGMP messages following the flow of processing IPTV service, and forwards the multicast data according to the multicast forwarding entry.

The service port that carries multicast transparent transmission service transparently transmits or drops the received IGMP messages according to the IGMP transparent transmission policy of the traffic stream, and transmits or drops the received unknown multicast data according to the unknown multicast transparent transmission policy of the traffic stream.
 - Single-service-port solution

IPTV service and multicast transparent transmission service are carried on one service port, whose SVLAN must not be the MVLAN.

When the Access Node receives upstream IGMP messages, it matches the multicast group address in IGMP messages to the programs in the MVLAN. If the group address successfully matches a program, the Access Node processes the messages as IPTV service. If the group address fails to match any program, the Access Node determines whether to transparently transmit the messages according to the IGMP transparent transmission policy of the SVLAN and service port. The Access Node transparently transmits the messages only when the IGMP transparent transmission policy is enabled for both the SVLAN and service port.

If the Access Node receives downstream IGMP messages that carry the MVLAN tag, the Access Node processes the IGMP messages as IPTV

service. If the messages carry the SVLAN tag, the Access Node forwards them according to the IGMP transparent transmission policy of the SVLAN and service port. The Access Node transparently transmits the messages only when the IGMP transparent transmission policy is enabled for both the SVLAN and service port.

If the Access Node receives the multicast data of IPTV service, the Access Node forwards the multicast data according to the multicast forwarding entry. If the multicast data is unknown, the Access Node forwards the data according to the unknown multicast transparent transmission policy of the VLAN and service port. The Access Node transparently transmits the data only when the unknown multicast transparent transmission policy is enabled for both the SVLAN and service port.

13.5 IPv6 Multicast

This topic describes the aspects unique to IPv6 multicast and the differences between IPv4 multicast and IPv6 multicast.

13.5.1 Introduction to IPv6 Multicast

Overview

As a substitution of IPv4, IPv6 uses a 128-bit address structure to resolve IP address shortage issues and also optimizes some features. The difference between IPv6-based multicast and IPv4-based multicast lies in the significant increase of IP addresses. Other functions of the two types of multicast, such as group member management, multicast packet forwarding, and multicast routing setup, are basically the same.

Purpose

After an IPv4 network evolves to an IPv6 network, IPv6 multicast technologies can be used to provide carriers with a comprehensive set of IPv6 video services, such as live TV and near video on demand (NVoD).

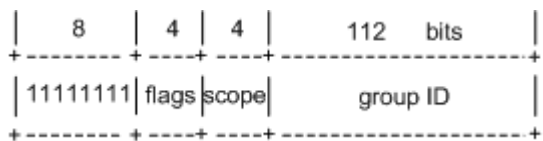
Using IPv6 multicast technologies, the network device can manage, control, and forward IPv6 video services and in this way meets carriers' requirements for provisioning IPv6 video services.

13.5.2 Principle

IPv6 Multicast Address

[Figure 13-59](#) shows the format of an IPv6 multicast address as defined in RFC4291.

Figure 13-59 Format of an IPv6 multicast address



The most significant eight bits of an IPv6 multicast address are consistently 11111111; therefore, an IPv6 multicast address always starts with FF.

Flags is a 4-bit field that indicates four flags set on the multicast address. The four flags are defined as |0|R|P|T|. The highest-order flag is always set to 0. The meanings of the other flags are as follows:

Table 13-25 Meaning of the flags Field

Name of the Bit	Value	Description
R	0	Indicates a multicast address that does not embed the unicast address on the rendezvous point (RP) of the multicast group.
	1	Indicates a multicast address that embeds the unicast address on the RP of the multicast group.
P	0	Indicates a multicast address that is not assigned based on the unicast prefix.
	1	Indicates a unicast-prefix-based multicast address.
T	0	Indicates a permanently assigned multicast address.
	1	Indicates a transient (not permanently assigned) multicast address. NOTE Currently, the multicast services of the device all use transient multicast addresses. Therefore, the T bit must be set to 1.

Scope is a 4-bit field that indicates the multicast scope. This field is used to signify the scope of a multicast group, that is, whether the multicast group contains nodes of the same local network, site, or organization, or nodes from the global address space. The values of this field are defined as follows:

Table 13-26 Meaning of the Scope Field

Value of the Scope Field	Description
0	Reserved

Value of the Scope Field	Description
1	Node/Interface-local scope
2	Link-local scope
3	Reserved
4	Admin-local scope
5	Site-local scope
8	Organization-local scope
E	Global scope
F	Reserved
6, 7, 9, and A-D	Unassigned

Group ID identifies the multicast group.

Ethernet Multicast MAC Address

RFC2464 defines a set of rules for mapping IPv6 multicast addresses to MAC addresses. An IPv6 address is mapped to the MAC address 3333.XXXX.XXXX, with the 32-bit XXXX.XXXX copied from the least significant 32 bits of the IPv6 address.

Protocol Interoperation

IPv6-based group members are managed using Multicast Listener Discovery (MLD).

MLD is a sub-protocol of Internet Control Message Protocol version 6 (ICMPv6). MLD establishes and maintains the multicast group membership between a user host and its immediately neighboring multicast router. MLD can be regarded as the Internet Group Management Protocol (IGMP) in IPv6, as MLD and IPv6 IGMP have similar implementations.

MLD has two versions: MLDv1 and MLDv2. MLDv2 is fully compatible with MLDv1 and includes all basic concepts of MLDv1.

- MLDv1 (defined in RFC2710)
MLDv1 is derived from IGMPv2 and supports any-source multicast (ASM), but supports source-specific multicast (SSM) through SSM mapping.
- MLDv2 (defined in RFC3810)
MLDv2 is a translation of IGMPv3 for IPv6 semantics and supports ASM and SSM. Compared with MLDv1 (defined in RFC2710), MLDv2 has the following improvements:
 - Batch report. The destination IP address in the IPv6 header of a report message is always filled in as FF02::1. In addition, the MLD payload can carry multiple group records, reducing the number of report messages between devices. In an MLDv1 report message, the destination

IP address must be filled in as the corresponding group IP address, so one MLDv1 report message cannot carry multiple group records.

- Longer maximum response time for a query message. The maximum response time for a query message is extended from 65.5s (in MLDv1) to 8387.5s (5000s supported by Huawei devices). Therefore, MLDv2 is applicable to large-scale networks.
- Source filter. With the source filter function, the host can receive or not receive the multicast data carrying the IP address of a specified multicast source. This function enables the device to better implement source-specific multicast (SSM) and support the multi-ISP scenario. MLDv1 supports only any-source multicast (ASM). The implementation of source filter in IPv6 is similar to that in IPv4.

Charging Mode

For multicast services, carriers or Internet service providers (ISPs) usually use two charging modes:

- Fixed charging. In this mode, programs are divided into different packages. Users need to pay a fixed amount of fee for each package in a fixed period (such as on a year or month basis). This charging mode does not restrict multicast users in the program-ordering count or the volume of traffic ordered.
- Pay per view (PPV): In this mode, users are charged according to how many times they order programs.

IPv6 multicast supports rights profiles and rights control and therefore supports fixed charging. IPv6 multicast does not support PPV because it does not support call detail record (CDR) reporting.

Program Ordering Behavior Analysis

IPv6 multicast supports local log recording and does not support log reporting. Log information can be obtained by local queries for analyzing program ordering behavior.

13.6 Configuring the Multicast Service

The MA5800 supports multicast cascading for reducing the number of ports used on the convergence device, and also supports Multiple Spanning Tree Protocol (MSTP) network protection. With these two functions, the network structure is optimized and the multicast service reliability is improved.

13.6.1 Differences Between IPv4 and IPv6 Multicast Configurations

IPv6 multicast refers to the multicast service implemented using the IPv6 protocol. Differences between IPv4 and IPv6 multicast configurations mainly relate to commands and functions. Before configuring IPv6 multicast, it is recommended that you familiarize yourself with the procedures and principles of configuring IPv4 multicast and be aware of the differences between IPv4 and IPv6 multicast configurations.

Differences Regarding Commands

NOTE

- The hyphen (-) indicates that the IPv4 command does not have a counterpart in IPv6. In other words, the corresponding multicast feature is not supported in IPv6.
- The multicast commands that are not listed in the table above are the commands supported by both IPv4 and IPv6.

Table 13-27 Differences between IPv4 and IPv6 multicast commands

IPv4	IPv6
Multicast additional functions	
igmp leave-proxy	igmp ipv6 leave-proxy
igmp priority	igmp ipv6 priority
igmp report-proxy	igmp ipv6 report-proxy
igmp echo	-
igmp encapsulation	-
igmp policy	-
igmp query-offline-user	-
igmp user-action-report	-
igmp mismatch	-
display igmp policy	-
Protocol parameters	
igmp proxy router gen-query-interval	igmp ipv6 router gen-query-interval
igmp proxy router gen-response-time	igmp ipv6 router gen-response-time
igmp proxy router robustness	igmp ipv6 router robustness
igmp proxy router sp-query-interval	igmp ipv6 router sp-query-interval
igmp proxy router sp-query-number	igmp ipv6 router sp-query-number
igmp proxy router sp-response-time	igmp ipv6 router sp-response-time
igmp initial-unsolicited-report interval	igmp ipv6 initial-unsolicited-report interval
igmp unsolicited-report interval	igmp ipv6 unsolicited-report interval
display igmp config vlan	display igmp ipv6 config vlan

IPv4	IPv6
igmp proxy router timeout	-
Multicast VLAN (MVLAN)	
igmp mode	igmp ipv6 mode
igmp match mode	igmp ipv6 match mode
igmp version	igmp ipv6 version
igmp match group	igmp ipv6 match group
display igmp config vlan	display igmp ipv6 config vlan
igmp send global-leave	-
Multicast users and rights	
debugging igmp	debugging igmp ipv6
Statistics measurement	
igmp statistic reset	igmp ipv6 statistic reset
display igmp statistic	display igmp ipv6 statistic
Logs	
display igmp log statistic	-
display igmp log	-

Differences Regarding Multicast Basic Service Configurations

IPv4 multicast can share VLANs with IPv6 multicast. Therefore, you can deploy IPv6 multicast in existing IPv4 MVLANs just by enabling IPv6 multicast in the IPv4 MVLANs and adding IPv6 multicast programs to the rights profiles. The parameters that have already been configured for users, such as the bound rights profiles and MVLANs, remain unchanged.

13.6.2 Configuring the Multicast Service on a Single NE

When the network structure is simple, the configuration of a single NE can meet multicast service requirements. Compared with cascading networking, single-NE networking is more secure and stable, and provides more bandwidth resources, but requires more line resources. The method of configuring multicast services for an NE in the cascading or MSTP networking scenario is the same as that in single-NE networking scenario.

Application Context

The multicast feature of the MA5800 is mainly applied to the live TV and near-video on demand (NVOD) multicast video services. The MA5800 runs the IGMP

proxy or IGMP snooping protocol, and the interconnected device can run the IGMP proxy, IGMP snooping, or multicast router protocol.

Currently, the multicast application of the MA5800 is oriented to Layer 2, and the MA5800 forwards data based on VLAN ID+multicast MAC address. A multicast program in the network is identified by VLAN ID + multicast IP address uniquely. The MA5800 differentiates multicast sources by VLAN ID. It allocates a unique VLAN ID to each multicast source, controls the multicast domain and the user right based on the multicast VLAN ID, and provides a platform for different ISPs to implement different multicast video services.

Data preparation

Before configuring the multicast video service, plan the data items as listed in [Table 13-28](#).

Table 13-28 Data plan for configuring the multicast service on a single MA5800

Device	Data Item
MA5800	Multicast VLAN
	Layer 2 multicast protocol
	IGMP version of the multicast VLAN
	IGMP version of the multicast user
	Multicast program configuration mode
	Multicast general query and group-specific query parameters
	NOTE The default values are adopted.
	Program list
	User authentication policy
	Program bandwidth, upstream port bandwidth, and user bandwidth
	Multicast ONT
	Multicast logging policy
Upper-layer multicast router	IGMP version
	NOTE The IGMP version of the upper-layer multicast router must not be earlier than the IGMP version of the multicast VLAN used by the MA5800.

Device	Data Item
Home gateway or modem	IGMP version NOTE The IGMP version of the home gateway or modem must not be earlier than the IGMP version of the multicast user on the MA5800.

Table 13-29 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	Disabled
IGMP version	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	Enabled
Multicast preview	Enabled
Multicast log function	Enabled

Configuration Flowchart

13.6.2.1 Configuring Multicast Global Parameters

The general parameters of Layer 2 multicast protocols (including IGMP proxy and IGMP snooping) configured for a device are applicable to all the multicast VLANs on the device.

Context

The multicast global parameters include general query, group-specific query, the policy of processing multicast packets and the multicast forwarding mode.

The description of a general query is as follows:

- Purpose: A general query packet is periodically sent by the MA5800 to check whether there is any multicast user who leaves the multicast group without sending the leave packet. Based on the query result, the MA5800 periodically updates the multicast forwarding table and releases the bandwidth of the multicast user that has left the multicast group.
- Principle: The MA5800 periodically sends the general query packet to all online IGMP users. If the MA5800 does not receive the response packet from a multicast user within a specified time (Robustness variable x General query interval + Maximum response time of a general query), it regards the user as having left the multicast group and deletes the user from the multicast group.

The description of a group-specific query is as follows:

- Purpose: A group-specific query packet is sent by the MA5800 after a multicast user that is not configured with the leave attribute sends the leave packet. The group-specific query packet is used to check whether the multicast user has left the multicast group.
- Principle: When a multicast user leaves a multicast group, for example, switches to another channel, the user unsolicitedly sends a leave packet to the MA5800. If the multicast user is not configured with the leave attribute, the MA5800 sends a group-specific query packet to the multicast group. If the MA5800 does not receive the response packet from the multicast user within a specified duration (Robustness variable x Group-specific query interval + Maximum response time of a group-specific query), it deletes the multicast user from the multicast group.

 NOTE

The configuration steps for IPv4 multicast and IPv6 multicast are similar but detailed commands are different. This topic describes the configuration steps for IPv4 multicast, and provides the configuration example for IPv6 multicast.

Table 13-30 lists the default settings of the multicast global parameters. In the actual application, you can modify the values according to the data plan.

Table 13-30 Default settings of the multicast global parameters

Parameter	Default Value
General query parameter	Query interval: 125s Maximum response time: 10s Robustness variable (query times): 2
Group-specific query parameter	Query interval: 1s Maximum response time: 0.8s. Robustness variable (query times): 2
Policy of processing multicast packets	IGMP packet: normal (IGMP packets are processed as controllable multicast) Unknown multicast packet: • For switch-oriented traffic streams: discard • For connection-oriented traffic streams: transparent transmission

Procedure

Step 1 Configure the general query parameters.

1. Run the **igmp proxy router gen-query-interval** command to set the general query interval. By default, the general query interval is 125s.
2. Run the **igmp proxy router gen-response-time** command to set the maximum response time of the general query. By default, the maximum response time of the general query is 10s.

3. Run the **igmp proxy router robustness** command to set the robustness variable (query times) of the general query. By default, the robustness variable (query times) is 2.

Step 2 Set the group-specific query parameters.

1. Run the **igmp proxy router sp-query-interval** command to set the group-specific query interval. By default, the group-specific query interval is 1s.
2. Run the **igmp proxy router sp-response-time** command to set the maximum response time of the group-specific query. By default, the maximum response time of the group-specific query is 0.8s.
3. Run the **igmp proxy router sp-query-number** command to set the robustness variable (query times) of the group-specific query. By default, the robustness variable (query times) is 2.

Step 3 Configure the policy of processing multicast packets.

The default values are adopted for multicast service and do not need to be modified. To control the forwarding of multicast packets when configuring other services, run the following commands to configure the policy.

1. Run the **igmp policy** command to set the policy of processing IGMP packets.
2. Run the **multicast-unknown policy** command to set the policy of processing unknown multicast packets(downstream UDP packets).

Step 4 Run the **display igmp config global** command to check whether the values of the multicast parameters are correct.

----End

Example

Example: To set the query interval to 150s, maximum response time to 20s, and number of queries to 3 in the multicast general query parameters for the IPv4 multicast VLAN 100 in IGMP V3, do as follows:

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp proxy router gen-query-interval 150
huawei(config-mvlan100)#igmp proxy router gen-response-time v3 200
huawei(config-mvlan100)#igmp proxy router robustness 3
```

Example: To set the query interval to 20s, maximum response time to 10s, and number of queries to 3 in the multicast group-specific query parameters for the IPv4 multicast VLAN 100 in IGMP V3, do as follows:

```
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp proxy router sp-query-interval 200
huawei(config-mvlan100)#igmp proxy router sp-response-time v3 100
huawei(config-mvlan100)#igmp proxy router sp-query-number 3
```

Example: To set the query interval to 150s, maximum response time to 20s, and number of queries to 3 in the multicast general query parameters for the IPv6 multicast VLAN 200 in MLD V2, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router gen-query-interval 150
huawei(config-mvlan200)#igmp ipv6 router gen-response-time v2 200
huawei(config-mvlan200)#igmp ipv6 router robustness 3
```

Example: To set the query interval to 20s, maximum response time to 10s, and number of queries to 3 in the multicast group-specific query parameters for the IPv6 multicast VLAN 200 in MLD V2, do as follows:

```
huawei(config)#multicast-vlan 200
huawei(config-mvlan200)#igmp ipv6 router sp-query-interval 200
huawei(config-mvlan200)#igmp ipv6 router sp-response-time v2 100
huawei(config-mvlan200)#igmp ipv6 router sp-query-number 3
```

13.6.2.2 Configuring the Multicast VLAN and the Multicast Program

In the application of multicast service, multicast VLANs (MVLANS) are used to distinguish multicast ISPs. Generally, an MVLAN is allocated to each multicast ISP for the VLAN-based management of multicast programs, multicast protocols, IGMP versions, and the VLAN-based control of multicast domain and user right.

Context

To create a multicast VLAN, a common VLAN must be created first. The multicast VLAN can be the same as the unicast VLAN. In this case, the two VLANs can share the same service stream channel. The multicast VLAN can be different from the unicast VLAN. In this case, the two VLANs use different service stream channels.

One user port can be added to multiple multicast VLANs under the following restrictions:

- Among all the multicast VLANs of a user port, only one multicast VLAN is allowed to have dynamically generated programs.
- One user port is not allowed to belong to multiple MVLANS that are in the IGMPv3 snooping mode.

The source IP address in the multicast packets that are sent to the upper device by the OLT may be as follows:

- If the IP address of the program VLAN interface is configured, the source IP address is the IP address of VLAN interface.
- If the IP address of the program VLAN interface is not configured, the source IP address is the host IP address of the program.
- If the host IP address is not configured, the default address 0.0.0.0 is used.

Table 13-31 lists the default settings of the MVLAN attributes, including the Layer 2 multicast protocol, IGMP version, multicast program, and multicast upstream port.

Table 13-31 Default settings of the MVLAN attributes

Parameter	Default Value
Program matching mode	enable (static configuration mode)
Multicast upstream port mode	default
Layer 2 multicast protocol	off (multicast function disabled)
IGMP version	v3

Parameter	Default Value
Priority of forwarding IGMP packets by the upstream port	6
Group filter mode	asm-ssm

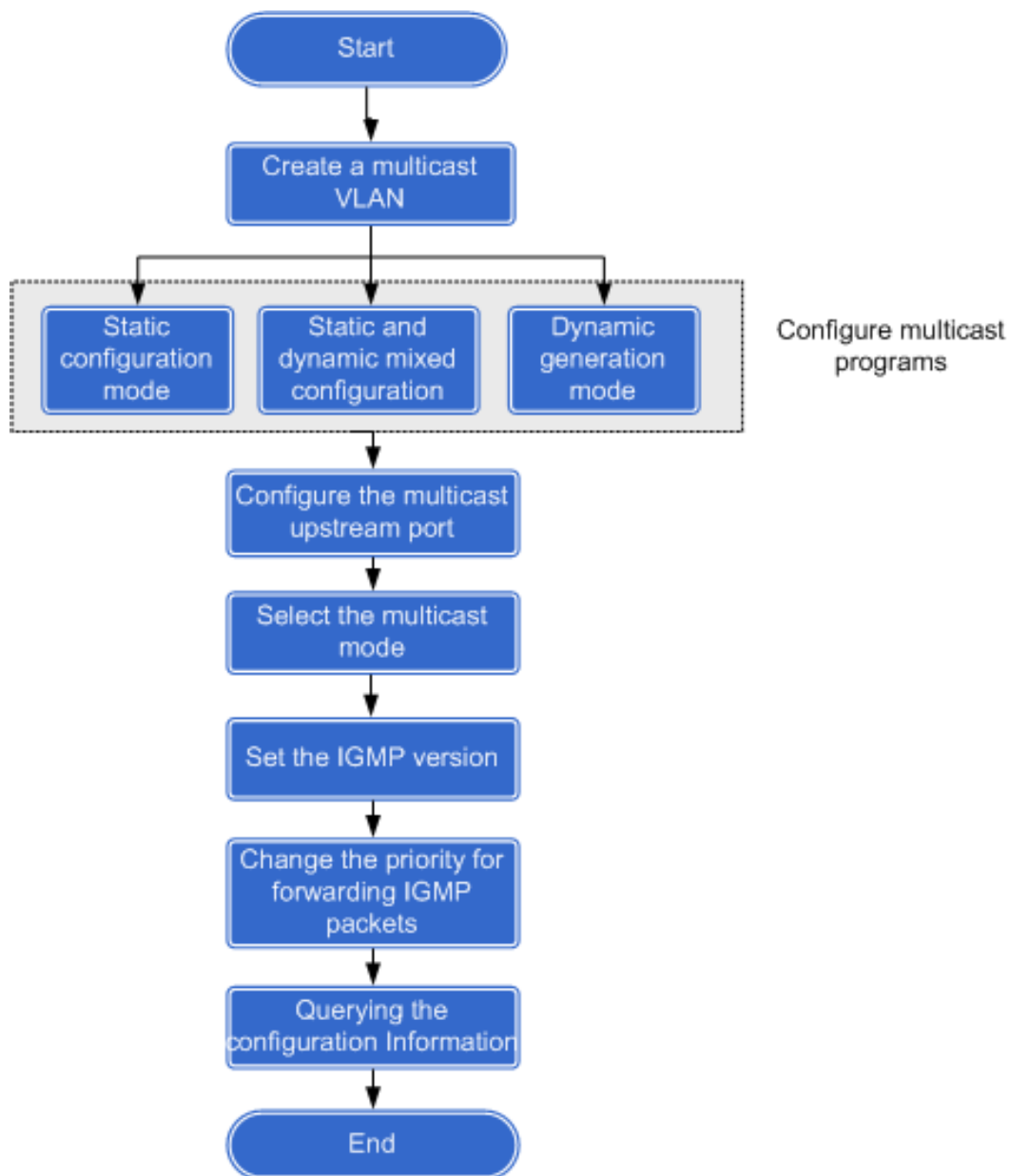
 NOTE

The device supports IPv4 and IPv6 multicast services. The two types of services have the same VLAN configurations and only differ in commands. The procedure in this topic uses IPv4 multicast as an example, and the example uses IPv6 multicast as an example.

Configuration Flowchart

[Figure 13-60](#) shows the flowchart for configuring the multicast VLAN and multicast program.

Figure 13-60 Flowchart for configuring the multicast VLAN and multicast program



Procedure

Step 1 Create a multicast VLAN.

1. Run the **vlan** command to create a VLAN, and set the VLAN type according to the actual application. For details on the VLAN configuration, see [Configuring VLAN](#).
2. Run the **multicast-vlan** command to set the created VLAN to a multicast VLAN. The VLAN with S+C forwarding mode cannot be set as a multicast VLAN.

Step 2 Configure multicast programs.

The multicast VLAN can be configured statically or generated dynamically. The program configuration of the MVLAN has three modes: static configuration, dynamic generation, and static and dynamic mixed configuration.

- Static configuration mode: Configure the program list before users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.
1. Run the **igmp match mode enable** or **igmp ipv6 match mode enable** command to set the static configuration mode. By default, the system adopts the static configuration mode.
 2. Run the **igmp program add** command to add a multicast program.

 NOTE

If the IGMP version of a multicast VLAN is v3, the program must be configured with a source IP address. If the IGMP version of a multicast VLAN is v2, the program must not be configured with a source IP address.

