SDNC 6.0 Multicast Technical Guide White Paper

Contents

1 Overview

1.1 Introduction

Multicast technology, an efficient solution for one-to-many data transmissions in IP networks, enables a single source to deliver data to multiple recipients simultaneously.

1.2 Background

Internet Protocol Television (IPTV) is a broadband cable network-based technology integrating internet, multimedia, and communication technologies. It provides a variety of interactive services, including digital television, to household users. IPTV is a common service in hotels. Just like reliable Wi-Fi, smooth IPTV services are essential for creating an excellent guest experience.

Delivering these services strains bandwidth and concurrency. By conserving bandwidth and reducing network load, multicast is now central to hotel IPTV deployments.

1.3 Purpose of this White Paper

This guide aims to:

1. Provide a detailed explanation of the principles and advantages of multicast technology.
2. Offer specific configuration guidelines and application strategies.
3. Demonstrate good practices for IPTV deployment in hotels.
4. Help network administrators master this technology and easily configure IPTV solutions for hotel scenarios.

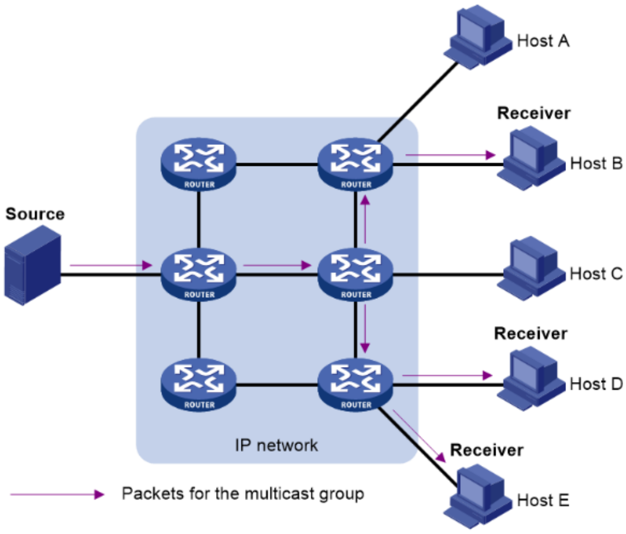
2 Introduction of Key Technologies

2.1 Basic Concepts

Multicast is an efficient transmission mode for one to many and many to many in IP networks

- One time transmission, multi-point reception
- Multicast address: IPv4 Class D address (224.0.0.0~239.255.255.255)

Principle: Source sends 1 stream >Copy only at fork point > Send only to recipients who have joined the group.



Technical Advantages

Multicast technology effectively addresses the challenge of one-to-many data transmission, enabling efficient point-to-multipoint data delivery in IP networks. It substantially reduces bandwidth consumption and network load. Leveraging multicast capabilities facilitates the provision of new value-added services, including live streaming, internet TV, distance learning, telemedicine, internet radio, real-time video conferencing, and other internet-based information services.

2.2 Market Demand

Overseas demand for multicast is robust, characterized by diverse application scenarios and cutting-edge technology. It is primarily driven by core sectors such as ultra-high-definition IPTV, finance, industry, and cloud gaming, and is maintaining an overall trend of rapid growth.

3 Key Technical Principles

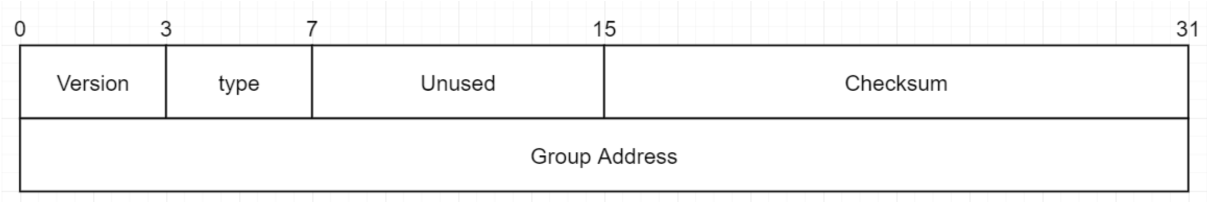
3.1 Protocol Analysis

3.1.1 IGMP/IGMP Snooping

The main protocols discussed in this white paper are IGMP/MLD and IGMP Snooping/MLD Snooping.

3.1.1.1 IGMPv1

RFC 1112 defines the specifications for IGMPv1. The packet format for IGMPv1 messages is shown below:



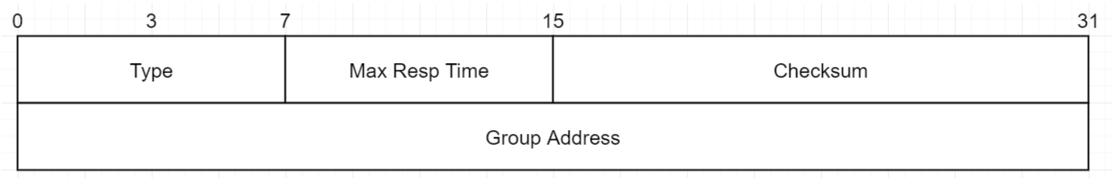
IGMPv1 supports only the following two types of messages:

- Membership query
- Membership report

The Host sends IGMP Membership Reports corresponding to specific multicast groups to express interest in joining a group. Gateways periodically send IGMP Membership Queries to verify whether at least one host on the subnet is still interested in receiving traffic directed to the group. If no response is received within a specified time, the gateway times out the group and stops forwarding traffic directed to that group.

3.1.1.2 IGMPv2

IGMPv2 is the next version of IGMPv1, which is backward compatible with IGMPv1. RFC 2236 defines the specifications for IGMPv2. The IGMPv2 message packet format is shown below:

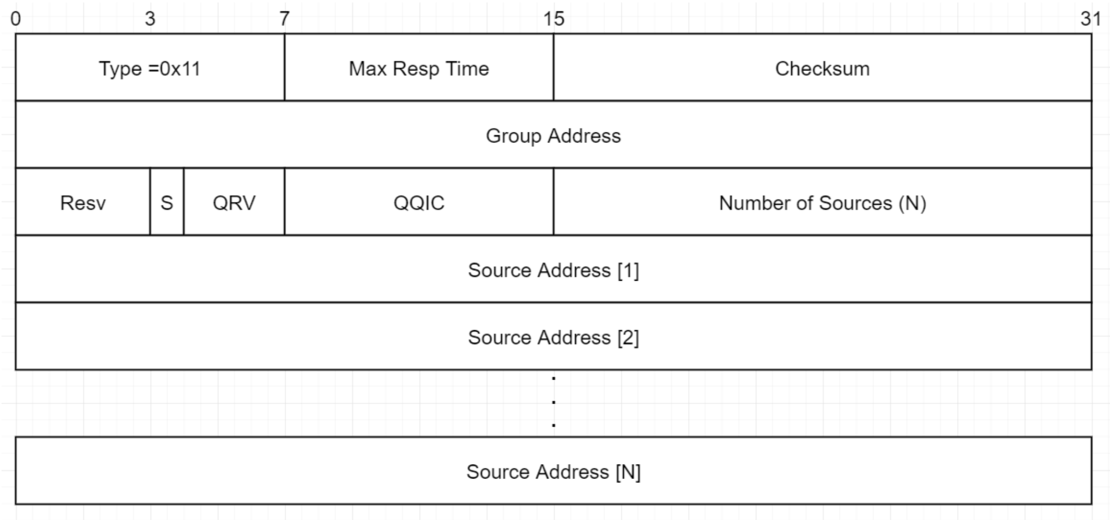


IGMPv2 operates fundamentally similarly to IGMPv1. The primary distinction lies in the introduction of a Leave Group message. Through this message, hosts can proactively communicate with their local multicast gateway to signal their intention to leave a group. The gateway then sends group-specific queries to determine whether any remaining hosts are interested in receiving traffic. If no response is received, the gateway will timeout the group and stop forwarding traffic. The addition of the Leave Group message in IGMPv2 significantly reduces leave latency compared to IGMPv1. Unwanted and unnecessary traffic can be terminated more rapidly.

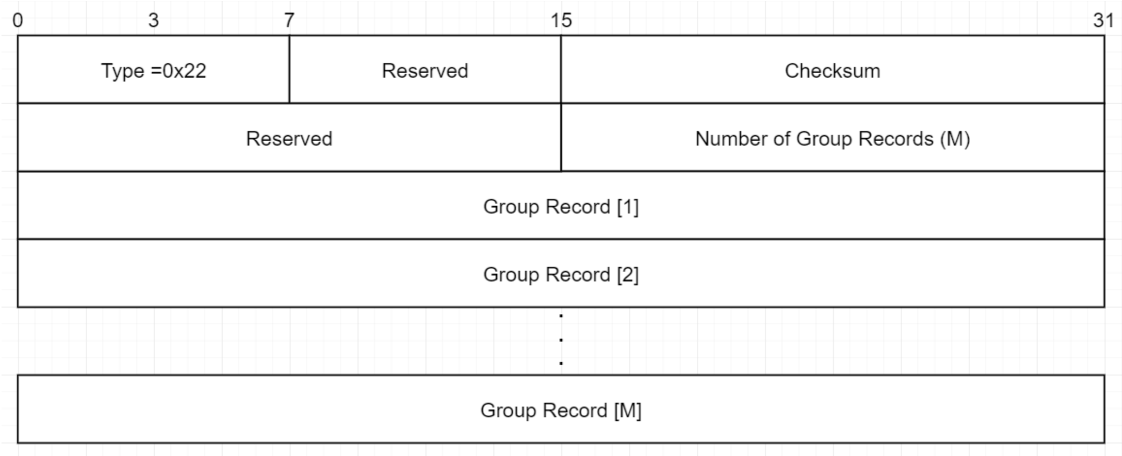
3.1.1.3 IGMPv3

IGMPv3 represents the next stage of IGMP development. It introduces support for "source filtering," enabling multicast receiver hosts to signal to the gateway both the multicast groups from which they wish to receive traffic and the intended sources of this traffic. This membership information allows devices to forward traffic solely from the sources requested by the receivers. RFC 3376 defines the specifications for IGMPv3.

The IGMPv3 Query message packet format is shown below:



The IGMPv3 Report message packet format is shown below:



IGMPv3 supports the following two types of messages:

- Version 3 membership query
- Version 3 membership report

IGMPv3 enables applications to explicitly signal the specific sources from which they wish to receive traffic. With IGMPv3, receivers indicate their membership to the multicast host group in one of the following two modes:

- **INCLUDE Mode**: In this mode, the receiver announces membership in a host group and provides a list of source addresses (INCLUDE list) from which it wishes to receive traffic.
- **EXCLUDE Mode**: In this mode, the receiver announces membership in a multicast group and provides a list of source addresses (EXCLUDE list) from which it does not wish to receive traffic. The host will receive traffic only from sources whose IP

addresses are not listed in the EXCLUDE list. To receive traffic from all sources (which aligns with IGMPv2 behavior), the host uses EXCLUDE mode membership with an empty EXCLUDE list.

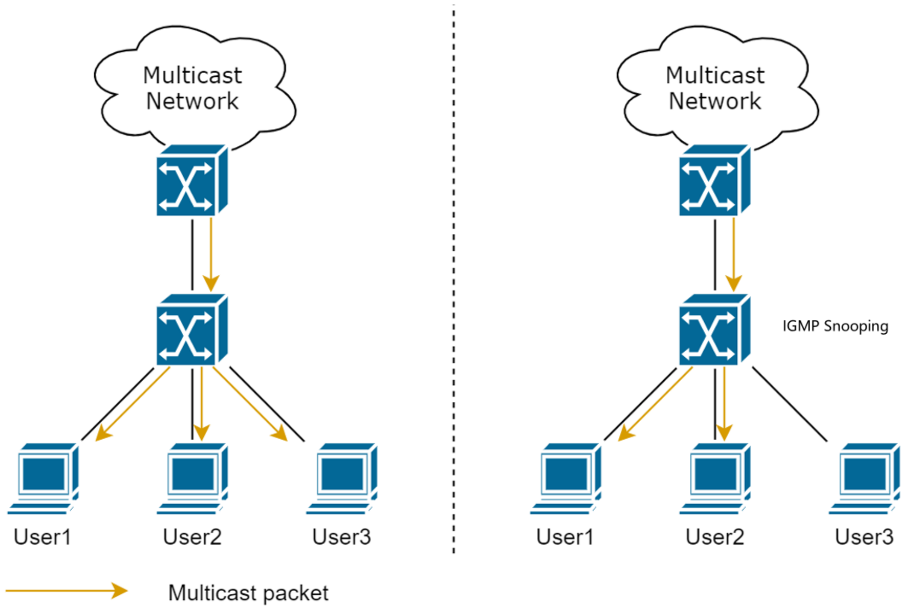
3.1.1.4 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP Snooping) is a fundamental L2 multicast feature. It is mainly used to optimize the forwarding behavior of multicast traffic on L2 devices, and enable the forwarding and control of multicast data at the data link layer.

In many scenarios, multicast packets inevitably traverse L2 switching devices, especially in L2 switched networks. When IGMP Snooping is not deployed on an L2 device (e.g., DeviceB), as illustrated in the figure below, the Ethernet L2 device DeviceB is connected to the multicast device DeviceA via Interface10 and also serves several users. Among these users, User1 and User2 are members of a specific multicast group, and will send IGMP Membership Reports to announce their membership. If DeviceA subsequently receives traffic destined for this multicast group, it will forward the traffic to the switched network, allowing group members User1 and User2 to receive the required multicast traffic. However, by default, when DeviceB receives unicast, multicast, or broadcast frames with unknown destination MAC addresses within a VLAN, it floods these frames throughout the same VLAN. Consequently, DeviceB will forward the multicast traffic destined for the group out of all its interfaces (e.g., Interface1, Interface2, and Interface3, assuming they belong to the same VLAN). Even if some users (e.g., User3 in the diagram) are not members of the multicast group, they will still receive the multicast traffic, resulting in wasted network bandwidth and device performance.

