IPTV Technical White Paper

Contents

1 Overview

1.1 Introduction

IPTV (Internet Protocol Television) is a solution that delivers television signals over the Internet Protocol. It transmits TV programs, on-demand video, and interactive media services to TVs or other terminal devices over IP networks.

1.2 Background

The rapid roll-out of digital fiber networks has accelerated the evolution of traditional broadcast TV services toward interactive IPTV services. After years of development, IPTV has formed a complete service ecosystem covering live TV, video on demand, replay, and value-added applications.

Due to long-term region-by-region deployment, however, network planning, technology adoption, and device deployment methods vary significantly, with fragmented technical reference materials and rarely standardized deployment solutions.

1.3 Purpose of This White Paper

This document summarizes IPTV-related technologies and fundamental principles, analyzes mainstream technical architectures, and consolidates officially recommended deployment solutions. The goal is to enable frontline personnel to independently complete standardized deployments, basic O&M, and self-troubleshooting of common issues based on this document, reducing repeated backend involvement and improving overall project delivery efficiency and on-site O&M quality.

2 Key Technologies

2.1 Basic Concepts

2.1.1 Introduction to IPTV

IPTV stands for Internet Protocol Television. It represents technology and service that delivers multimedia content, such as TV programs and video on demand, over a high-speed, quality-assured broadband network (e.g., fiber, xDSL, Ethernet, etc.) using the Internet Protocol.

Simply put, IPTV "packages" traditional TV signals into data packets and transmits them over an IP network to the user's premises. The user then decodes the content via a set-top box and watches it on the TV.

The core components of an IPTV network include:

- **Set-top box (STB)**: A device that connects a TV to an external signal source. It

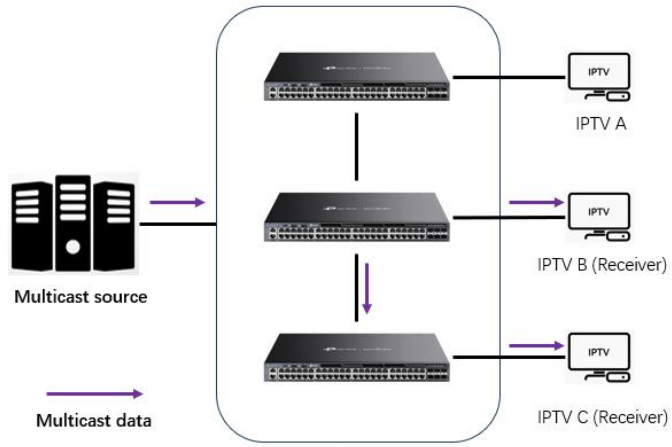
converts compressed digital signals into TV content and displays it on the TV. As an IP access terminal, STB must support a series of service-related protocols. It receives service packets and renders the video on the IPTV display. Considering that some IPTV devices on the market already have a built-in STB and support wireless signal reception, "IPTV" in the figures below refers to "IPTV + STB," unless otherwise specified.

- **IP transport network**: The transmission backbone of IPTV. It requires high bandwidth, low latency, high stability, and Quality of Service (QoS) assurance capabilities.
- **Multicast source devices**: These devices are typically used in scenarios such as hotels and are mainly used to provide live TV programs to guests. Common multicast source devices include IPTV headends and digital TV modulators.

2.1.2 IPTV Multicast Technology

Traditional unicast and broadcast communication methods cannot achieve one-to-many delivery with minimal network overhead. IP multicast technology addresses this problem in a timely manner.

As shown in the figure below, when some hosts in an IP network (i.e., receivers) require information, multicast allows the multicast source (i.e., the source) to send only one copy of the data. With the help of multicast routing protocols, a multicast distribution tree is built, and the data is replicated and distributed only at network nodes as far away from the multicast source as possible. IPTV A has not joined the multicast group, so it cannot receive the corresponding multicast traffic.



2.1.3 IPTV Casting Technology

This technology projects the screen or video from a phone/PC/tablet (smaller screen) to a TV/projector (larger screen) over the network.

It can be divided into two types:

- **Mirroring**: The entire phone screen is replicated to the larger screen in real time (for gaming and presentations).

- **Casting**: Only the video link is sent, and the large-screen device downloads and plays the video standalone (for TV series and movies).

2.2 Advantages

Multicast and casting are the core functions of IPTV.

The main advantages of multicast include:

- **Improved efficiency:** Reduces the load on the source server and the CPU of network devices.
- **Optimized performance:** Reduces redundant traffic.
- **Distributed delivery:** Uses minimal network resources to achieve point-to-multipoint delivery.

The main advantages of casting include:

- **Cable-free:** No HDMI cable required; one-tap casting from a phone; zero cabling for homes and meeting rooms.
- **Small screen to big screen:** Enlarges phone videos, games, online classes, and meeting content for a better experience.
- **Multi-device compatibility:** Interoperability among phones, PCs, tablets, TVs, and projectors.
- **Low cost:** Most smart TVs/TV boxes have built-in casting, with no additional hardware required.

2.3 Market Demand

The global IPTV market continues to grow steadily. Hotels and MDUs are key commercial deployment scenarios for IPTV. With the adoption of fiber networks and 4K technologies, market demand remains strong. In hotel scenarios, in addition to basic audio-visual services, customized user interfaces, multilingual support, and system integration features are commonly required, along with high requirements for playback stability and concurrent capacity. MDUs, including apartments and homestays, focus on lightweight deployment, batch management, and day-to-day O&M convenience. As business travel and rental markets continue to grow, IPTV demand in these two scenarios is steadily increasing, making them key focus areas for industry expansion.

3 Key Technical Principles

3.1 Protocol Analysis

In hotel/MDU scenarios, the most commonly used IPTV functions are multicast and casting. This section introduces common multicast protocols—IGMP Snooping, IGMP, PIM, and MSDP—as well as casting protocols such as DLNA, AirPlay, and Chromecast.

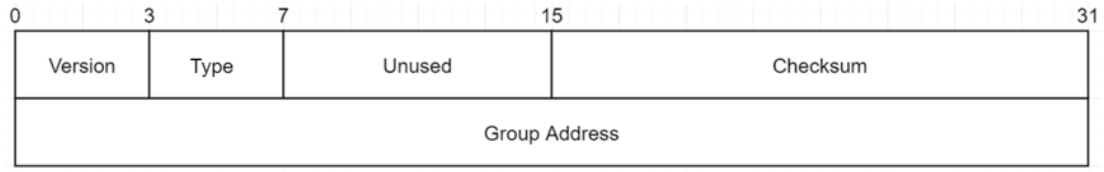
3.2 Principle Analysis

3.2.1 IGMP

The Internet Group Management Protocol (IGMP) is the protocol in the TCP/IP suite responsible for IPv4 multicast membership management. It is used to establish and maintain multicast group membership between IP hosts and directly adjacent multicast devices. To date, there are three versions of IGMP: IGMPv1, IGMPv2, and IGMPv3.

3.2.1.1 IGMPv1

RFC 1112 illustrates the specification of IGMPv1. The packet format of an IGMPv1 message is shown in the figure below.



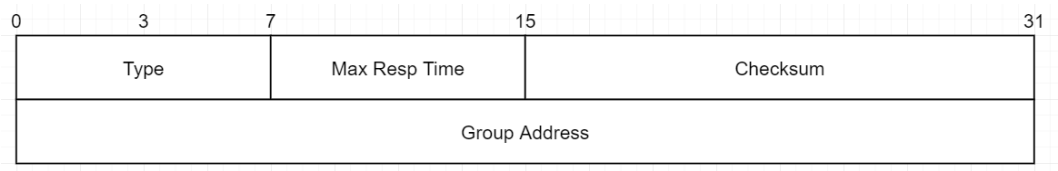
IGMPv1 contains only two types of IGMP messages:

- Membership query
- Membership report

Hosts send an IGMP Membership Report for a specific multicast group to indicate that they are interested in joining the group. Routers periodically send IGMP Membership Queries to verify whether at least one host on the subnet is still interested in receiving traffic destined for that group. If no IGMP Membership Report is received within a certain period, the router times out and stops forwarding traffic destined for that group.