3. Add a right profile.

In the BTV mode, run the **igmp profile add** command to add a right profile.

4. Bind the program to the right profile.

In the BTV mode, run the **igmp profile** command to bind the program to the right profile, and set the right to watch.

 NOTE

When a user is bound to multiple right profiles, and the right profiles have different rights to a program, the right with the highest priority prevails. You can run the **igmp right-priority** command to adjust the priorities of the four rights: watch, preview, forbidden, and idle. By default, the priorities of the four rights are forbidden > preview > watch > idle.

- Dynamic generation mode: A program list is dynamically generated according to the programs requested by users. In this mode, the program list does not need to be configured or maintained; however, the functions such as program management, user multicast bandwidth management, program preview, and program prejoin are not supported.
1. Run the **igmp match mode disable** or **igmp ipv6 match mode disable** command to set the dynamic generation mode.

NOTICE

The **igmp match mode** or **igmp ipv6 match mode** command can be executed only when the multicast mode is disabled. If the multicast mode is set to off, users are forced to go offline. You are advised to perform initial configuration before service provisioning.

2. Run the **igmp match group** or **igmp ipv6 match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.

- Static and dynamic mixed configuration: Configure the program list before users watch the video programs. In this mode, the right profile can be used to implement controllable multicast. The program list and the right profile, however, need to be maintained according to the change of the video service. The program host, program prejoin, and multicast bandwidth management functions are supported.
- 1. Run the **igmp match mode disable** or **igmp ipv6 match mode disable** command to set the mode to the dynamic generation mode.
- 2. Run the **igmp match group** or **igmp ipv6 match group** command to configure the IP address range of the program group that can be dynamically generated. Users can order only the programs whose IP addresses are within the specified range.
- 3. Run the **igmp program add [name name] ip ip-addr [sourceip ip-addr] [hostip ip-addr]** command to add a multicast static program.

 NOTE

When the range of static program IP addresses and the range of dynamic program IP addresses overlap each other, static programs can go online with priority.

- 4. Run the **igmp group-filter-mode** command to set the group filter mode based on multicast VLAN (MVLAN).

 NOTE

- When the group filter mode of an MVLAN is configured to **asm-only** or **asm-ssm**, only one program with the unique multicast IP address is generated in the MVLAN. The [* , G] multicast forwarding table is used for this MVLAN instance on the forwarding plane.
- When the group filter mode of an MLVAN is configured to **ssm-only**, multiple programs with the same multicast IP addresses but different source IP addresses can be generated in the MVLAN. The [s, g] multicast forwarding table is used for this VLAN instance on the forwarding plane.

 NOTE

The source IP addresses are regarded as different ones when they have different least significant 20 bits from each other.

- The maximum number of programs is calculated according to the number of actually-generated programs. For example:
 - When a multicast user joins an MVLAN with the multicast filter mode **asm-ssm** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates only one multicast program with the multicast IP address G1 for the multicast user;
 - When a multicast user joins an MVLAN with the multicast filter mode **ssm-only** and the system receives two packets with IP addresses [S1, G1] and [S2, G1], the system generates two multicast programs with IP addresses [S1, G1] and [S2, G1].

Step 3 Configure the multicast upstream port.

- 1. Run the **igmp uplink-port** command to configure the multicast upstream port. The packets of the MVLAN corresponding to the upstream port are forwarded and received by this upstream port.
- 2. In the BTV mode, run the **igmp uplink-port-mode** command to change the mode of the multicast upstream port. By default, the port is in the default mode. In the MSTP network, the port adopts the MSTP mode.

- Default mode: If the MVLAN contains only one upstream port, the IGMP packets that go upstream can be sent only by this port. If the MVLAN contains multiple upstream ports, the IGMP packets that go upstream are sent by all the upstream ports.
- MSTP mode: This mode is adopted in the MSTP network.

Step 4 Select the multicast mode.

Run the **igmp mode { proxy | snooping }** command to select the Layer 2 multicast mode. By default, the multicast mode is disabled.

In terms of multicast processing mode, the MA5800 supports the Internet Group Management Protocol (IGMP) Proxy and IGMP Snooping Layer 2 multicast protocols. IGMP proxy and IGMP snooping both support multicast video data forwarding; however, the two modes have different processing mechanisms.

- In IGMP snooping, the related information for maintaining multicast forwarding entries is obtained by listening to the IGMP packets between the user and the multicast router.
- IGMP proxy intercepts the IGMP packets between the user and the multicast router, processes the IGMP packets, and then forwards the IGMP packets to the upper-layer multicast router. For the multicast user, the MA5800 is a multicast router that implements the router functions in the IGMP protocol; for the multicast router, the MA5800 is a multicast user.

In the IGMP snooping mode, proxy can be enabled for the report packet and the leave packet. When a multicast user joins or leaves a multicast program, the MA5800 can implement IGMP proxy. IGMP snooping and IGMP proxy are controlled separately.

- Run the **igmp report-proxy enable** command to enable the proxy of the snooping report packet. When the first user requests to join a program, after authenticating the user, the MA5800 sends the user report packet to the network side and receives a corresponding multicast stream from the multicast router. The report packets of the users who follow the first user are not sent by the MA5800 to the network side.
- Run the **igmp leave-proxy enable** command to enable the proxy of the snooping leave packet. When the last user requests to leave the program, the MA5800 sends the user leave packet to the network side to request the upper-layer device to stop sending multicast streams. The leave packets of the users who precede the last user are not sent by the MA5800 to the network side.

Step 5 Set the IGMP version.

Run the **igmp version{ v2 | v3 }** command to set the IGMP version. By default, IGMP v3 is enabled in the system. If the upper-layer and lower-layer devices in the network are IGMP v2 devices and cannot recognize the IGMP v3 packets, run this command to change the IGMP version.

IGMP v3 is compatible with IGMP v2 in packet processing. If IGMP v3 is enabled on the MA5800 and the upper-layer multicast router switches to IGMP v2, the MA5800 automatically switches to IGMP v2 when receiving the IGMP v2 packets. If the MA5800 does not receive any more IGMP v2 packets within the preset IGMP v2 timeout time, it automatically switches back to IGMP v3. In the BTV mode, run

the **igmp proxy router timeout** command to set the IGMP v2 timeout time. By default, the timeout time is 400s.

Step 6 Change the priority for forwarding IGMP packets.

Run the **igmp priority** command to change the priority for forwarding the IGMP packets by the upstream port. By default, the priority is 6 and does not need to be changed.

- In the IGMP proxy mode, the IGMP packets sent from the upstream port to the network side adopt the priority set through the preceding command in the MVLAN.
- In the IGMP snooping mode, the IGMP packets forwarded to the network side adopt the priority of the user service stream. The priority of the service stream is set through the traffic profile.

Step 7 Check whether the configuration is correct.

- Run the **display igmp config vlan** command to query the attributes of the multicast VLAN.
- Run the **display igmp program vlan** command to query the information about the program of the MVLAN.

----End

Example

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IP address: 224.1.1.1
- Source IP address: 10.10.10.10; host IP address: 10.0.0.254
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/9/0
- Protocol: IGMP proxy; IGMP version: v3
- Group filter mode: ssm-only

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode enable
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip 10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/9/0
huawei(config-mvlan101)#igmp mode proxy
Are you sure to change IGMP mode?(y/n)[n]:y
Command is being executed. Please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp version v3
huawei(config-mvlan101)#igmp group-filter-mode ssm-only
```

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

- MVLAN ID: 101
- Program configuration mode: dynamic generation

- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- MVLAN upstream port: 0/9/0
- Protocol: IGMP proxy; IGMP version: v3

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode disable
This operation will delete all the programs in current multicast vlan
Are you sure to change current match mode? (y/n)[n]: y
Command is being executed, please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp uplink-port 0/9/0
huawei(config-mvlan101)#igmp mode proxy
Are you sure to change IGMP mode?(y/n)[n]:y
Command is being executed. Please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp version v3
```

To configure the MVLAN and multicast program for the IPv4 multicast, do as follows:

- MVLAN ID: 101
- Program configuration mode: static and dynamic mixed configuration
- MVLAN upstream port: 0/9/0
- IP address of the static program: 224.1.1.1; source IP address: 10.10.10.10; host IP address: 10.0.0.254; program bandwidth: 5000 kbit/s
- Address range of the dynamic program group: 224.1.1.10 to 224.1.1.50
- Protocol: IGMP proxy; IGMP version: v3

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp match mode disable
This operation will delete all the programs in current multicast vlan
Are you sure to change current match mode? (y/n)[n]: y
Command is being executed, please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp match group ip 224.1.1.10 to-ip 224.1.1.50
huawei(config-mvlan101)#igmp program add name movie ip 224.1.1.1 sourceip 10.10.10.10
hostip 10.0.0.254 bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/9/0
huawei(config-mvlan101)#igmp mode proxy
Are you sure to change IGMP mode?(y/n)[n]:y
Command is being executed. Please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp version v3
```

To configure the MVLAN and multicast program for the IPv6 multicast, do as follows:

- MVLAN ID: 101
- Program configuration mode: static configuration; program IPv6 address:ffff::1
- Source IPv6 address: 2001:db8::1
- Program bandwidth: 5000 kbit/s
- MVLAN upstream port: 0/9/0
- Protocol: IGMP proxy; IGMP version: v2

```
huawei(config)#vlan 101 smart
huawei(config)#multicast-vlan 101
```

```
huawei(config-mvlan101)#igmp ipv6 match mode enable
huawei(config-mvlan101)#igmp program add name movie ipv6 ffff::1 source-ipv6 2001:db8::1
bandwidth 5000
huawei(config-mvlan101)#igmp uplink-port 0/9/0
huawei(config-mvlan101)#igmp ipv6 mode proxy
Are you sure to change IGMP mode?(y/n)[n]:y
Command is being executed. Please wait...
Command has been executed successfully
huawei(config-mvlan101)#igmp ipv6 version v2
```

13.6.2.3 Configuring the Multicast GPON ONT

When the MA5800 is connected with an ONT or an MDU, you need to configure the multicast interconnection data to forward the multicast traffic streams.

Prerequisites

Before configuring a multicast GPON ONT, you must add the ONT correctly. For the configuration method, see [Configuring the GPON ONT](#).

Context

- When the OLT is connected with an ONT, the MA5800 manages the ONT in the OMCI mode. In this case, you need to configure the ONT line profile and the ONT service profile, configure the multicast data in the ONT service profile, and bind the profiles to the ONT to issue the multicast service.
- When the OLT is connected with an MDU, the MA5800 manages the MDU in the SNMP mode. In this case, you do not need to configure the ONT service profile. You only need to configure the multicast data on the MDU interconnected with the MA5800 to forward the multicast traffic streams.

Procedure

Step 1 Add an ONT line profile.

For the configuration method, see [Configuring the GPON ONT Line Profile](#).

Step 2 Add an ONT service profile.

Run the **ont-srvprofile gpon** command to add a GPON ONT service profile, and then enter the GPON ONT service profile mode.

If the ONT management mode is the SNMP mode, you do not need to configure the service profile. After adding a GPON ONT service profile, directly enter the GPON ONT service profile mode to configure the related multicast data.

1. Run the **ont-port** command to configure the port capability set of the ONT. The port capability set in the ONT service profile must be the same as the actual ONT capability set.
2. Run the **port vlan** command to configure the port VLAN of the ONT.
3. Configure the multicast mode of the ONT.

Run the **multicast mode { igmp-snooping|olt-control|unconcern }** command to select the multicast mode.

- **igmp-snooping**: IGMP snooping obtains the related information and maintains the multicast forwarding entries by listening to the IGMP packets in the communication between the user and the multicast router.
 - **olt-control**: It is the dynamic controllable multicast mode. A multicast forwarding entry can be created for the multicast join packet of the user only after the packet passes the authentication.
 - **unconcern**: It is the unconcern mode. After this mode is selected, the OLT does not limit the multicast mode, and the multicast mode on the OLT automatically matches the multicast mode on the ONT.
4. (Optional)Configure the multicast forwarding mode.

Run the **multicast-forward { untag | tag { translation vlanid | transparent } | unconcern** command to configure the multicast forwarding mode and multicast forwarding VLAN. The forwarding mode is not concerned by default.

- **tag**: Specifies the multicast forwarding mode as tag. If the VLAN tag of the multicast packet needs to be transparently transmitted, use **transparent**; if the VLAN tag of the multicast packet needs to be switched, use **translation** and set the VLAN tag used after the switching. When the ONT is directly connected to the home gateway in the application, use this parameter.
 - **untag**: Specifies the multicast forwarding mode as untag, that is, the downstream multicast packet from the ONT's Ethernet port to a next directly connected device does not carry the VLAN tag. When the ONT is directly connected to the set top box (STB) or PC, use this parameter.
 - **unconcern**: Indicates that the multicast forwarding mode is not concerned. When the ONT multicast mode need not be configured by the OLT and is determined by the ONT condition, use **unconcern**. This value is the default value.
5. After the configuration is complete, run the **commit** command to make the configured service profile take effect.

NOTE

For an ONT that is added through the **ont add** command or an automatically found ONT that is confirmed through the **ont confirm** command, if you run the **commit** command after modifying the ONT line profile parameters and the ONT service profile parameters, the modified profile parameters take effect immediately.

----End

Example

To configure the ONT service profile 10 of 4 ETH ports, 2 POTS ports, the VLAN of the ETH port as 10, the multicast mode as IGMP snooping, the multicast forwarding mode as unconcern, do as follows:

```
huawei(config)#ont-srvprofile gpon profile-id 10
huawei(config-gpon-srvprofile-10)#ont-port eth 4 pots 2
huawei(config-gpon-srvprofile-10)#port vlan eth 1 10
huawei(config-gpon-srvprofile-10)#multicast mode igmp-snooping
huawei(config-gpon-srvprofile-10)#multicast-forward unconcern
huawei(config-gpon-srvprofile-10)#commit
huawei(config-gpon-srvprofile-10)#quit
```

13.6.2.4 Configuring a Multicast User

This topic describes how to configure a multicast user and the related user right for provisioning the multicast service.

Prerequisites

Before configuring a multicast user, create a service channel. The procedure is as follows:

- Configuring a GPON multicast user
 - a. [Configure the VLAN.](#)
 - b. [Configure the upstream port.](#)
 - c. [Configure the multicast GPON ONT.](#)
 - d. [Configure the GPON user port.](#)
 - e. [Configure the GPON traffic stream.](#)

Context

Add a multicast user, and bind the multicast user to the multicast VLAN to create a multicast member. Bind the multicast user to a right profile to implement multicast user authentication.

[Table 13-32](#) lists the default settings of the attributes related to the multicast user.

Table 13-32 Default settings of the attributes related to the multicast user

Parameter	Default Value
Maximum number of programs that can be watched by the multicast user	8
Maximum number of programs of different priorities that can be watched by the multicast user	no limit
Quick leave mode of the multicast user	MAC-based
Global switch of multicast user authentication	enable
IGMP version of the multicast user	v3

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure a multicast user and the multicast user attributes.

1. Add a multicast user.

Run the **igmp user add service-port** command to add a multicast user.

2. Configure the maximum number of programs that can be watched by the multicast user.
 - Run the **igmp user add service-port index max-program { max-program-num | no-limit }** command to configure the maximum number of programs that can be watched by the multicast user concurrently.
 - Run the **igmp user watch-limit service-port { hdtv | sdtv | streaming-video }** command to configure the maximum number of programs of different priorities that can be watched by the multicast user.

3. Set the quick leave mode of the multicast user.

Run the **igmp user add service-port index quickleave { immediate | disable | mac-based }** command to configure the quick leave mode of the multicast user. By default, the quick leave mode is the MAC-based mode.

- **Immediate:** After receiving the leave packet of the multicast user, the system immediately deletes the multicast user from the multicast group.
- **Disable:** After receiving the leave packet of the multicast user, the system sends an ACK packet to confirm that the multicast user leaves, and then deletes the multicast user from the multicast group.
- **MAC-based:** It is the quick leave mode based on the MAC address. The system checks the MAC address in the leave packet of the user. If it is the same as the MAC address in the report packet of the user and it is the last MAC address of multicast user, the system immediately deletes the multicast user from the multicast group. Otherwise, the system does not delete the multicast user. This mode is applied to the scenario with multiple terminals.

4. Set the IGMP version for the multicast user.

Run **igmp user add service-port index igmp-version { v2 | v3 | v3-forced | v2-with-query }** command to set the IGMP version for the multicast user. Each multicast user has an independent querier instance. This command specifies the IGMP version (default: v3) for the multicast user querier.

- v2: specifies the IGMP version to v2 for the multicast user querier. When this setting applies, the system processes only IGMP v2 packets and directly drops IGMP v1 packets and IGMP v3 packets.
- v3: specifies the v3-compatible mode (default setting for the system). When this setting applies, the system automatically specifies the IGMP version according to the version of the IGMP packets sent by users, but it directly drops IGMP v1 packets.
- v3-forced: forcibly specifies the IGMP version to V3 for the multicast user querier. When this setting applies, the system processes only IGMP v3 packets but directly drops IGMP v1 packets and IGMP v2 packets.
- v2-with-query: specifies the user querier version to IGMP v2 and can receive the IGMP v3 packet sent from the user side. When the system receives an IGMP v3 packet sent from the user side, the system sends a common query packet of the IGMP v2 version and discards the IGMP v3 packet.

Step 3 Configure multicast user authentication.

To control the right of a multicast user, you can enable the multicast user authentication function.

1. Configure the multicast user authentication function.

Run the **igmp user add service-port index { auth | no-auth }** command to configure whether to authenticate a multicast user.

 NOTE

After configuring multicast user authentication, you need to enable the global authentication function to make the configuration take effect. By default, the global authentication function is enabled. You can run the **igmp proxy authorization** command to change the configuration.

2. Bind the multicast user to the right profile. This operation is to implement user authentication.

Run the **igmp user bind-profile** command to bind the user to a right profile. After the binding, the multicast user has the rights to the programs as configured in the profile.

Step 4 Bind the multicast user to a multicast VLAN.

In the multicast VLAN mode, run the **igmp multicast-vlan member** command to bind the user to the multicast VLAN. Then, the multicast user becomes a multicast member of the multicast VLAN and can request the programs configured in the multicast VLAN.

Step 5 Run the **display igmp user** command to check whether the related multicast user information is correctly configured.

----End

Example

To add multicast user (port) 0/2/1 to multicast VLAN 101, enable user authentication, enable log report, set the maximum bandwidth to 10 Mbit/s, set IGMP version of the multicast user to v3-forced, and bind the user to right profile **music**, do as follows:

```
huawei(config)#service-port 100 vlan 101 gpon 0/2/1 ont 1 eth 0 multi-service user-vlan 101 rx-cttr 2 tx-cttr 2
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 100 auth log enable max-bandwidth 10240 igmp-version v3-forced
huawei(config-btv)#igmp user bind-profile service-port 100 profile-name music
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp multicast-vlan member service-port 100
```

13.6.2.5 (Optional) Configuring the Multicast Bandwidth

To limit the multicast bandwidth of a user, you can enable multicast bandwidth management, that is, connection admission control (CAC), and then control the bandwidth of a multicast user by setting the program bandwidth and the user bandwidth.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

If the CAC function is enabled and a user requests a multicast program, the system compares the remaining bandwidth of the user (bandwidth configured for the user - total bandwidth of the online programs of the user) with the bandwidth of the multicast program. If the remaining bandwidth of the user is sufficient, the system adds the user to the multicast group. If the bandwidth is insufficient, the system does not respond to the request of the user.

If the CAC function is disabled, the system does not guarantee the bandwidth of the multicast program. When the bandwidth is not guaranteed, problems such as mosaic and delay occur in the multicast program.

Table 13-33 lists the default settings of the CAC parameters.

Table 13-33 Default settings of the CAC parameters

Parameter	Default Value
Global CAC function	enable
Bandwidth of the multicast program	5000 kbit/s
Bandwidth of the multicast user	no-limit
Bandwidth of the GPON port	716800 kbit/s

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global CAC function.

By default, the global CAC function is already enabled. You can run the **igmp bandwidthCAC { enable | disable }** command to change the setting.

Step 3 Configure the bandwidth of the multicast user.

Run the **igmp user add service-port index max-bandwidth** command to allocate the maximum bandwidth of the multicast user.

Step 4 Configure the bandwidth of the multicast program.

- Run the **igmp program add ip ip-addr bandwidth** command to configure the bandwidth of a single multicast program. The program bandwidth is an attribute of a multicast program, specifying the bandwidth requirement of the program being played.
- Run the **igmp bandwidth port frameid/slotid/portid max-bandwidth{ bandwidth | no-limit }** command to configure the program bandwidth of a physical port on a board. This command is available for only the GPON port. The default bandwidth of a port is 716800 kbit/s. Configuring the total program bandwidth for a single port is a way of traffic management, which helps avoid network congestion caused by the excessively-large total program bandwidth on a port. When the total program bandwidth of a port

exceeds the value configured using the **igmp bandwidth port frameid/slotid/portid max-bandwidth{ bandwidth | no-limit }** command, subsequent programs ordered by users on this port cannot be played.

Step 5 Check whether the multicast bandwidth configuration is correct.

- Run the **display igmp config global** command to check the status of the global CAC function.
- Run the **display igmp program** command to query the bandwidth allocated to the multicast program.
- Run the **display igmp user** command to query the maximum bandwidth and the occupied bandwidth of the multicast user.

----End

Example

To enable bandwidth management for multicast users, set the user bandwidth to 10 Mbit/s when adding multicast user 0/2/1, and configure the program bandwidth to 1 Mbit/s when adding multicast program 224.1.1.1.