When IGMP Snooping is configured on DeviceB, as User1 and User2 send IGMP Membership Reports to announce their membership, DeviceB not only forwards these reports to DeviceA but also parses their content. It binds the multicast group addresses to the corresponding interfaces (e.g., Interface1 and Interface2) and creates L2 forwarding entries. Subsequently, when DeviceB receives multicast traffic from DeviceA, it forwards the traffic solely through Interface1 and Interface2 based on the L2 forwarding table. Non-member User3 will not receive this multicast traffic. Thus, with IGMP Snooping deployed, DeviceB forwards multicast traffic only through the correct interfaces.

- If DeviceB is not running IGMP Snooping, multicast data is broadcast at the data link layer.
- If DeviceB is running IGMP Snooping and certain users do not need to receive multicast data from the group, the multicast data will not be broadcast at the data link layer. Instead, it will be forwarded through the L2 multicast forwarding table to the intended receivers via the corresponding interfaces: interface1 and interface2.



3.1.2 MLD/MLD Snooping

Multicast Listener Discovery (MLD) is a protocol responsible for IPv6 multicast group membership management. It establishes and maintains multicast group membership relationships between IPv6 member hosts and their directly adjacent multicast gateways. MLD manages group membership by exchanging MLD messages between member hosts and multicast gateways. These MLD messages are encapsulated within IPv6 packets.

To date, MLD includes two versions:

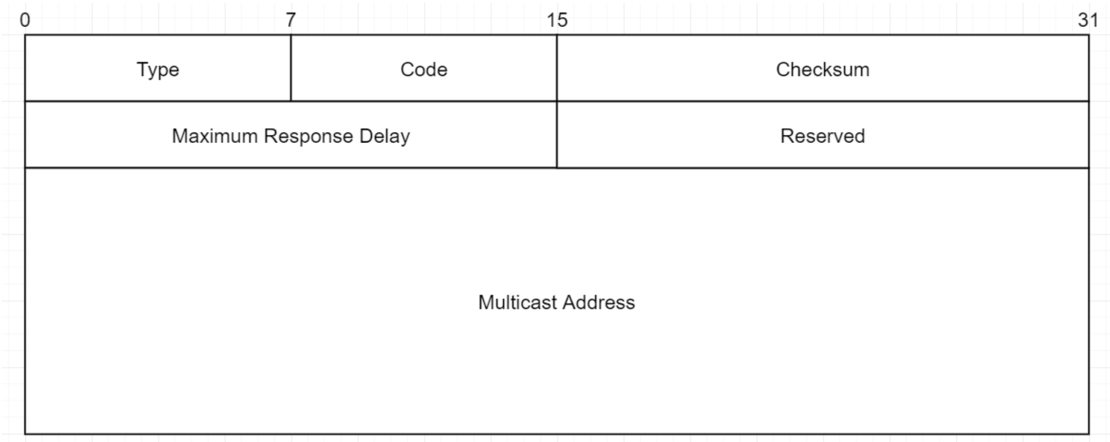
- MLDv1, corresponding to IGMPv2.
- MLDv2, corresponding to IGMPv3.

3.1.2.1 MLDv1

The working mechanism of MLDv1 is the same as that of IGMPv2. It defines a querier election mechanism, a general query and response mechanism, a new member join mechanism, and a leave mechanism.

The MLD querier periodically sends General Query messages to all hosts and multicast routers within the local network segment. It maintains group membership relationships based on Report messages fed back by member hosts. When the MLD querier receives a Done message from a member host for a specific group, it sends a Multicast Address Specific Query to determine whether members of that group still exist in the network segment. If no members are found, the corresponding group membership relationship will be deleted. The MLD querier decides whether to forward multicast data packets of a specific group to the network segment based on the group membership relationships.

The MLDv1 message packet format is shown below:



MLDv1 includes four types of messages:

- **General Query**: Sent by the querier to all hosts and routers on a shared network to identify which multicast groups have members.
- **Multicast Address Specific Query**: Sent by the querier to a specific multicast group within a shared network segment to check whether members of that group exist.
- **Multicast Listener Report**: Sent by a host to the querier to apply for joining a multicast group or to respond to a query message.
- **Multicast Listener Done**: Sent proactively by a host to the querier when leaving a multicast group to announce its departure from the group.

3.1.2.2 MLDv2

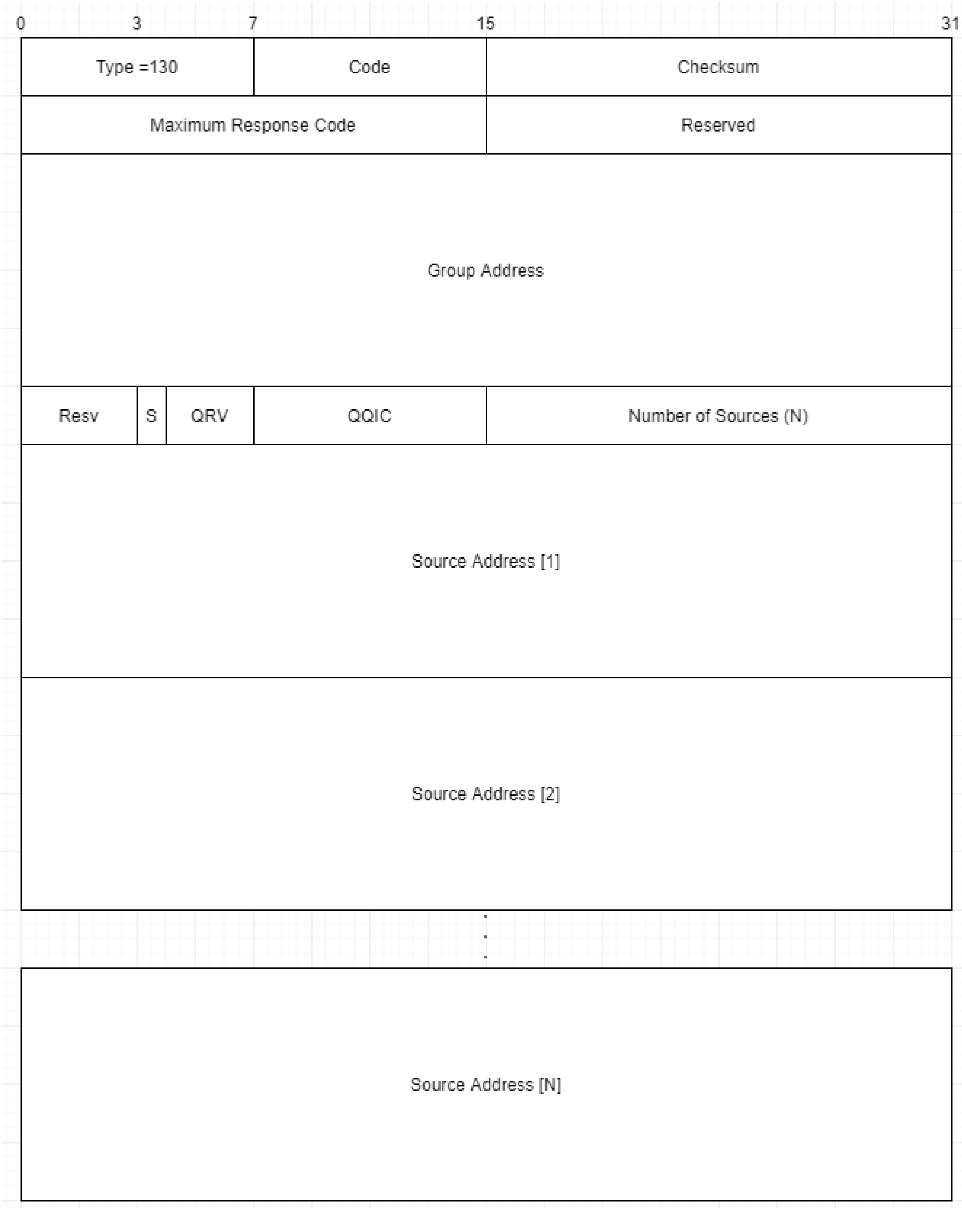
Compared to MLDv1, MLDv2 introduces the following changes in its messages:

- MLDv2 messages fall into two main categories: Query messages and Membership Report messages. MLDv2 does not define a Leave message; instead, member leave notifications are conveyed through specific types of Report messages.
- In addition to General Query and Multicast Address Specific Query messages, Query messages now include a new type: Multicast Address and Source Specific Query. This message is sent by the querier to specific multicast group members within a shared network segment to inquire whether they are willing to receive data from specific sources. This is achieved by carrying one or more multicast source addresses in the message.
- Membership Report messages not only include the multicast groups a host intends to join but also specify the multicast sources from which the host wants to receive

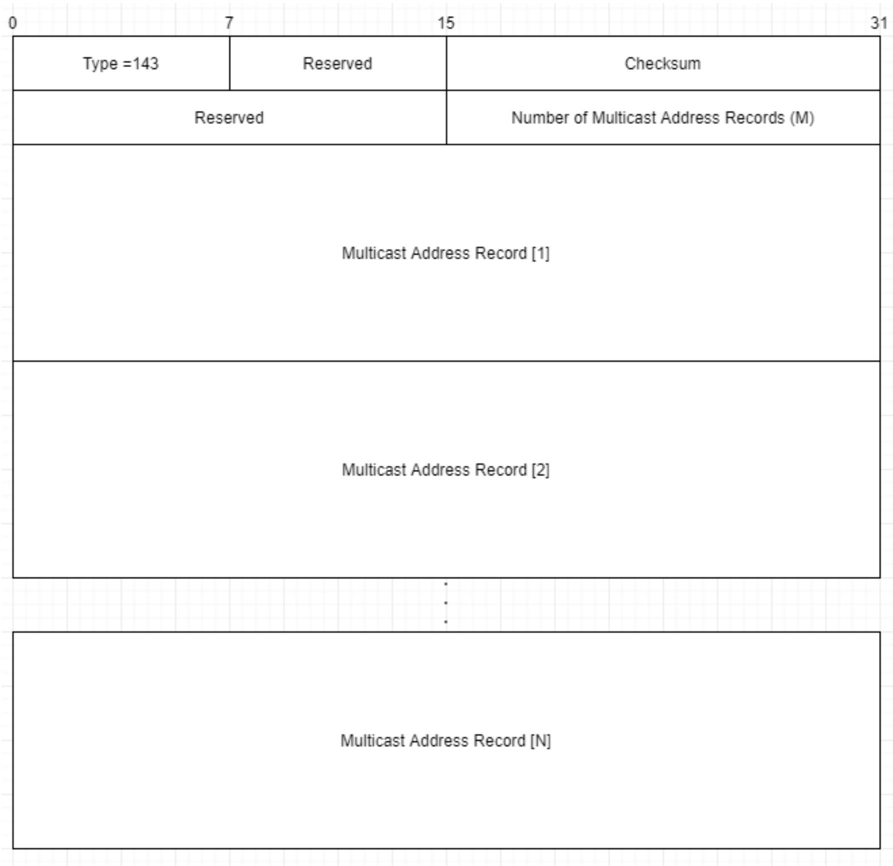
data. MLDv2 introduces source filtering modes (INCLUDE/EXCLUDE) to succinctly represent the relationship between multicast groups and source lists. For example:

- (G, INCLUDE, (S1, S2...)) indicates that the host will only receive data sent to group G from sources S1, S2...
- (G, EXCLUDE, (S1, S2...)) indicates that the host will receive data sent to group G from all sources except S1, S2...
- When the relationship between a multicast group and its source list changes, the MLDv2 Report message will include this change in the Multicast Address Record field and sends it to the MLD querier.

The MLDv2 Query message packet format is shown below:



The MLDv2 Report message packet format is shown below:



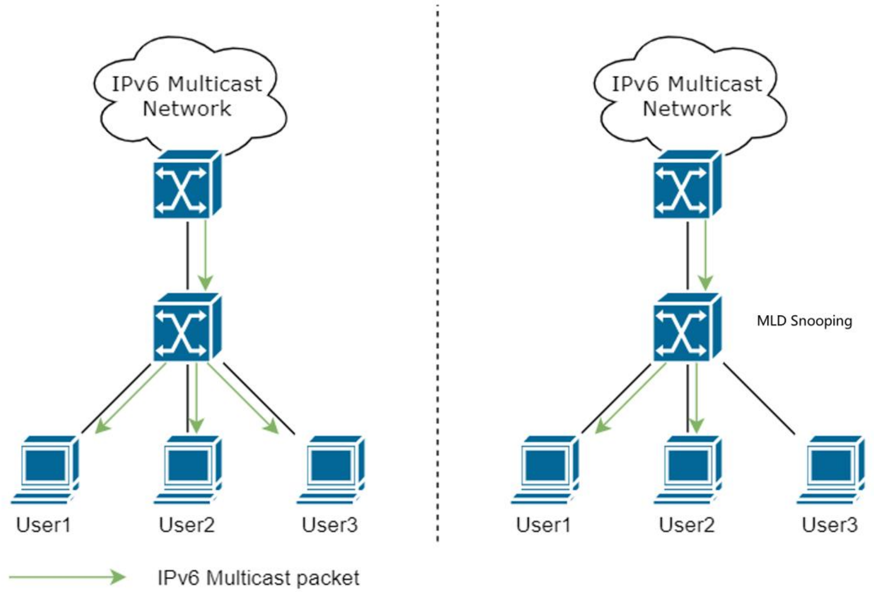
3.1.2.3 MLD Snooping

Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 L2 multicast protocol. It maintains egress port information for multicast packets by snooping on multicast protocol messages exchanged between L3 multicast devices and user hosts, thereby managing and controlling the forwarding of multicast data packets at the data link layer.