3.2.1.2 IGMPv2

Now, IGMPv1 has been replaced by IGMPv2, which is backward compatible with IGMPv1. RFC 2236 illustrates the specification of IGMPv2. The packet format of an IGMPv2 message is shown in the figure below.



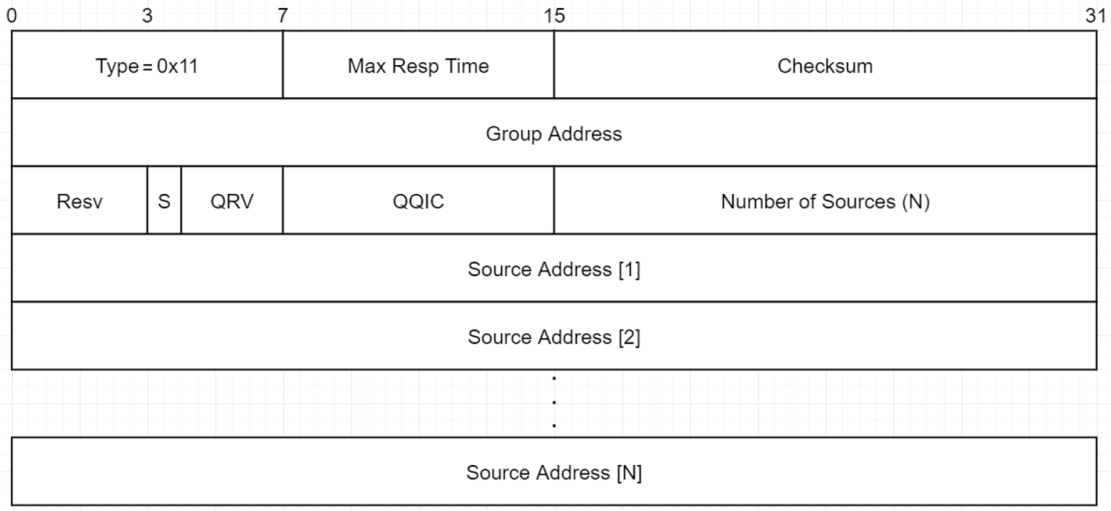
IGMPv2 operates in basically the same way as IGMPv1. The main difference is the addition of a Leave Group message. With this message, a host can proactively notify the local multicast router that it intends to leave the group. The router then sends a group-specific query to determine whether any remaining hosts are still interested in receiving the traffic. If

no response is received, the router times out the group and stops forwarding the traffic. Compared with IGMPv1, the Leave Group message in IGMPv2 significantly reduces leave latency, allowing unwanted and unnecessary traffic to stop more quickly.

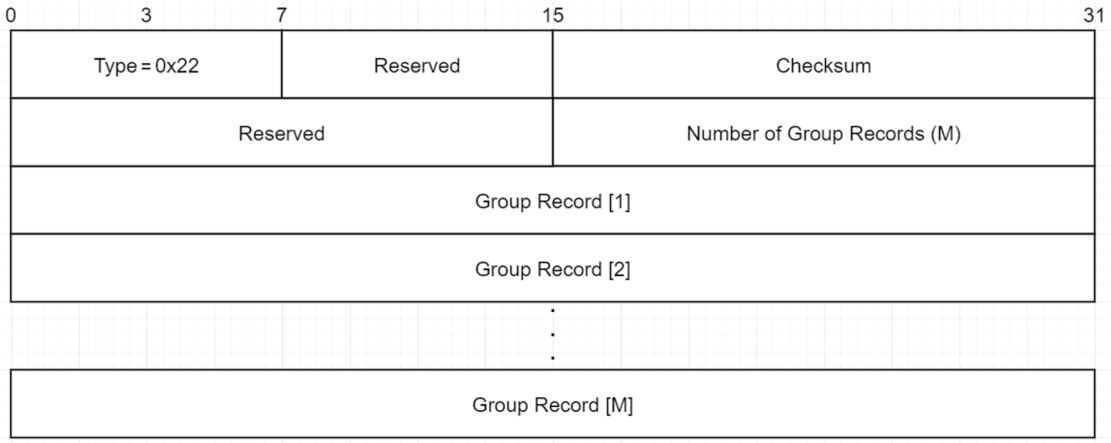
3.2.1.3 IGMPv3

IGMPv3 is the next evolution of IGMP. IGMPv3 adds support for source filtering, allowing multicast receiver hosts to transmit to routers both the multicast group they want to receive and the expected source(s) of that traffic. This membership information enables devices to forward only traffic from sources requested by receivers. RFC 3376 illustrates the specification of IGMPv3.

The query packet format of an IGMPv3 message is shown in the figure below.



The report packet format of an IGMPv3 message is shown in the figure below.



IGMPv3 contains the following types of IGMP messages:

• Version 3 membership query

• Version 3 membership report

IGMPv3 supports applications that explicitly signal the source(s) from which traffic should be received. With IGMPv3, receivers signal membership to a multicast group in the following two modes:

- **INCLUDE mode:** In this mode, the receiver announces membership in the multicast group and provides a list of source addresses from which it wants to receive traffic (the INCLUDE list).
- **EXCLUDE mode:** In this mode, the receiver announces membership in the multicast group and provides a list of source addresses from which it does not want to receive traffic (i.e., the EXCLUDE list). The host receives traffic only from sources whose IP addresses are not in the EXCLUDE list. To receive traffic from all sources (i.e., the IGMPv2 behavior), a host uses EXCLUDE mode membership with an empty EXCLUDE list.

3.2.1.4 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is a basic L2 multicast feature. It is mainly used to optimize multicast forwarding behavior on L2 devices, enabling multicast traffic to be controlled and forwarded at Layer 2.

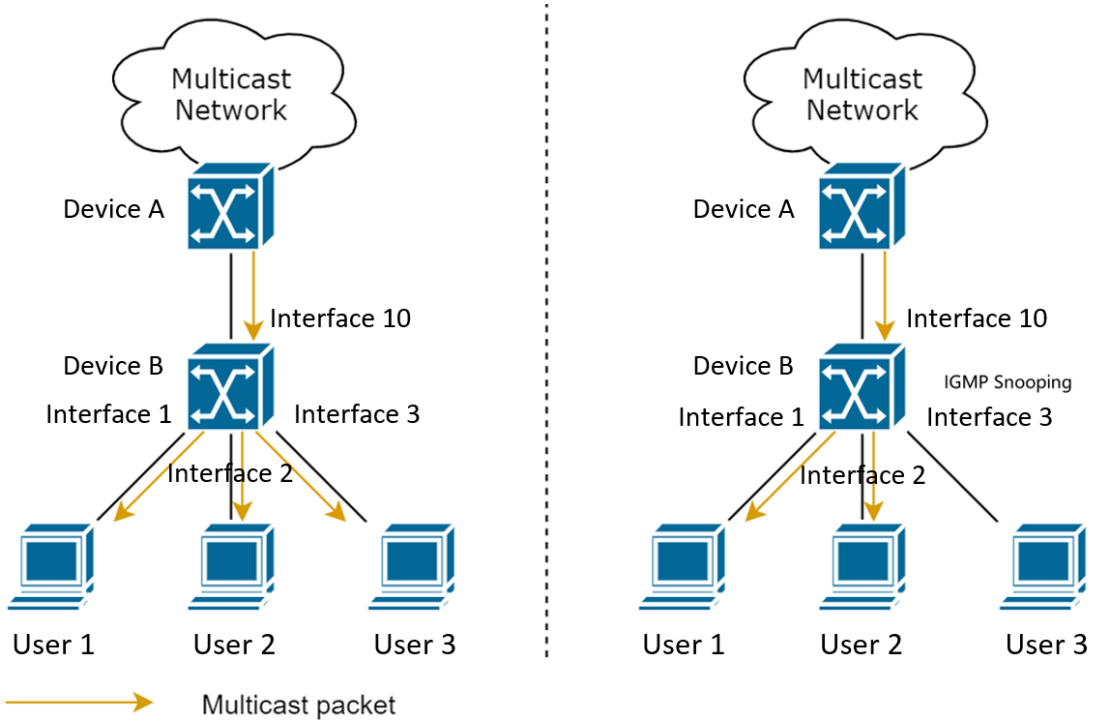
In many cases, multicast packets inevitably pass through L2 switching devices, especially in L2 switched networks. If the L2 device (Device B) does not have IGMP Snooping deployed, as shown in the figure below, Device B connects to the multicast device (Device A) through Interface 10 and also connects to multiple users. Among these users, User 1 and User 2 are members of a multicast group and will send IGMP Membership Report messages to the network to announce that they have joined the group. After that, when Device A receives traffic destined for the multicast group, it forwards the traffic into the switched network; User 1 and User 2 will receive the required multicast traffic.