```
huawei(config)#btv
huawei(config-btv)#igmp bandwidthcac enable
huawei(config-btv)#igmp user add port 0/2/1 max-bandwidth 10240
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 bandwidth 1024
```

13.6.2.6 (Optional) Configuring Multicast Preview

Multicast preview is an advertising method provided by carriers for ISPs. The purpose is to allow users to have an overview of a program in a controlled way. In other words, the duration, interval, and count of the user previews are controlled.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

The difference between program preview and normal program watching is that, after the user goes online, the duration of the preview is restricted. When the duration expires, the user goes offline. The user can request the program again only after the preview interval expires. The count by which the user can request the program within a day (the start time can be configured) is restricted by the preview count of the user.

Multicast preview parameters are managed through the preview profile. One program can be bound to only one preview profile, but one preview profile can be referenced by multiple programs.

Table 13-34 lists the default settings of the multicast preview parameters.

Table 13-34 Default settings of the multicast preview parameters

Parameter	Default Value
Global multicast preview function	enable
Preview profile	Preview profile with index 0
Preview profile parameters	Maximum preview duration: 120s Maximum preview count: 8 Minimum interval between two previews: 120s
Time for resetting the preview record	4:00:00 am
Valid duration of multicast preview	30s

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Enable the global multicast preview function.

By default, the global multicast preview function is enabled. You can run the **igmp preview{ enable | disable }** command to change the setting.

Step 3 Configure the preview profile.

Run the **igmp preview-profile add** command to configure the preview profile, and set the parameters: maximum preview duration, maximum preview count, and minimum interval between two previews. The system has a default preview profile with index 0.

Step 4 Bind the program to the preview profile.

In the multicast VLAN mode, run the **igmp program add ip ip-addr preview-profile index** command to bind the program to be previewed to the preview profile so that the program has the preview attributes as defined in the preview profile. By default, the program is bound to the preview profile with index 0.

Step 5 Change the time for resetting the preview record.

Run the **igmp preview auto-reset-time** command to change the time for resetting the preview record. The preview record of the user remains valid within one day. On the second day, the preview record is reset. By default, the system resets the preview record at 4:00:00 a.m.

Step 6 Modify the valid duration of multicast preview.

Run the **igmp proxy recognition-time** or **igmp preview recognition-time** command to modify the valid duration of multicast preview. If the actual preview duration of the user is shorter than the valid duration, the preview is not regarded as a valid one and is not added to the preview count. By default, the valid duration of multicast preview is 30s.

 NOTE

If you use **igmp proxy recognition-time** and **igmp preview recognition-time** commands to set the valid duration of multicast preview concurrently, the one set by the **igmp preview recognition-time** command takes effect.

Step 7 Run the **display igmp config global** command to check whether the values of the multicast preview parameters are correct.

----End

Example

To enable preview of multicast programs by using the system default preview profile, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
```

To enable preview of multicast programs, create preview profile 1, set the maximum preview time to 150s, the maximum preview count to 10, and apply this preview profile when adding program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp preview enable
huawei(config-btv)#igmp preview-profile add index 1 duration 150 times 10
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 preview-profile 1
```

13.6.2.7 (Optional) Configuring Program Prejoin

In program prejoin, the MA5800 receives in advance the multicast stream of a program from the upper-layer multicast router to the upstream port before a user sends a request to join a program, shortening the waiting time of the user for requesting the program.

Prerequisites

The program matching mode of the multicast VLAN must be the static configuration mode.

Context

Multicast program prejoin is the same as program request. The MA5800 plays the role of a user and sends the report packet for receiving in advance the multicast stream from the upper-layer multicast router to the upstream port.

After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled so that the user can request the program quickly. Generally, the upper-layer multicast router processes the user request by responding to the group-specific query and the general query.

 NOTE

The configuration steps for IPv4 multicast and IPv6 multicast are similar but detailed commands are different. This topic describes the configuration steps for IPv4 multicast, and provides the configuration example for IPv6 multicast.

Table 13-35 lists the default settings of the prejoin parameters.

Table 13-35 Default settings of the prejoin parameters

Parameter	Default Value
Prejoin function	disable
Unsolicited report of IGMP packets	disable

Procedure

Step 1 Enable the prejoin function.

Run the **igmp program add ip ip-addr prejoin enable** command to enable the prejoin function of a program. By default, the prejoin function is disabled.

Step 2 After the prejoin function is enabled, if the upper-layer multicast router does not support static multicast entry forwarding, the unsolicited report function needs to be enabled for IGMP packets.

- Run the **igmp program add ip ip-addr unsolicited enable** command to enable the unsolicited report function for IGMP packets. By default, the unsolicited report function is disabled.
- Run the **igmp unsolicited-report interval** command to modify the interval for unsolicitedly reporting IGMP packets. By default, the interval is 10s.

Step 3 Check whether the prejoin function is configured correctly.

- Run the **display igmp program** command to query the status of the prejoin function and the unsolicited report function.
- Run the **display igmp config vlan** command to query the interval for unsolicitedly reporting IGMP packets.

----End

Example

(IPv4)To enable the prejoin function when adding program 224.1.1.1 on multicast VLAN 101 for reduce the program waiting time of the users, do as follows:

```
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ip 224.1.1.1 prejoin enable
```

(IPv6)To enable the prejoin function when adding program ffff::1 on multicast VLAN 101 for reduce the program waiting time of the users, do as follows:

```
huawei(config)#multicast-vlan 101
huawei(config-mvlan101)#igmp program add ipv6 ffff::1 prejoin enable
```

13.6.2.8 (Optional) Configuring the Multicast Logging Function

Multicast log serves as a criterion for carriers to evaluate the viewership of multicast programs.

Prerequisites

If the syslog is used for reporting multicast logs, the syslog server must be properly configured.

If the syslog server is not configured, you can run the **igmp syslog disable** command to disable the multicast syslog reporting function to save system resources.

Context

Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled.

When the user stays online for longer than the valid time for generating logs, the system generates logs in any of the following conditions:

- The user goes offline naturally, by force, or abnormally.
- The user is blocked or deleted.
- The program is deleted.
- The program priority is changed.
- The upstream port to which the program is bound changes.
- The VLAN of the upstream port to which the program is bound changes.
- The right mode is switched.
- The user preview times out.
- The IGMP mode is switched.
- The bandwidth CAC is not passed.

When the user goes online, the system records only the online date and time. The system generates a complete log only when the user goes offline.

The MA5800 can report the multicast log to the log server in the syslog mode and the call detailed record (CDR) mode. By default, the MA5800 reports the log in the syslog mode.

- Syslog mode: Logs are reported to the syslog server in the form of a single log.
- CDR mode: Logs are reported to the log server in the form of a log file (.cvs). One log file contains multiple logs.

Table 13-36 lists the default settings of the multicast logging parameters.

Table 13-36 Default settings of the multicast logging parameters

Parameter	Default Value
Report mode of the multicast log	Syslog mode
Logging function at the multicast VLAN level	enable

Parameter	Default Value
Logging function at the multicast user level	enable
Logging function at the multicast program level	enable
Action report function of the multicast user	disable
Interval for automatically logging	2 hours
Minimum online duration for generating a valid log	30s
Parameters of the log report in the CDR mode	Report interval: 600s Maximum number of logs that can be reported each time: 200

Procedure

- Configure the parameters of the logging function of the multicast host.
 - a. Enable the multicast logging functions.

Multicast logs have three control levels: multicast VLAN level, multicast user level, and multicast program level. The system generates logs only when the logging functions at the three levels are enabled. By default, the three functions are enabled.

- In the Multicast VLAN mode, run the **igmp log { enable | disable }** command to configure the logging function at the multicast VLAN level.
- In the BTV mode, run the **igmp user add service-port index log { enable | disable }** command to configure the logging function at the multicast user level.

In the BTV mode, run the **igmp log record { user | mac }** command to configure the log record object. After the configuration, the device can record ordering action of users or multicast terminals identified by MAC addresses.
- In the Multicast VLAN mode, run the **igmp program add ip ip-addr log { enable | disable }** command to configure the logging function at the multicast program level.

- b. Modify the interval for automatically logging.

In the BTV mode, run the **igmp proxy log-interval** command to modify the interval for automatically logging. When the user stays online for a long time, the system generates logs at the preset interval. This is to prevent the problem that a log is not generated when the user leaves the multicast group without sending a leave packet, which can affect the accounting. By default, the interval is two hours.

- c. Modify the minimum online duration for generating a valid log.

In the BTV mode, run the **igmp proxy recognition-time** or **igmp log recognition-time** command to modify the minimum online duration for generating a valid log. If the user is in a multicast group (such as to preview a program) for shorter than the preset duration, the user operation is not regarded as a valid one and a log is not generated. A log is generated only when a user stays online for longer than the specified duration. By default, the minimum online duration is 30s.

 NOTE

If you use **igmp proxy recognition-time** and **igmp log recognition-time** commands to set the minimum online duration for generating a valid log concurrently, the one set by the **igmp log recognition-time** command takes effect.

- (Optional) Configure the action report function of the multicast user.

By default, the system uses the syslog mode to report multicast logs. You can run the **igmp user-action-report** command to configure the action report function of the multicast user. By default, the action report function of the multicast user is disabled.

- **enable**: Enables the action report function of the multicast user. Logs are reported to the syslog server when a multicast user goes online and offline.
- **disable**: Disables the action report function of the multicast user. Logs are reported to the syslog server only when a multicast user goes offline.

- Configure the function of CDR-mode log report.

- a. Configure the multicast log server and the data transmission mode for the CDR-mode log report.

Run the **file-server auto-backup cdr** command to configure the active and standby multicast log servers.

- b. Enable the function of CDR-mode log report.

In the BTV mode, run the **igmp cdr { enable | disable }** command to configure the function of CDR mode log report. After the function is enabled, the MA5800 reports the local multicast logs to the multicast log server in the form of a file. After the function is disabled, the MA5800 reports each single log to the syslog server in the default syslog mode.

- c. Configure the parameters of the log report in the CDR mode.

- In the BTV mode, run the **igmp cdr-interval** command to set the report interval. By default, the interval is 600s.
- In the BTV mode, run the **igmp cdr-number** command to set the maximum number of logs that can be reported each time. When the number of the multicast logs in the CDR file reaches the preset value, the MA5800 reports the logs. By default, the maximum number is 200.

- d. Check whether the configuration is correct.

- Run the **display file-server** command to query the configuration of the CDR multicast log server.

- Run the **display igmp config global** command to query the status and other parameters of the function of CDR-mode log report.

----End

Example

To configure the multicast log to be reported to log server 10.10.10.1 in the CDR mode, and use the SFTP transmission mode, do as follows:

```
huawei(config)#file-server auto-backup cdr primary 10.10.10.1 sftp path temp user
huawei(config)#btv
huawei(config-btv)#igmp cdr enable
```

13.6.2.9 (Optional) Configuring the Maximum Number of Programs That Can Be Watched by the Multicast User

This topic describes how to configure the maximum number of programs that can be ordered by the multicast user at the same time. You can configure the maximum number of all programs that can be watched by the multicast user at the same time, or configure the maximum number of the different-level programs that can be watched by the multicast user.

Prerequisites

When you configure the maximum number of programs based on the program level, the program level must be configured at the same time and the programs must be configured statically.

Context

[Table 13-37](#) lists the default settings of the max-program parameters.

Table 13-37 Default settings of the multicast max-program parameters

Parameter	Default Value
Maximum number of programs that can be watched by the multicast user	8
Grade of the multicast program	no-grade
Maximum number of programs of different priorities that can be watched by the multicast user	no-limit

Procedure

Step 1 In the global config mode, run the **btv** command to enter the BTV mode.

Step 2 Configure the max-program of the multicast user.

Run the **igmp user add service-port index max-program max-program-num** command to set the maximum number of programs that can be watched by the multicast user.

Step 3 Configure the maximum number of programs of different priorities that can be watched by the multicast user.

Run the **igmp user watch-limit service-port index** command to set the maximum number of programs of different priorities that can be watched by the multicast user.

Step 4 Configure the grade of the multicast program.

In the multicast VLAN mode, run the **igmp program add ip ip-addr grade** command to configure the grade of a multicast program.

Step 5 Check whether the multicast max-program configuration is correct.

- Run the **display igmp user** command to query the maximum number of programs that can be watched and watching by the multicast user.
- Run the **display igmp program** command to query the grade of the multicast program.
- Run the **display igmp user extended-attributes service-port** command to query the maximum number of programs that can be watched and watching by the multicast user.

----End

Example

To set the user max-program to 10 when adding multicast service-port 0, set the user can watch 2 HDTV program, and configure the program grade to hdtv when adding multicast program 224.1.1.1, do as follows:

```
huawei(config)#btv
huawei(config-btv)#igmp user add service-port 0 max-program 10
huawei(config-btv)#igmp user watch-limit service-port 0 hdtv 2
huawei(config-btv)#quit
huawei(config)#multicast-vlan 101
huawei(config-multicast-vlan 101)#igmp program add ip 224.1.1.1 grade hdtv
```

13.6.2.10 (Optional) Configuring the Maximum Rate for Sending IGMP Packets

When the multicast and anti-DoS attack functions are enabled, the system reports DoS attack alarms and drops IGMP packets over the rate limit, if a user port sends such IGMP packets to the CPU. When the anti-DoS attack function is disabled, the system always sends IGMP packets to the CPU. If they are sent to the CPU at a rate higher than the limit, the system drops the IGMP packets that exceed the rate limit but does not report DoS attack alarms.

Prerequisites

The multicast function is enabled.

Context

When the multicast function is enabled, the system will always send the received IGMP packets to the CPU if no control is implemented over the process. Then if a user port receives a large number of IGMP packets, the IGMP packets for other users will not be processed and directly dropped instead.

Table 13-38 lists the default maximum rate settings for sending user IGMP packets to the CPU.

Table 13-38 Default rate settings for sending user IGMP packets to the CPU

Parameter	Default Value
Anti-DoS attack function	disable
Maximum rate for sending IGMP packets to the CPU	63 pps

Procedure

Step 1 Enable the anti-DoS attack function.

Run the **security anti-dos { enable | disable }** command to enable the anti-DoS attack function, which is disabled by default.

Step 2 Specify the maximum rate for sending IGMP packets to the CPU.

Run the **security anti-dos control-packet igmp rate frameid/slotid/portid { value | ont | no-limit }** command to specify the maximum rate for sending IGMP packets to the CPU, which is 63 by default.

----End

Example

Example: Specify the maximum rate for sending IGMP packets to the CPU to 63 pps for user port 0/2/1 and enable the system to report the port to the blacklist if it sends IGMP packets over the rate limit to the CPU.

```
huawei(config)#security anti-dos enable
huawei(config)#security anti-dos control-packet igmp rate 0/2/1 ont 0 gemport 2 20
```

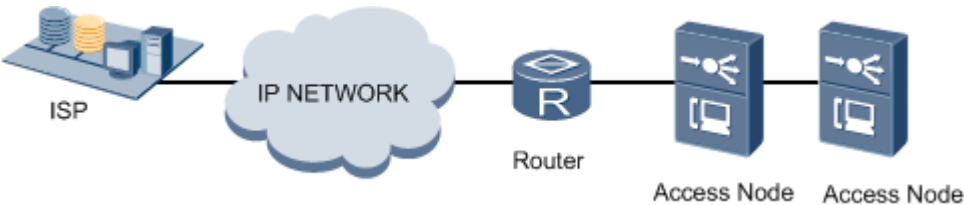
13.6.3 Configuring the Multicast Service on a Cascading Network

This topic describes how to configure the multicast service on the MA5800 on a cascading network.

Application Context

Figure 13-61 shows the application context of the multicast service in a cascading network. When a cascaded device needs to provision the multicast service, the cascading port on the cascading device needs to be configured as a multicast cascading port. In this way, the cascading device regards the cascaded device as an IGMP user.

Figure 13-61 Application context of multicast service in a cascading network



Default Configuration

Table 13-39 lists the default settings of the multicast service of the MA5800.

Table 13-39 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	off (multicast function disabled)
IGMP version, includes multicast user version and multicast VLAN version.	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	enabled
Multicast preview	enabled
Multicast log function	enabled

Precaution

The multicast program list of the cascading device must cover the multicast program list of the cascaded device.

Procedure

The procedure for configuring the cascaded device is the same as described in [Configuring the Multicast Service in a Single-NE Network](#).

The procedure of configuring the cascading device is as follows:

1. For details on configuring the multicast service, see [Configuring the Multicast Service in a Single-NE Network](#).

2. Configure the multicast cascading port.
Run the **igmp cascade-port frameid/slotid/portid** command to configure the cascading port as the multicast cascading port. The multicast upstream port cannot be configured as a multicast cascading port.
3. When the cascaded device requires the quick leave function of the multicast user, run the **igmp cascade-port frameid/slotid/portid quickleave enable** command to enable the quick leave attribute on the multicast cascading port.

NOTICE

If the lower-layer device does not support the proxy of the IGMP leave packet, all the users requesting the program may go offline when a user requesting the same program goes offline. Therefore, when the quick leave attribute is enabled on the multicast cascading port, it is recommended that the lower-layer device use the IGMP proxy function, or switch to the IGMP snooping mode with the IGMP leave packet proxy function enabled.

13.6.4 Configuring the Multicast Service in an MSTP Network

This topic describes how to configure the multicast service in an MSTP network.

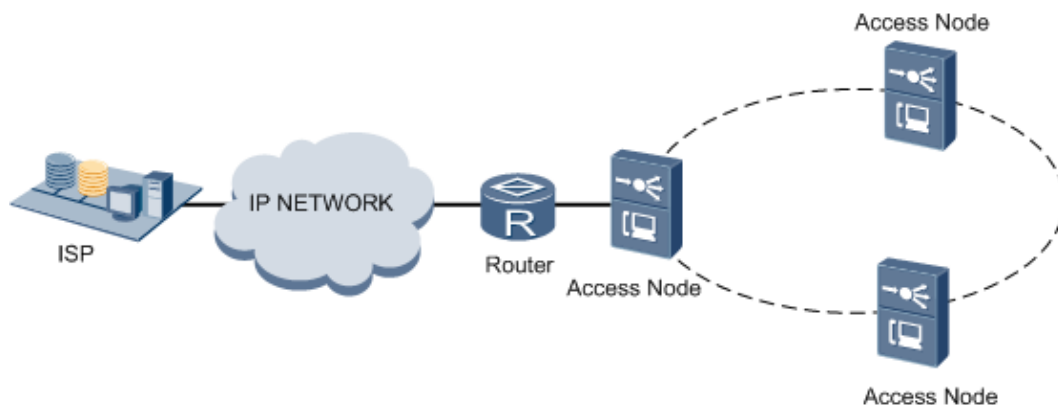
Prerequisites

Basic configurations for the MSTP network are complete. For details about configuring the MSTP network, see [Configuring the MSTP](#).

Application Context

Figure 13-62 shows the application context of the multicast service in an MSTP network. When the multicast service is provisioned in an MSTP ring network, the multicast upstream port and the cascading port need to be added to the multicast VLAN. According to the running result of the MSTP protocol, the multicast request packets are sent from the root port or the default port (when the device is a root bridge), and the other ports in the VLAN serve as cascading ports.

Figure 13-62 Application context of the multicast service in an MSTP network



Default Configuration

Table 13-40 Default settings of the multicast service

Feature	Default Settings
Multicast protocol	off (multicast function disabled)
IGMP version, includes multicast user version and multicast VLAN version.	V3
Multicast program configuration mode	Static configuration mode
Multicast bandwidth management	enabled
Multicast preview	enabled
Multicast log function	enabled

Procedure

For details on configuring the MSTP ring network, see [Configuring the MSTP](#).

- For details on configuring the multicast service, see [Configuring the Multicast Service in a Single-NE Network](#).
- Configure the MSTP multicast upstream port.

When multicast service is provisioned in an MSTP network, the multicast upstream port needs to be set to the MSTP mode, and the default upstream port of the multicast VLAN can be specified. After the configuration is completed, multicast packets are forwarded by the root port or default port of the multicast VLAN.

 - Run the **igmp uplink-port-mode mstp** command to set the upstream port to the MSTP mode.
 - Run the **igmp default uplink-port** command to specify the default upstream port of the multicast VLAN. When the upstream port is set to the MSTP mode and an MSTP root port is not available in the multicast VLAN, the multicast VLAN by default adopts the upstream port as the multicast upstream port.
- Configure the multicast cascading port.

Run the **igmp cascade-port** command to configure the cascading port as the multicast cascading port.
- Configure multicast quick convergence in the case of an MSTP network topology change.

Multicast quick convergence means that the device can quickly join the multicast group through a new upstream port when the MSTP network topology changes. The device can unsolicitedly send the new upstream port the IGMP join packet for an online program so that the device joins all the multicast groups. Or, the device can send the IGMP global leave packet to the upstream port. Then, the upper-layer querier sends a query packet for generating a new multicast forwarding tree.

Run the **igmp send global-leave** command to enable the function of sending the IGMP global leave packet. When this function is enabled, the device sends the IGMP global leave packet to the upper-layer multicast router. When this function is disabled, the device sends the IGMP join packet to the upper-layer multicast router. By default, the function of sending the IGMP global leave packet is enabled.

13.6.5 Configuring the PIM Service

This topic describes how to configure the Protocol Independent Multicast (PIM) service.

Prerequisites

- The access network is enabled with routing and can obtain the rendezvous point (RP) or routing information about an ISP device.
- The upper-layer device interconnected with the access device is enabled with PIM.

Context

A multicast network requires multicast protocols to replicate and forward multicast data. PIM is a widely used intra-domain multicast protocol that builds MDTs to transmit multicast data between routers in the same domain.

PIM can create multicast routing entries on demand, forward packets based on multicast routing entries, and dynamically respond to network topology changes.

Concurrently, the access node supports PIM-SM (used in an IPv4 network) and PIM-SSM (used in IPv4 and IPv6 networks).

Application Context

Figure 13-63 shows the PIM networking. The access node exchanges with the upper-layer device through PIM and exchanges with the user-side device through IGMP.

Figure 13-63 PIM networking



Procedure

- Step 1** Create a multicast VLAN and VLAN of the upstream PIM interface, and add the upstream port to the VLAN of the PIM interface.
1. Run the **vlan** command to create a multicast VLAN and VLAN of the upstream PIM interface.

2. Run the **port vlan vlan-list frameid/slotid portlist** to add the upstream port to the VLAN of the PIM interface.

Step 2 Enable the multicast function.

Run the **multicast routing-enable** command to enable multicast or run the **multicast ipv6 routing-enable** command to enable IPv6 multicast.

Step 3 Set upstream multicast mode to PIM.

- If PIM-SM is used in the upstream direction, run the **multicast upstream-mode pim-sm** command to set the upstream multicast exchange mode to PIM-SM.
- If PIM-SSM is used in the upstream direction, run the **multicast upstream-mode pim-ssm** command to set the upstream multicast exchange mode to PIM-SSM.

Step 4 Create the VLAN interface of the upstream PIM interface, configure the IP address of the Layer 3 interface, and enable PIM on this Layer 3 interface.

1. Run the **interface vlanif** command to create the VLAN interface of the upstream PIM interface.
2. Run the **ip address** or **ipv6 address** command to configure the IP addresses of the Layer 3 interface.
3. Run the **pim sm** or **pim ipv6 sm** command to enable PIM on the Layer 3 interface.

Step 5 Create the multicast VLAN interface, configure the IP address of the Layer 3 interface, and enable multicast on this Layer 3 interface.

1. Run the **interface vlanif** command to create a multicast VLAN interface.
2. Run the **ip address** or **ipv6 address** command to configure the IP addresses of the Layer 3 interface.

Step 6 (Optional) If PIM-SM is enabled in the upstream direction, static RPs need to be configured.

Run the **static-rp** command to configure static RPs.

Step 7 Configure multicast programs.

Run the **igmp program add** command to configure a multicast program.

Step 8 Configure multicast users.

Run the **igmp user add** command to configure a multicast user.

----End

Example

To enable PIM-SSM in the upstream direction and IGMP in the downstream direction, do as follows:

- Upstream port: 0/9/0
- VLAN of the upstream PIM-SSM interface: 200; IP address of the Layer 3 interface: 10.1.1.1; mask: 24
- Multicast VLAN: 100; IP address of the Layer 3 interface: 10.2.2.2; mask: 24

- Service VLAN 100 for the multicast service; all users in the VLAN are added as multicast users in batches; Set all multicast users in the service VLAN as members of the multicast VLAN.

- Multicast program: static; program name: movie; program IP address: 232.1.1.1; source IP address: 10.1.1.2; program bandwidth: 5000 kbit/s