When MLD protocol messages exchanged between hosts and upstream L3 devices pass through an L2 device, MLD Snooping analyzes the information carried in these messages. Based on this information, it establishes and maintains an L2 multicast forwarding table, which guides the on-demand forwarding of multicast data at the data link layer.

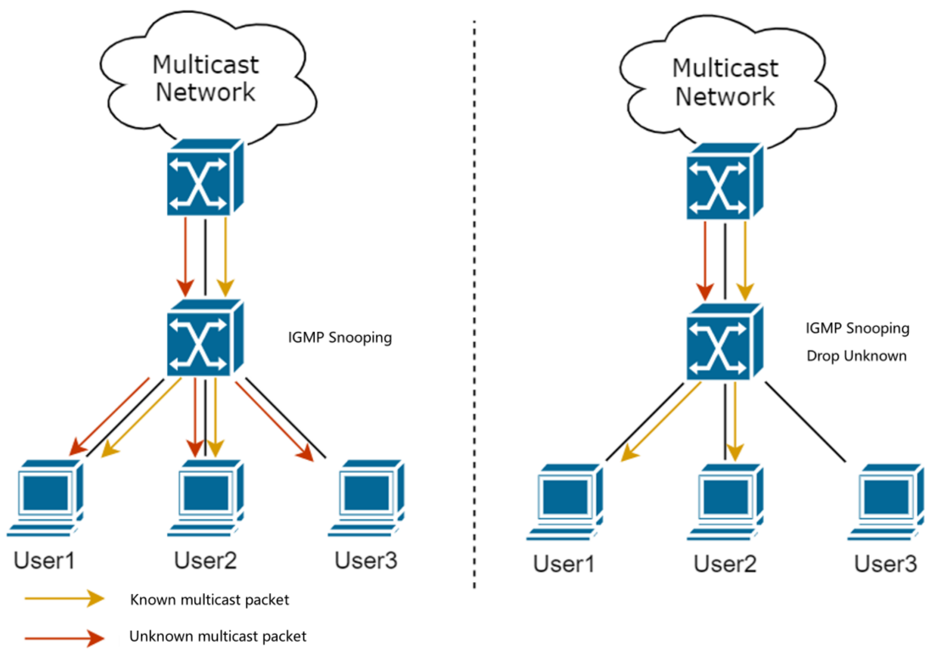
As shown in the diagram below, in an IPv6 multicast network, when multicast data is forwarded from an L3 multicast device (gateway) downward, the L2 device (switch) at the access edge is responsible for forwarding the multicast information to users, enabling them to access the requested content. When the L2 device does not have MLD Snooping enabled, multicast data is broadcast at Layer 2. When MLD Snooping is enabled on the L2 device, multicast data for known groups is not broadcast but is instead multicast to specified recipients.

After enabling MLD Snooping, the L2 device snoops on MLD messages exchanged between hosts and upstream L3 devices. By analyzing the information carried in these messages (such as message type, multicast group address, and interface receiving the message), it establishes and maintains an L2 multicast forwarding table, thereby guiding the on-demand forwarding of multicast data at the data link layer.



3.1.3 Drop Unknown

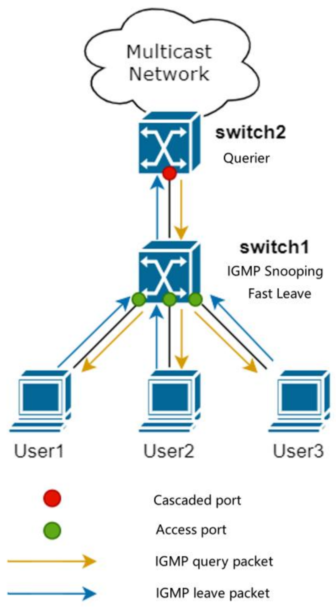
By default, ungrouped multicast data streams are broadcast within the VLAN. When Drop Unknown is enabled, these data streams will be directly discarded, saving bandwidth. It is recommended to enable Drop Unknown in general scenarios.



3.1.4 Fast Leave

By default, when a leave message from a multicast member is received, the aging time of the member port is set to the Leave Time (default 1s, configurable range 1s-30s). When Fast Leave is enabled, the switch immediately removes the member from the group upon receiving a leave message. It is recommended to enable this feature only on the ports directly connected to receivers on the switch. Cascade ports should not have this feature enabled.

Application Scenario:

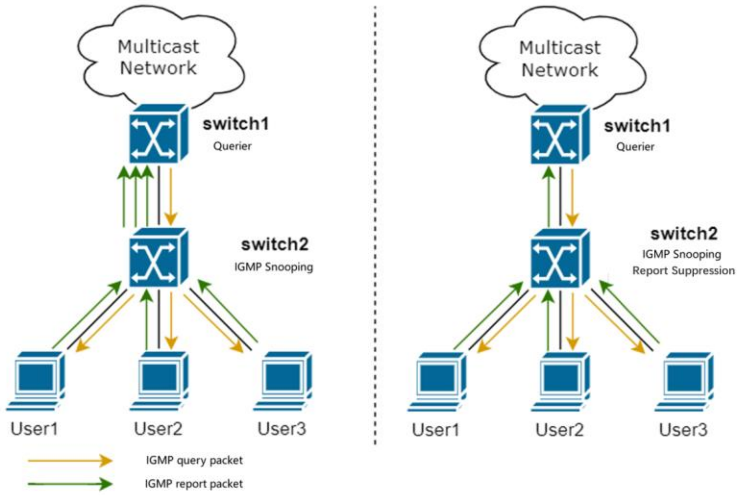


Assuming User1, User2, and User3 in this topology join the same multicast group, it is recommended to enable Fast Leave only on the Switch2 ports connected to the users. The cascade port between Switch2 and Switch1 should not have this feature enabled. Otherwise, when User1 leaves the group, Switch2 forwards the leave message to Switch1, causing Switch1 to immediately remove the cascade port from the group, which would prevent other users from receiving multicast data.

3.1.5 Report Suppression

By default, the switch forwards all Report messages to the router port. When Report Suppression is enabled, only the first Report message received downstream after each Query message is forwarded to the Router Port. This function reduces the transmission of Report messages in the network, thus saving bandwidth.

Application Scenario:

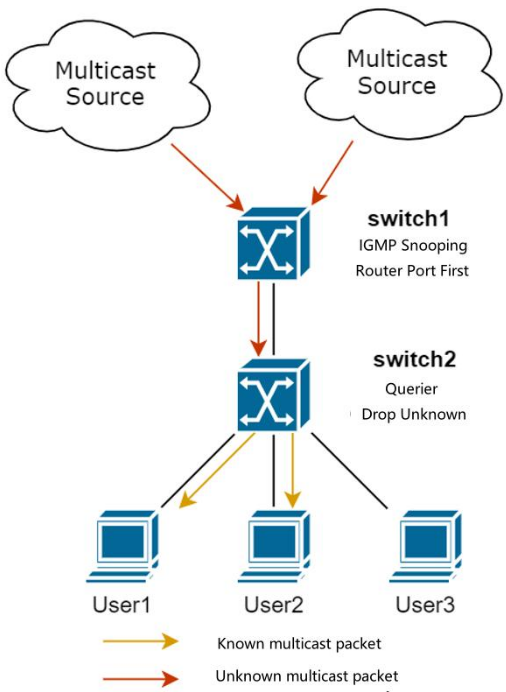


As shown in the diagram: Assuming User1, User2, and User3 join the same multicast group, when Switch1 sends a Query message, User1, User2, and User3 will all reply with Report messages. If Report Suppression is enabled on Switch2, Switch2 will only forward the first Report message received to Switch1. This helps reduce bandwidth usage between Switch2 and Switch1.

3.1.6 Router Port First

By default, ungrouped multicast data streams are broadcast within the VLAN. When Router Port First is enabled, if no Router Port exists, unknown multicast traffic will be broadcast within the VLAN. Once a Router Port is present, unknown multicast traffic will be forwarded through the Router Port.

Application Scenario:



If the querier is not configured on the device closest to the multicast source, (e.g., the source is on Switch1 but the querier is on Switch2) and Router Port First is disabled on Switch1, multicast traffic won't reach Switch2 because Switch1 can't send Join messages upstream. In this case, enabling Router Port First on Switch1 will allow Switch1 to forward all received multicast source data to Switch2.

Note: At this point, Drop Unknown should be enabled on Switch2. Otherwise, if a set-top box is directly connected to Switch2, unknown multicast traffic may impact its performance.

3.2 Typical Problems and Troubleshooting

Problem	Possible Cause	Troubleshooting
Screen Tearing/ Lagging	Multicast Packet Loss	▪ Check if multicast rate limiting is configured on the port
		▪ Check if port bandwidth utilization has reached 100%, causing overflow and packet loss.
	Multicast Source/Set-Top Box Impacted by Packets	Capture packets to check if there is a large amount of broadcast traffic (e.g., mDNS and ARP) impacting the multicast source/set-top box.
Video Streaming Interruption, Temporarily Unwatchable	Misconfigured Fast Leave causing temporary interruption when multiple TVs watch the same channel and one switches the channel.	Check if Fast Leave is enabled on upstream cascade devices in a cascaded scenario.
	Querier Interval configured shorter than multicast member aging time (MTime), causing intermittent interruptions.	Verify whether the Querier Interval and MTime configurations across devices are correct (MTime should be greater than the Querier Interval).

Cannot Join Multicast Group	L2 multicast disabled in interface mode, preventing the interface from joining multicast groups.	Check if L2 multicast is enabled on the interface.
	L2 multicast profile restrictions limit the range of joinable multicast groups.	Check if the L2 multicast profile is configured correctly.
	The switch's L2 multicast version is too low and incompatible with the host's version.	Check the switch's L2 multicast version
Successfully Joined Group but Unable to Play	Multicast packet errors (e.g., invalid UDP port number)	Capture packets to analyze whether multicast traffic is normal.
High CPU Utilization on Network Devices	Multiple L2 multicast Queriers in the same VLAN without Report Suppression enabled, causing excessive query/report packets.	Ensure only one Querier exists per VLAN to maintain multicast membership; check if multiple devices have Querier enabled.
Other Multicast-Based Protocols Malfunction After Enabling Multicast	Drop-Unknown discards relevant protocol packets.	Disable Drop-Unknown and check if normal operation resumes.

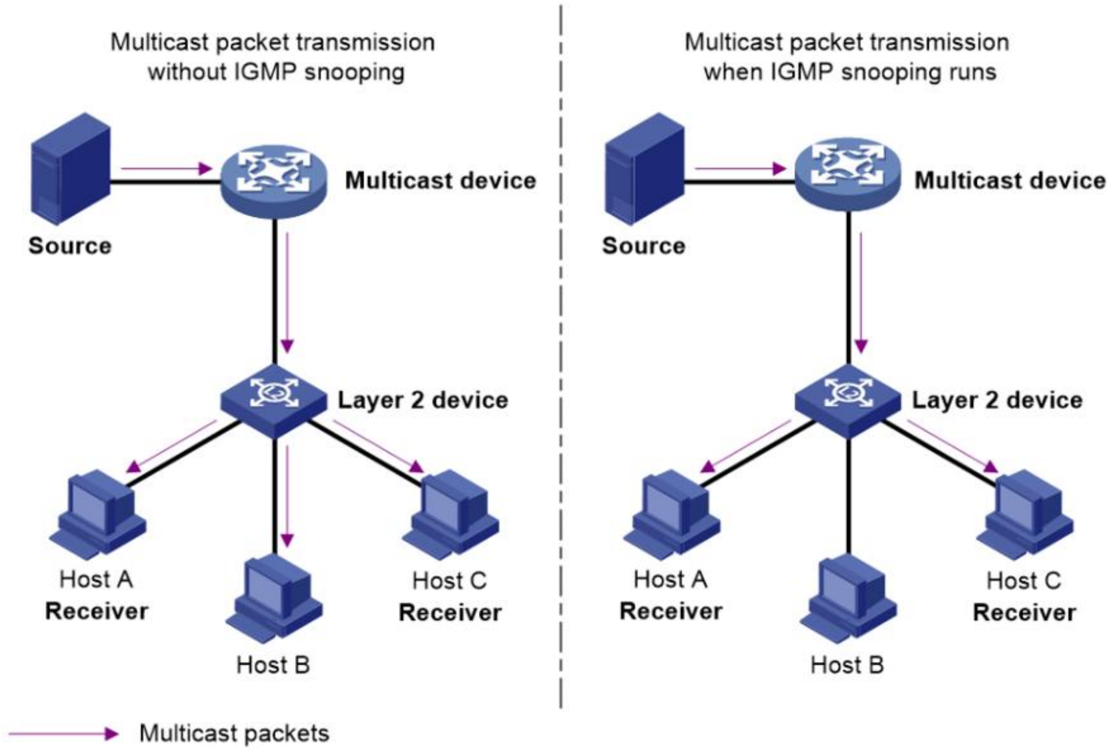
4 Application Scenarios & Solutions

This chapter primarily introduces the tutorial for configuring multicast entirely through the controller after adopting devices in the Omada Controller 6.0.

Currently, the Omada Controller 6.0 supports only IGMP Snooping v3 and MLD Snooping v2. The multicast-related configurations include global querier settings, enabling Report Suppression for all adopted devices, configuring drop/forwarding of unknown multicast traffic and forwarding to router ports for all adopted devices, setting up static router ports, and configuring Fast Leave on ports.