However, by default, when Device B receives an unknown unicast frame, a multicast frame, or a broadcast frame within a VLAN, it floods the frame within the same VLAN. Therefore, Device B forwards the traffic destined for the multicast group out of Interface 1, Interface 2, Interface 3, and other interfaces (assuming they belong to the same VLAN). In this case, even users who are not members of the multicast group (for example, User 3) will also receive the multicast traffic, wasting network bandwidth and device resources.

After IGMP Snooping is deployed on Device B, when group members User 1 and User 2 announce that they have joined the group through IGMP Membership Report messages, Device B not only forwards these messages to Device A but also parses the message contents and binds the multicast group address to interface information such as Interface 1 and Interface 2, thereby creating L2 forwarding entries. After that, when Device B receives multicast traffic sent by Device A, it forwards the traffic out of Interface 1 and

Interface 2 based on the entries in the L2 forwarding table. Non-member User 3 will not receive the multicast traffic. Therefore, after IGMP Snooping is deployed, Device B forwards multicast traffic only out of the correct interfaces.

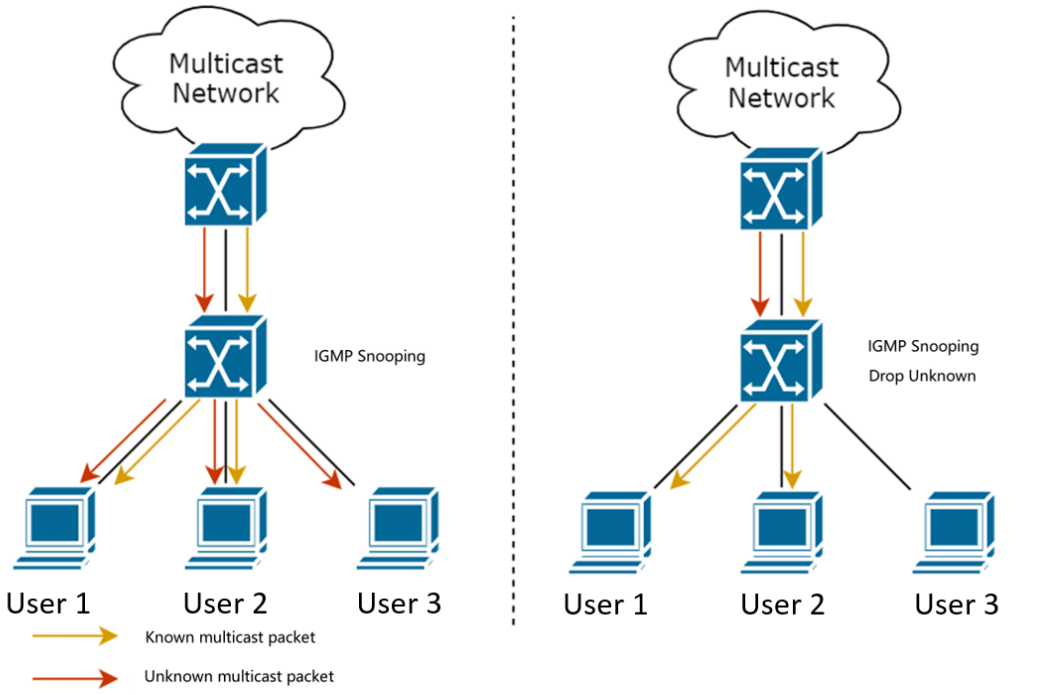
- If Device B is not running IGMP Snooping, multicast traffic is broadcast at the data link layer.
- If Device B is running IGMP Snooping, multicast traffic is not broadcast at the data link layer. Instead, it is forwarded to the required receivers through the L2 multicast forwarding table via the corresponding ports Interface 1 and Interface 2.



3.2.2 Common L2 Multicast Parameters

3.2.2.1 Drop Unknown

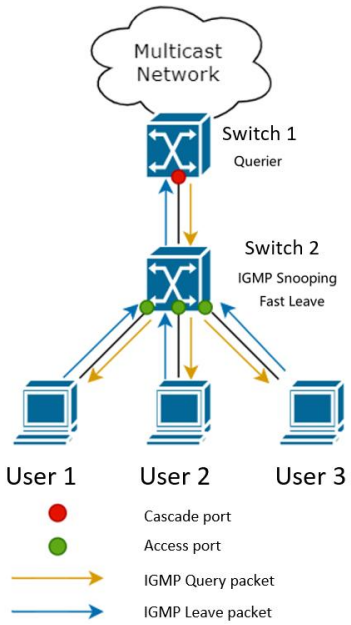
By default, multicast streams that have not been joined are flooded within the VLAN. When Drop Unknown is enabled, the streams are dropped directly, which can save bandwidth utilization. In typical scenarios, enabling Drop Unknown is recommended.



3.2.2.2 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 (i.e., Leave latency). The default is 1s, and the configurable range is 1s to 30s. When Fast Leave is enabled, upon receiving a Leave message from a multicast member, the port leaves the group immediately. It is recommended to enable this feature only on switch ports directly connected to receivers. It should not be enabled on cascade ports.

Application scenario:

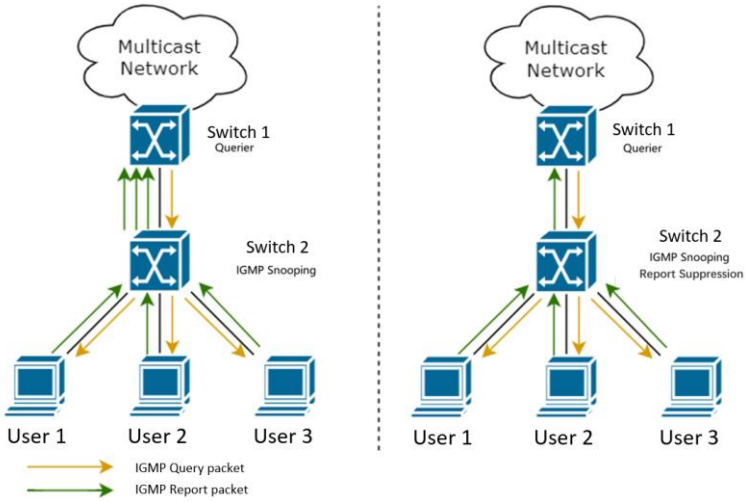


Assume that User 1, User 2, and User 3 in this topology join the same multicast group. We recommend enabling Fast Leave only on the ports on Switch 2, which connect to the users, and not on the cascade port between Switch 2 and Switch 1. Otherwise, when User 1 leaves the group, Switch 2 forwards the Leave message to Switch 1, and Switch 1 will immediately remove the cascade port from the group, causing the other users to stop receiving multicast traffic.

3.2.2.3 Report Suppression

By default, the switch forwards all Report messages it receives to the router port. When Report Suppression is enabled, each time a Query message is received, only the first Report message received from downstream is forwarded to the router port. This feature reduces the transmission of Report messages in the network and saves bandwidth.