```
huawei(config)#vlan 100
huawei(config)#vlan 200
huawei(config)#port vlan 200 0/9 0
huawei(config)#multicast routing-enable
huawei(config)#multicast upstream-mode pim-ssm
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 10.1.1.1 24
huawei(config-if-vlanif200)#pim sm
huawei(config-if-vlanif200)#quit
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.2.2.2 24
huawei(config-if-vlanif100)#quit
huawei(config)#btv
huawei(config-btv)#igmp user add smart-vlan 100
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp multicast-vlan member smart-vlan 100
huawei(config-mvlan100)#igmp program add name movie ip 232.1.1.1 sourceip 10.1.1.2
bandwidth 5000
huawei(config-mvlan100)#quit
```

13.6.6 Configuring the Layer 2 Reverse Multicast Service

This topic describes how to configure the Layer 2 reverse multicast service.

Prerequisites

- An OLT has been installed.
- The IP route between the OLT and the network-side devices is reachable. The OLT and ONUs can be managed by eSight/Cloud Campus.
- The link between the OLT and ONUs is normal, and the ONUs can register with the OLT and go online.

Context

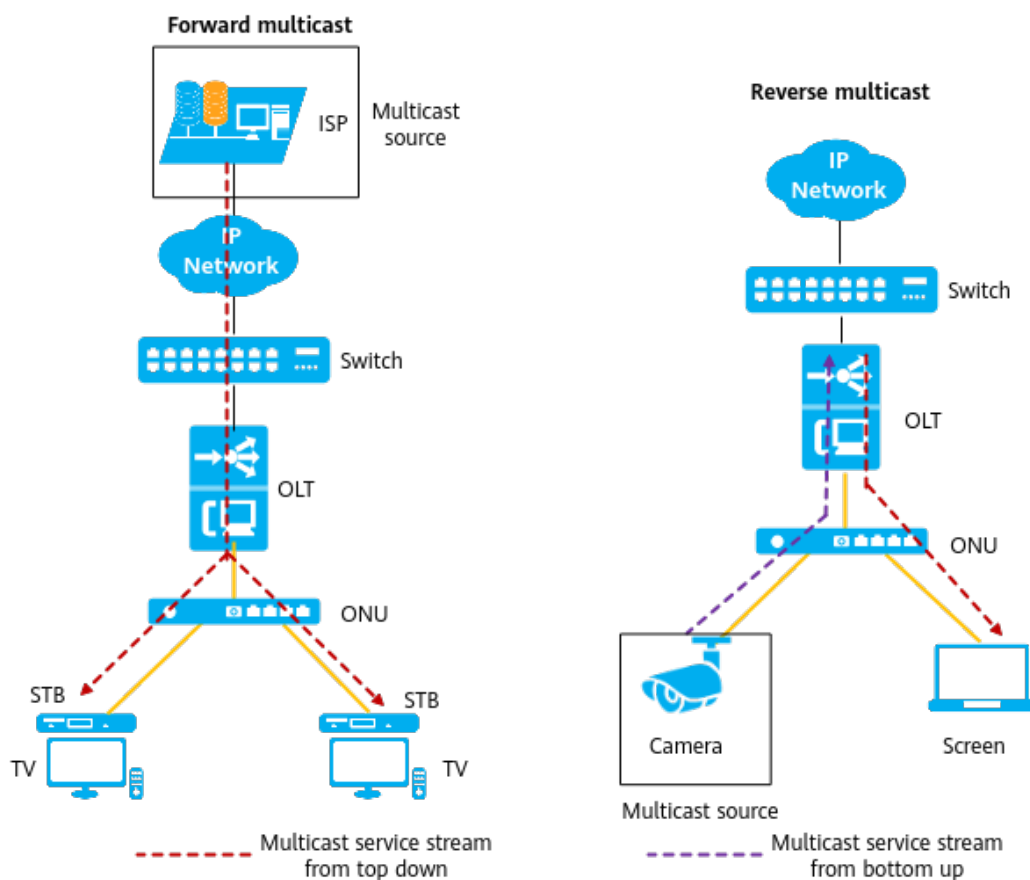
Generally, the upper-layer devices of an OLT, such as video servers, are considered as multicast sources. A video server issues the service stream of multicast programs to users from top down. This is forward multicast. However, in some scenarios, for example, in a subway station with a surveillance center and multiple sub-surveillance centers, reverse multicast is required when the stream of some cameras needs to be displayed on several large screens.

In reverse multicast, the multicast source comes from a user under the OLT. The service stream from the multicast source is replicated on the OLT and then sent to other multicast users in the same multicast VLAN. [Figure 13-64](#) shows forward multicast and reverse multicast services.

NOTE

In the reverse multicast scenario, the multicast source must be directly connected to an ONU. Layer 2 or Layer 3 multicast networking is not supported under the ONU.

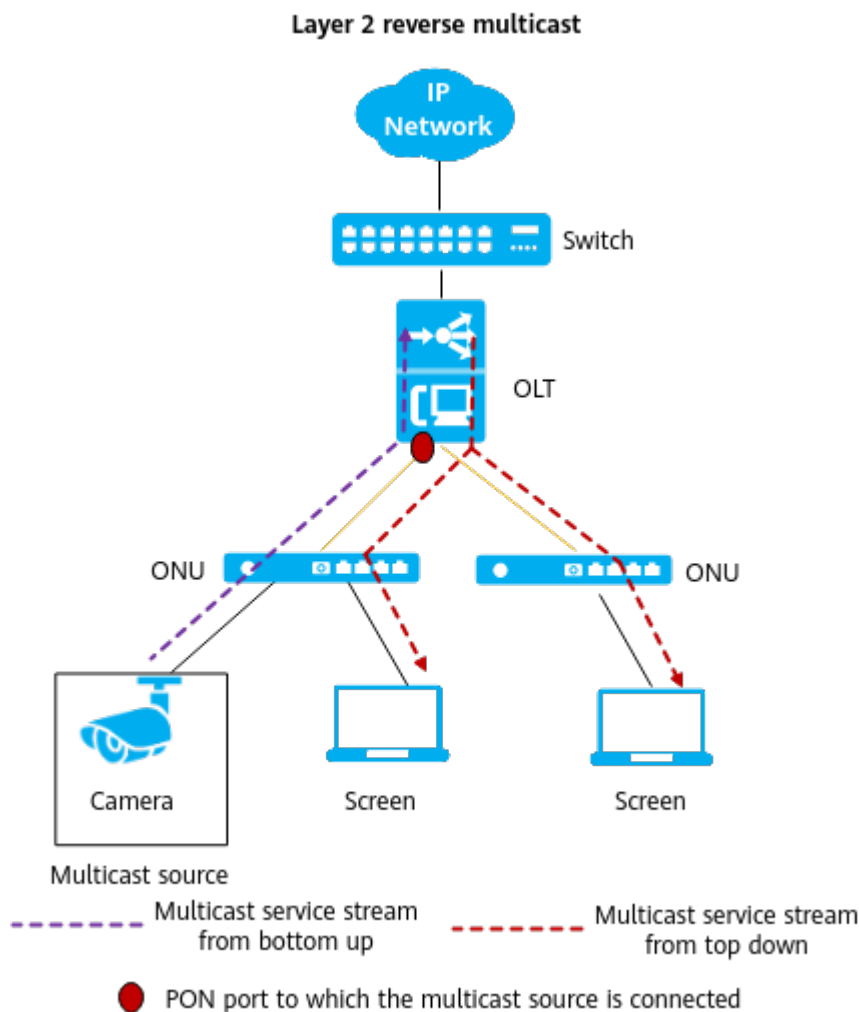
Figure 13-64 Reverse multicast diagram



Application Environment

Figure 13-65 shows the application of Layer 2 reverse multicast. Users receiving the multicast service stream can be connected to the same ONU or different ONUs.

Figure 13-65 Layer 2 reverse multicast application diagram



Procedure

Step 1 Enable the reverse multicast function.

Run the **multicast-source port** command to enable reverse multicast.

Step 2 Enable the ONU reverse multicast stream forwarding function.

Run the **port multicast-source eth ont-portlist enable** command to enable an ONU to forward reverse multicast stream in an ONU service profile.

Step 3 Create a multicast VLAN, and configure multicast programs and multicast users.

- Run the **multicast-vlan** command to create a multicast VLAN.
- Run the **igmp program add** command to configure multicast programs.
- Run the **igmp user add** command to configure multicast users.

Step 4 Configure reverse multicast service ports.

1. Configure C-VLAN = S-VLAN = M-VLAN for multicast users on the PON port directly connected to the multicast source. The C-VLAN and S-VLAN can be

set using the **service-port** *service-port* **vlan** *SVLAN* **gpon** *frameid/slotid/portid* **ont** *ontid* **gemport** *gemindex* **multi-service** **user-vlan** *CVLAN* command, and the M-VLAN can be set using the **multicast-vlan** command.

NOTE

The multicast source ingress of the same multicast program must be unique, either a forward multicast source ingress or a reverse multicast source ingress.

----End

Example

Configure Layer 2 reverse multicast for a single device with the following configurations:

- The multicast source is directly connected to port eth 1 on ONU 0 which is connected to PON port 0/2/0. Set the service profile ID to 100, service port ID to 0, and S-VLAN and C-VLAN IDs to 100.
- Set the multicast VLAN ID to 100, multicast program mode to static, program name to movie, program IP address to 231.1.1.1, source IP address to 10.1.1.2, and program bandwidth to 5000 Kbit/s.
- Plan service VLAN 100 for the multicast service, and add all users in the VLAN as multicast users in batches.

```
huawei(config)#btv
huawei(config-btv)#multicast-source port 0/2 0
huawei(config-btv)#quit
huawei(config)#ont-srvprofile gpon profile-id 100
huawei(config-gpon-srvprofile-100)#port multicast-source eth 1 enable
huawei(config-gpon-srvprofile-100)#commit
huawei(config-gpon-srvprofile-100)#quit
huawei(config)#vlan 100
huawei(config)#service-port 0 vlan 100 gpon 0/2/0 ont 0 gemport 0 multi-service user-vlan 100
huawei(config)#btv
huawei(config-btv)#igmp user add smart-vlan 100
huawei(config-btv)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name movie ip 231.1.1.1 sourceip 10.1.1.2 bandwidth 5000
huawei(config-mvlan100)#igmp multicast-vlan member smart-vlan 100
```

13.6.7 Configuring the Layer 3 Reverse Multicast Service

This topic describes how to configure the Layer 3 reverse multicast service.

Prerequisites

- An OLT has been installed.
- The IP route between the OLT and the network-side devices is reachable. The OLT and ONUs can be managed by eSight/Cloud Campus.
- The link between the OLT and ONUs is normal, and the ONUs can register with the OLT and go online.

Context

Generally, the upper-layer devices of an OLT, such as video servers, are considered as multicast sources. A video server issues the service stream of multicast

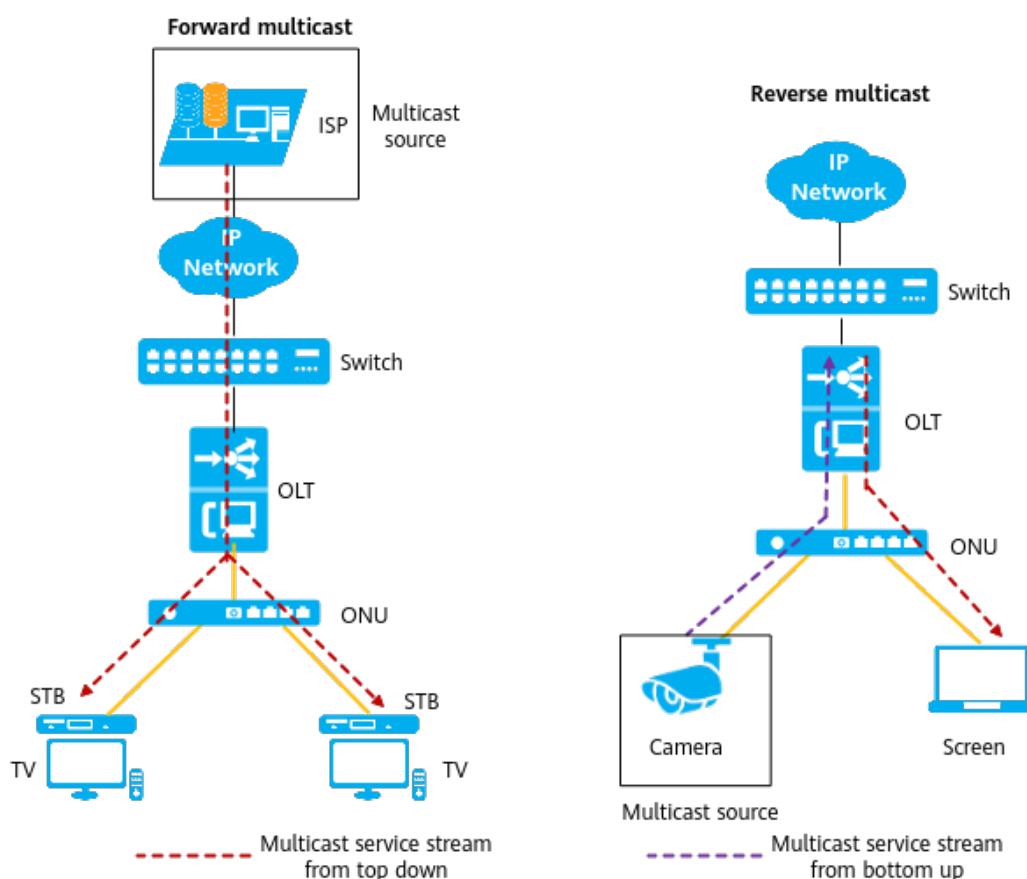
programs to users from top down. This is forward multicast. However, in some scenarios, for example, in a subway station with a surveillance center and multiple sub-surveillance centers, reverse multicast is required when the stream of some cameras needs to be displayed on several large screens.

In reverse multicast, the multicast source comes from a user under the OLT. The service stream from the multicast source is replicated on the OLT and then sent to other multicast users in the same multicast VLAN. **Figure 13-66** shows forward multicast and reverse multicast services.

NOTE

- In the reverse multicast scenario, the multicast source must be directly connected to an ONU. Layer 2 or Layer 3 multicast networking is not supported under the ONU.
- You are not allowed to set the group filter mode in a PIM-enabled multicast VLAN.

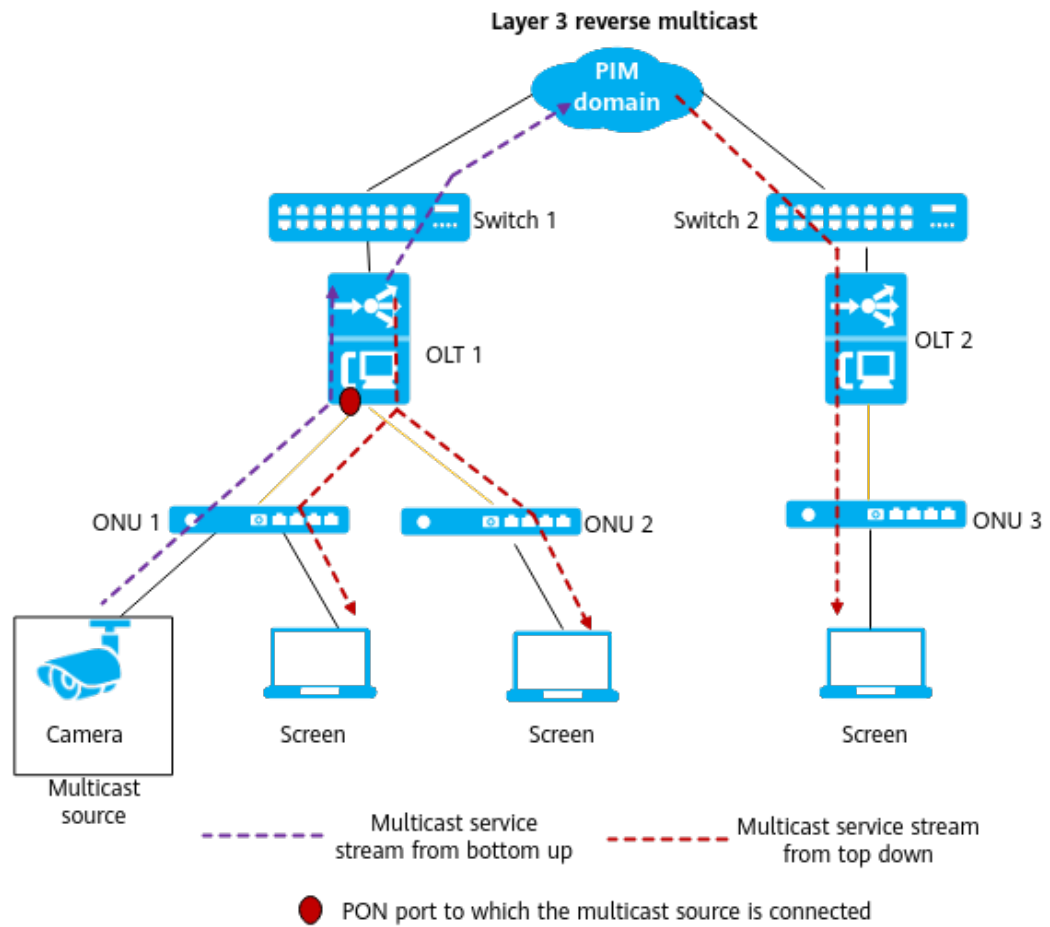
Figure 13-66 Reverse multicast diagram



Application Environment

Figure 13-65 shows the application of Layer 3 reverse multicast. Users receiving the multicast service stream are connected to different OLTs.

Figure 13-67 Layer 3 reverse multicast application diagram



Procedure

Step 1 Enable the reverse multicast function.

Run the **multicast-source port** command to enable reverse multicast.

Step 2 Enable the ONU reverse multicast stream forwarding function.

Run the **port multicast-source eth ont-portlist enable** command to enable an ONU to forward reverse multicast stream in an ONU service profile.

Step 3 Create a multicast VLAN and an upstream PIM interface VLAN, and add the PIM router port to the PIM interface VLAN.

1. Run the **vlan** command to create a multicast VLAN and upstream PIM interface VLAN.
2. Run the **port vlan vlan-list frameid/slotid portlist** command to add the PIM router port to the PIM interface VLAN.

Step 4 Enable the multicast function.

Run the **multicast routing-enable** command to enable the multicast function.

Step 5 Set the multicast upstream mode to PIM.

- If PIM-SM is used in the upstream direction, run the **multicast upstream-mode pim-sm** command to set the upstream multicast exchange mode to PIM-SM.
- If PIM-SSM is used in the upstream direction, run the **multicast upstream-mode pim-ssm** command to set the upstream multicast exchange mode to PIM-SSM.

Step 6 Create the VLAN Layer 3 interface of the upstream PIM interface, configure the IP address of the Layer 3 interface, and enable PIM on this Layer 3 interface.

1. Run the **interface vlanif** command to create the VLAN Layer 3 interface for the upstream PIM interface.
2. Run the **ip address** command to configure the IP address of the Layer 3 interface.
3. Run the **pim sm** command to enable PIM on the Layer 3 interface.

Step 7 Create a multicast VLAN Layer 3 interface, configure the IP address of the Layer 3 interface, and enable the multicast function on the Layer 3 interface.

1. Run the **interface vlanif** command to create a multicast VLAN Layer 3 interface.
2. Run the **ip address** command to configure the IP address of the Layer 3 interface.

Step 8 (Optional) If PIM-SM is enabled in the upstream direction, static rendezvous points (RPs) need to be configured.

Run the **static-rp** command to configure static RPs.

Step 9 Configure multicast programs and multicast users.

- Run the **igmp program add** command to configure multicast programs.
- Run the **igmp user add** command to configure multicast users.

Step 10 Configure reverse multicast service ports.

- Configure C-VLAN = S-VLAN = M-VLAN for multicast users on the PON port directly connected to the multicast source. The C-VLAN and S-VLAN can be set using the **service-port service-port vlan SVLAN gpon frameid/slotid/portid ont ontid gempont gemindex multi-service user-vlan CVLAN** command, and the M-VLAN can be set using the **multicast-vlan** command.

NOTE

The multicast source ingress of the same multicast program must be unique, either a forward multicast source ingress or a reverse multicast source ingress.

----End

Example

When PIM-SSM is used in the upstream direction and IGMP is used in the downstream direction for the multicast service, configure Layer 3 reverse multicast with the following configurations:

- The multicast source is directly connected to port eth 1 on ONU 0 which is connected to PON port 0/2/0. Set the service profile ID to 100 and service port ID to 0.
- The PIM router port is 0/9/0.
- On the PIM router side, the VLAN of the PIM-SSM interface is 200, the IP address of the Layer 3 interface is 10.1.1.1, and the mask is 24. The PIM router side sets up the Layer 3 multicast relationship with the OLT by sending PIM packets carrying multicast sources.
- The multicast VLAN ID is 100, the IP address of the Layer 3 interface is 10.2.2.2, and the mask is 24.
- Set the multicast program mode to static, program name to movie, program IP address to 232.1.1.1, source IP address to 10.1.1.2, and program bandwidth to 5000 Kbit/s.
- Plan service VLAN 100 for the multicast service, and add all users in the VLAN as multicast users in batches.