In most scenarios, multicast sources and client receivers are within an L2 network (i.e., within the same VLAN domain), the multicast protocol typically required is IGMP Snooping. An L2 device running IGMP Snooping analyzes received IGMP packets to establish mapping relationships between ports and MAC multicast addresses, and forwards multicast data based on these mappings.

When IGMP Snooping is not enabled on the L2 device, multicast data is broadcast across the L2 network. Once IGMP Snooping is enabled, known multicast data is no longer broadcast but is multicast only to specified receivers. In a network without L3 multicast devices, since L2 devices do not support IGMP, they cannot perform the functions of an IGMP Querier. To address this, the IGMP Snooping Querier can be enabled on L2 devices, allowing them to establish and maintain multicast forwarding entries at the data link layer, thereby ensuring normal multicast data forwarding at this layer.



4.1 Preliminary Preparation

4.1.1 Device Requirements

The premise for this configuration guidance is that the devices are managed by the Omada Controller. Therefore, before proceeding with the subsequent configuration steps, ensure the following prerequisites:

1. The Omada Controller version must be 6.0 or above.
2. The switch firmware must be updated to the latest version available on the official website.

Note that some switches may not support features like the querier (refer to the model's manuals on the official website). It is recommended to use Omada Smart/L2+/L3 Switches as the querier.

3. There are no specific functional requirements for the Omada Gateway, but in real customer scenarios, ER8411 is typically used.
4. There are no specific functional requirements for Omada EAPs, but in real customer scenarios, wired connections are preferred.

4.2 Typical Configuration

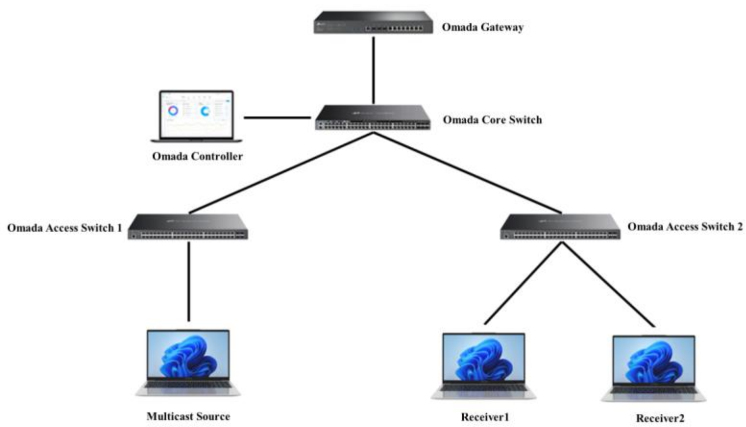
4.2.1 Typical Topology

This topology is suitable for most wired networking scenarios, which typically feature:

1) Tree-hierarchical distribution.

2) Both the Multicast Source and Receiver are within the same VLAN.

3) The core switch is generally configured as the querier, replacing the gateway-based multicast management function.



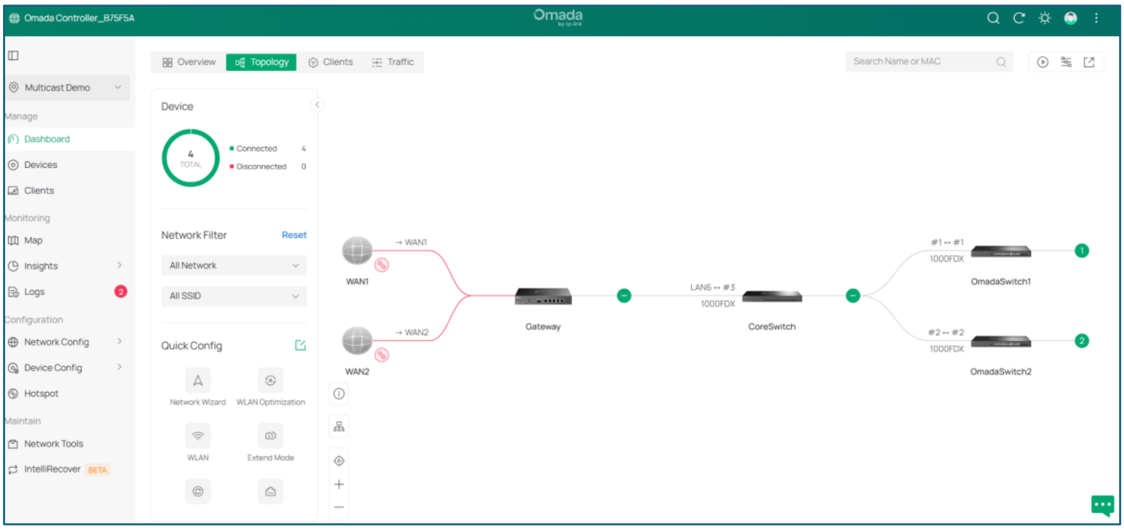
4.2.2 Configuration Objectives

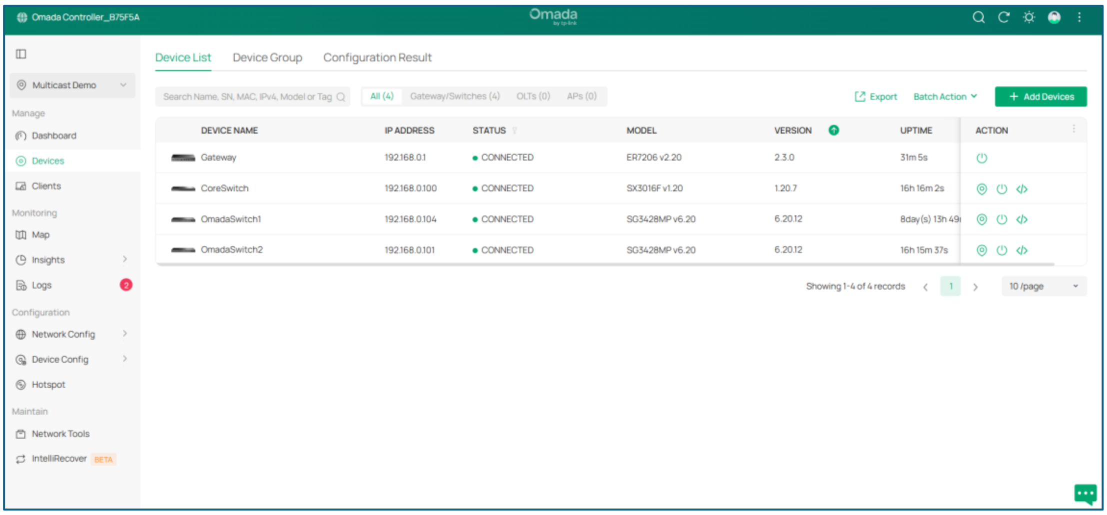
1) Use the Omada Controller 6.0 to adopt devices with the management address set to VLAN1, subnet 192.168.0.0/24.
2) Enable IGMP Snooping on VLAN1, configure the Core Switch as the querier, and set unknown multicast to Router Port First.
3) The multicast source pushes video streams. Receivers 1 and 2 join the multicast group, receive video while joined, and stop receiving after leaving the multicast group.

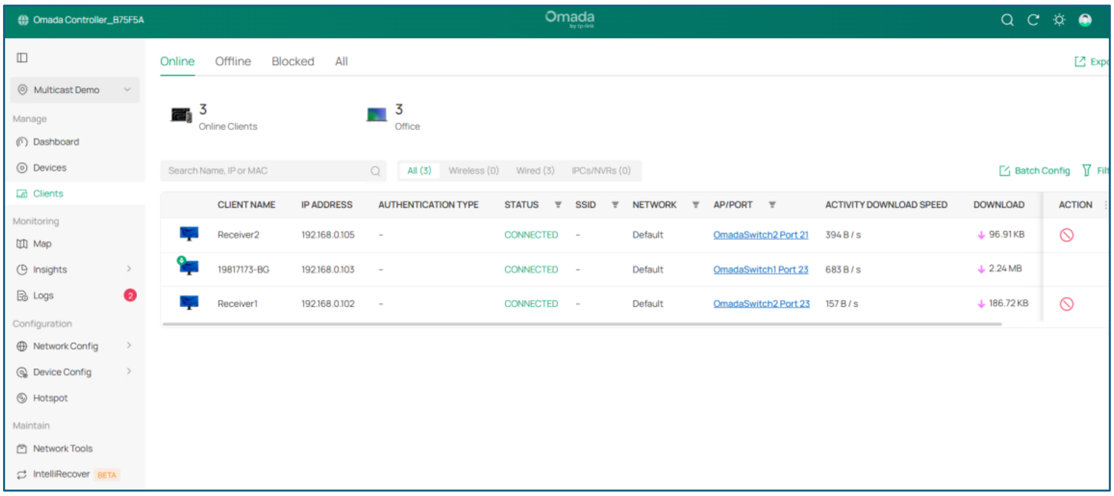
4.2.3 Configuration Steps

Note: This configuration demonstration uses an ER7206 v2.20 as the gateway, an SX3036F v1.20 as the core switch, and an SG3428MP v6.20 as the access switch. Three PCs running VLC player software are used as one multicast source and two receivers.

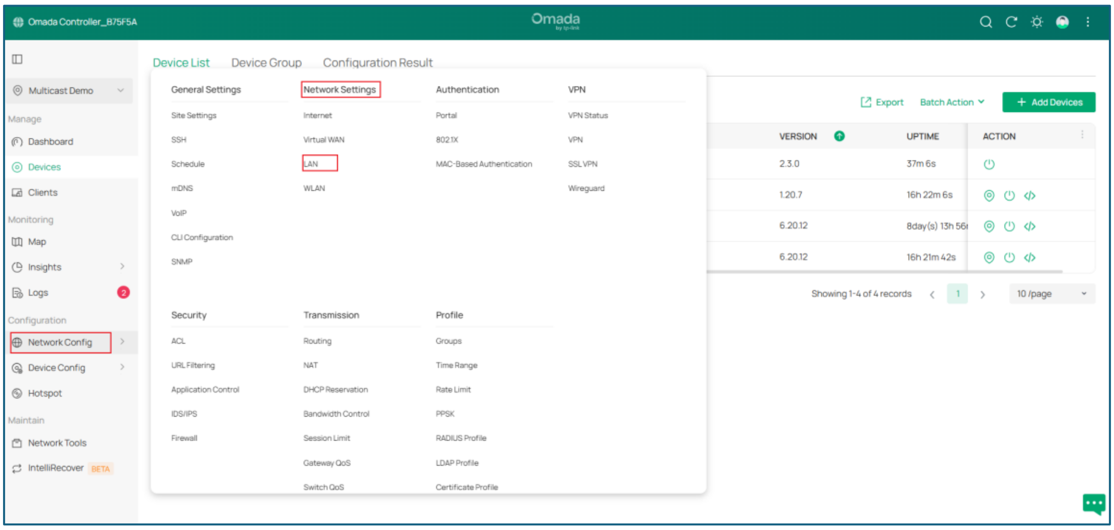
Step 1: Use the Omada Controller 6.0 to adopt devices according to the network topology. Ensure all devices are upgraded to firmware versions supporting Controller 6.0 or above. Set the management address to VLAN1, subnet 192.168.0.0/24, and ensure the multicast source and receivers are on the same subnet.