Application scenario:

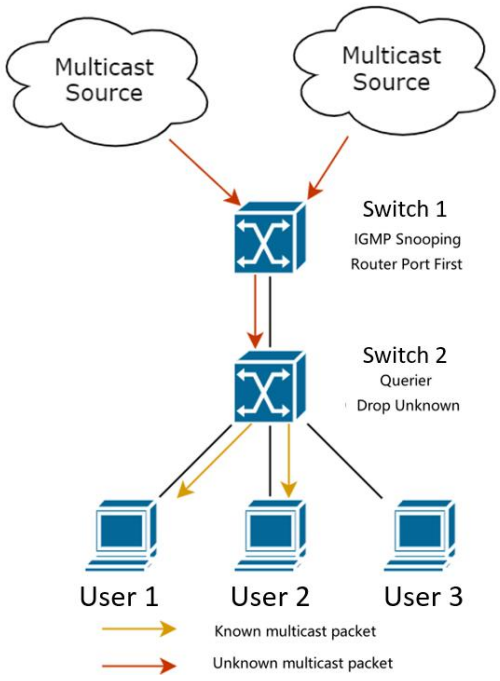


As shown in the figure, assume User 1, User 2, and User 3 join the same multicast group. After Switch 1 sends a Query message, User 1, User 2, and User 3 all reply with Report messages. If Report Suppression is enabled on Switch 2, Switch 2 forwards only the first Report message it receives to Switch 1. This helps reduce bandwidth usage between Switch 2 and Switch 1.

3.2.2.4 Router Port First

By default, multicast streams that have not been joined are flooded within the VLAN. When Router Port First is enabled, if no router port exists, unknown multicast streams are flooded within the VLAN. If a router port exists, unknown multicast streams are forwarded through the router port.

Application scenario:



If the Querier is not configured on the device closest to the multicast source, as shown in the figure, the multicast source is directly connected to Switch 1, but the Querier is on Switch 2. If Router Port First is not enabled on Switch 1, Switch 1 cannot send Join messages to Switch 2, and the multicast traffic cannot reach Switch 2. In this case, enable Router Port First on Switch 1, and Switch 1 will forward all received multicast source traffic to Switch 2.

Note: In this case, Drop Unknown should be enabled on Switch 2. Otherwise, if a set-top box is directly connected to Switch 2, unknown multicast traffic may impact the set-top box.

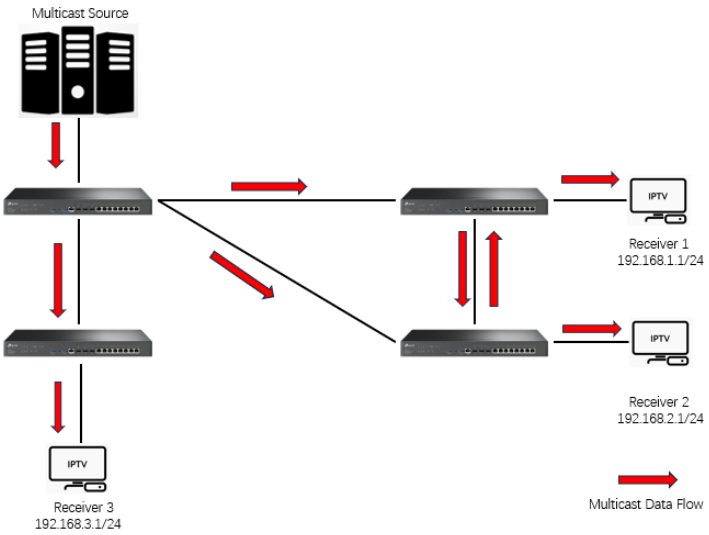
3.2.3 PIM

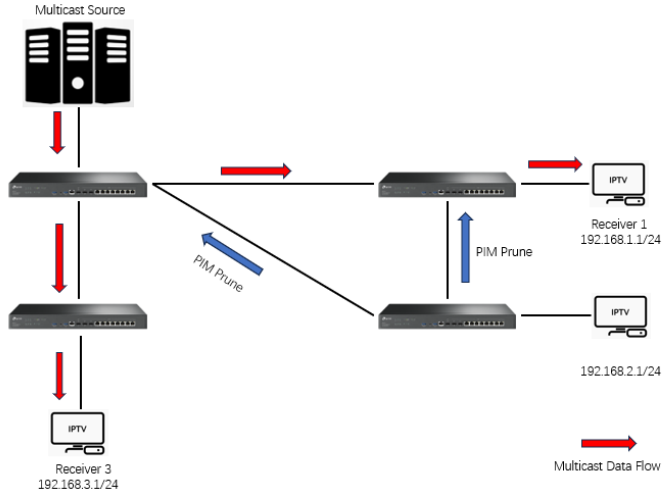
PIM is a multicast protocol used in L3 networks. It includes PIM-DM and PIM-SM.

3.2.3.1 PIM-DM

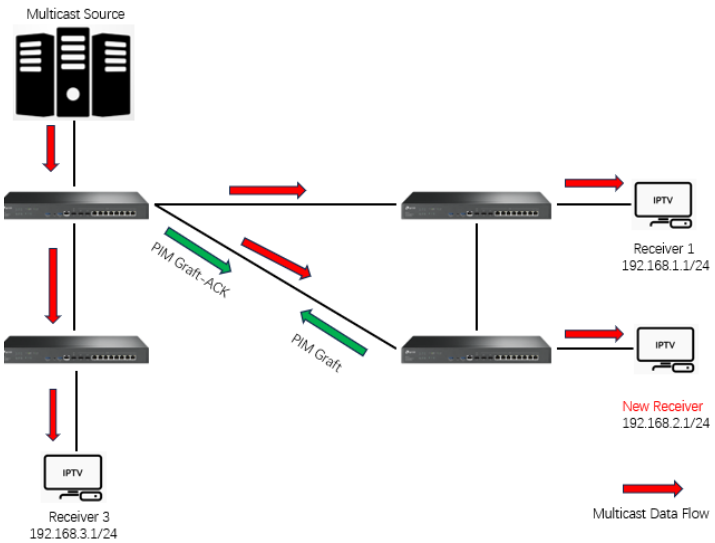
In a PIM-DM domain, routers running PIM-DM periodically send PIM Hello messages to discover adjacent PIM routers. PIM-DM is a dense-mode multicast routing protocol that uses a "push" model to deliver multicast traffic. It is typically suitable for small networks with relatively dense multicast group members. Its basic principles are as follows:

- PIM-DM assumes that each subnet in the network has at least one multicast group member, so multicast traffic is disseminated to all nodes in the network. Then, PIM-DM prunes branches that do not need to forward multicast traffic, retaining only the branches that contain receivers. This "flood-and-prune" behavior occurs periodically, and pruned branches can also periodically return to the forwarding state.





- When a multicast group member appears on a node of a pruned branch, the node actively sends a Graft message upstream to transition from the pruned state back to the forwarding state, restoring multicast forwarding.

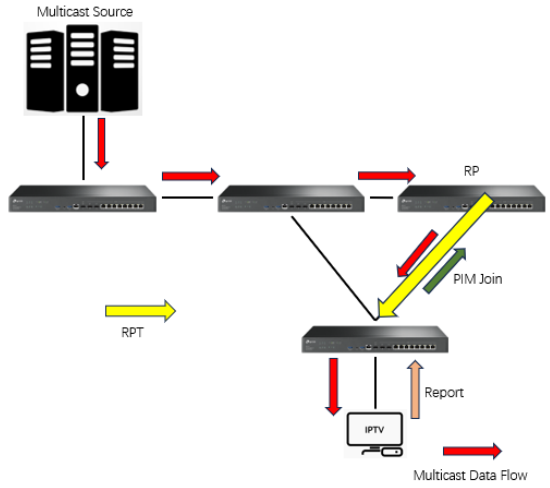


3.2.3.2 PIM-SM

In a PIM-SM domain, routers running PIM-SM periodically send PIM Hello messages to discover adjacent PIM routers and are responsible for electing a DR (Designated Router) on multi-access networks. The DR sends Join/Prune messages toward the root of the multicast tree on behalf of directly connected group members, or forwards multicast traffic from directly connected multicast sources onto the multicast distribution tree.