```
huawei(config)#btv
huawei(config-btv)#multicast-source port 0/2 0
huawei(config-btv)#quit
huawei(config)#ont-srvprofile gpon profile-id 100
huawei(config-gpon-srvprofile-100)#port multicast-source eth 1 enable
huawei(config-gpon-srvprofile-100)#commit
huawei(config-gpon-srvprofile-100)#quit
huawei(config)#vlan 100
huawei(config)#vlan 200
huawei(config)#port vlan 200 0/9 0
huawei(config)#service-port 0 vlan 100 gpon 0/2/0 ont 0 gempport 0 multi-service user-vlan 100
huawei(config)#multicast routing-enable
huawei(config)#multicast upstream-mode pim-ssm
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip address 10.1.1.1 24
huawei(config-if-vlanif200)#pim sm
huawei(config-if-vlanif200)#quit
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip address 10.2.2.2 24
huawei(config-if-vlanif100)#quit
huawei(config)#multicast-vlan 100
huawei(config-mvlan100)#igmp program add name movie ip 232.1.1.1 sourceip 10.1.1.2 bandwidth 5000
huawei(config-mvlan100)#quit
huawei(config)#btv
huawei(config-btv)#igmp user add smart-vlan 100
```

13.7 Multicast Maintenance and Diagnosis

13.7.1 Multicast Emulation

A multicast emulation test remotely emulates an end user going online, and engineers query the real-time traffic of the multicast program to determine whether the multicast function is running properly.

13.7.1.1 Introduction

In multicast emulation, an access device remotely emulates an end user going online. Engineers query the real-time traffic of the multicast program to determine whether the multicast function is running properly.

Multicast emulation is used in acceptance tests or fault location. The following table lists the comparison between the multicast emulation test and traditional tests.

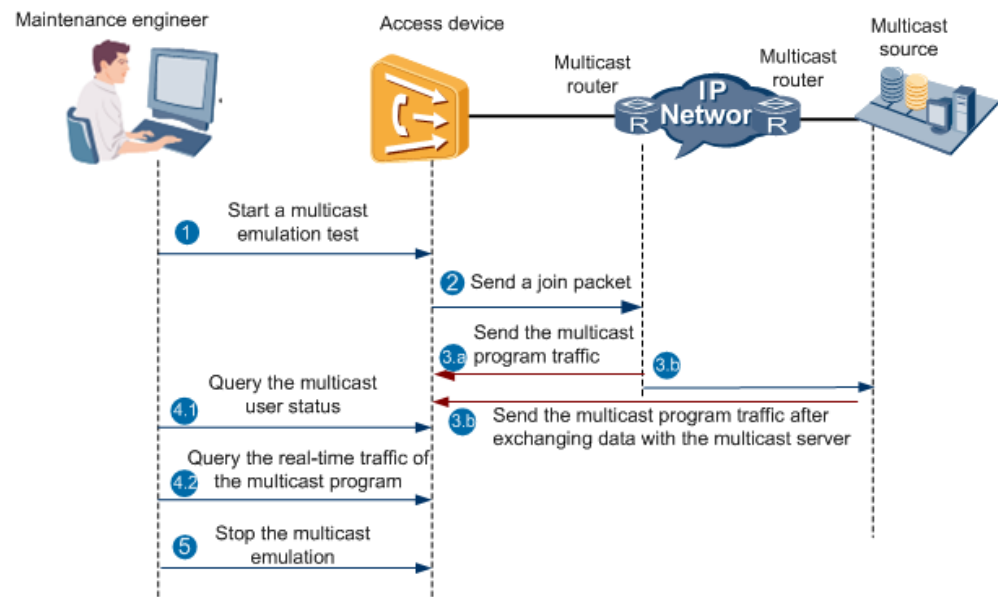
Table 13-41 Comparison between the multicast emulation test and traditional tests

Scenario	Task	Traditional Test	Multicast Emulation
Acceptance test	After an access device is installed and configured with data, a test engineer needs to check whether the multicast service has been provisioned to the access device successfully.	The test engineer visits the site where the access device is installed and uses an external tester or a portable computer to perform a multicast test on each port of the device.	The test engineer remotely logs in to the access device to perform a multicast emulation test and determines the service status based on the test results.
Fault location	The multicast service is abnormal, and a maintenance engineer needs to quickly locate the network segment of the fault to facilitate subsequent troubleshooting.	The maintenance engineer visits all sites where the access devices are installed and performs tests.	The maintenance engineer remotely logs in to an access device and performs a multicast emulation test to preliminarily determine the network segment of the fault. Based on the test results, the engineer diagnoses the fault cause and rectifies the fault. NOTE A multicast emulation test cannot check the status of the line between an end user and an access device.

13.7.1.2 Principles

Figure 13-68 shows the principles of multicast emulation.

Figure 13-68 Principles of multicast emulation



1. A maintenance engineer remotely logs in to an access device and starts a multicast emulation test on a user port.
The engineer sets parameters, such as the user information, program IP address, and multicast VLAN ID.
2. The access network device constructs a join packet and sends the packet to the multicast router for joining a multicast group.
3. The multicast router checks whether the multicast program traffic exists.
 - If the multicast program traffic exists, the multicast router sends the multicast program traffic to the access device.
 - If the multicast program traffic does not exist, the multicast source sends the multicast program traffic to the access device after exchanging data with the multicast router.
4. The maintenance engineer queries the status of the emulation user and the real-time traffic of the multicast program.
 - Checks whether the multicast emulation user is online to determine whether the user successfully orders the program.
 - Checks the real-time traffic of the multicast program to determine whether the communication between the access device and the multicast source is normal.
5. After the multicast emulation is complete, the maintenance engineer stops the emulation manually using the CLI to release resources.

13.7.1.3 Usage Scenario

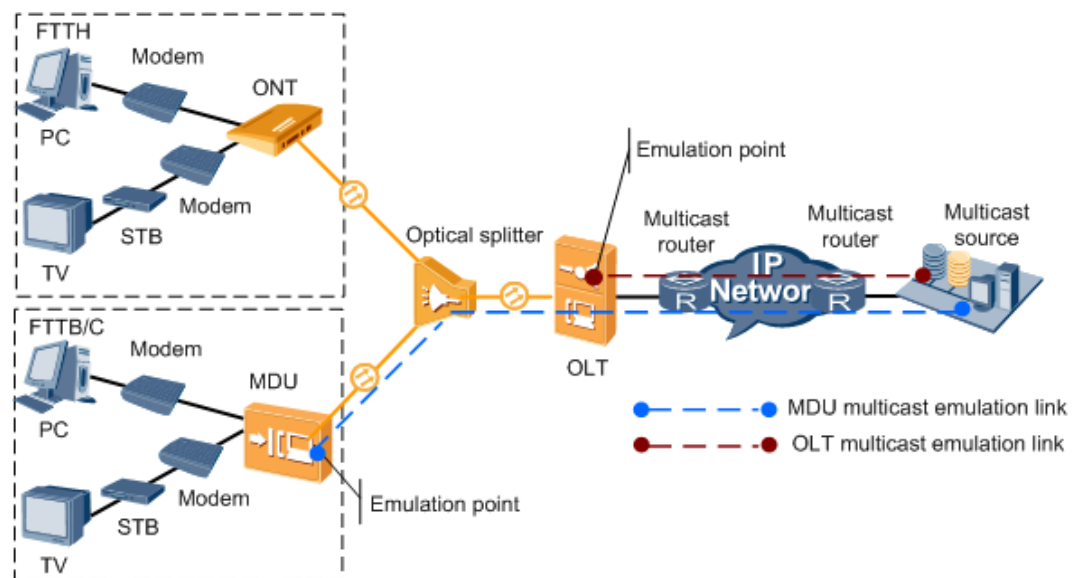
Context

On fiber to the x (FTTx) networks, access devices are located closer to user terminals and widely distributed. In a multicast emulation test, an access node emulates the multicast user to implement remote acceptance for services and locate faults, which reduces the O&M costs.

Scenario

Figure 13-69 shows the multicast emulation on a typical FTTx network.

Figure 13-69 Multicast emulation on a typical FTTx network



NOTE

In **Figure 13-69**, the MDU and ONT can provide the video on demand (VoD) service for a user through the PC. The MDU and ONT can also provide the BTV service using a set top box (STB).

In IPTV service acceptance or fault location:

- For MDU multicast users, multicast emulation can be performed on the MDU in service acceptance.
- For ONT multicast users, multicast emulation can be performed on the OLT.

NOTE

ONTs do not support multicast emulation. To emulate an ONT multicast user, perform an emulation test on the PON board of the OLT.

Fault Location

After the multicast emulation, you can query the user status and multicast program's real-time traffic through the CLI. The following table lists troubleshooting suggestions based on the query results.

NOTE

Data configurations are seldom changed in daily operation and maintenance. Therefore, multicast faults are usually caused by hardware problems. Hardware must be checked prior to data configuration during fault location.

Table 13-42 Multicast emulation results and troubleshooting suggestions

Command	Results	Description	Troubleshooting Suggestions
display igmp user	The user status parameter State is online .	The multicast user can go online successfully.	• If the user can go online and the access device can communicate with the multicast source, the fault may be caused by a communication failure between the access device and the set-top box (STB). The reasons are as follows: – The hardware of the port on the access device is faulty. – The physical line between the access device and the modem is faulty. – The modem is faulty. – The STB is faulty. • If the user can go online but the traffic on the access device's uplink port is abnormal, the fault may be that the hardware connection between the access device and the upper-layer device (multicast router or multicast server) is incorrect, or the software configuration is incorrect. The common software configuration faults are as follows: – The remaining multicast bandwidth of the user is lower than the required

Command	Results	Description	Troubleshooting Suggestions
			bandwidth of the ordered program. - The number of programs watched by the multicast user reaches the upper limit so that the user cannot order a new program. - The multicast user does not have the permission to watch the program. - The program ordered is not in the MVLAN to which the multicast user belongs. - The multicast user does not have the permission to order certain types of programs (such as HDTV). - The number of programs at a level watched by the multicast user reaches the upper limit so that the user cannot order a new program at this level. - The rate configured in the traffic profile bound to the traffic stream is far lower than the bandwidth of the multicast program. - There are too many prejoined static programs, occupying too many bandwidths.

Command	Results	Description	Troubleshooting Suggestions
			The common software configuration problems of the upper layer device are as follows: - The program is not configured on the multicast server. - The TTL value set on the multicast server for the multicast stream is very small.

Command	Results	Description	Troubleshooting Suggestions
	The user status parameter State is offline .	The multicast user fails to go online and therefore fails to order a program in the emulation.	The case is more complicated than the scenario in which the user is online. Handling suggestions are as follows: Enable the multicast debugging function and start the multicast emulation again to check whether the access device receives the report packet from the user for ordering a program. Run the following commands to enable the multicast debugging function: <pre>huawei(config)#terminal debugging huawei(config)#terminal monitor huawei(config)#debugging igmp service-port index</pre> NOTE index is the ID of the multicast user's service port. • If the access device receives the report packet, the multicast link is normal but the access device fails to create a corresponding multicast entry. This is generally caused by incorrect multicast configurations on the access device. • If the access device does not receive the report packet, the multicast link fails. This is mainly caused by incorrect access device data configurations, faulty physical link between the access device and the modem, or

Command	Results	Description	Troubleshooting Suggestions
			hardware faults of terminals.
	The user status parameter State is block .	The multicast user is locked and therefore fails to order a program.	Run the undo igmp user block command to unblock the user.
display multicast flow-statistic	The multicast program's real-time traffic parameter Multicast flow statistic result is a small value or zero.	The program's traffic on the uplink port is small or zero.	The hardware connection between the access device and the upper-layer device (multicast router or multicast server) is incorrect, or the software configuration is incorrect. troubleshoot the fault based on the suggestions provided when the user can go online but the traffic on the access device's uplink port is abnormal.

Command	Results	Description	Troubleshooting Suggestions
	The multicast program's real-time traffic parameter Multicast flow statistic result is close to the program's bandwidth.	The device uplink port can communicate with the multicast source.	• If the user can go online and the access device can communicate with the multicast source, the fault may be caused by a communication failure between the access device and the STB. The reasons are as follows: – The hardware of the port on the access device is faulty. – The physical line between the access device and the modem is faulty. – The modem is faulty. – The STB is faulty. • If the access device can communicate with the multicast source but the user cannot go online, troubleshoot the fault based on the suggestions provided when the user status parameter State is offline.

13.7.1.4 Configuration

Context

- The configuration of the multicast port is correct.
- The multicast user for whom the multicast emulation test is performed has the rights to watch the configured multicast programs.

Procedure

Step 1 Run the **igmp static-join** command to perform the multicast emulation test for the multicast user.

```
huawei(config)#btv
huawei(config-btv)#igmp static-join service-port 500
{ ip<K>|ipv6<K> }:ip
{ ip-addr<I><X.X.X.X> }:224.1.1.1
{ vlan<K> }:vlan
{ vlanid<U><1,4093> }:4002
```

Step 2 Run the **display igmp user** command to query the status of the multicast user.

- If the multicast user is in **offline** state, the multicast user fails to request for programs.
- If the multicast user is in **online** state, the multicast user requests for programs successfully.
- If the multicast user is in **block** state, the multicast user is blocked. In this case, run the **undo igmp user block** command to unblock the user.

```
huawei(config)#display igmp user service-port 500
User          : 0/1/1
State: online // The multicast user is online.
Authentication : auth
Quick leave    : MAC-based
IGMP flow ID   : 500
Video flow ID  : 500
Log switch     : enable
Bind profiles  : 2
IGMP version   : IGMP v3
Current version : IGMP v3
.....
```

Step 3 Run the **display multicast flow-statistic** command to query the real-time traffic of the programs that the multicast user requests for in the multicast emulation test.

- If the real-time traffic of the multicast programs is a smaller value or 0, the multicast source does not deliver multicast programs or the multicast service stream does not arrive at the device. That is, the communication between the device and the multicast source is abnormal.
- If the real-time traffic of the multicast programs approaches the bandwidth of the multicast programs, the multicast source delivers the multicast programs to the device. That is, the communication between the device and the multicast source is normal.

```
huawei(config)#btv
huawei(config-btv)#display multicast flow-statistic vlan 4002 ip 224.1.1.1
Command is being executed, please wait...
Multicast flow statistic result: 29600(kbps) //The real-time traffic of multicast program 224.1.1.1 is
29600 kbit/s. This indicates that the multicast source issues multicast traffic.
```

Step 4 Run the **undo igmp static-join** command to stop multicast emulation.

```
huawei(config)#btv
huawei(config-btv)#undo igmp static-join service-port 500
{ ip<K>|ipv6<K> }:ip
{ ip-addr<I><X.X.X.X> }:224.1.1.1
{ vlan<K> }:vlan
{ vlanid<U><1,4093> }:4002
```

----End

13.7.1.5 Multicast Emulation Reference Standards and Protocols

- RFC-2236: Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997
- RFC 3376: B. Cain., "Internet Group Management Protocol, Version 3", RFC 3376, October 2002

- RFC 4607: H. Holbrook, "Source-Specific Multicast for IP", RFC 4607, August 2006

13.7.2 Video Quality Monitoring

Video quality monitoring enables an access device to remotely monitor affected video programs on configured monitoring points for fault demarcation.

13.7.2.1 Introduction

Background

After a fault occurs in the video service of a residential user, the user reports this fault to the carrier. Then, the carrier's maintenance personnel detect and rectify the fault. Before rectifying the fault, the maintenance personnel must demarcate the fault, involving the following cases:

- If multiple users report the fault related to an IPTV or VoD program within a period of time, and these users connect to different optical line terminals (OLTs), the IPTV server or core switching network may be faulty. In this case, the maintenance personnel only need to troubleshoot the IPTV server or core switching network.
- If only few users report the fault, and these users connect to the same OLT, the maintenance personnel must diagnose the video quality on the network for fault demarcation.

However, the maintenance personnel relies on home visits for troubleshooting. In the fiber to the home (FTTH) scenario, optical network terminals (ONTs) are located at user homes. Therefore, onsite diagnosing is not only time-consuming but also costly. In this case, an effective method of remotely diagnosing video quality is urgently required.

Overview

In video quality monitoring, monitoring points are configured on the OLT and ONTs. Each monitoring point is used for monitoring quality indicators of each video program. Maintenance personnel can remotely enable video quality monitoring and obtain monitoring results on the NMS or OLT. Based on monitoring results obtained from each monitoring point, the maintenance personnel comprehensively identify fault points, thereby reducing fault locating costs.

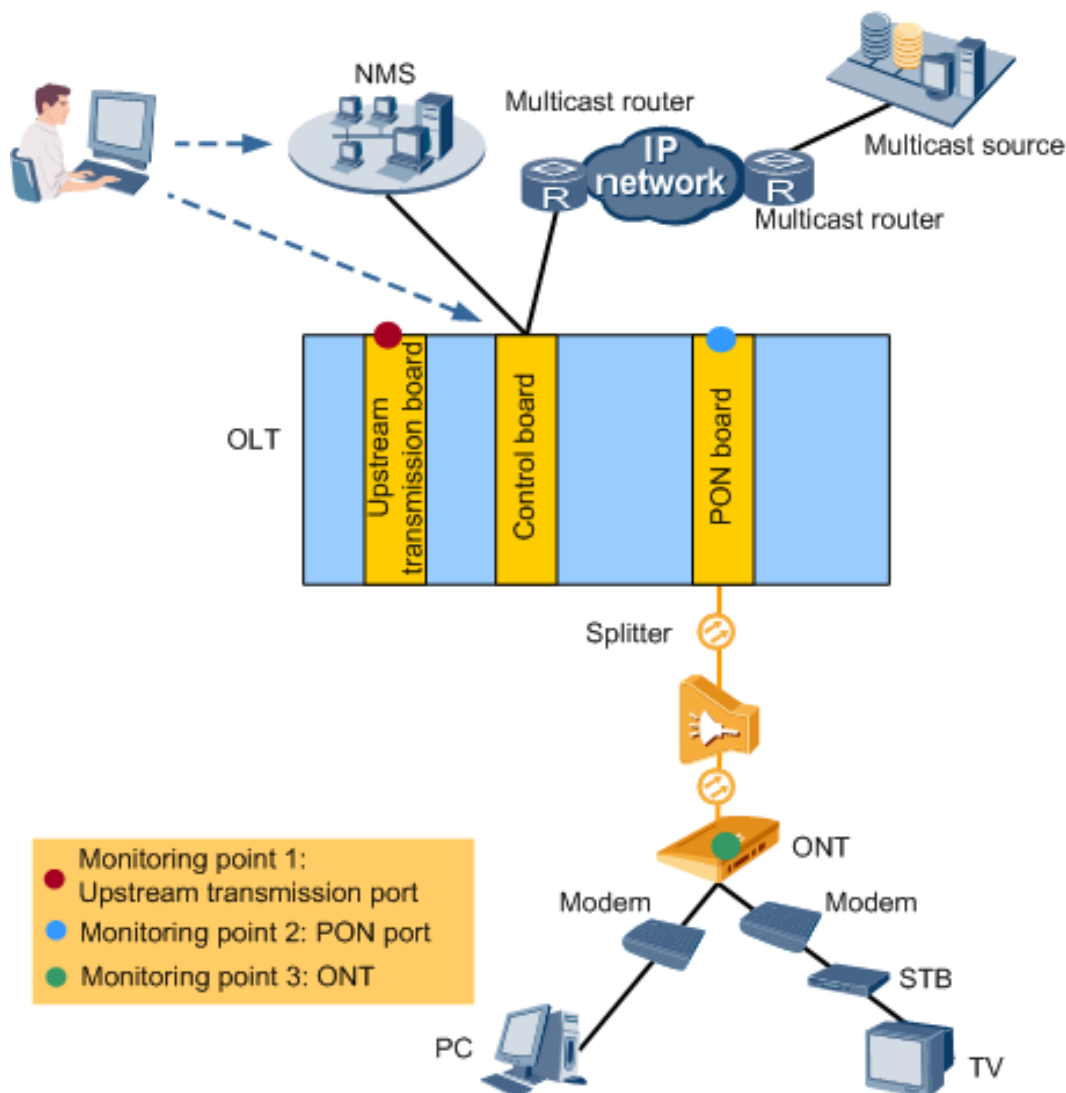
Compared with the video quality monitoring enabled using the OLT, the video quality monitoring enabled using the NMS has the following advantages:

- The NMS can store more video quality monitoring results than the OLT. In addition, the NMS supports monitoring result dumping, meeting the requirement of long-term video quality monitoring. Major video quality-related faults occur randomly. Therefore, the identification of such faults requires long-term video quality monitoring data.
- The NMS can display monitoring results in graphs. These trend graphs for each channel of program facilitate information obtaining.

Video quality monitoring points can be configured on uplink ports, PON ports of the OLT, and ONTs. In addition, the quality of both common videos and 4K videos can be monitored.

Figure 13-70 shows the application scenario of video quality monitoring.

Figure 13-70 Application scenario of video quality monitoring



13.7.2.2 Basic Concepts

Video quality monitoring involves the following quality indicators: media delivery index (MDI), mean opinion score for video (VMOS), and packet loss rate (PLR), which are described as follows:

MDI

MDI, defined in RFC 4445, is a quantitative number assigned to the quality of video streams transmitted over a network.

The MDI consists of two components: the delay factor (DF) and the media loss rate (MLR).

- DF is the maximum difference, observed at the end of each media data packet, between the arrival of media data and the forwarding of media data. This indicator reflects the delay and jitter of the tested video stream. A large jitter leads to a large DF value, which promotes high requirements on the buffer of the decoding device. Therefore, the smaller the DF value, the better. Recommended DF value range is 0-50 ms. Any DF value less than 200 ms is accepted.
- MLR specifies the number of media data packets lost per second. This indicator determines video quality. By measuring MLR, maintenance personnel can detect, identify, and trace media data packet loss on a network. According to WT126, the maximum accepted MLRs for standard definition (SD)/VoD programs and high definition (HD) programs are 5 media data packets per 30 minutes and 5 media data packets per 240 minutes, respectively.

VMOS

VMOS is a subjective method of evaluating the quality of a video program.

A VMOS value is measured on a continuous scale of 1 to 5, representing the video quality of unsatisfactory, poor, fair, good, and excellent, respectively.

PLR

PLR specifies the number of IP packets lost per second. PLR is different from MLR, which specifies the number of media data packets lost in one sampling period. One IP packet contains seven media data packets.

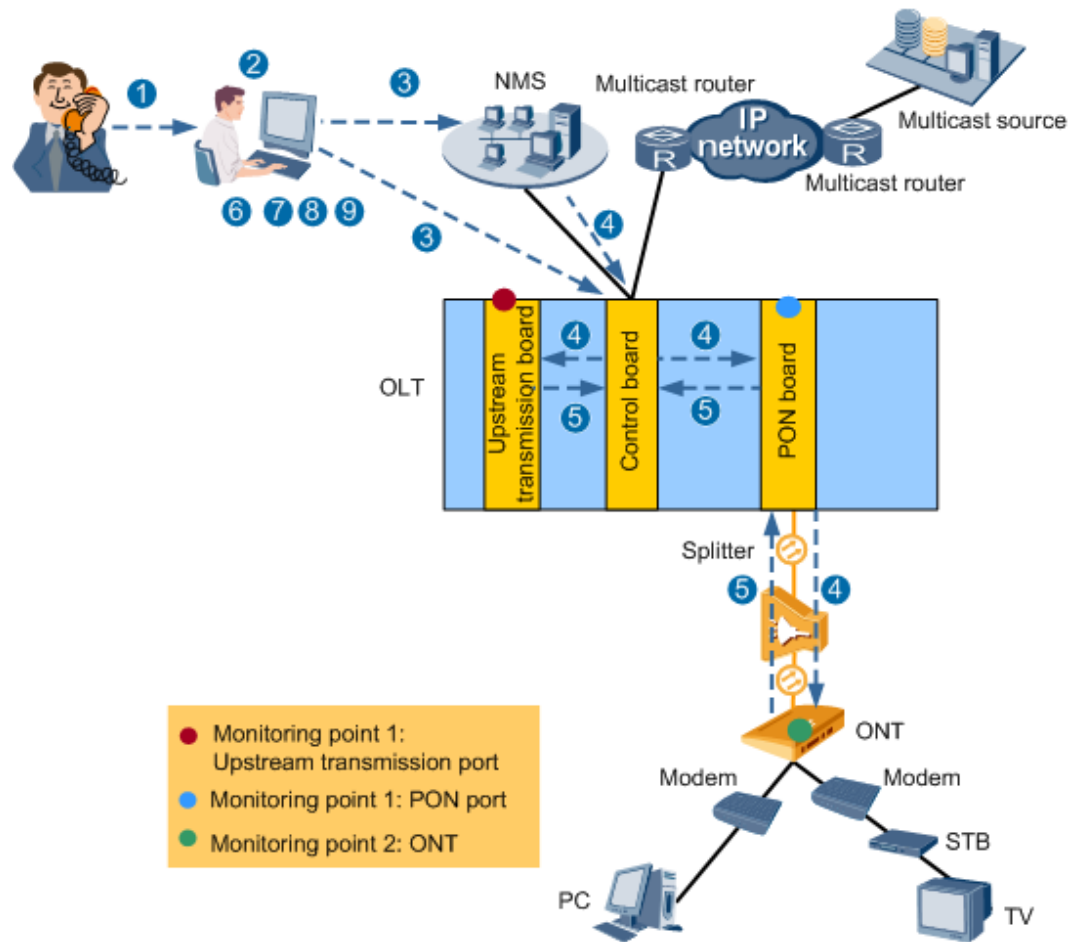
By measuring PLR, maintenance personnel can detect, identify, and trace IP packet loss on a network.

13.7.2.3 Principles

Implementation Process

[Figure 13-71](#) shows the process of implementing video quality monitoring.

Figure 13-71 Process of implementing video quality monitoring



The process is as follows:

1. After a fault occurs in the video service of a residential user, the user reports this fault to the carrier.
2. The carrier's maintenance personnel exclude communication faults after checking the head end system or performing an Internet Group Management Protocol (IGMP) emulation test.
3. The maintenance personnel enable video quality monitoring using the OLT or NMS.

Video quality monitoring can be enabled on uplink ports, PON ports or ONTs.

NOTE

If video quality monitoring is enabled on an uplink port, only the quality of inbound video streams can be monitored. If video quality monitoring is enabled on a non-uplink port, only the quality of outbound video streams can be monitored.

- To monitor the quality of an IPTV program, specify a multicast VLAN and multicast address.
 - To monitor the quality of a VoD program, specify the source and destination IP addresses of this program, destination IP address, destination port, and transmission protocol.
4. The OLT or NMS issues a command for enabling video quality monitoring to each monitoring point. After receiving this command, these monitoring points

configure hardware based on the program information carried in the command. Then, the hardware captures video streams, adds timestamps to them, and sends the video streams to the CPU for monitoring indicator calculation.

5. The CPU sends calculated results to each monitoring point in real time, and the monitoring points periodically report these results to the control board of the OLT.
6. Video quality monitoring stops when the preset monitoring duration times out or the maintenance personnel disable this function.
7. The maintenance personnel obtain monitoring results from the OLT or NMS.
8. The maintenance personnel demarcate the fault based on monitoring results.
9. The maintenance personnel rectify the fault.

Fault Locating

After completing video quality monitoring, the maintenance personnel obtain monitoring results to learn program quality on each monitoring point for fault demarcation. [Table 13-43](#) shows fault demarcation rules.

Table 13-43 Fault demarcation rules

Monitoring Point on an Uplink Port	Monitoring Point on a PON Port	Monitoring Point on an ONT	Conclusion
POK	POK	POK	The fault may occur on the upper-layer network or head end system. Detect the upper-layer metropolitan area network (MAN) of the OLT.
OK	POK	POK	The fault may occur between the PON board and the control board/upstream transmission board on OLT. Detect the inner OLT.

Monitoring Point on an Uplink Port	Monitoring Point on a PON Port	Monitoring Point on an ONT	Conclusion
OK	OK	POK	The fault may occur between the PON board and the outbound port on the ONT (including the inner ONT).
OK	OK	OK	The fault may occur at user home, such as the Internet network or set top box (STB).

13.7.2.4 Configuring Video Quality Monitoring

Prerequisites

The carrier's maintenance personnel have excluded communication faults after checking the head end system or performing an multicast emulation test.

Procedure

- Step 1** (Optional) Run the **video-quality-monitor** command to configure video quality monitoring indicator thresholds and a monitoring period.

Perform this step if default video quality monitoring indicator thresholds and monitoring period fail to meet network requirements. The monitoring indicators include DF, MLR, VMOS, and PLR.

- Step 2** Start video quality monitoring.

Run the **video-quality-monitor start** command to start a video quality monitoring instance. You can configure one monitoring point on an upstream port, GPON port or an ONT, or on all of them.

- Step 3** (Optional) Stop video quality monitoring.

To stop video quality monitoring before the monitoring duration times out, run the **video-quality-monitor stop** command to stop the video quality monitoring instance.

- Step 4** Query video quality monitoring results of the instance.

Run the **display video-quality-monitor result** command to query the monitoring results and demarcate the fault.

1. Query the 5-minute VMOS availability ratio (AR) on each monitoring point.

 NOTE

The 5-minute VMOS AR is the ratio of the number of available VMOS seconds to the total duration of 300s (5 minute x 60 seconds). When the VMOS value is greater than or equal to the fair threshold configured in the VMOS threshold profile, the VMOS value is available.

2. If the VMOS AR of a monitoring point is low, further query the detailed results of the video quality monitoring instance for fault identification.

----End

Example

 NOTE

Terminal display significantly varies based on video quality monitoring instances. Therefore, the following example does not provide terminal display for queried commands. For details about the terminal display and parameter description, see the OLT Command Reference.

The NMS provides monitoring results in graphs for simple information obtaining. Therefore, if the NMS is available, use it to enable video quality monitoring and query monitoring results.

The following is an example configuration of the video quality monitoring feature:

- Excellent, good, and fair VMOS thresholds are 44, 33, and 22, respectively.
- Video quality monitoring points are configured on upstream port 0/9/0, GPON port 0/2/0 and ONT 0 connected to port 0/2/0.
- The multicast VLAN is 100.
- The IP address of the multicast program is 224.1.1.1.