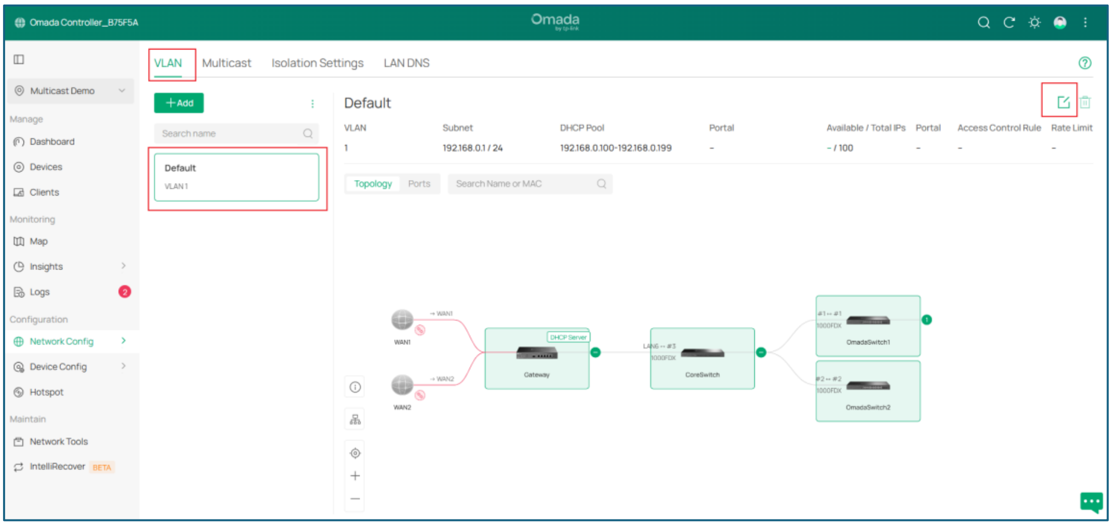


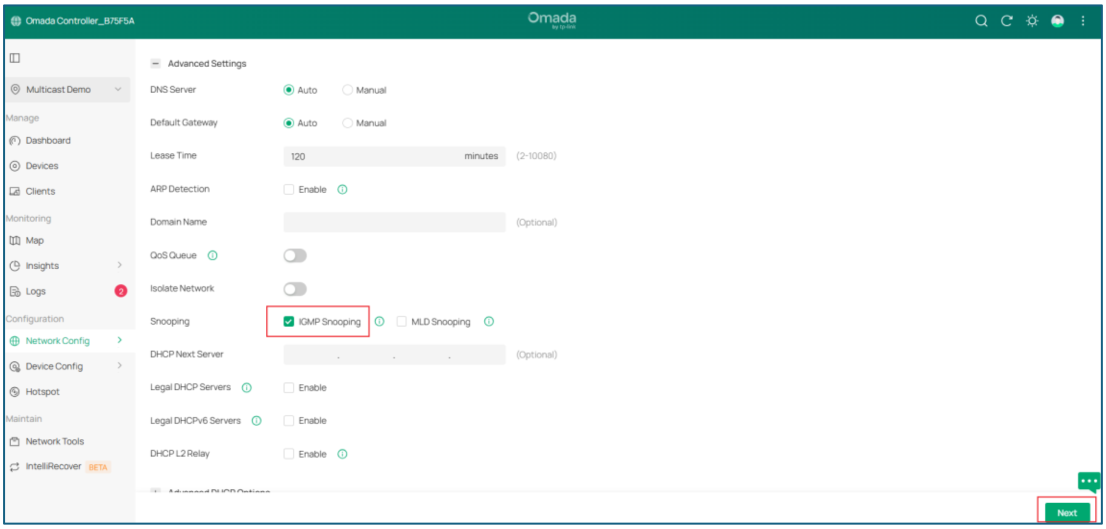




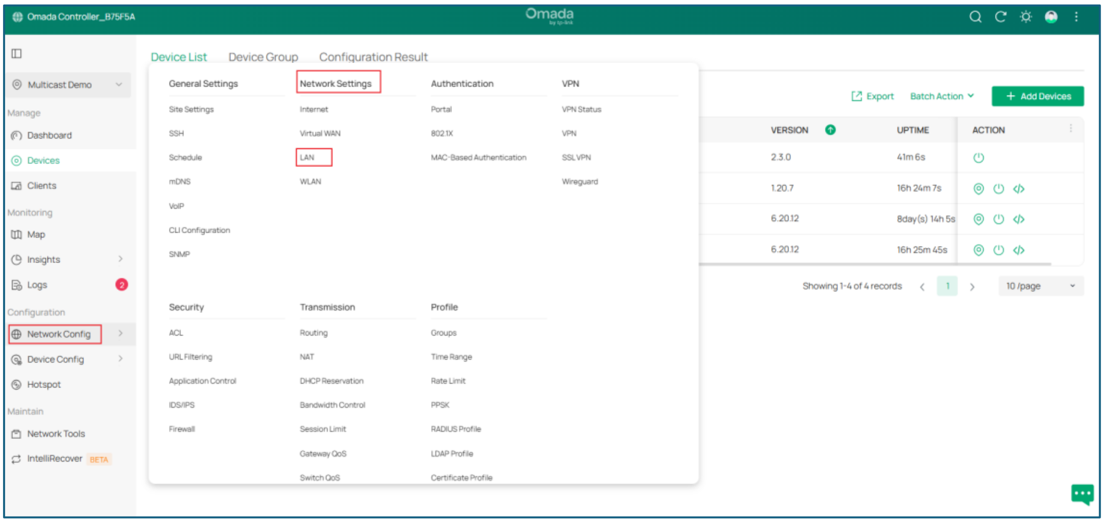
Step 2: Go to Network Config > Network Settings > LAN > VLAN and click Edit to enable IGMP Snooping (IPv4) for VLAN1.

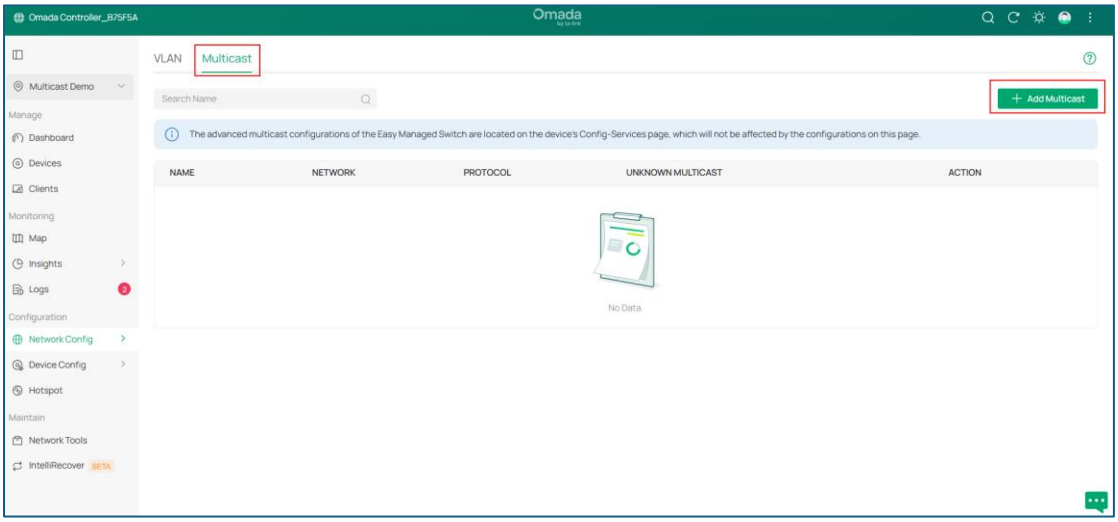


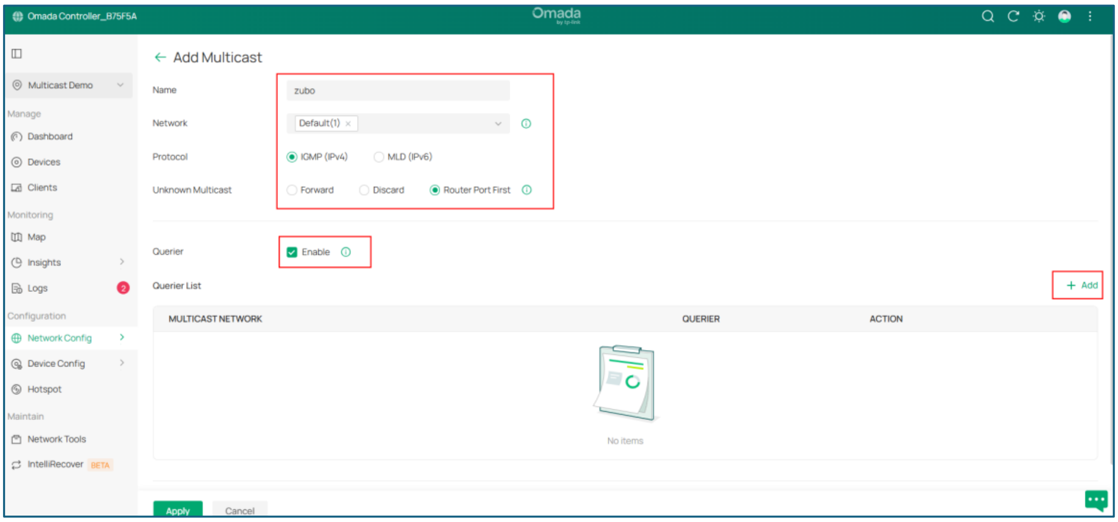


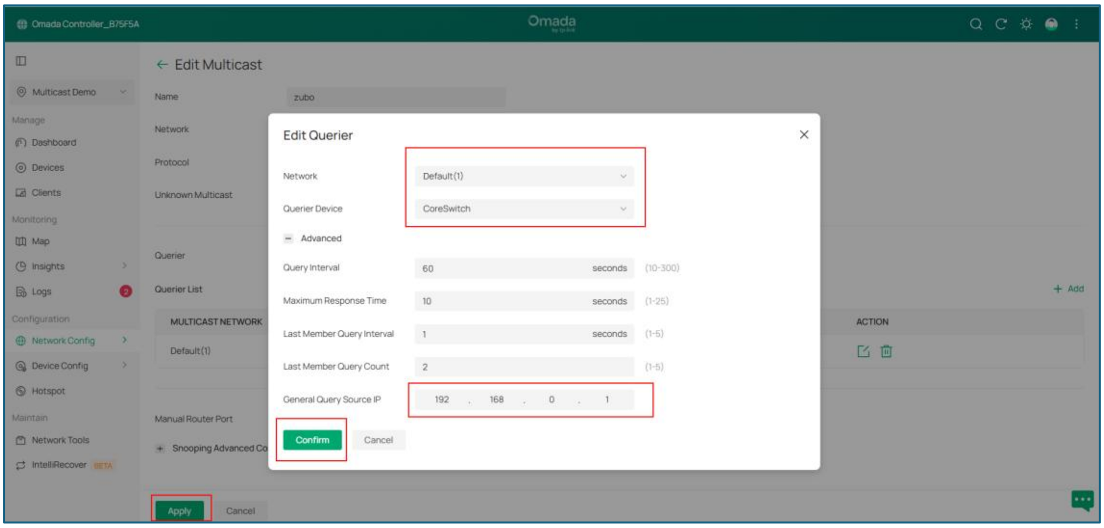


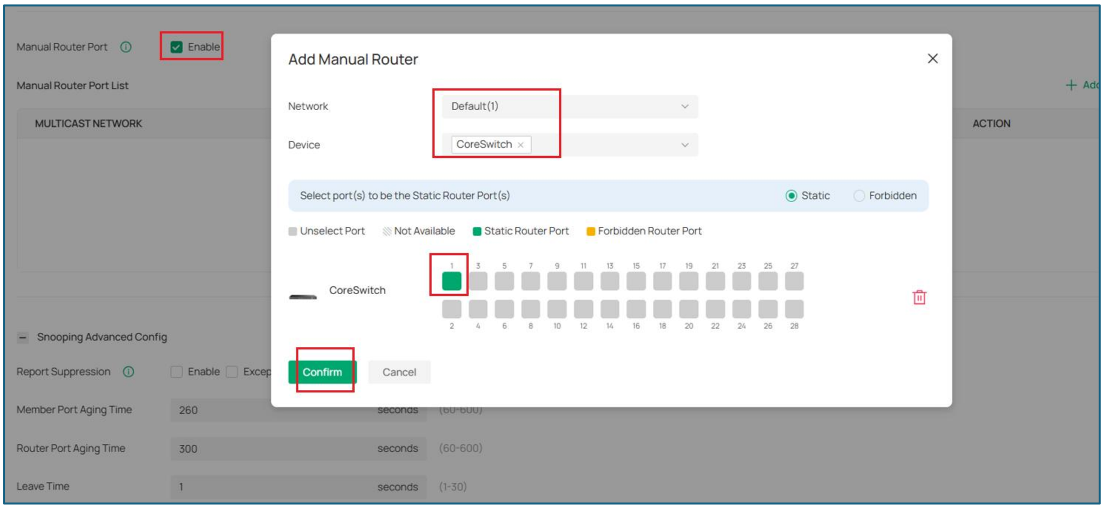
Step 3: Go to Network Config > Network Settings > LAN > Multicast, and create a new multicast configuration. Set the Core Switch as the Querier, select Discard for Unknown Multicast, choose VLAN1 for the Network, and set the General Query Source IP to the gateway's LAN port address. Set the port connected to Omada Switch 1 as a static routing port on the core switch.




Omada Controller_B75F5A
Omada
VLAN
Multicast
Multicast Demo
Manage
Dashboard
Devices
Clients
Monitoring
Map
Insights
Logs
Configuration
Network Config
Device Config
Hotspot
Maintain
Network Tools
IntelliRecover
BETA
Search Name
Add Multicast
The advanced multicast configurations of the Easy Managed Switch are located on the device's Config-Services page, which will not be affected by the configurations on this page.
NAME
NETWORK
PROTOCOL
UNKNOWN MULTICAST
ACTION
No Data

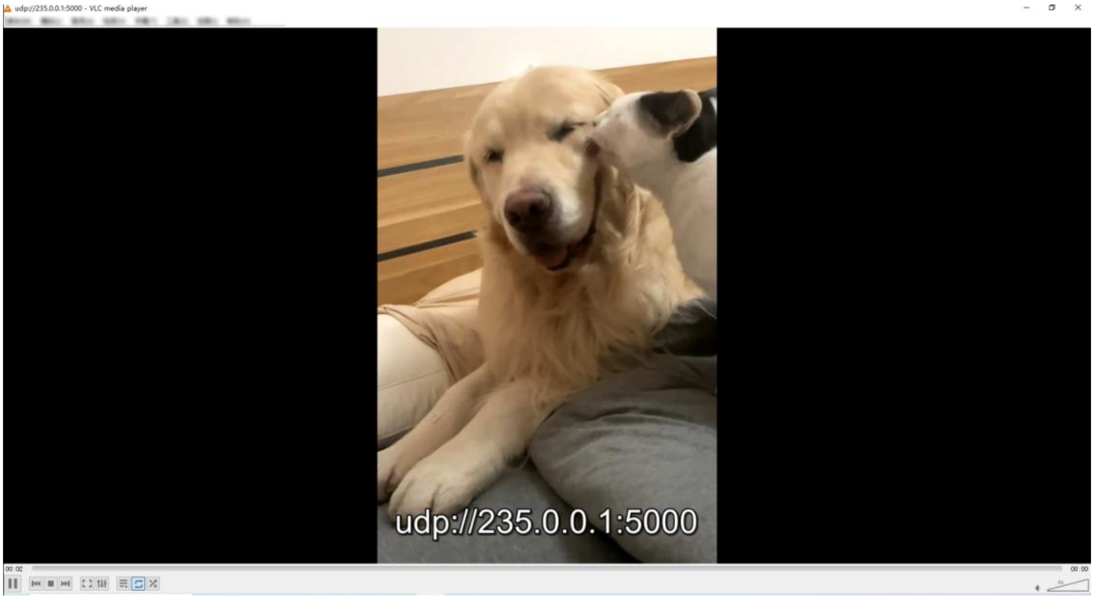

Omada Controller_B75F5A
Omada
Add Multicast
Name
zubo
Network
Default(1)
Protocol
IGMP (IPv4)
MLD (IPv6)
Unknown Multicast
Forward
Discard
Router Port First
Querier
Enable
Querier List
Add
MULTICAST NETWORK
QUERIER
ACTION
No items
Apply
Cancel