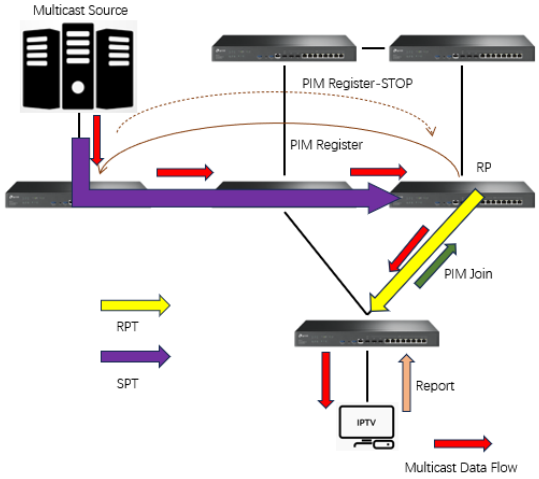
PIM-SM is a sparse-mode multicast routing protocol that uses a "pull" model to deliver multicast traffic. It is typically suitable for medium-to-large networks where multicast group members are relatively sparse and distributed across a wide area. Its basic principles are as follows:

- PIM-SM assumes that no hosts need to receive multicast traffic unless they explicitly request it. It forwards traffic only to hosts that explicitly request multicast traffic. The core task of PIM-SM multicast forwarding is to build and maintain an RPT (Rendezvous Point Tree). An RPT uses a router in the PIM domain as a shared root node, the RP (Rendezvous Point). Multicast traffic is forwarded to receivers through the RP along the RPT. A router connected to receivers sends a Join message to the RP for a specific multicast group. The Join message is forwarded hop by hop to the RP, and the traversed path forms a branch of the RPT.



- When a multicast source sends multicast traffic to a multicast group, the DR directly connected to the source first registers the source with the RP by sending a Register message to the RP via unicast. When the Register message reaches the RP, it triggers the establishment of an SPT (Shortest Path Tree). The SPT between the RP and the multicast source is based on the unicast best path. As shown in the figure, the RP has two paths to the multicast source; under equal conditions, the path that traverses the fewest devices is selected to build the SPT. The multicast source then sends multicast traffic to the RP along the SPT. After the multicast traffic reaches the RP, it is replicated

and forwarded to receivers along the RPT.



3.2.4 MBGP/MSDP

Inter-domain multicast routing is used to transmit multicast information between autonomous systems (ASes). Mature solutions include:

- **MBGP (Multicast BGP):** An extension to standard BGP-4. It is not a standalone protocol but a set of extensions that allow BGP to carry multicast routing information while also carrying unicast routing information.
- **MSDP (Multicast Source Discovery Protocol):** Allows RPs in different PIM-SM domains (i.e., different ASes) to inform each other about active multicast sources within their respective domains.

3.2.4.1 MBGP

MBGP is the multiprotocol extension of BGP-4. Its full name is Multiprotocol Extensions for BGP-4, and it is also known as BGP-4+. Based on BGP-4, MBGP adds support for multiple network-layer protocols, enabling it to carry routing information for IPv4 unicast, multicast, IPv6, and more.

Through these extensions, MBGP can maintain both unicast and multicast routing tables simultaneously and allow the two topologies to exist independently. The protocol defines two optional attributes, MP_REACH_NLRI and MP_UNREACH_NLRI, which are used to advertise reachable routes and withdraw unreachable routes, respectively. Protocol Independent Multicast (PIM) uses this multicast routing information to build distribution trees, making it suitable for scenarios where multicast communication links need to be differentiated.

MBGP is applicable when multicast sources and receivers are located in different ASes and is a key protocol for inter-AS multicast forwarding. Deploying MBGP enables a multicast

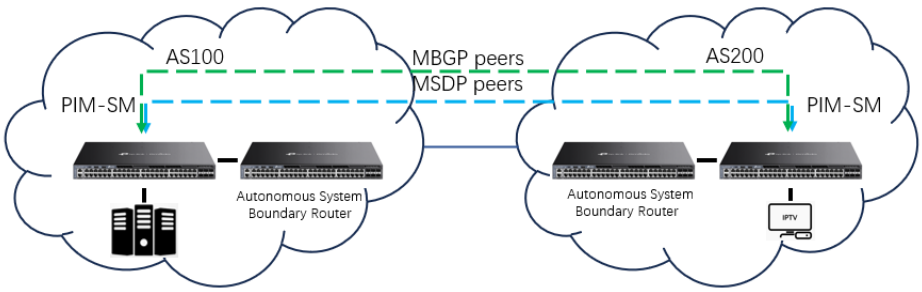
routing table that is independent of the unicast routing table, allowing multicast traffic to be forwarded through this dedicated routing table. This separates unicast and multicast paths and optimizes network control.

3.2.4.2 MSDP

In a basic PIM-SM deployment, multicast sources register only with the RP within their own PIM-SM domain, and multicast source information is isolated between domains. As a result, an RP knows only the multicast sources within its own domain and can build multicast distribution trees only within that domain to deliver multicast traffic from local sources to local users. For an autonomous system, it is undesirable to rely on an RP in another autonomous system to forward multicast traffic. At the same time, it is still necessary to receive multicast data from sources regardless of where the source RP is located.

MSDP is an inter-domain multicast solution developed to interconnect multiple PIM-SM domains and discover multicast source information from other PIM-SM domains. MSDP establishes MSDP peer relationships between appropriate devices in the network to connect the RPs of different PIM-SM domains. Multicast source information is shared between MSDP peers by exchanging SA (Source-Active) messages.

Although MSDP was designed for inter-domain multicast, it also has a special application within a PIM-SM domain—Anycast RP. Anycast RP refers to configuring two or more RPs with the same IP address within the same PIM-SM domain and establishing MSDP peer relationships among these RPs to achieve load sharing and redundancy.



3.2.5 Casting Protocols

Mainstream casting protocols can be categorized into the four types in the table below. Omada devices support all the data transport protocols listed. For casting to work properly, the client and the device must be able to discover each other. Currently, the mainstream discovery protocols are SSDP and mDNS.

Name	Device Discovery Protocol	Data Transmission
Miracast (Wi-Fi Display, WFD)	1. SSDP 2. Wi-Fi Direct (P2P)	**Control:** RTSP (SDP negotiates codec/resolution/frame rate)

		Media: RTP/UDP encapsulated H.264/AAC, HDCP encryption
DLNA (Digital Living Network Alliance)	SSDP	**Control:** HTTP + SOAP (AVTransport/RenderingControl services, delivering playback commands and URLs) **Media:** HTTP/S (the receiver directly requests the media URL from the DMS, supporting HLS/MP4, etc.)
AirPlay	mDNS/Bonjour(_airplay._tcp)	**Mirroring Mode:** RTP/UDP (H.264/AAC, encrypted), RTCP synchronization **Push Mode:** HTTP/S (URL push; the receiver pulls directly) **Control:** HTTP (playback control, status synchronization)
Chromecast	mDNS/Bonjour(_googlecast._tcp)	**Push Mode:** HTTP/S (the sender only provides the app ID and media URL; the receiver pulls directly from the cloud/CDN) **Mirroring Mode:** RTP/UDP (desktop/tab is encoded and then transmitted) **Control:** WebSocket (low-latency bidirectional control, real-time status synchronization)

3.2.5.1 SSDP

SSDP is the "discovery protocol" in the UPnP (Universal Plug and Play) framework. It enables automatic discovery and online/offline announcements of devices and services within the same L2/LAN network. It is commonly used in scenarios such as DLNA casting, smart TVs, routers/gateways, NAS, and cameras. Its basic characteristics are as follows:

- **Transport layer:** UDP
- **Multicast address/port (IPv4):** 239.255.255.250:1900
- **Multicast address/port (IPv6):** FF02::C (link-local scope)

SSDP has two core mechanisms:

A. NOTIFY: Devices "announce their presence"

When a device/service comes online, it periodically sends an NTS: ssdp:alive message. When it goes offline, it sends an NTS: ssdp:byebye message. The destination address is the multicast address, allowing control points on the same subnet to cache device information. Common key fields include:

- **NT:** Notification Type
- **USN:** Unique Service Name (unique identifier, usually including a UUID)
- **LOCATION:** URL of the device description document (XML)
- **CACHE-CONTROL:** max-age = seconds until advertisement expires
- **SERVER:** Device software/system information (may expose version information)

B. M-SEARCH: Control points "search for a service provider"

A control point sends an M-SEARCH request to the multicast address. If a device matches the search target, it replies via unicast with HTTP/1.1. Key fields include:

- **ST:** Search Target (the type being searched for, e.g., a device/service class)
- **MAN:** "ssdp:discover" (fixed directive)
- **MX:** Maximum wait time in seconds (devices reply with a random delay to avoid response storms)

The following example describes a basic DLNA casting flow:

1. IPTV comes online and broadcasts a NOTIFY ssdp:alive message that includes LOCATION.
2. The mobile app sends an M-SEARCH request (to find the IPTV).
3. The TV replies via unicast with HTTP/1.1 200 OK and returns LOCATION.
4. The mobile phone accesses LOCATION to obtain the device description XML (capabilities, service list, and control URL).
5. The process then proceeds to the UPnP control/event phase (beyond the scope of SSDP).