```
huawei(config)#video-quality-monitor vmos excellent-threshold 44 good-threshold 33 medium-threshold 22
huawei(config)#video-quality-monitor start port 0/9/0 port 0/2/0 ont 0/2/0 0 destination-ip 224.1.1.1
vlan 100
huawei(config)#display video-quality-monitor result port 0/9/0 ratio vmos
huawei(config)#display video-quality-monitor result port 0/2/0 ratio vmos
huawei(config)#display video-quality-monitor result ont 0/2/0 0 ratio vmos
huawei(config)#display video-quality-monitor result port 0/9/0 detail
huawei(config)#display video-quality-monitor result port 0/2/0 detail
huawei(config)#display video-quality-monitor result ont 0/2/0 0 detail
```

13.7.3 RTP Video Quality Monitoring

In Real-Time Transport Protocol (RTP) video quality monitoring, the quality of multicast video streams is monitored by means of RTP packet detection. Maintenance personnel can identify multicast service failures based on the detection results.

Basic Principle

RTP packets are encapsulated in User Datagram Protocol (UDP) packet headers, as shown in [Figure 13-72](#).

Figure 13-72 IP+UDP packet format

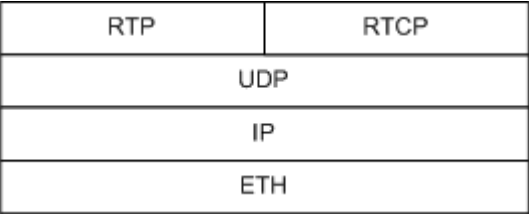
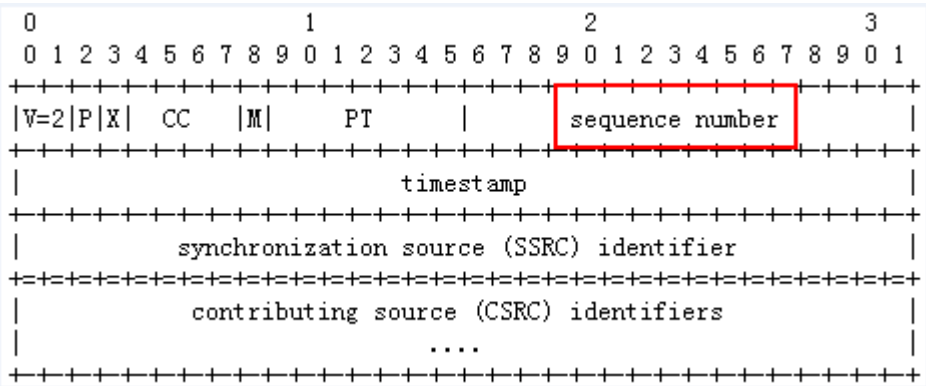


Figure 13-73 shows the format of the RTP packet header. **sequence number** indicates the sequence number of the RTP packet, with a length of 16 bits. The initial value is generated at random, and the sequence number is incremented by 1 when 1 RTP packet is sent. For details about the RTP packet header, see RFC3550.

Figure 13-73 Format of the RTP packet header



In RTP video quality monitoring, RTP sequence numbers in multicast program streams are periodically detected, to identify packet loss, error packets, and duplicate packets in the multicast program streams. During RTP packet loss detection, the system records the number of lost, error, and duplicate packets and records the start and end sequence numbers of packets within the detection period. The program segments with poor quality can be identified based on the start and end sequence numbers of packets within the detection period.

NOTE

- Statistics cannot be collected on segmented packets because segmented packets do not contain RTP packet headers. Therefore, it is recommended that the maximum transmission unit (MTU) in the system be set to less than 1500, to avoid network segmentation.
- The system clears all monitoring data upon active/standby switchover.
- For monitoring points in a link aggregation group, the command is delivered only to the specified port, without affecting other ports.
- For ports in a protection group, the command is delivered only to the active port. When port switchover is performed, the monitoring function must be configured again.

Operating Process

RTP video quality monitoring of the OLT applies to non-cascading and cascading scenarios. Figure 13-74 and Figure 13-75 show the RTP video quality monitoring processes in non-cascading and cascading scenarios respectively.

Figure 13-74 RTP video quality monitoring process in non-cascading scenarios

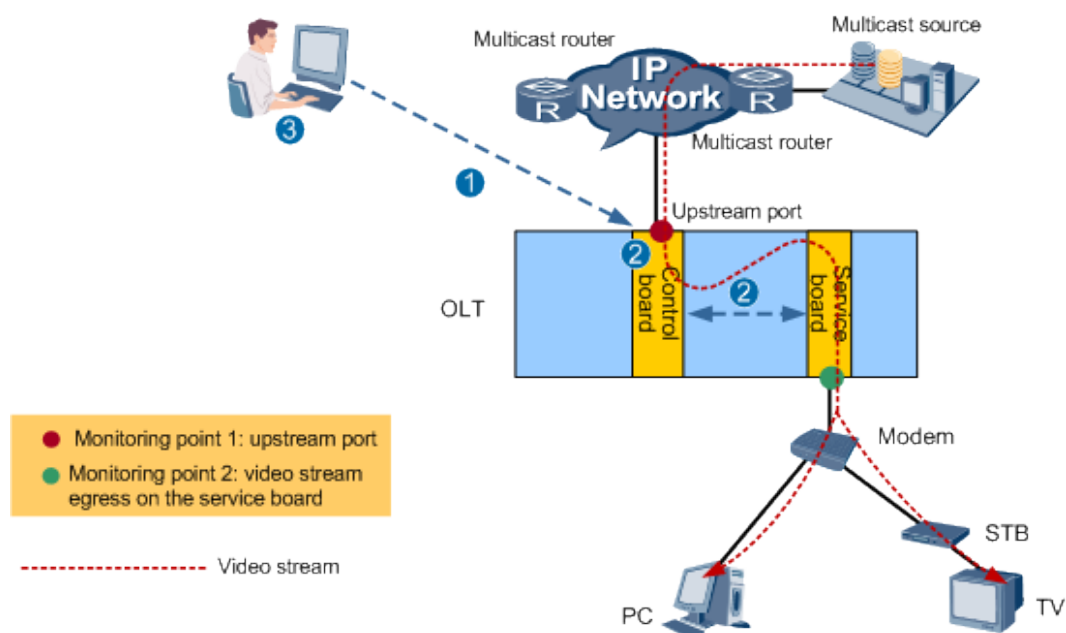
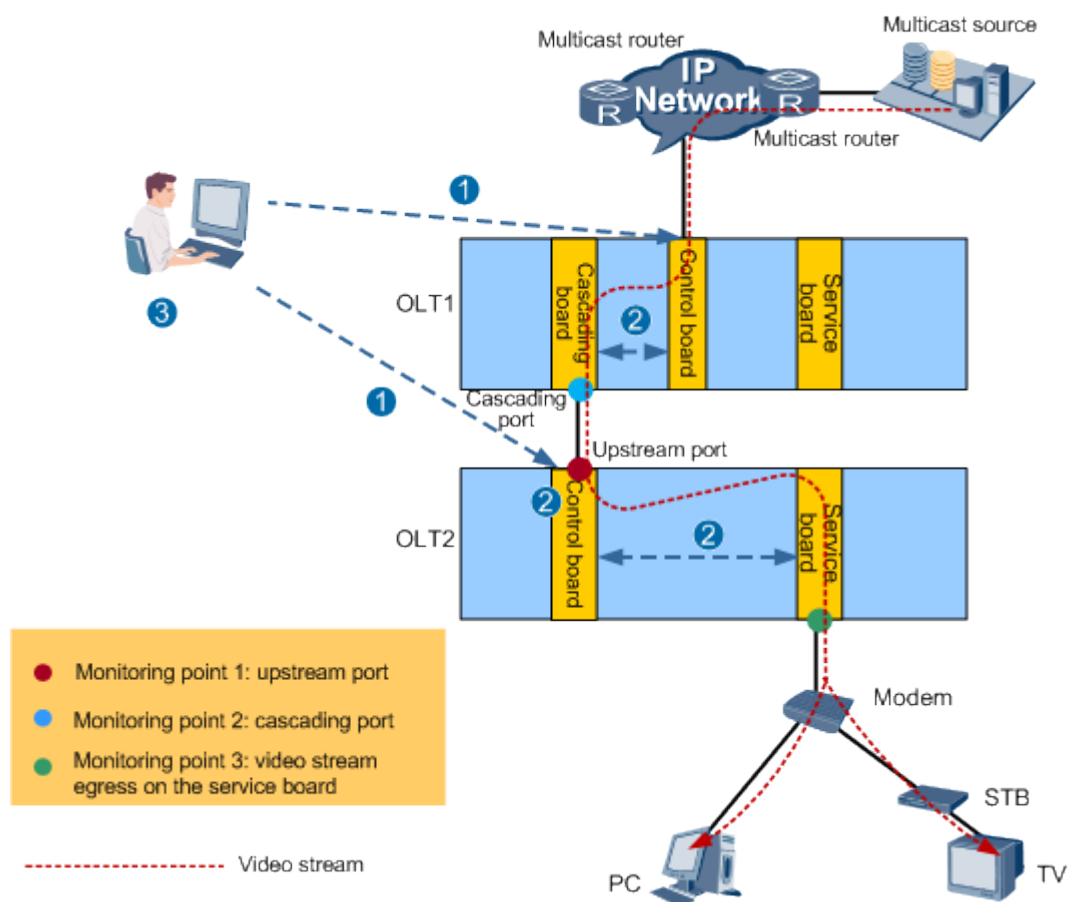


Figure 13-75 RTP video quality monitoring process in cascading scenarios



The RTP video quality monitoring process is as follows:

1. Maintenance personnel run the **rtp multicast statistic** command on the OLT CLI to enable RTP video quality monitoring and specify program information. The OLT supports RTP video quality monitoring at upstream ports, cascading ports, and video stream egresses on service boards. Monitoring can be enabled for a single monitoring point or for all monitoring points in a unified manner.

 NOTE

In cascading scenarios, RTP video quality monitoring can be enabled on OLT1 to monitor cascading ports, and can be enabled on OLT2 to monitor upstream ports or video stream egresses on service boards.

2. The control board of the OLT delivers an enabling message to the monitoring points. After receiving the enabling message, the monitoring points detect RTP packets based on the program information and periodically (*interval* configurable) send detection results to the CPU of the control board.
3. In the monitoring duration, maintenance personnel can run the **display rtp multicast statistic** command to view the monitoring results and perform troubleshooting based on the monitoring results.

 NOTE

- The system records logs only for abnormal packets.
- When the monitoring duration exceeds the preset value, the system clears all monitoring records.

Fault Diagnosis

After RTP video quality monitoring is completed, maintenance personnel query the monitoring results on the OLT CLI and obtain program quality of each monitoring point. Based on the monitoring results, maintenance personnel can perform fault diagnosis, as described in [Table 13-44](#).

OK indicates that the total number of lost, duplicate, and error packets is 0. **POK** indicates that the total number of lost, duplicate, or error packets is not 0.

Table 13-44 Fault diagnosis based on monitoring results

Cascading Port	Upstream Port	Video Stream Ingress of a Service Board	Conclusion
POK	POK	POK	• The upper-layer access device (OLT1) is faulty. • The upper-layer network or headend system encounters a problem. Check the upper-layer MAN of the OLT.

Cascading Port	Upstream Port	Video Stream Ingress of a Service Board	Conclusion
OK	POK	POK	The cascading devices are not properly connected.
OK	OK	POK	The lower-layer access device (OLT2) is faulty.
OK	OK	OK	The Internet connection fails, or the STB is faulty.

13.7.4 eMDI Video Quality Monitoring for the Multicast Service

Unlike video mean opinion score (VMOS), Media Delivery Index (MDI), or Real-Time Transport Protocol (RTP) video quality monitoring that features passive O&M, Enhanced Media Delivery Index (eMDI) video quality monitoring supports real-time multicast program monitoring and periodic result reporting to servers. It enables fast video fault locating, realizes proactive O&M, and guarantees the video services for VIP users.

13.7.4.1 Introduction

Context

For video quality monitoring, video program monitoring points are set on network devices to monitor the quality indicators of video programs. O&M personnel locate video faults by remotely querying and evaluating monitoring results, avoiding unnecessary door-to-door visits.

Existing VMOS, MDI, and RTP video quality monitoring solutions are all passive O&M solutions. For these solutions, carriers' O&M personnel enable video monitoring only after users report multicast artifacts or frame freezing. Such solutions have the following disadvantages:

- VMOS and MDI monitoring solutions feature high algorithm overheads, so long-time video monitoring in real time is not supported. After users report faults, O&M personnel can only wait for fault reproduction before locating.
- VMOS, MDI, and RTP monitoring solutions do not support large-scale concurrent program monitoring, so worldwide deployment is not supported.
- These solutions do not support monitoring indicators in forward error correction (FEC) and retransmission (RET) scenarios, so monitoring results in FEC and RET scenarios are inaccurate.

eMDI video quality monitoring properly solves the preceding problems of VMOS, MDI, and RTP video monitoring solutions.

- For eMDI video quality monitoring, real-time monitoring can be enabled for a long time and monitoring results are uploaded to servers. O&M personnel can implement proactive O&M and guarantee the video services for VIP users by querying the monitoring results.
- An OLT supports concurrent eMDI video quality monitoring of 1024 programs. Therefore, the eMDI monitoring solution can be deployed on the entire network, covering numerous programs.
- eMDI video quality monitoring supports monitoring indicators in FEC and RET scenarios, so monitoring results are more convincing.

Table 13-45 compares 3 video quality monitoring solutions.

Table 13-45 Comparison of video quality monitoring solutions

Solution	Monitoring Indicator	Monitored Program Stream Type
VMOS/MDI video quality monitoring	• Video key quality indicators (KQIs) that reflect subjective user experience. • Video key performance indicators (KPIs) that reflect objective network conditions.	RTP-encapsulated and non-RTP-encapsulated video program streams
RTP video quality monitoring	Video KPIs	RTP-encapsulated MPEG2-TS video program streams
eMDI video quality monitoring	Video KPIs	RTP-encapsulated MPEG2-TS video program streams NOTE • For an OLT, eMDI, VMOS/MDI, and RTP video quality monitoring solutions are not mutually exclusive and can be enabled at the same time. • For an ONT, eMDI and VMOS/MDI video quality monitoring solutions cannot be enabled at the same time.

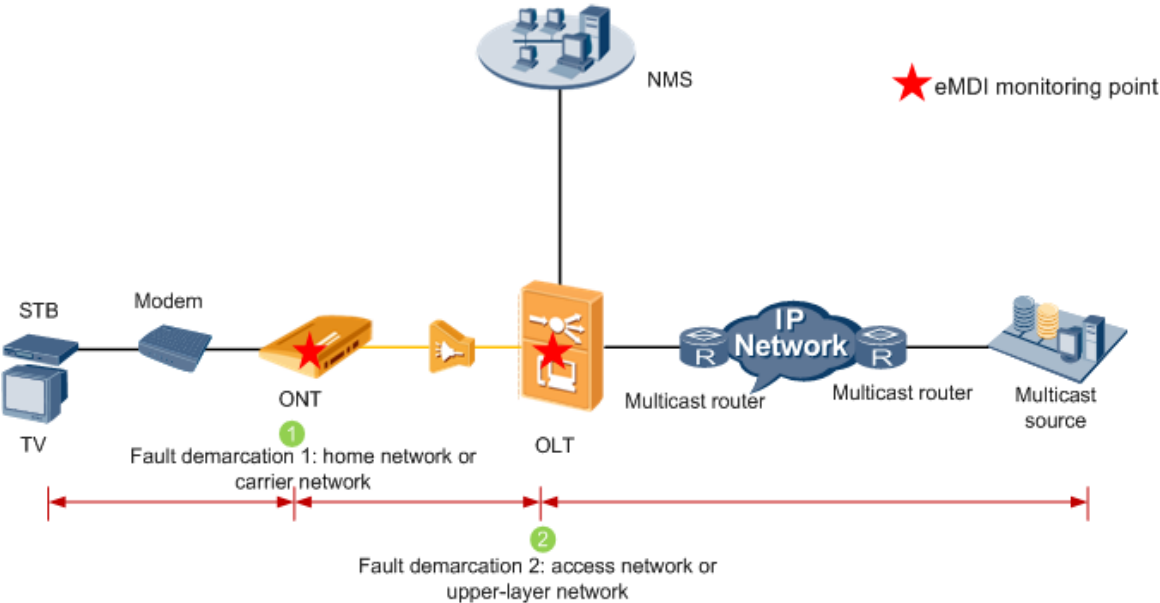
Overview

eMDI video quality monitoring is an enhanced solution on the basis of MDI video quality monitoring. The eMDI solution monitors videos based on the RTP sequence number, and calculates the RTP packet loss density and number of consecutively

lost RTP packets, providing more accurate monitoring results than the MDI solution does in FEC and RET scenarios.

eMDI monitoring points can be set on an OLT board or ONT, as shown in [Figure 13-76](#). O&M personnel can use the NMS or OLT CLI to enable and disable eMDI video quality monitoring, or query monitoring results.

Figure 13-76 eMDI video quality monitoring



Monitoring Point Location	Maximum Number of Concurrently Monitored Programs	Supported Encapsulation Format of Monitored Video Program Streams
ONT	1	• IPoE • PPPoE
OLT board	1024	IPoE

- NOTE**
- eMDI video quality monitoring supports only IPv4 video program streams and does not support IPv6 video program streams.
 - eMDI video quality monitoring supports only live IPTV programs and does not support video on demand (VoD) programs.

13.7.4.2 eMDI Video Quality Monitoring Indicators

eMDI video quality monitoring indicators include RTP loss rate (RTP-LR), RTP sequence error (RTP-SE), RTP loss period (RTP-LP), and RTP effective loss factor for FEC (RTP-ELF).

Compared with MDI video quality monitoring, eMDI video quality monitoring supports a sequence number monitoring indicator based on the RTP packet

header. During eMDI video quality monitoring, the RTP sequence number in a video program stream is periodically detected to determine the number of lost packets and that of disordered packets. [Figure 13-77](#) shows the format of the RTP packet header. Specifically, **sequence number** indicates the sequence number of an RTP packet and its length is 16 bits. Its initial value is random, and its value is increased by 1 with each RTP packet sent. For details about the RTP packet header, see RFC3550. The receiver detects the value of sequence number to determine whether packet loss occurs or disordered packets exist, as shown in [Figure 13-78](#).

 NOTE

Delay factor (DF) and media loss rate (MLR) indicators defined in MDI have great impacts on the CPU performance and long-time monitoring is not supported, so these 2 indicators are not measured for the OLT and its lower-level network devices during eMDI video quality monitoring.

Figure 13-77 Format of the RTP packet header

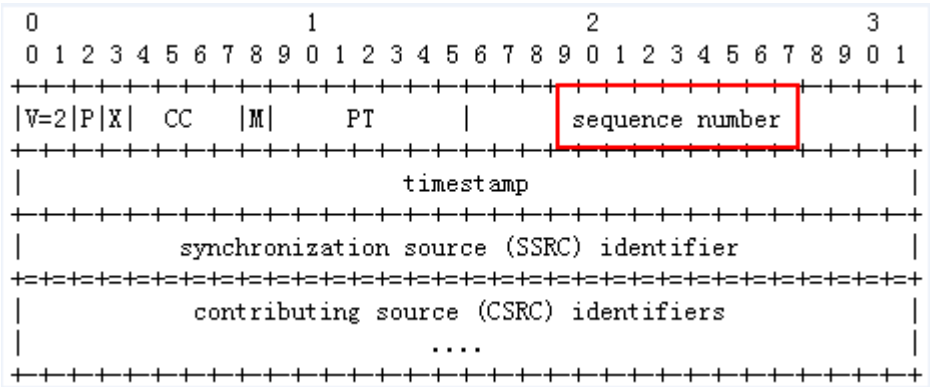


Figure 13-78 Example of detection based on the sequence number in the RTP packet header

	Packet Sequence Number	Detection Result
Normal	1.0 2.0 3.0 4.0	The packet sequence is normal. No packet is lost or disordered.
Packet loss	1.0 3.0 4.0	One packet is lost.
Disordered	1.0 3.0 2.0 4.0	One packet is disordered and one packet is lost.

RTP-LR

RTP-LR: indicates the number of lost packets in a statistical period. If this value is greater than 0, a video fault occurs.

RTP-SE

RTP-SE: indicates the number of disordered packets in a statistical period. If this value is greater than 0, a video fault occurs.

RTP-LP

RET is a packet loss recovery mechanism that introduces automatic retransmission requests when multicast or unicast packet loss occurs. This function reduces

network quality deterioration caused by packet loss and improves the video quality of live and VoD programs.

RTP-LP: indicates the maximum number of consecutively lost RTP packets in a statistical period. If the RET threshold is set for a carrier's network, O&M personnel can compare RTP-LP and the threshold to determine whether a video fault occurs. When the RET function is enabled, a small number of lost packets will be retransmitted. A greater RTP-LP value indicates more difficult packet retransmission.

RTP-ELF

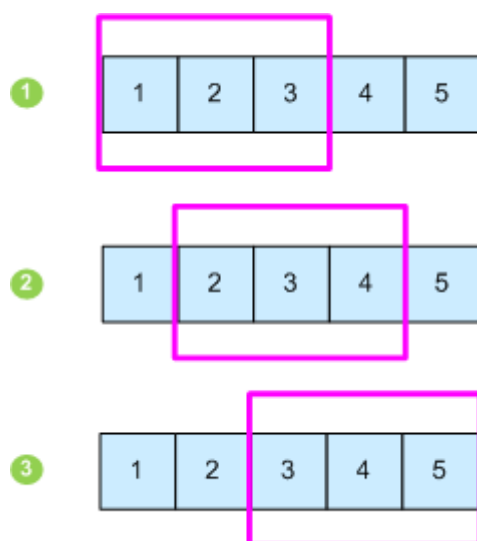
FEC is short for forward error correction. Redundant error-correcting codes can be added to transmission codes. When specified conditions are met, incorrect transmission codes can be automatically corrected during decoding, reducing the bit error rate of Rx signals and minimizing the frequency of artifacts and frame freezing.

RTP-ELF: indicates the effective loss factor for FEC in a statistical period. When the IPTV video service supports FEC and RET functions, a small number of data packets lost within a certain packet range or time period can be compensated through FEC and RET. This reduces the chance of IPTV video artifacts.

The value of RTP-ELF can be calculated by using the sliding window and threshold. In a statistical period, after a packet is slid, check whether the number of lost data packets in the sliding window is greater than the threshold. If the number of lost data packets is greater than the threshold, packet loss occurs. In this case, the number of packet loss windows is increased by 1, and window sliding stops when the monitoring period ends. If the total number of packet loss windows is greater than 0 in a statistical period, a video fault occurs.

As shown in [Figure 13-79](#), if the sliding window contains 3 frames and the threshold is set to 2 frames, the sliding window can compensate 2 packets at most through FEC and RET. If more than 2 packets are lost, the excessive lost packets cannot be compensated, affecting video quality.

Figure 13-79 Sliding window

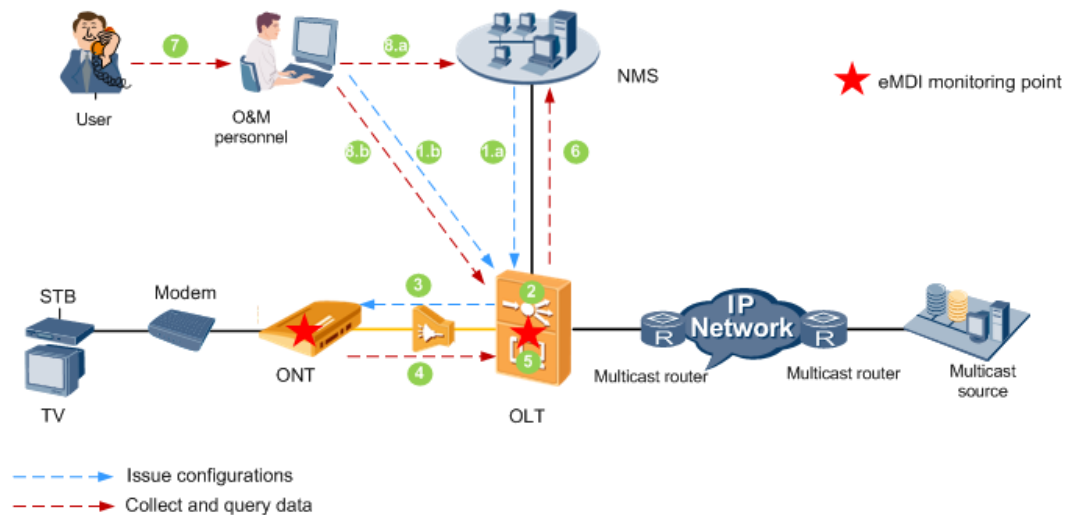


13.7.4.3 Principle

Implementation Process

Figure 13-80 shows the implementation process of eMDI video quality monitoring.

Figure 13-80 Implementation process of eMDI video quality monitoring



The implementation process of eMDI video quality monitoring is as follows:

- eMDI video quality monitoring is enabled.
 - O&M personnel can use the NMS to enable eMDI video quality monitoring of multicast programs on an OLT or ONT, and issue the enabling information to the OLT through MIB.
 - O&M personnel can run the **emdi monitor udp start** command to enable eMDI video quality monitoring of multicast programs on an OLT or ONT.

NOTE

- In scenarios where an inter-board aggregation group, protection group, or VRRP is configured on the multicast upstream port, if an inter-board switchover occurs on the ingress of monitored multicast program traffic, the eMDI video quality monitoring result reported during the switchover may be incorrect.
- For an OLT, monitoring points can be set on the upstream board, cascade board, or service board. All multicast programs on a specified board or a specified program on a specified board can be monitored.
- For an ONT, only one multicast program can be monitored at the same time. When enabling eMDI video quality monitoring, O&M personnel can specify an ONT and multicast program for monitoring, or specify an ONT without specifying any multicast program. If no multicast program is specified, when users order multiple programs, the system automatically selects the program with the highest data rate for monitoring. If monitoring is enabled with both the ONT and multicast program specified, after the specified multicast program is deleted, the system also selects the multicast program with the highest data rate for monitoring.
- If the monitoring point is set on the upstream board of an OLT, only inbound video streams can be monitored; if the monitoring point is set on a non-upstream board of an OLT, only outbound video streams can be monitored.

2. The OLT control board issues a message to enable monitoring of multicast programs of specified boards.
3. The OLT PON board records the eMDI monitoring configurations of the ONT and issues a message to the ONT. After receiving the message, the ONT monitors multicast programs in real time.
4. The OLT PON board collects the eMDI monitoring data of the ONT through OMCI or OAM messages every 5 minutes.
5. The OLT control board obtains the eMDI monitoring data of all boards every 5 minutes and saves the data.
6. The OLT control board reports monitoring results to the server every 5 minutes.

eMDI fault data of the ONT and all OLT boards is summarized into a data file every 5 minutes. The OLT serves as an SFTP client and uploads this file to the SFTP server of the NMS after compressing the file. Rules for generating monitoring records are as follows:

- When video traffic exists but no packet disorder or loss occurs, no monitoring record is generated, but the total number of packets needs to be recorded and reported.
- When packet loss or disorder occurs, monitoring records are generated based on the monitoring period.
- When no video traffic exists, no monitoring record is generated.

The following table lists the parameters to be reported.

Parameter	Description
Time	Monitoring time, in DTS format.
Monitoring device	Device name or IP address
Monitoring point	• Subrack ID and slot ID • Subrack ID, slot ID, port ID, and ONT ID
Channel	Multicast program SIP, GIP, and VLAN ID
Data 1	OLT board data collected and summarized every 5 minutes NOTE The system generates a monitoring data record every minute. The OLT control board collects and summarizes the monitoring results of OLT boards with monitoring enabled, and reports the results to the server every 5 minutes. The OLT control board does not summarize the ONT monitoring data.

Parameter	Description
Data 2	Monitoring data records with the maximum number of lost packets and disordered packets within 5 minutes NOTE The system generates a monitoring data record every minute. If the OLT control board reports all monitoring data to the server every 5 minutes, the service processing performance of the OLT will be affected. Therefore, the OLT control board uploads to the server a record with the maximum number of lost packets and another with the maximum number of disordered packets respectively for OLT boards and the ONT every 5 minutes.

7. A user reports a video program quality issue to the carrier.
8. O&M personnel remotely query historical monitoring data and locate the fault.
 - Query the records in all monitoring periods on the NMS.
 - Run the **display emdi monitor udp result** command on the OLT to query the monitoring records.

 **NOTE**

Only the monitoring results of the current and previous statistical periods can be queried by running commands.
9. O&M personnel further troubleshoot the fault based on the fault locating result.

Fault Locating

After completing eMDI video quality monitoring, O&M personnel can query the monitoring results by running commands on the OLT or through the NMS, and learn the program quality of each monitoring point. Based on such information, they can locate the video quality fault by adhering to the following principles shown in [Table 13-46](#).

Table 13-46 Faulting locating roadmap for eMDI video quality monitoring

Monitoring Point on an OLT Upstream Board	Monitoring Point on an OLT Non-upstream Board	Monitoring Point on an ONT	Conclusion
POK	POK	POK	The upper-layer network or headend system may be faulty. O&M personnel should focus on checking the metropolitan area network (MAN) in the upstream direction of the OLT.
OK	POK	POK	The OLT may be faulty.
OK	OK	POK	The ONT or the line between the PON board and the ONT egress may be faulty.
OK	OK	OK	The interconnection or STB in the user's home may be abnormal.

13.7.4.4 Configuring eMDI Video Quality Monitoring

Prerequisites

The multicast service is configured.

Procedure

Step 1 (Optional) Run the **emdi interval** command to configure the period of eMDI video quality monitoring.

Perform this step if the default period of eMDI video quality monitoring does not meet actual network requirements. The default period is 60s.

Step 2 (Optional) Run the **emdi fec** command to configure the sliding window and threshold for eMDI video quality monitoring.

In forward error correction (FEC) and retransmission (RET) scenarios, perform this step if the default sliding window and threshold for eMDI video quality monitoring do not meet actual network requirements. The default sliding window contains 100 frames and the threshold is 5 frames.

- Step 3** Run the **emdi monitor udp start** command to enable an eMDI video quality monitoring instance.
- When eMDI video quality monitoring is enabled, if only the OLT board is specified, all programs on the board are monitored; if both the OLT board and program information (including the multicast VLAN, multicast IP address, and multicast source IP address) are specified, only the specified program on the specified board is monitored.
 - When eMDI video quality monitoring is enabled, if only the ONT is specified, only the program with the highest data rate is monitored; if both the ONT and program information (including the multicast VLAN, multicast IP address, multicast source IP address, and destination port ID) are specified, only the specified program on the specified ONT is monitored.
- Step 4** (Optional) To terminate video quality monitoring in advance, run the **emdi monitor udp stop** command to stop the created monitoring instance.
- Step 5** Run the **file-server auto-backup emdi** command to configure the server to which eMDI monitoring data is uploaded.
- Step 6** (Optional) Run the **display emdi monitor udp result** command to query the result of eMDI video quality monitoring, and perform fault locating based on the queried result.
- Step 7** (Optional) Run the **display emdi monitor udp instance** command to query the information about the configured eMDI video quality monitoring instance.
- Step 8** (Optional) Run the **display emdi info** command to check whether the period of eMDI video quality monitoring, sliding window, and threshold are correctly configured.

----End

Example

To configure the period of eMDI video quality monitoring to 30s, sliding window to 110 frames, and threshold to 10 frames, and enable the following 2 eMDI video quality monitoring instances, do as follows:

- Upstream port: 0/9, multicast VLAN: 100, multicast program IP address: 224.1.1.1.
- ONT port: GPON port 0/2/0, ONT ID: 0, multicast VLAN: 100, multicast program IP address: 224.1.1.2.