Omada Controller_B75F5A
Omada
Edit Multicast
Name
zubo
Network
Protocol
Unknown Multicast
Querier
Querier List
MULTICAST NETWORK
Default(1)
ACTION
Manual Router Port
Snooping Advanced Co
Edit Querier
Network
Default(1)
Querier Device
CoreSwitch
Advanced
Query Interval
60
seconds
(10-300)
Maximum Response Time
10
seconds
(1-25)
Last Member Query Interval
1
seconds
(1-5)
Last Member Query Count
2
(1-5)
General Query Source IP
192 . 168 . 0 . 1
Confirm
Cancel
Apply
Cancel

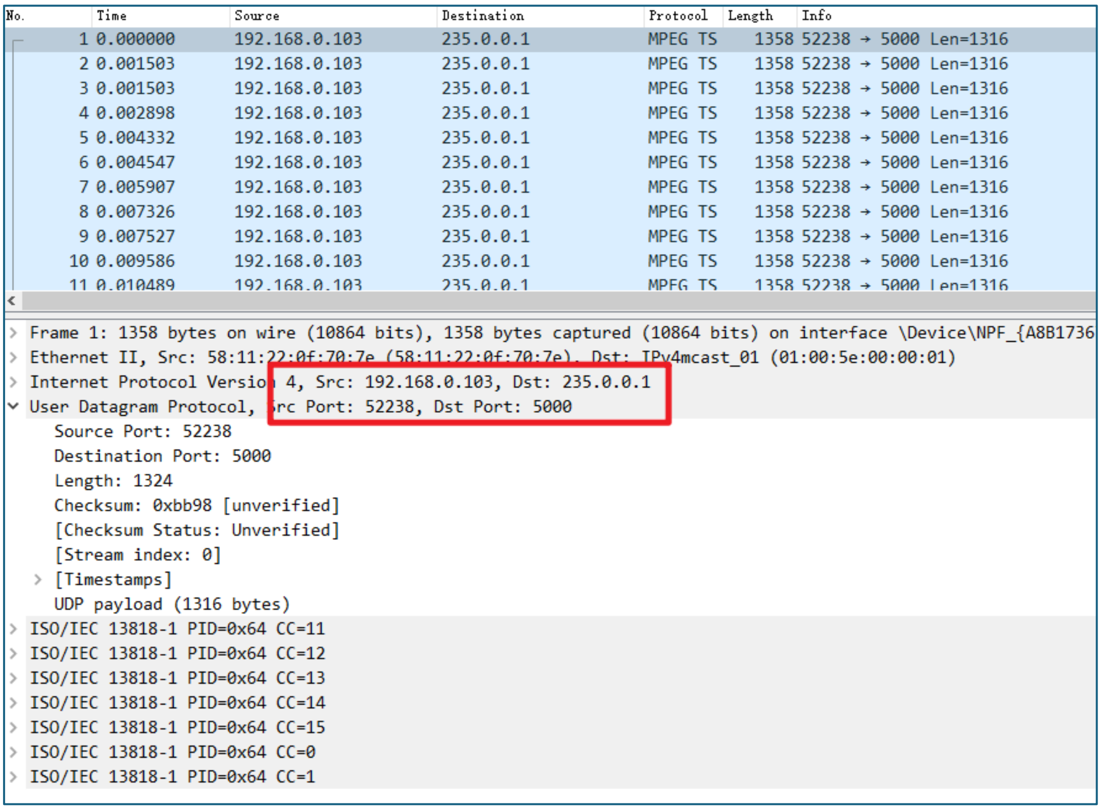


Step 4: On the multicast source (192.168.0.103) under OmadaSwitch1, use VLC to configure multicast group addresses: 235.0.0.1 UDP PORT: 5000 and 237.1.1.1 UDP PORT: 1234, and start pushing streams. Under OmadaSwitch2, Receiver1 joins 235.0.0.1 and Receiver2 joins 237.1.1.1 to view the video and capture packets.

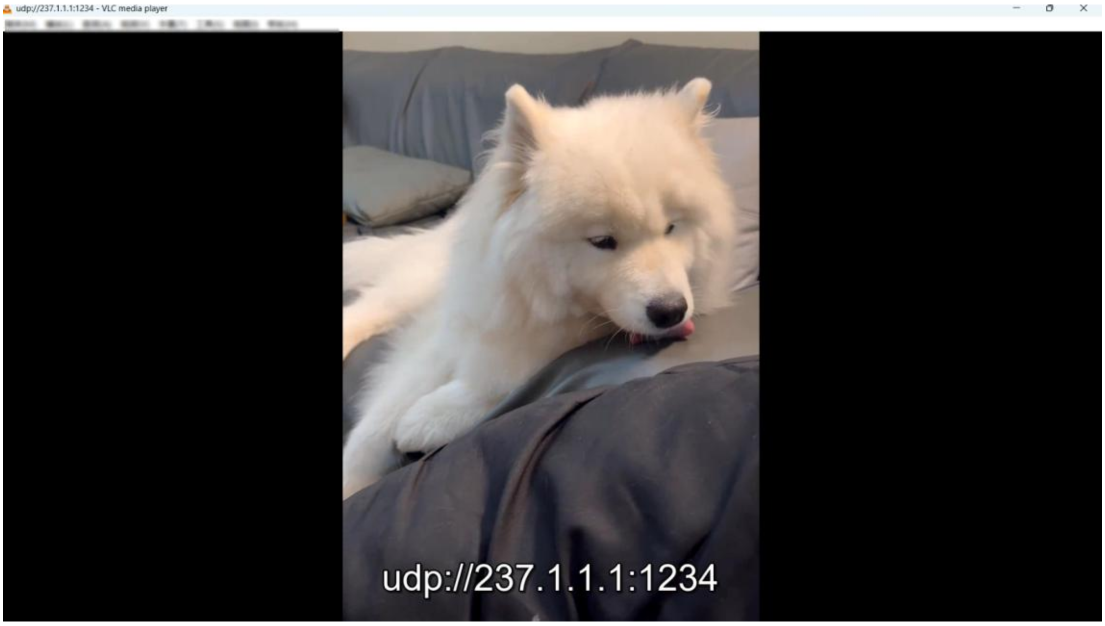
Receiver1 joins 235.0.0.1 and successfully receives the corresponding video stream:



Receiver1 packet capture shows multicast group data packets. The source address and destination port match the multicast source:



Receiver2 joins 237.1.1.1 and successfully receives the corresponding video stream:

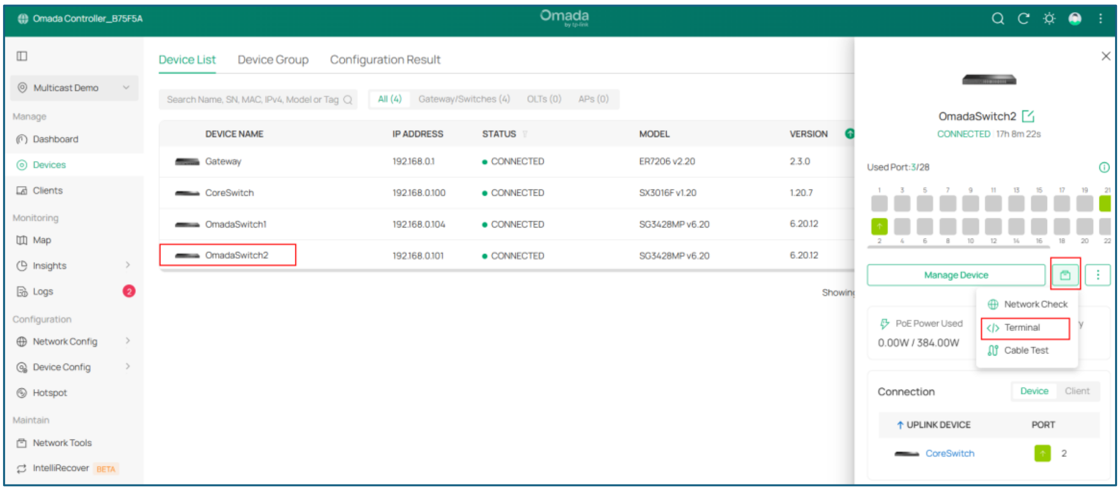


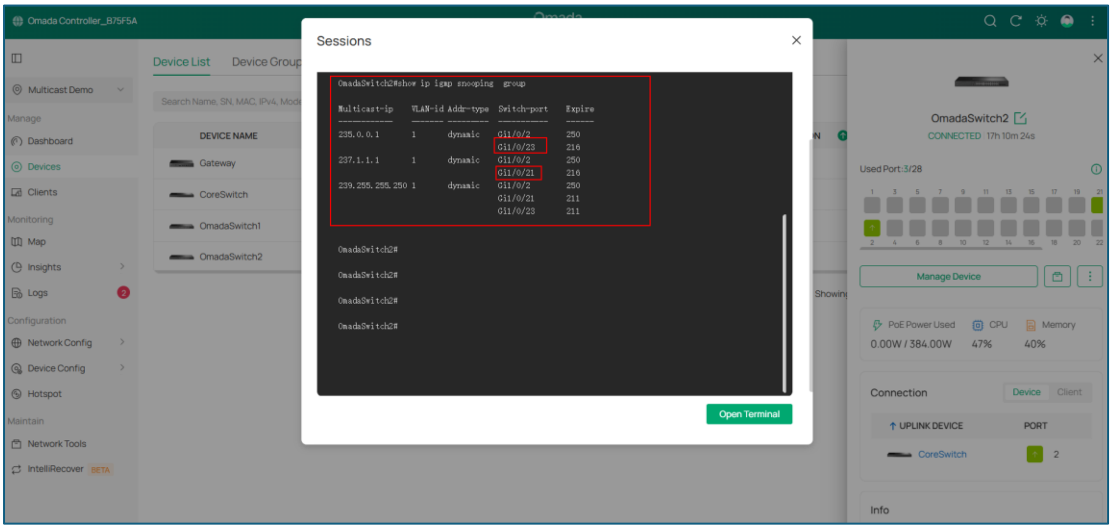
Receiver2 packet capture shows multicast group data packets. The source address and destination port match the multicast source:

No.	Time	Source	Destination	Protocol	Length	Info
10	0.008297	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
11	0.016778	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
12	0.017100	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
13	0.017229	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
14	0.017364	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
15	0.017656	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
16	0.017911	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
17	0.017956	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
18	0.018207	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
19	0.019857	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
20	0.020020	192.168.0.103	237.1.1.1	MPEG TS	1358	[MP2T fragment of a reassembled packet
21	0.021314	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
22	0.022806	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
23	0.022806	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
24	0.024285	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
25	0.026775	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
26	0.026884	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316

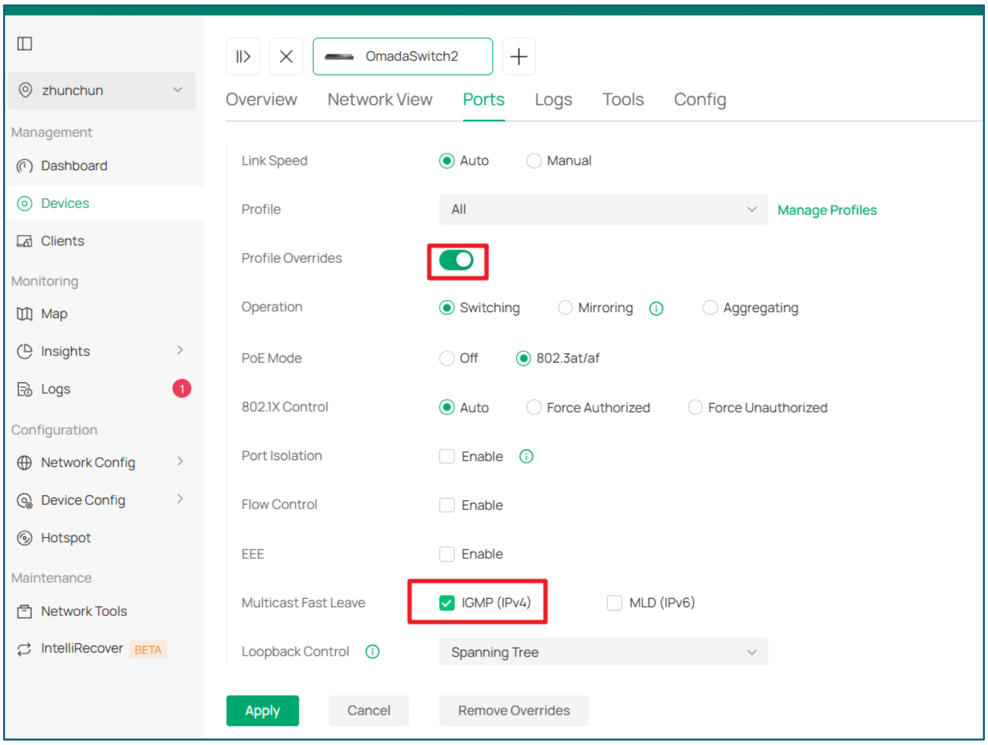
```
> Frame 1: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits) on interface \Device\NPF_{A8B17367-B912-4
> Ethernet II, Src: 58:11:22:0f:70:7e (58:11:22:0f:70:7e), Dst: IPv4mcast_01:01:01 (01:00:5e:01:01:01)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 237.1.1.1
> User Datagram Protocol, Src Port: 59457, Dst Port: 1234
> ISO/IEC 13818-1 PID=0x64 CC=15
> ISO/IEC 13818-1 PID=0x64 CC=0
> ISO/IEC 13818-1 PID=0x64 CC=1
> ISO/IEC 13818-1 PID=0x64 CC=2
> ISO/IEC 13818-1 PID=0x64 CC=3
> ISO/IEC 13818-1 PID=0x64 CC=4
> ISO/IEC 13818-1 PID=0x64 CC=5
```