3.2.5.2 mDNS

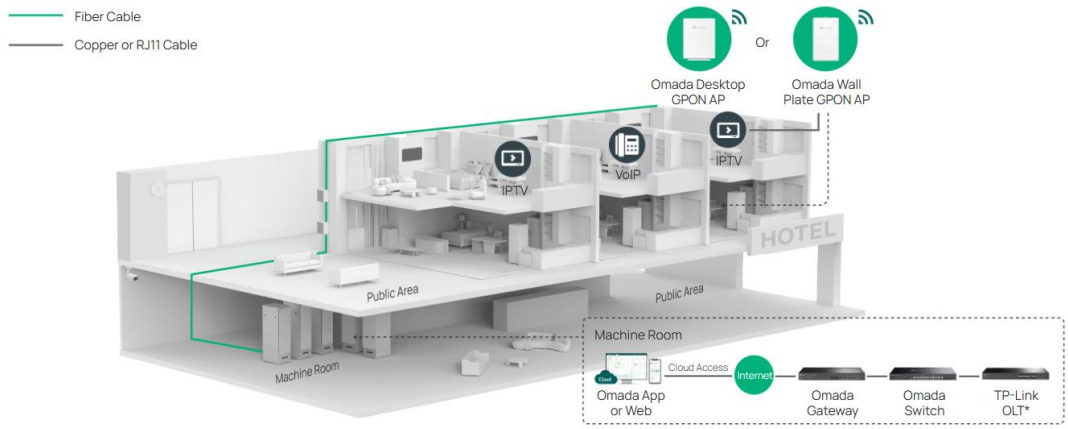
mDNS (Multicast DNS) is a zero-configuration networking protocol mainly used in small networks without a local DNS server to resolve hostnames to IP addresses. It is based on RFC 6762 and uses UDP multicast packets. mDNS is widely used, most commonly for casting between Google and Apple devices, as well as interconnection in small smart home/IoT environments.

mDNS typically operates within a LAN, using a specific IP address (224.0.0.251) and a specific port (5353). Its purpose is to enable service discovery, queries, and registrations within the local network.

3.3 Application Scenario Analysis

In hotel/MDU scenarios, IPTV provides guests with high-quality casting and video viewing services. IPTV can be deployed across different types of networks. Taking a hotel

optical-network deployment as an example, as shown in the figure below, an all-optical hotel network built with Omada devices connects IPTV via wired access to GPON APs to achieve casting and multicast functions. The Omada Controller provides unified device management, unified configuration provisioning, unified O&M, and policy synchronization, ensuring that the hotel network maintains high performance at all times.



IPTV can also be deployed in an Ethernet network. As shown in the MDU scenario below. The functions are basically the same as described above.

4 Application Scenarios and Solutions

4.1 Recommended L2 Ethernet IPTV Deployment Solution

Note: The following solutions are largely similar in configuration. Solution 1 is described in detail, while Solutions 2 and 3 show only the core configuration.

4.1.1 Solution 1

4.1.1.1 Prerequisites

This configuration guide assumes that the devices are managed by the Omada Controller. Therefore, before performing the subsequent configuration steps, make sure the following requirements are met:

1. The recommended Omada Controller version is 6.0 or above.

2. Switch firmware must be upgraded to the latest version available on the official website. Note that some switches may not support the Querier function (for details, refer to the user guide for the corresponding model on the official website). It is recommended to use an Omada Smart/L2+/L3 switch as the Querier.

3. There are no specific functional requirements for the gateway. However, in real customer scenarios, ER8411 is commonly used. Other Omada gateway models may be used in this deployment solution.

4. For Omada EAPs, the Wall series and Desktop series are more popular in real customer scenarios.

4.1.1.2 Topology

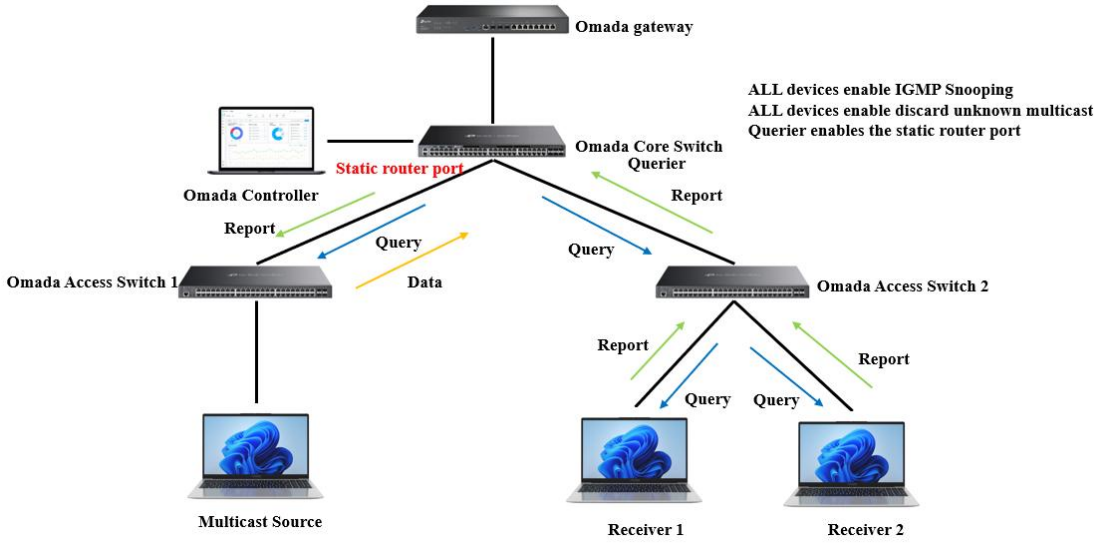
This topology applies to most wired-network scenarios and typically features the following:

1) A hierarchical tree topology.

2) Both the multicast source and receivers are in the same VLAN.

3) The core switch is typically configured as the Querier, replacing gateway-based multicast management.

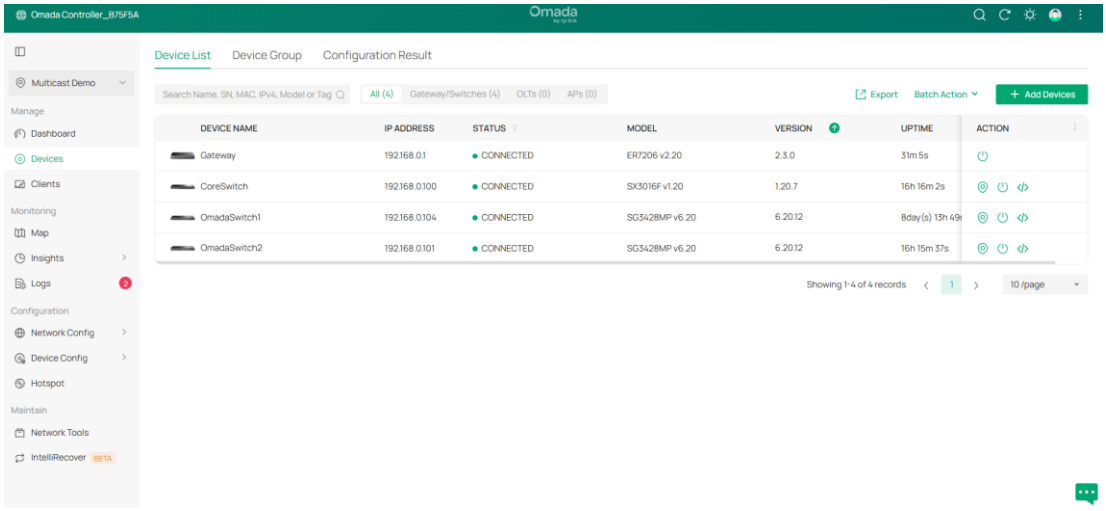
4) Key configurations are marked in the figure.