```
huawei(config)#emdi interval 30s
huawei(config)#emdi fec window 110 threshold 10
huawei(config)#emdi monitor udp start instance board 0/9 vlan 100 destination-ip 224.1.1.1
huawei(config)#emdi monitor udp start instance ont 0/2/0 0 vlan 100 destination-ip 224.1.1.2
huawei(config)#display emdi info
```

```
-----
eMDI interval (unit: s)           : 30
Window for RTP effective loss factor (unit: frame) : 110
Threshold for RTP effective loss factor (unit: frame) : 10
-----
```

```
huawei(config)#display emdi monitor udp instance all
```

Instance	F/S/P	ONT	VLAN	Destination IP	Source IP
0	0/9/-	-	100	224.1.1.1	-
1	0/2/0	0	100	224.1.1.2	-

Total: 2

13.7.5 eMDI Video Quality Monitoring for the Unicast Service

Enhanced Media Delivery Index (eMDI) video quality monitoring for the unicast service mainly applies to video services such as video surveillance, video of demand (VoD), and over the top (OTT) videos. It helps O&M personnel efficiently demarcate video quality faults in proactive O&M mode.

13.7.5.1 Introduction to eMDI for Unicast Services

Purpose of Introducing eMDI

As video services develop rapidly, users have higher requirements on video experience. Therefore, it is important to quickly demarcate and resolve video quality faults. Traditional demarcation requires O&M personnel to locate and analyze faults onsite, which is time-consuming and inefficient. Video quality monitoring can help O&M personnel remotely demarcate faults, avoiding unnecessary home visits and improving demarcation efficiency.

The existing Video Mean Opinion Score (VMOS), Media Delivery Index (MDI), and Real-Time Transport Protocol (RTP) video quality monitoring solutions can help O&M personnel remotely demarcate video quality faults. However, these solutions have the following limitations:

- **Passive O&M and low demarcation efficiency:** Video quality monitoring cannot be performed in real time for a long time. O&M personnel starts video quality monitoring only after a fault is reported, and can demarcate a fault only after it recurs.
- **Low demarcation accuracy:** These solutions do not support monitoring indicators in the forward error correction (FEC) or retransmission (RET) scenarios, resulting in inaccurate monitoring results in these scenarios.

NOTE

- RET is a lost packet recovery mechanism by automatic retransmission in multicast and unicast scenarios. This function can mitigate data quality deterioration caused by packet loss and improve the video quality of live TV and VOD programs.
- FEC is a mechanism that adds redundant error correction codes to the transmission code column. When decoding is performed under certain conditions, incorrect codes can be automatically corrected. This reduces the bit error rate of received signals and the frequency of artifacts and frame freezing.
- **Low monitoring capacity:** These solutions can monitor only a small number of programs at the same time, and cannot be widely deployed on an entire network.
- **Limited services to monitor:** These solutions can demarcate only faults in video services carried by the User Datagram Protocol (UDP), and cannot demarcate faults in video services carried by the Transmission Control Protocol (TCP).

To solve the preceding problems, Huawei launches the Enhanced Media Delivery Index (eMDI) video quality monitoring solution. eMDI offers the following benefits:

- **Proactive O&M and efficient demarcation:** The solution can monitor the video quality in real time over a long period of time and upload the monitoring results to a server. When a fault occurs, O&M personnel can quickly demarcate the fault based on the collected monitoring data.
- **Accurate demarcation:** For video services carried over UDP, effective packet loss factors are proposed under the FEC/RET compensation mechanism to accurately describe the impact of packet loss on video services and improve demarcation accuracy.
- **Network-wide deployment:** Multiple unicast video streams can be monitored at the same time. More video programs can be monitored through network-wide deployment.
- **More services to monitor:** The solution can monitor the quality of video services carried by both UDP and TCP.

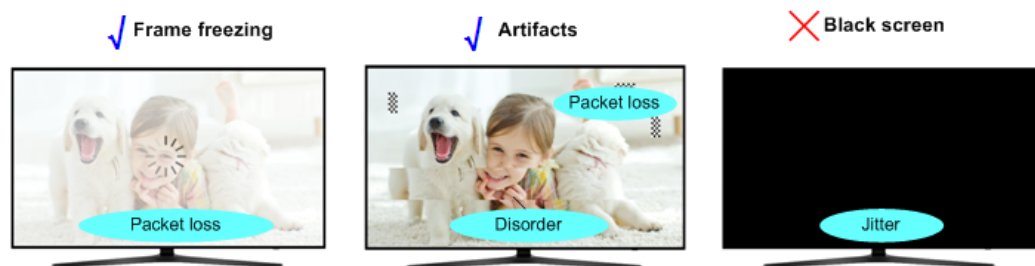
What is eMDI?

eMDI is an enhanced video quality monitoring solution developed based on MDI. It deploys monitoring points on network devices to monitor the quality of video streams in real time and periodically reports monitoring results to a server. By remotely viewing and evaluating monitoring results, O&M personnel can quickly demarcate video quality faults and provide assurance for VIP users.

Video fault symptoms to be monitored by eMDI

Packet loss, disorder, and jitter are three key factors that affect video quality. Even if the packet loss rate and disorder rate are less than 0.01%, frame freezing and artifacts can occur on a terminal, while jitter may cause black screens on a terminal. eMDI video quality monitoring applies only to frame freezing and artifact faults in videos.

Figure 13-81 Video fault symptoms that can be monitored by eMDI

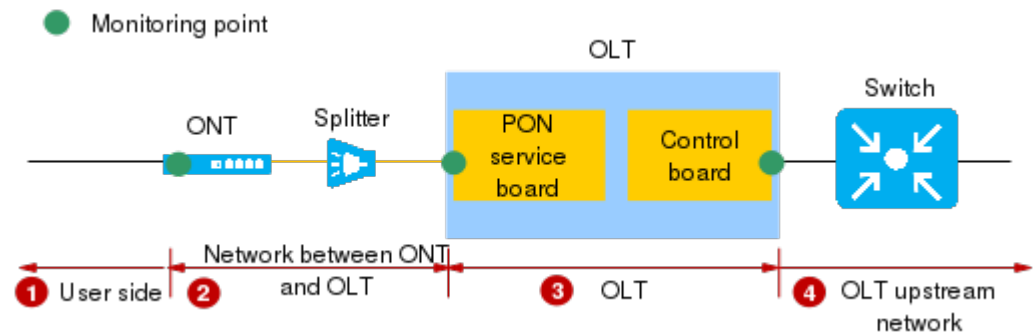


Positions for deploying monitoring points

eMDI video quality monitoring for unicast services supports monitoring of upstream and downstream unicast UDP/TCP packets. eMDI monitoring points can be deployed on the ONT, PON service port of the OLT, and upstream port of the OLT. The three monitoring points can be used to quickly demarcate faults on four network segments, as shown in [Figure 13-82](#).

O&M personnel can also deploy monitoring points at one or two positions. For example, if monitoring points are deployed only on PON service ports of the OLT, it can be determined that a fault occurs in the OLT or OLT upstream network when packet loss or disorder occurs in downstream video streams of a PON service port. When packet loss or disorder is detected in the upstream video stream of a PON service port, it can be determined that a fault occurs in the downstream network and devices of the OLT.

Figure 13-82 eMDI video quality monitoring points



Fault Locating

After eMDI video quality monitoring is enabled, O&M personnel can query the monitoring results on the OLT command line interface (CLI) or on the server to learn about the program quality on each monitoring point for fault demarcation. The following table shows fault demarcation rules.

Table 13-47 Fault demarcation based on eMDI video quality monitoring for downstream video streams (POK indicates that packet loss or disorder occurs, and OK indicates that no packet loss or disorder occurs.)

Monitoring Point on OLT Upstream Port	Monitoring Point on OLT PON Service Port	Monitoring Point on ONT	Conclusion
POK	POK	POK	The fault may occur in the upper-layer network or headend system. Check the metro network above the OLT.
OK	POK	POK	The fault may occur inside the OLT.
OK	OK	POK	The ONT or the line between the PON board and the ONT egress port may be faulty.
OK	OK	OK	The fault may occur in the user's home network (Internet or STB).

Table 13-48 Fault demarcation based on eMDI video quality monitoring for upstream video streams (POK indicates that packet loss or disorder occurs, and OK indicates that no packet loss or disorder occurs.)

Monitoring Point on OLT Upstream Port	Monitoring Point on OLT PON Service Port	Monitoring Point on ONT	Conclusion
POK	POK	POK	The fault may occur in the user's home network (Internet or STB).
POK	POK	OK	The ONT or the line between the PON board and the ONT egress port may be faulty.
POK	OK	OK	The fault may occur inside the OLT.
OK	OK	OK	The fault may occur in the upper-layer network or headend system. Check the metro network above the OLT.

13.7.5.2 eMDI Monitoring Indicators for Unicast Services

eMDI video quality monitoring periodically collects monitoring data at monitoring points and uploads the data to the server for O&M personnel to analyze and demarcate faults. The eMDI monitoring indicators for UDP and TCP services are different.

Indicators for monitoring UDP video services

For video services carried over UDP, faults are analyzed by monitoring the sequence numbers of Real-time Transport Protocol (RTP) packets in video program streams. RTP is a transport layer protocol that provides real-time end-to-end data transmission services. It is widely used in communication and entertainment over streaming media, such as webcast, network TV, and video conference.

Figure 13-83 shows the format of an RTP packet header. **sequence number** indicates the sequence number of an RTP packet. The initial value is randomly generated and is incremented by 1 each time an RTP packet is sent. By monitoring the sequence numbers of RTP packets on monitoring points, O&M personnel can determine whether packet loss or disorder occurs in the video program stream, as shown in **Figure 13-84**.

Figure 13-83 RTP packet format

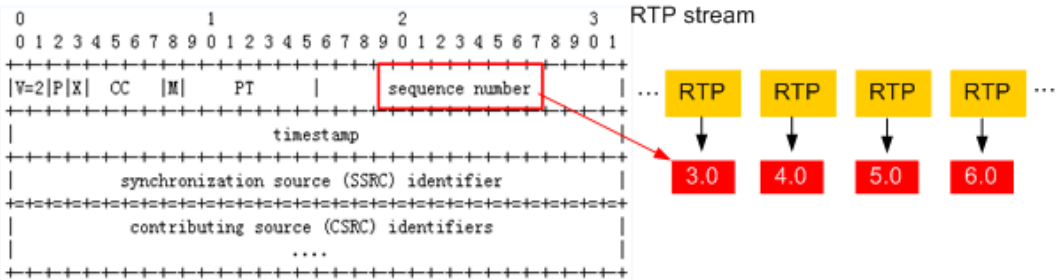


Figure 13-84 Packet monitoring based on sequence numbers in RTP packet headers

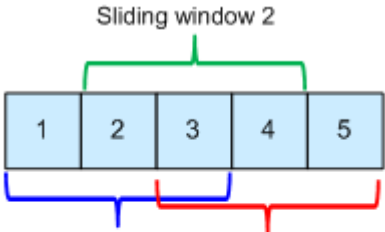


Table 13-49 lists the monitoring indicators for UDP video streams

Table 13-49 Monitoring indicators for UDP video streams

Monitoring Indicator	Definition	Formula
RTP-LC	RTP Loss Count: number of lost packets in a statistical period	If the value of RTP-LC is greater than 0, a fault has occurred.
RTP-LR	RTP Loss Rate: rate of lost packets in a statistical period	$\text{RTP-LR} = \frac{\text{Number of lost packets}}{\text{Number of received packets} + \text{Number of lost packets} - \text{Number of disordered packets}}$ If the value of RTP-LP is greater than 0, a fault has occurred.
RTP-SE	RTP Sequence Error: number of disordered RTP packets in a statistical period	If the value of RTP-SE is greater than 0, a fault has occurred.

Monitoring Indicator	Definition	Formula
RTP-SER	RTP Sequence Error Rate: rate of disordered RTP packets in a statistical period	$\text{RTP-SER} = \frac{\text{Number of disordered packets}}{\text{Number of received packets} + \text{Number of lost packets} - \text{Number of disordered packets}}$ If the value of RTP-SER is greater than 0, a fault has occurred.
RTP-LP	RTP Loss Period: maximum number of consecutively lost RTP packets in a statistical period	If the RET threshold is set for an operator's network, O&M personnel can compare RTP-LP and the threshold to determine whether a fault has occurred. If RTP-LP is greater than the threshold, a fault has occurred.

Monitoring Indicator	Definition	Formula
RTP-ELF	RTP Effective Loss Factor for FEC: effective FEC packet loss factor in a statistical period	If the IPTV video service supports FEC, a small number of data packets lost within a certain packet range or time period can be compensated through FEC. This reduces the probability of IPTV video artifacts. RTP-ELF can be calculated based on the number of packets in a sliding window (L) and the packet loss threshold (R). In a statistical period, each time a packet is sent, the system checks whether the number of lost packets in the sliding window L is greater than the packet loss threshold R. If yes, the window is a valid packet loss window. In this case, the value of RTP-ELF increases by 1 until the monitoring period ends, as shown in Figure 13-85. If the value of RTP-ELF is greater than 0, a fault has occurred. Figure 13-85 Sliding window  Note: If the number of lost packets that cannot be compensated within the sliding window is greater than or equal to 1, the window is an effective packet loss window.

Indicators for monitoring TCP video services

Faults in TCP video services are analyzed based on TCP packet monitoring results. TCP is a connection-oriented, reliable, and byte stream-based transport layer communication protocol. [Table 13-50](#) lists the monitoring indicators for TCP video streams. O&M personnel compare the TCP monitoring indicators with the thresholds set on a server to demarcate faults.

Table 13-50 Monitoring indicators for TCP video streams

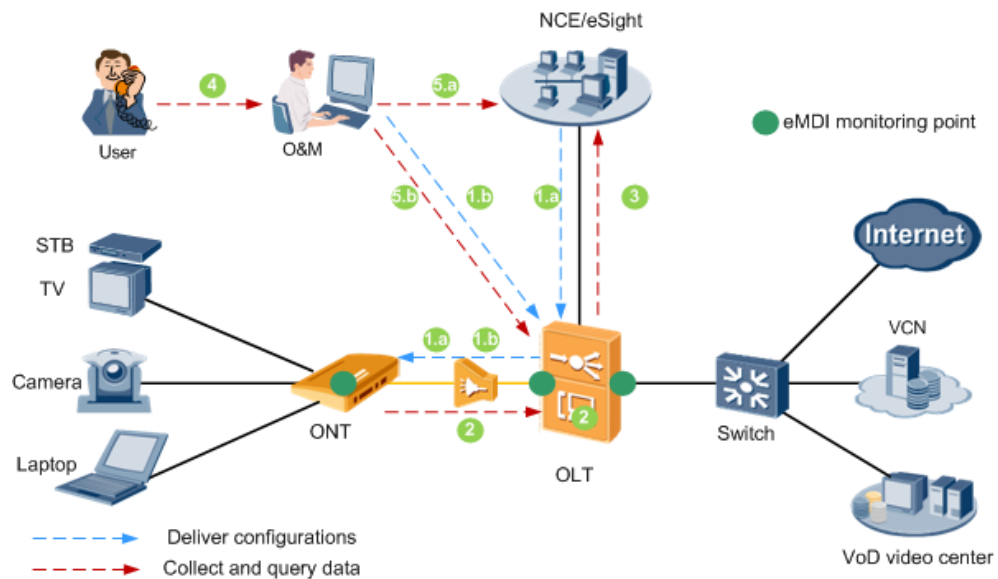
Monitoring Indicator	Definition	Formula
MFR	Mean Flow Rate: average bitrate in a statistical period	MFR = Total length of packets received within the statistical period/Actual valid streaming time (unit: kbit/s) If the value of MFR is small, the server transmits data for a limited period of time, and no data is transmitted for an extended period during video streaming.
UPLR	Upstream Packet Loss Rate: packet loss rate on the upstream devices of a monitoring point within a statistical period	If no packet is lost, the sequence number of the current packet plus the packet length is equal to the expected sequence number of the next packet. If the sequence number of a packet is greater than expected, packet loss has occurred on an upstream device. The number of lost packets can be calculated based on the average packet size. UPLR = Number of upstream lost packets/(Total number of received packets + Total number of lost packets) UPLR can be used to determine whether packet loss occurs in the upstream of a monitoring point.

Monitoring Indicator	Definition	Formula
DPLR	Downstream Packet Loss Rate: packet loss rate on the downstream devices of a monitoring point within a statistical period	If no packet is lost, the sequence number of the current packet plus the packet length is equal to the expected sequence number of the next packet. If the sequence number of a packet is smaller than expected, the packet is considered as a retransmitted packet. The number of retransmitted packets is considered as the total number of lost packets. Number of downstream lost packets = Total number of lost packets - Number of upstream lost packets $DPLR = \text{Number of downstream lost packets} / (\text{Total number of received packets} + \text{Total number of lost packets})$ DPLR can be used to determine whether packet loss occurs in the downstream of a monitoring point.
DRTT	Downstream Round-Trip Time (DRTT): average downstream two-way latency at a monitoring point in a statistical period	$DRTT = T2 - T1$ A received non-retransmitted packet is randomly selected, and its timestamp is recorded as T1. The expected sequence number of the next packet is calculated based on the sequence number and length of the current packet. If the sequence number of an upstream packet sent from a downstream device is greater than or equal to the expected sequence number, the timestamp of this packet is recorded as T2.

13.7.5.3 eMDI Interaction Process for Unicast Services

eMDI video quality monitoring for unicast services can be deployed in the upstream and downstream directions for both UDP and TCP video streams.

Figure 13-86 shows the interaction process of eMDI video quality monitoring.

Figure 13-86 Interaction process of eMDI video quality monitoring

1. O&M personnel deploy monitoring points as required and start eMDI video quality monitoring for the OLT and ONTs on the NCE/eSight server or CLI.

NOTE

For unicast packets, the video stream to be monitored needs to be specified using a quintuple which includes the protocol type (TCP/UDP), destination IP address, source IP address, destination port number, and source port number.

2. If there is a monitoring point on an ONT, the ONT periodically reports video monitoring data to the OLT.
3. The OLT summarizes the video monitoring data on the ONT and OLT monitoring points and periodically reports the data to the NCE/eSight server.
4. After a fault occurs in the video service of a user, the user reports this fault to the operator.
5. O&M personnel can remotely view historical monitoring data on the NCE/eSight server or by running commands, and evaluate and demarcate the fault based on the historical monitoring data.
6. O&M personnel can troubleshoot the fault based on the demarcation result.

13.7.5.4 Network Application of eMDI for Unicast Services

Unicast video services include video backhaul, VOD, and OTT video services. eMDI video quality monitoring helps O&M personnel efficiently demarcate faults in such services.

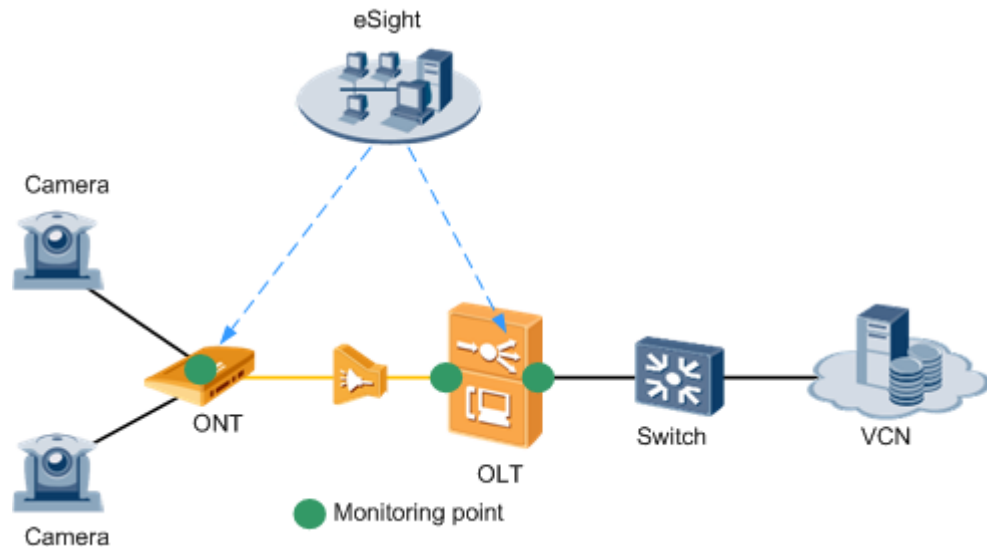
eMDI Video Quality Monitoring in the Video Backhaul Scenario

Regarding the O&M solution for a video backhaul network, customers are concerned about the online rate and intact rate of IP cameras (IPCs). In complex networks with multiple systems, if IPCs go offline or experience faults such as packet loss, the fault may be difficult to demarcate and troubleshoot, resulting in high O&M costs and hindering the development of the public security video

backhaul networks. eMDI video quality monitoring can help O&M personnel resolve this problem.

On a video backhaul network shown in [Figure 13-87](#), O&M personnel can use the eSight to deploy eMDI monitoring points on OLT upstream ports, OLT PON access ports, and ONTs to monitor video streams and collect monitoring indicators. When a video cloud node (VCN) detects that the data transmission quality deteriorates, O&M personnel can demarcate the fault by analyzing collected monitoring indicators.

Figure 13-87 eMDI video quality monitoring in the video backhaul scenario

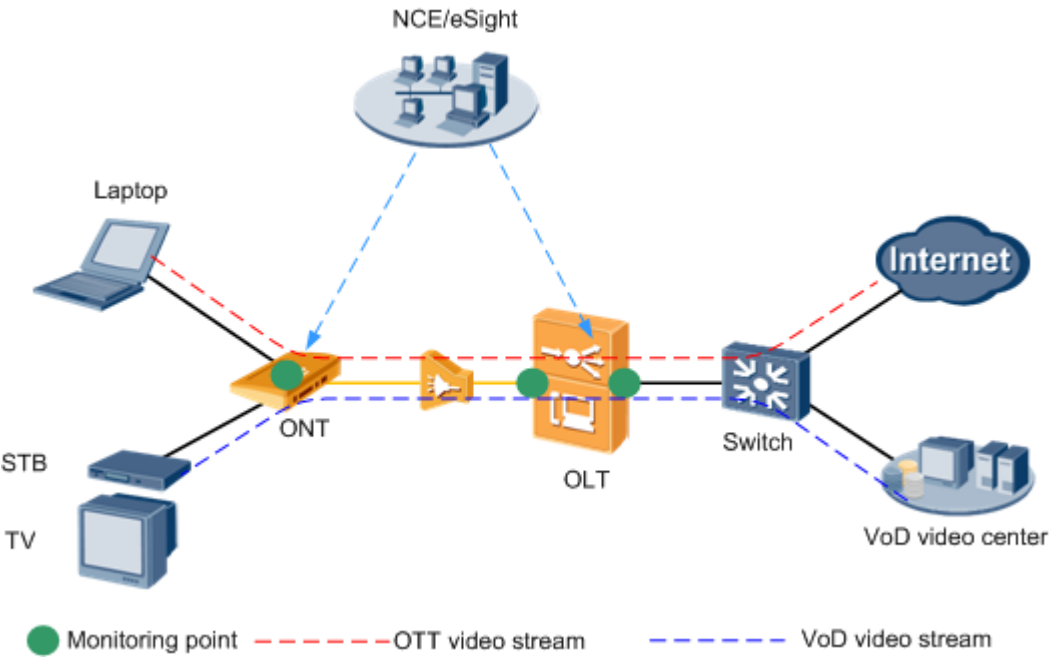


eMDI Video Quality Monitoring for VOD and OTT Scenarios

With the emergence of video services, users have ever higher requirements on video quality, and video quality monitoring becomes very important. eMDI video quality monitoring helps O&M personnel remotely demarcate faults, avoiding unnecessary home visits.

As shown in [Figure 13-88](#), O&M personnel can use the NCE/eSight server to deploy eMDI monitoring points on OLT upstream ports, OLT PON access ports, and ONTs to monitor video streams and collect monitoring indicators. After a user reports a fault, O&M personnel can demarcate the fault by analyzing collected monitoring indicators.

Figure 13-88 eMDI video quality monitoring for VOD and OTT video scenarios



13.7.5.5 Configuring eMDI Video Quality Monitoring

This topic describes the process of configuring eMDI video quality monitoring for unicast services.

Prerequisites

A video service has been configured.

Context

Table 13-51 Default settings of eMDI video quality monitoring

Parameter	Default Value
Monitoring Period	60s
Sliding Window	100 frames
FEC Threshold	5 frames

Procedure

- Step 1** Run the **file-server auto-backup emdi-unicast** command to configure the server to which eMDI monitoring data is uploaded.
- Step 2** (Optional) Run the **emdi interval** command to configure the period of eMDI video quality monitoring.

Perform this step if the default period of eMDI video quality monitoring does not meet actual network requirements.

Step 3 (Optional) Run the **emdi fec** command to configure the sliding window and FEC threshold for eMDI video quality monitoring.

Perform this step if FEC and RET are enabled but the default sliding window and FEC threshold for eMDI video quality monitoring do not meet actual network requirements.

Step 4 Start an eMDI video quality monitoring instance.

- For UDP packets, run the **emdi monitor udp start** command.
- For TCP packets, run the **emdi monitor tcp start** command.

When starting eMDI video quality monitoring for a unicast service, you need to specify the monitoring point, monitoring direction (inbound: downstream; outbound: upstream), and source and destination IP addresses and port numbers of monitored video streams.

Step 5 (Optional) To cancel video quality monitoring in advance, run the either of the following commands:

- For UDP packets, run the **emdi monitor udp stop** command.
- For TCP packets, run the **emdi monitor tcp stop** command.

Step 6 (Optional) Query the eMDI video quality monitoring result and demarcate faults based on the query result.

- For UDP packets, run the **display emdi monitor udp result** command.
- For TCP packets, run the **display emdi monitor tcp result** command.

Step 7 (Optional) Query information about a configured eMDI video quality monitoring instance.

- For UDP packets, run the **display emdi monitor udp instance** command.
- For TCP packets, run the **display emdi monitor tcp instance** command.

Step 8 (Optional) Run the **display emdi info** command to check whether the period of eMDI video quality monitoring, sliding window, and threshold are correctly configured.

----End

Example

Example 1: Configure eMDI video quality monitoring for unicast UDP packets, with the data upload server IP address of 10.20.20.1, monitoring period of 30s, sliding window of 110 frames, and FEC threshold of 10 frames. Start the following three eMDI video quality monitoring instances:

- On upstream port 0/9/0, monitor the inbound unicast video stream whose destination IP address is 10.10.10.1, source IP address is 10.10.10.2, destination port number is 30, source port number is 30; and report the monitoring data to the server in real time.
- On PON port 0/2/0, monitor the inbound unicast video stream whose destination IP address is 10.10.10.1, source IP address is 10.10.10.2, destination port number is 30, source port number is 30; and report the monitoring data to the server in real time.
- On ONT 0 connected to GPON port 0/2/0, monitor the inbound unicast video stream whose destination IP address is 10.10.10.1, source IP address is

10.10.10.2, destination port number is 30, source port number is 30; and report the monitoring data to the server in real time.