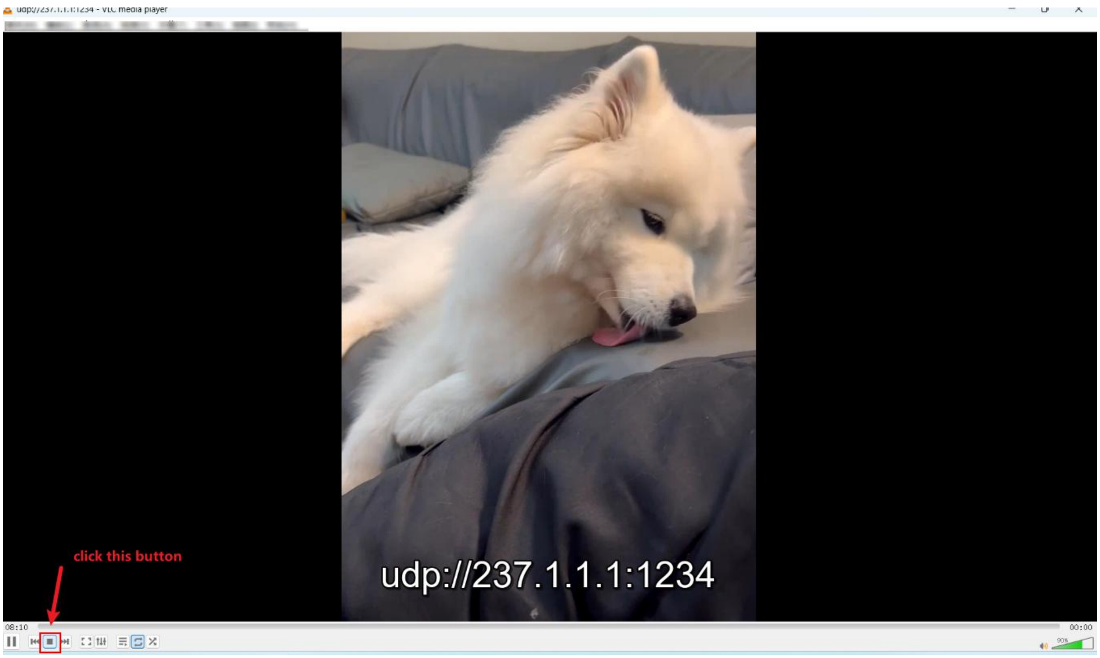
Step 5: Check the IGMP Snooping group status under OmadaSwitch2: The ports connected to Receiver1 and Receiver2 have joined the corresponding multicast groups.



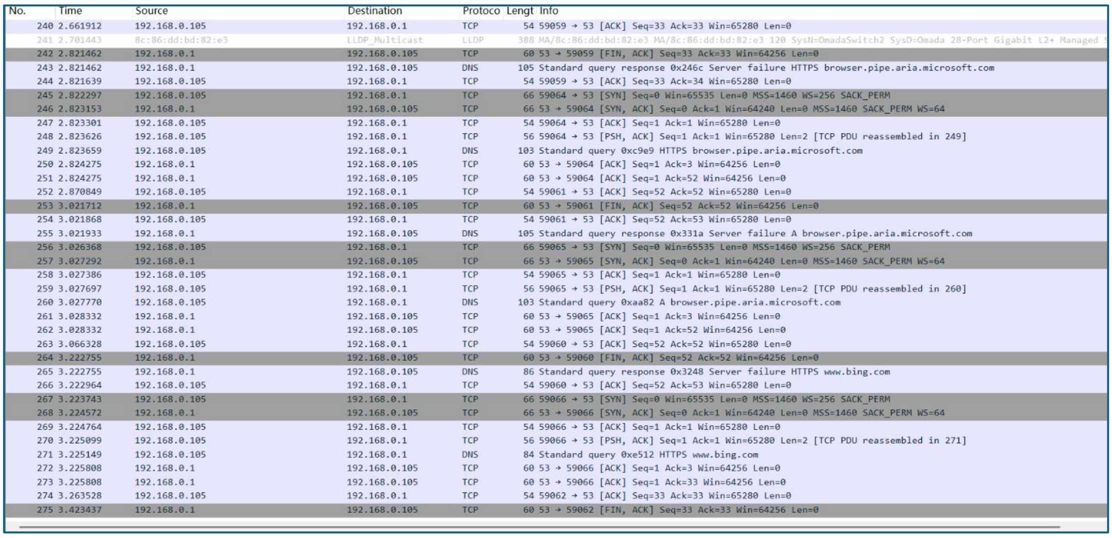


Step 6: Enable Fast Leave on the port connecting Receiver2 to the switch. Receiver2 clicks the stop button in the VLC (equivalent to sending a leave message). Packet capture on Client2 shows no multicast video packets are received. Check the OmadaSwitch2 IGMP Snooping multicast table: the entry for 237.1.1.1 is no longer present, confirming a successful leave.

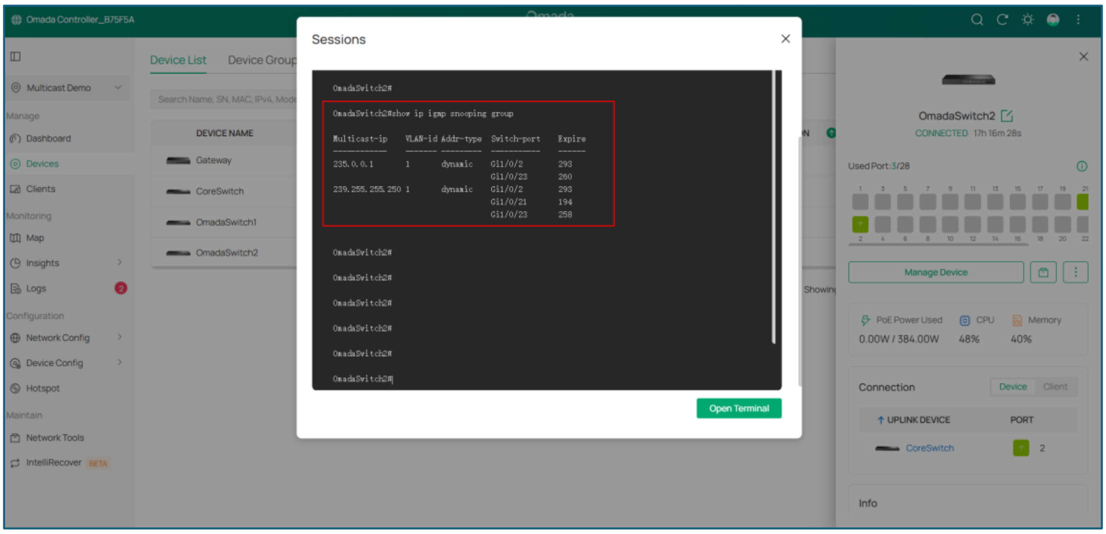




No multicast data packets detected:



Receiver2 successfully left the group:



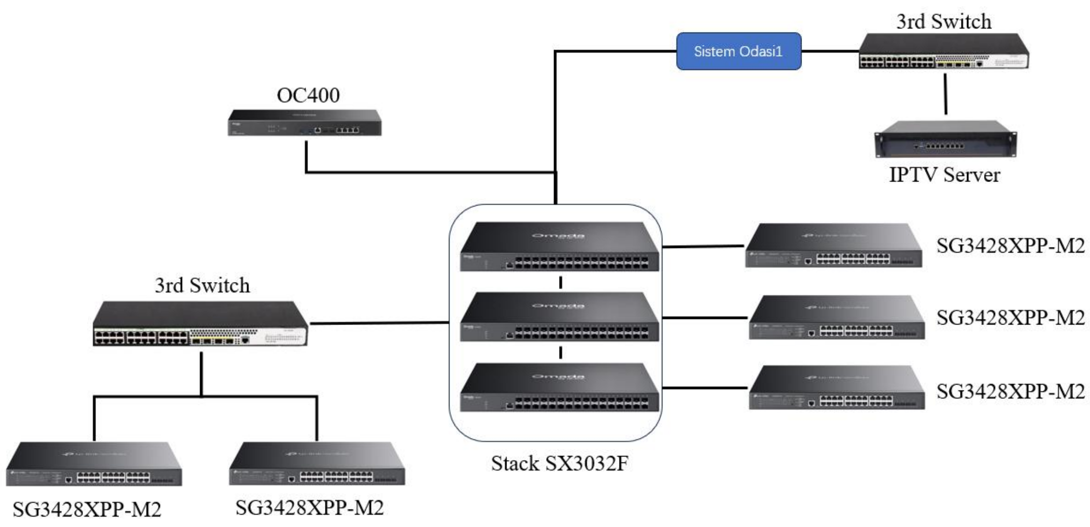
4.3 Case Studies

4.3.1 Case 1: A Hotel Case in Turkey

1) Background and Requirements:

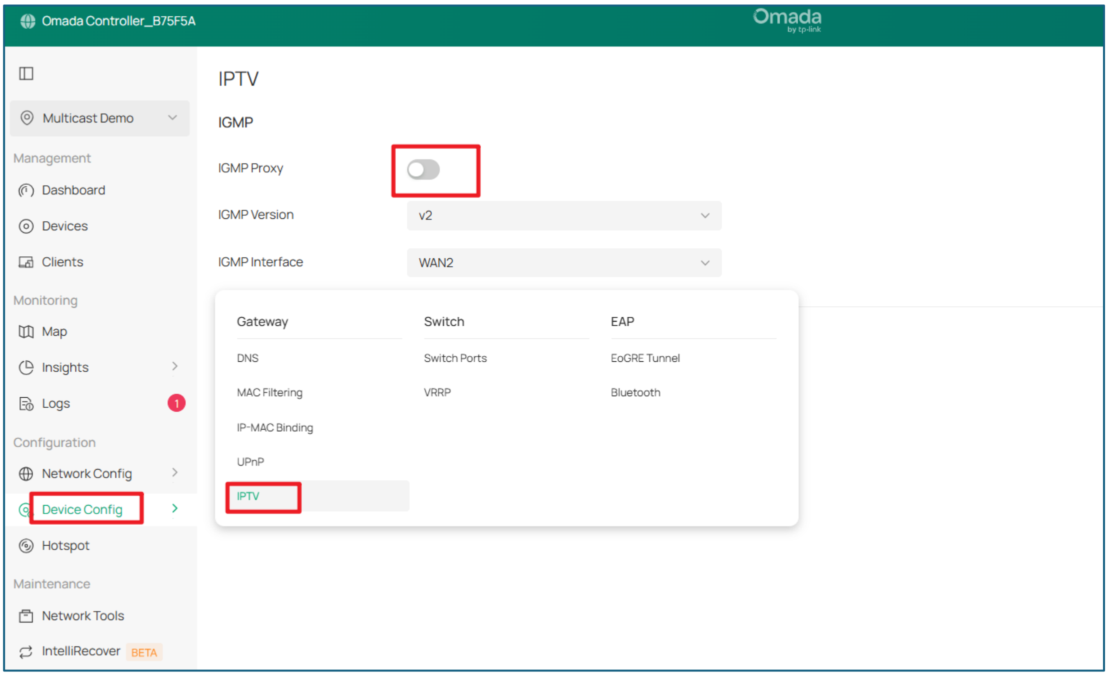
This customer is a benchmark in Turkey's hotel industry: peers know this hotel adopted our products and have shown strong interest. After deploying our switches, the hotel manager asked our technical team to recommend multicast configurations for the existing topology.