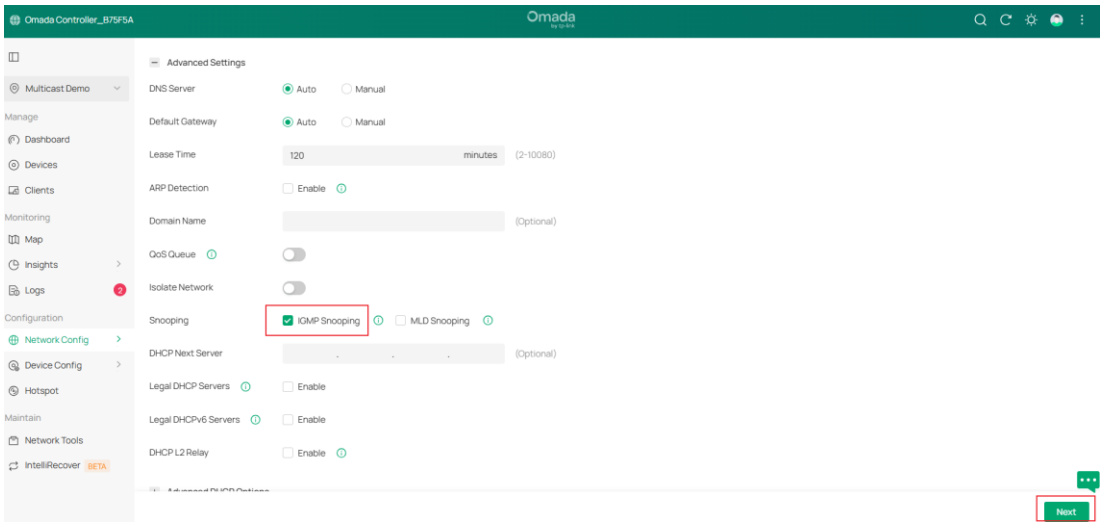
4.1.1.3 Configuration Steps

This example 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 run VLC Player: one PC acts as the multicast source, and the other two act as receivers.

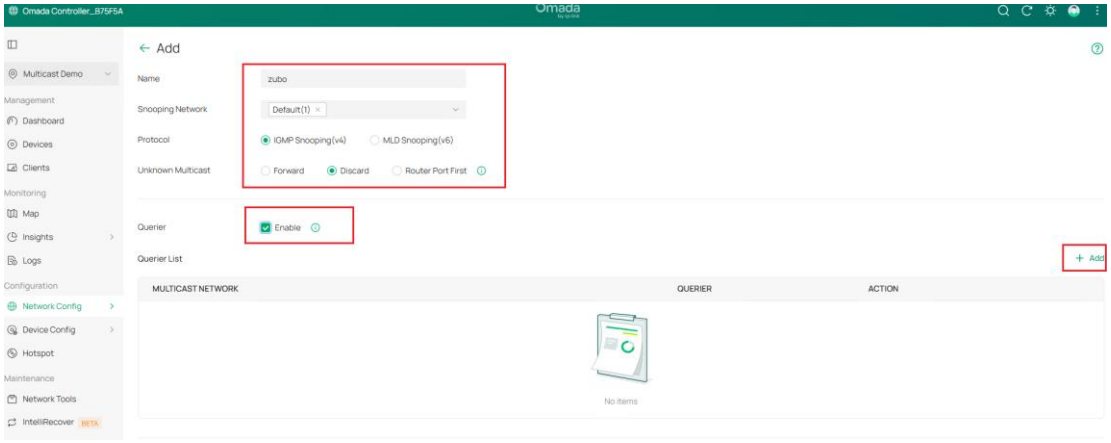
Step 1: Use Omada Controller 6.0 to adopt devices according to the network topology. Ensure all devices are upgraded to firmware versions supporting Controller 6.0 or above. Set the management address to VLAN1, subnet 192.168.0.0/24, and ensure the multicast source and receivers are on the same subnet.

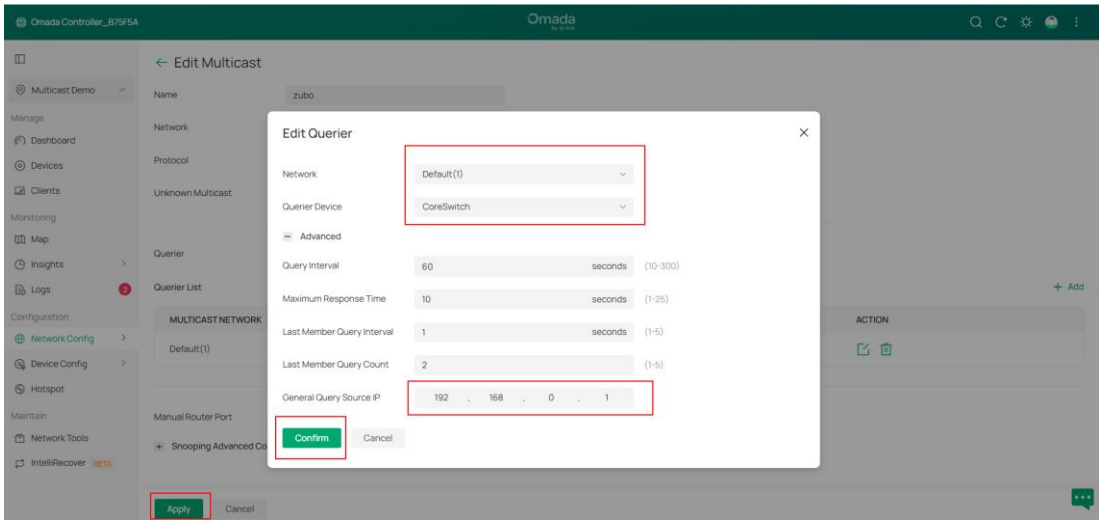


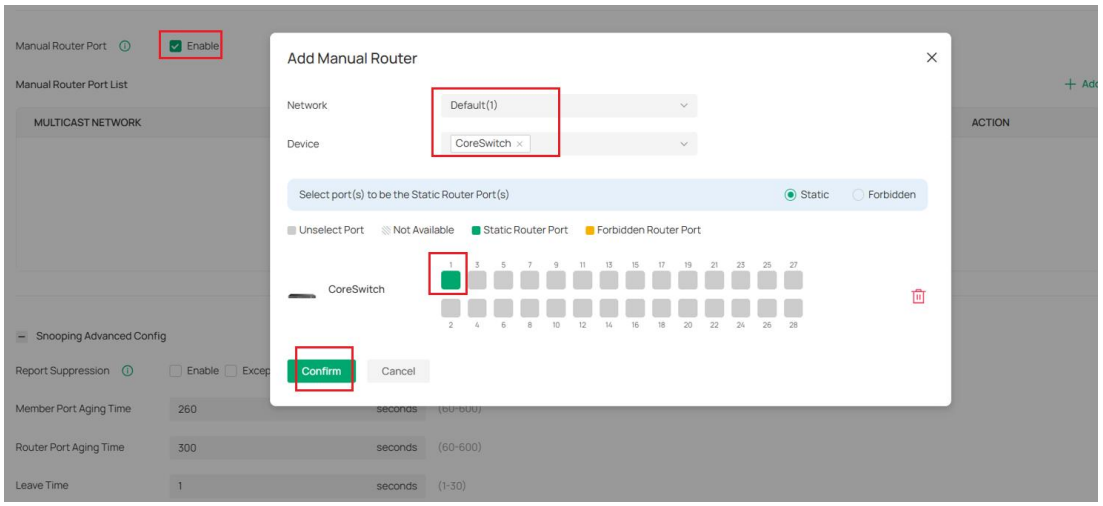
Step 2: Go to Network Config > Network Settings > LAN > VLAN and click Edit to enable IGMP Snooping (IPv4) for VLAN1.