```
huawei(config)#file-server auto-backup emdi-unicast primary 10.20.20.1 sftp user
huawei(config)#emdi interval 30s
huawei(config)#emdi fec window 110 threshold 10
huawei(config)#emdi monitor udp start instance port 0/9/0 inbound destination-ip 10.10.10.1
source-ip 10.10.10.2 destination-port 30 source-port 30 instance-type realtime
huawei(config)#emdi monitor udp start instance port 0/2/0 inbound destination-ip 10.10.10.1
source-ip 10.10.10.2 destination-port 30 source-port 30 instance-type realtime
huawei(config)#emdi monitor udp start instance ont 0/2/0 0 inbound destination-ip 10.10.10.1
source-ip 10.10.10.2 destination-port 30 source-port 30 instance-type realtime
huawei(config)#display emdi info
```

```
-----
eMDI interval (unit: s)                : 30
Window for RTP effective loss factor (unit: frame) : 110
Threshold for RTP effective loss factor (unit: frame) : 10
-----
```

```
huawei(config)#display emdi monitor udp instance all unicast
```

```
-----
Instance  F/S/P  ONT  VLAN  Destination IP  Source IP  Instance
          F/S/P      Destination port  Source port  Dir  Type
-----
0  0/9/0  -    -   10.10.10.1      10.10.10.2
          30          30      IN  realtime
1  0/2/0  -    -   10.10.10.1      10.10.10.2
          30          30      IN  realtime
2  0/2/0  0    -   10.10.10.1      10.10.10.2
          30          30      IN  realtime
-----
```

Total: 3

Example 2: Configure eMDI video quality monitoring for unicast TCP packets, with the data upload server IP address of 10.20.20.2, monitoring period of 30s, sliding window of 110 frames, and threshold of 10 frames. Start the following three eMDI video quality monitoring instances:

- On upstream port 0/9/0, monitor the outbound unicast video stream whose destination IP address is 10.10.10.3, source IP address is 10.10.10.4, destination port number is 40, source port number is 40; and report the monitoring data to the server periodically.
- On PON port 0/2/0, monitor the outbound unicast video stream whose destination IP address is 10.10.10.3, source IP address is 10.10.10.4, destination port number is 40, source port number is 40; and report the monitoring data to the server periodically.
- On ONT 0 connected to GPON port 0/2/0, monitor the outbound unicast video stream whose destination IP address is 10.10.10.3, source IP address is 10.10.10.4, destination port number is 40, source port number is 40; and report the monitoring data to the server periodically.

```
huawei(config)#file-server auto-backup emdi-unicast primary 10.20.20.2 sftp user
huawei(config)#emdi interval 30s
huawei(config)#emdi fec window 110 threshold 10
huawei(config)#emdi monitor tcp start instance port 0/9/0 outbound destination-ip 10.10.10.3
source-ip 10.10.10.4 destination-port 40 source-port 40 instance-type cycle
huawei(config)#emdi monitor tcp start instance port 0/2/0 outbound destination-ip 10.10.10.3
source-ip 10.10.10.4 destination-port 40 source-port 40 instance-type cycle
huawei(config)#emdi monitor tcp start instance ont 0/2/0 0 outbound destination-ip 10.10.10.3
source-ip 10.10.10.4 destination-port 40 source-port 40 instance-type cycle
huawei(config)#display emdi info
```

```
-----
eMDI interval (unit: s)                : 30
Window for RTP effective loss factor (unit: frame) : 110
Threshold for RTP effective loss factor (unit: frame) : 10
-----
```

```
huawei(config)#display emdi monitor tcp instance all
```

Instance	F/S/P	ONT	VLAN	Destination IP Destination port	Source IP Source port	Dir	Type	Instance
0	0/9/0	-	-	10.10.10.3	10.10.10.4			
			40	30	OUT		cycle	
1	0/2/0	-	-	10.10.10.3	10.10.10.4			
			30	30	OUT		cycle	
2	0/2/0	0	-	10.10.10.3	10.10.10.4			
			30	30	OUT		cycle	
Total: 3								

13.7.6 Common Multicast Maintenance Methods

This topic describes only the principles of fault diagnosis for multicast services. For details about troubleshooting (from fault symptom to troubleshooting procedure), see the *Troubleshooting* manual.

User Log

The device log records the program order history of users. The log includes the port to which a user is connected, IP address of the program group, multicast VLAN (MVLAN), time when a user starts watching a program, time when a user stops watching a program, and log mode (for example, watch, preview, idle, or preview threshold crossing).

A log is generated in any of the following scenarios:

- Normal channel switching. In such switching, the interval between receiving a leave packet to receiving a join packet is longer than the defined time.
- Ordering failure. The common causes of an ordering failure are as follows:
 - The user does not have the right to watch the program.
 - The maximum number of programs the user can watch concurrently is exceeded.
 - The bandwidth CAC fails.
- Daily preview threshold crossing.
- Quiet leaving. In quiet leaving, the user does not respond to the general query of the device.
- Long-time program watching. "Long-time watching" means that the watch time reaches the maximum duration configured in the system.
- Operations that cause a user to go offline, for example, deleting or blocking a user.

Logs can be queried according to different query criteria, including by user, by program, by a specified period with regard to a user, and by a specified period with regard to a program. If users need to learn only the log quantity, the log statistics function is recommended. This frees users from reading multiple pages of numerous logs that are generated after the device has been running for a long time.

Users can also use the log clearing function to delete unwanted old logs. Logs of all users or of a specified user be deleted.

Table 13-52 Commonly used multicast log commands

Command	Function
display igmp log	Query multicast logs.
display multicast failure-log	Query the multicast online and offline failure logs.
igmp log reset	Manually delete multicast logs.

IGMP Packet Statistics

A multicast program is ordered using the Internet Group Management Protocol (IGMP). Therefore, correctly sending, receiving, and processing IGMP packets is the prerequisite for successful program ordering. To facilitate fault locating in IGMP packet transmission/reception, the device supports three levels of IGMP packet statistics: global level, MVLAN level, and traffic stream level.

On the network side, the number of received IGMP query packets and number of sent IGMPv2/v3 join/leave packets can be queried based on MVLAN. According to the packet count, whether the upper-layer router is faulty can be determined.

On the user side, the number of received IGMPv2/v3 join/leave packets and number of sent IGMP query packets can be queried based on traffic stream. According to the packet count, whether a device in the home network is faulty can be determined.

Run the **display igmp statistic** command to query the multicast packet statistics.

Multicast Traffic Statistics Query

By querying multicast traffic statistics, users can determine whether multicast data reaches the ingress/egress of the device at the forwarding layer or whether packet loss occurs due to a low rate.

The device supports four query modes on the network side:

- A1: querying the number of sent/received multicast packets on an Ethernet port. Run the **display port statistics** command to query the statistics. The command output contains **Number of transmitted multicast frames** and **Number of received multicast frames**.
- A2: querying the ingress traffic (unit: kbit/s) of a specified multicast program (a pre-configured or dynamic program) or of a specified multicast upstream port. Run the **display multicast flow-statistic** command to query the traffic.
- A3: querying the number of required multicast packets (filtered by ACL) in the inbound direction of an Ethernet port.
- A4: querying the number of sent/received multicast frames on a PON port of an MDU that uses GPON upstream transmission. Run the **display gpon-port statistic** command to query the number. The command output contains **Received multicast frames** and **Sent multicast frames**.

On the user side, the device supports the following query modes for the GPON board:

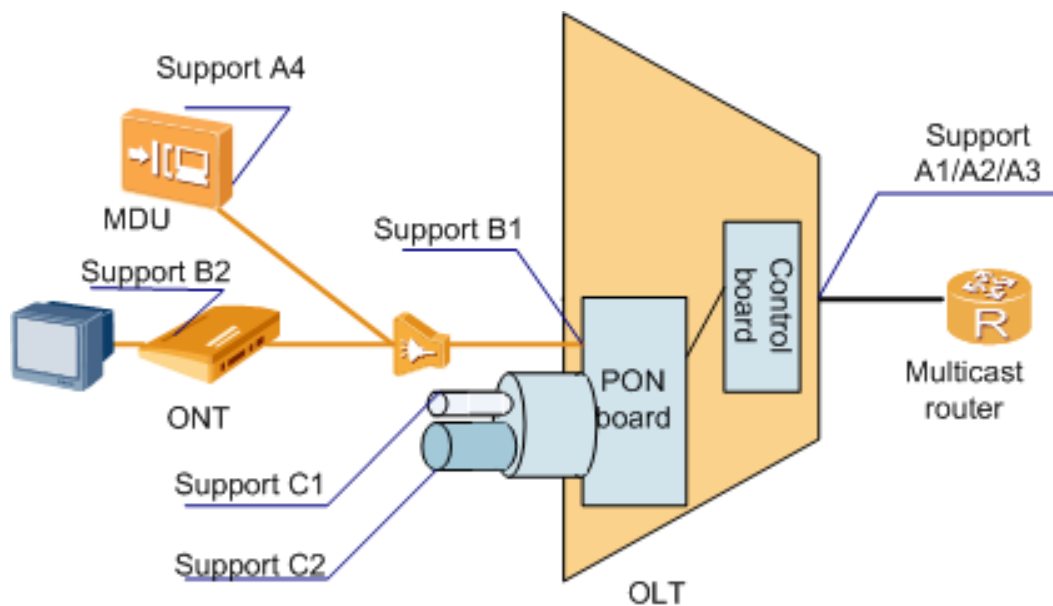
- B1: querying the number of sent/received multicast frames and number of sent bytes on a PON port. Run the **display statistics port ethernet** command to query the number. The command output contains **Received multicast frames** and **Sent multicast frames**.
- B3: querying the number of sent/received multicast frames on an Ethernet port of a specified ONT. Run the **display statistics ont-eth** command to query the number. The command output contains **Received multicast frames** and **Sent multicast frames**.

The following two methods can also be used to query the user-side multicast traffic statistics:

- C1: For the multicast traffic copied to service ports (for P2P boards, and GPON boards that use multi-copy duplication), the traffic statistics (sent/received bytes) of a specified service port can be queried to obtain the multicast traffic statistics. This method is not suitable when a service port carries other services besides the multicast service.
- C2: For P2P boards, or GPON boards that use single-copy duplication, the number of sent packets of queues on a specified port can be queried to obtain the multicast traffic statistics. This method is not suitable when queues on a port carry other services besides the multicast service.

Figure 13-89 shows the points where multicast traffic can be queried.

Figure 13-89 Points of multicast traffic query



Program Ordering Behavior Analysis

Compared with traditional TV services, in the case of IP multicast service, users' order behavior can be measured and analyzed at a finer grain, such as statistics measurement of hottest programs, analysis of user interest, and peak hours of program ordering. For such purposes, the device needs to precisely record the order behavior of each user in the form of logs and output the content of the logs

through an open interface. According to different output modes, the device supports two log transfer modes: by CDR or by syslog (RFC 3164). The formats of the two modes are the same. For details, see "[Charging Mode](#)." The following table lists the pros and cons of the two modes.

Table 13-53 Pros and cons of the two log transfer modes

Log Mode	Pro	Con
CDR	Reliable transfer. TFTP, FTP, or SFTP can be selected as the transfer protocol. NOTE FTP and TFTP have security risks due to protocol restrictions. SFTP is recommended.	Logs are reported to the file server only when specified reporting conditions are met (the reporting interval expires or the number of logs reaches the reporting threshold).
syslog	Timely report. Once a log is generated, it is uploaded to the syslog server.	Unreliable transfer. Syslog adopts the UDP protocol.

13.8 Multicast Standards and Protocols Compliance

Table 13-54 Reference standards and protocols

Standard NO.	Standard Description	Application Scope
TR101	Technical Report DSL Forum, TR-101 Migration to Ethernet-Based DSL Aggregation, April 2006	IPv4 and IPv6 Multicast
TR156	Technical Report Broadband Forum, TR-156 Using GPON Access in the context of TR-101, December 2008	IPv4 and IPv6 Multicast
RFC 1112	Deering, S., "Host Extensions for IP Multicasting",STD 5, RFC 1112, August 1989	IPv4 and IPv6 Multicast
RFC-2236	Fenner, W., "Internet Group Management Protocol, Version 2", RFC 2236, November 1997	IPv4 and IPv6 Multicast
RFC 3376	B. Cain., "Internet Group Management Protocol, Version 3 ", RFC 3376,October 2002	IPv4 and IPv6 Multicast
RFC 3569	S. Bhattacharyya, "An Overview of Source-Specific Multicast (SSM)", RFC 3569, July 2003	IPv4 and IPv6 Multicast

Standard NO.	Standard Description	Application Scope
RFC 4601	B. Fenner, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC4601, August 2006	IPv4 and IPv6 Multicast
RFC 4604	H. Holbrook, "Using IGMPv3 and MLDv2 for Source-Specific Multicast", RFC 4604, August 2006	IPv4 and IPv6 Multicast
RFC 4605	B. Fenner, "IGMP/MLD Proxying", RFC 4605, August 2006	IPv4 and IPv6 Multicast
RFC 4607	H. Holbrook , "Source-Specific Multicast for IP", RFC 4607, August 2006	IPv4 and IPv6 Multicast
RFC 4541	M. Christensen, "Considerations for IGMP and MLD Snooping Switches", RFC 4541, May 2006	IPv4 and IPv6 Multicast
RFC 2710	S. Deering,"Multicast Listener Discovery (MLD) for IPv6",RFC 2710, October 1999	IPv6 Multicast
RFC 3810	R. Vida, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004	IPv6 Multicast

13.9 Multicast Feature Updates

Product Version	Change Description
V100R022C00	Added 13.6.6 Configuring the Layer 2 Reverse Multicast Service and 13.6.7 Configuring the Layer 3 Reverse Multicast Service .
V100R020C10	- Added 13.4.2.2 PIM-SM 13.7.5 eMDI Video Quality Monitoring for the Unicast Service supported configuring the mode of reporting the monitoring data to the server.
V100R020C00	Added 13.7.5 eMDI Video Quality Monitoring for the Unicast Service
V100R019C20	The IPv6 multicast preview function is added.