2) Network Topology:

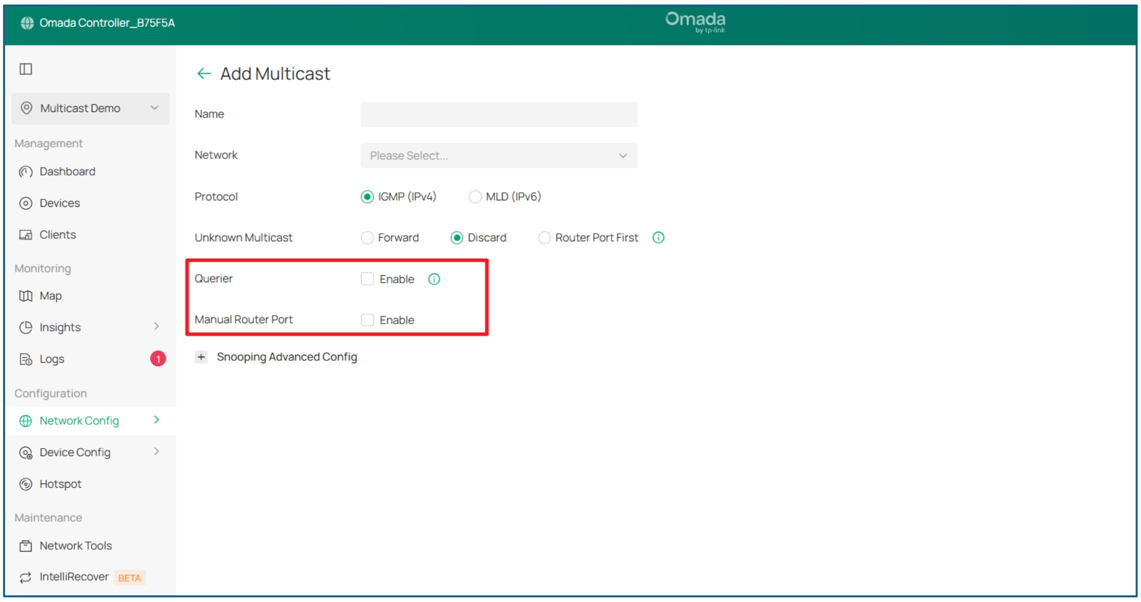


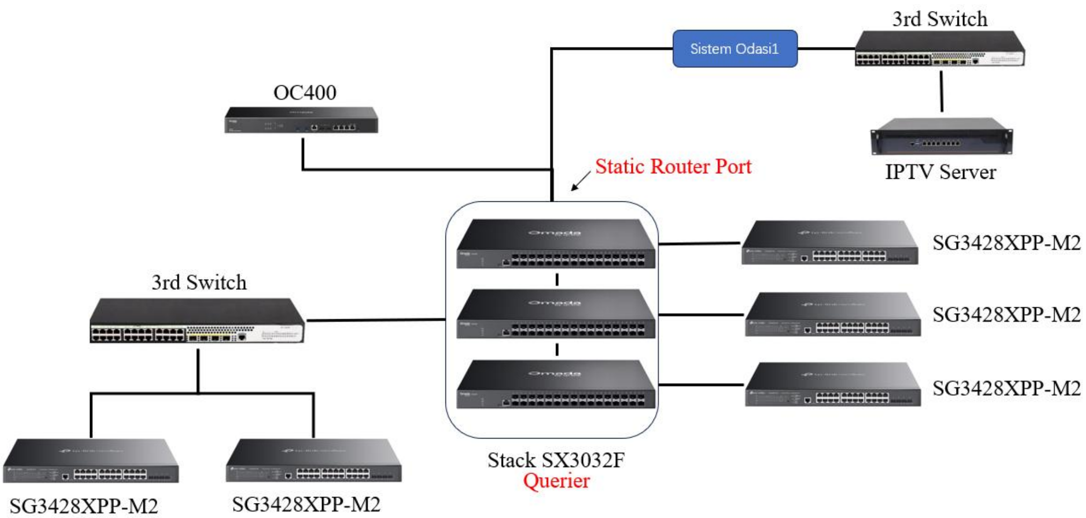
3) Solution and Configuration Recommendations:

1. Optimize multicast-related configurations by enabling IGMP Snooping globally. Since the multicast source is typically on the LAN side in the Hotel IPTV scenario, the gateway's IGMP functionality was disabled in this case.



2. It is recommended to configure the querier on the switch closest to the multicast source. Therefore, the first SX3032F switch was selected as shown in the diagram below. Considering there is only one multicast source and a single link between the multicast source and the querier, a Static Router port was configured on this switch pointing to the switch connected to the Source. This ensures that member reports are consistently sent to the multicast source through this port.



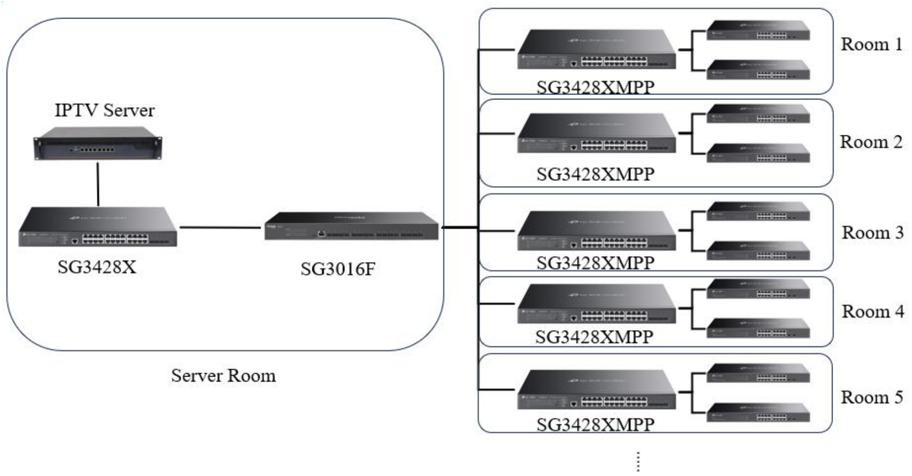


4.3.2 Case 2: A Hotel Case in Thailand

1) Background and Requirements:

This five-star hotel has significant influence in the local industry and has purchased a large quantity of our switches. It serves as a benchmark for our IPTV solutions in Southeast Asia. The responsible personnel reported that due to the large number of switches purchased and the relatively complex topology, they required our technical team to recommend IPTV multicast configurations to ensure smooth IPTV playback without lag.

2) Network Topology:



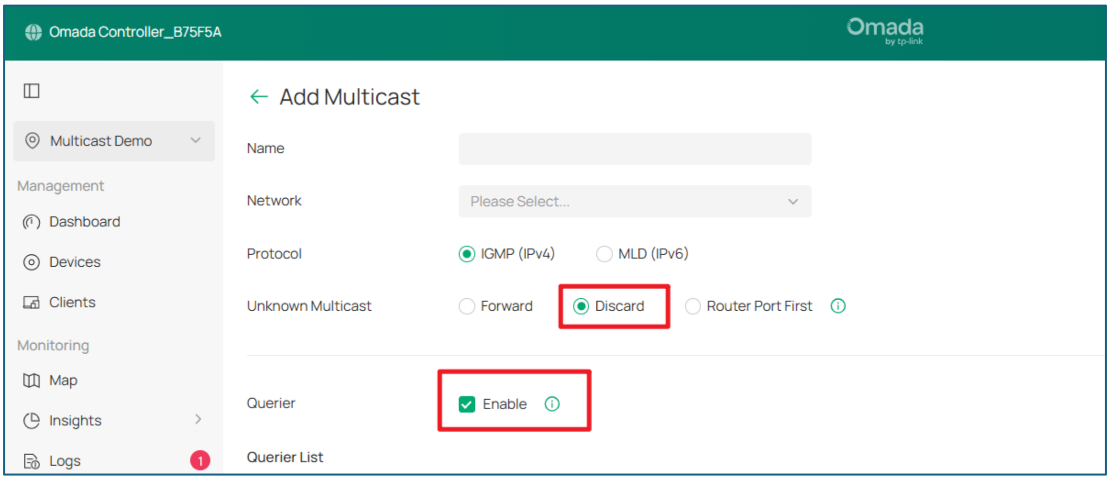
3) Solution and Configuration Recommendations

The diagram above shows that the network cabling is structured in a three-tier architecture: core equipment server room - floor aggregation - room access, so we recommend:

1 . Enable IGMP Querier only on the SG3428X directly connected to the IPTV Server.

2 . To ensure that SG3428X reliably receives multicast packets, enable Router Port First on this device. All other switches should discard Unknown Multicast to reduce unnecessary flooding.

Note: Since current configurations for Discard are applied to all adopted switches collectively, specific CLI commands are required for the core switch. Run the following command in the site template:
ip igmp snooping vlan-config 1 route-unknown

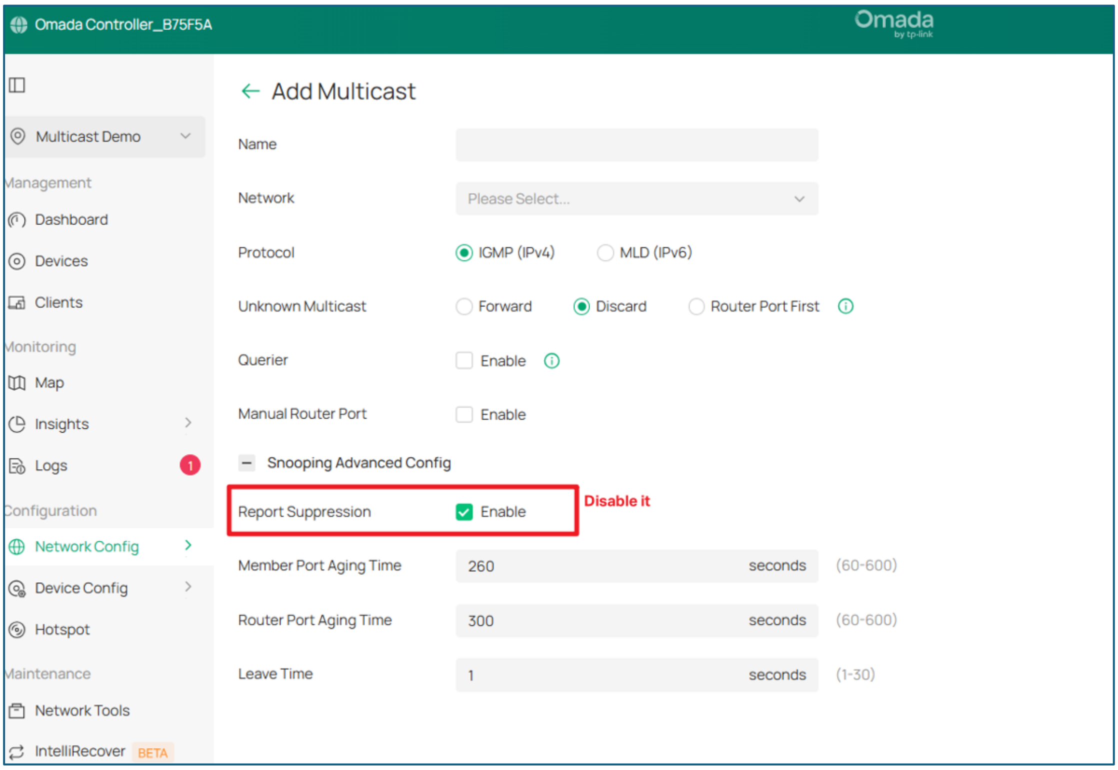


3 . Given the large number of IPTV connections in this scenario, we need to optimize the IPTV leave process and reduce additional traffic generated by member reports:

Enable Report Suppression on switches directly connected to IPTV devices and enable Fast Leave on the ports.

Note 1: The Report Suppression in multicast configuration applies to all switches connected to IPTV devices. Therefore, this feature needs to be disabled on other switches via CLI, or enabled on required switches using CLI.

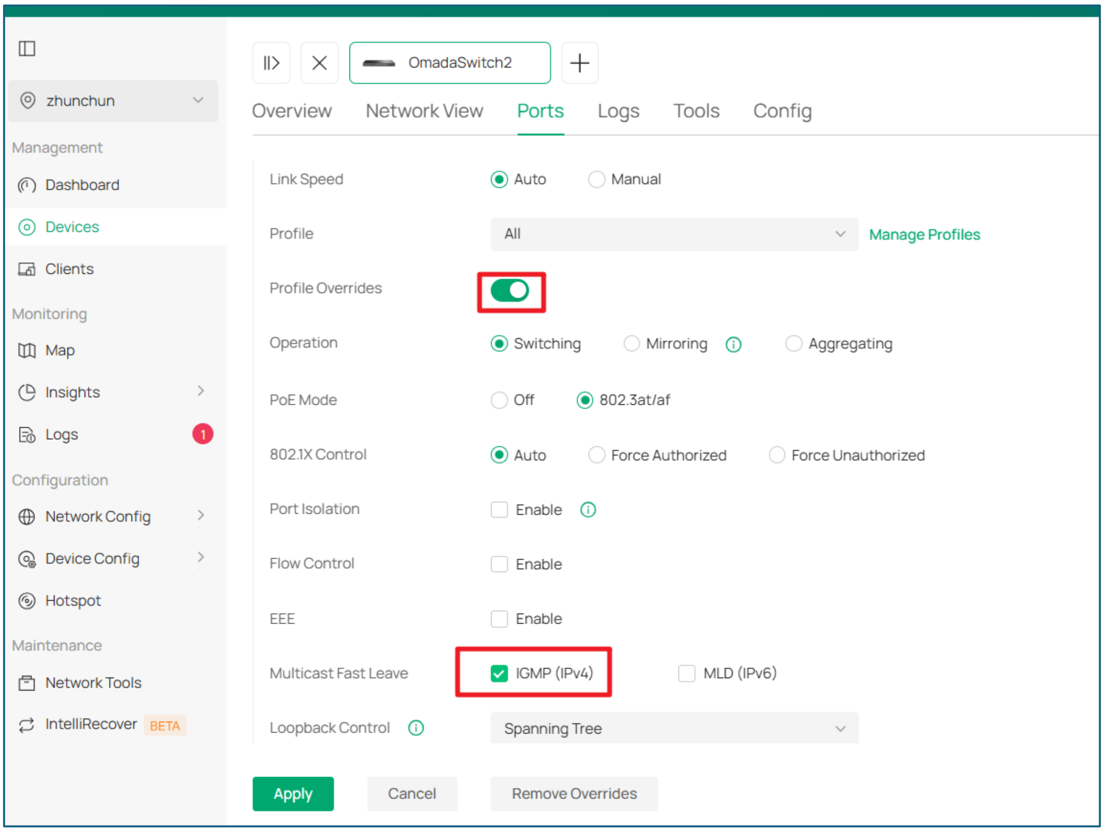
Disable Report Suppression on Controller.2



On the corresponding switch, configure the CLI template and apply the following command:

ip igmp snooping vlan-config 1 report-suppression

Note 2: The Fast Leave feature is designed for multicast receivers, so it is recommended to configure it only on the ports of switches directly connected to IPTV devices.



5 Appendix

Term	Description
IGMP	Internet Group Management Protocol
MLD	Multicast Listener Discovery
IGMP Snooping	Internet Group Management Protocol Snooping
MLD Snooping	Multicast Listener Discovery Snooping
IPTV	Internet Protocol Television