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.



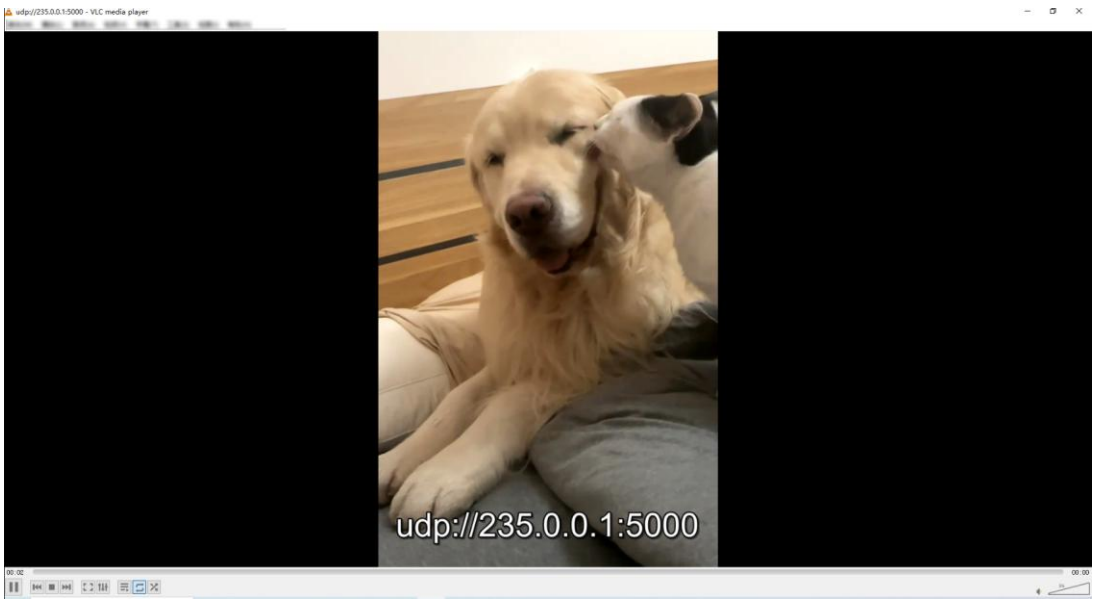




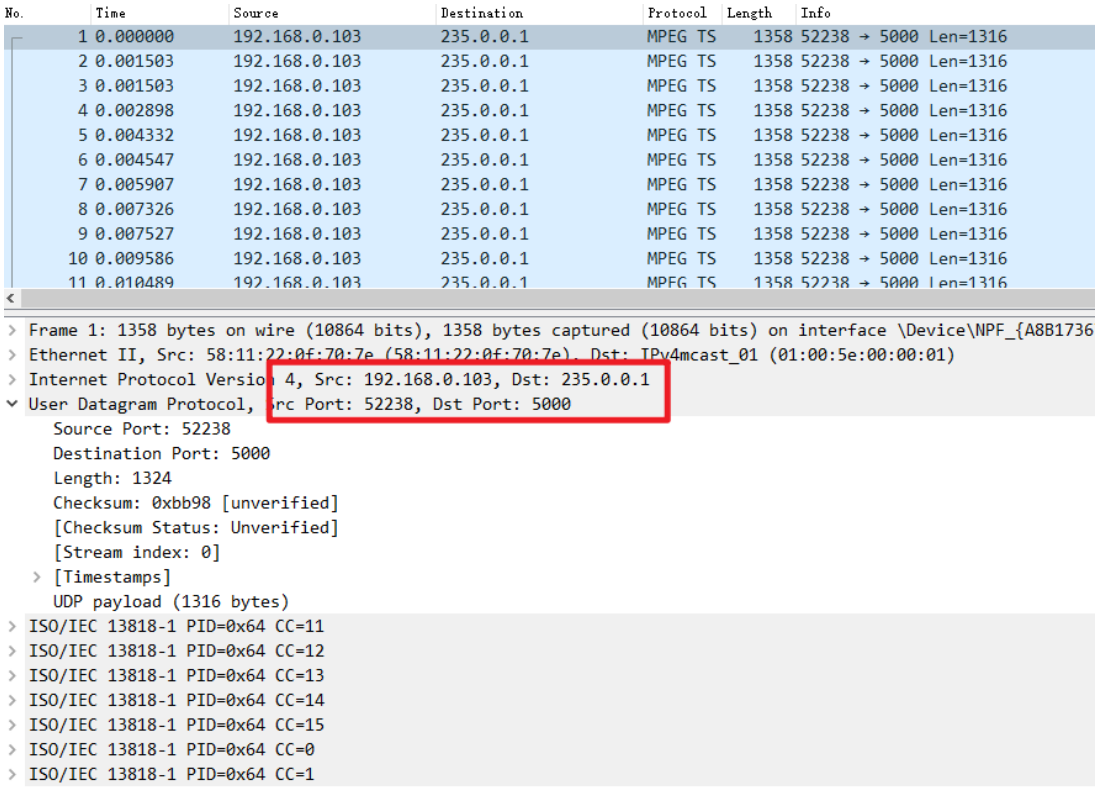
4.1.1.4 Verify Configuration

Step 1: On the multicast source (192.168.0.103) under Omada Switch 1, 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 Omada Switch 2, Receiver 1 joins 235.0.0.1 and Receiver 2 joins 237.1.1.1 to view the video and capture packets.

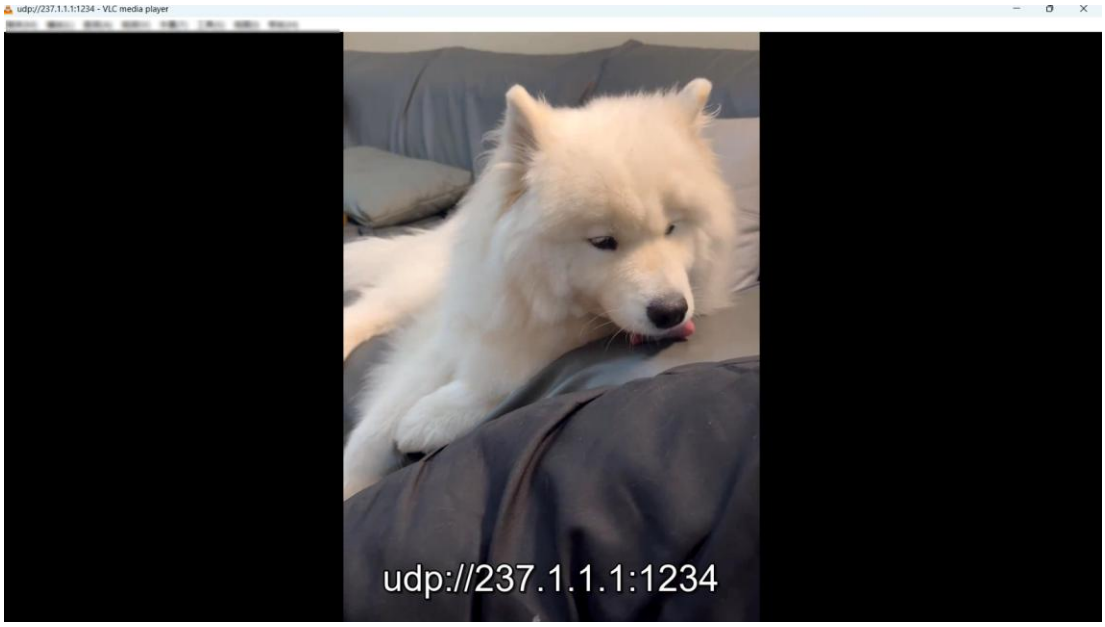
Receiver 1 joins 235.0.0.1 and successfully receives the corresponding video stream:



Receiver 1 packet capture shows multicast group data packets. The source address and destination port match the multicast source:



Receiver 2 joins 237.1.1.1 and successfully receives the corresponding video stream:

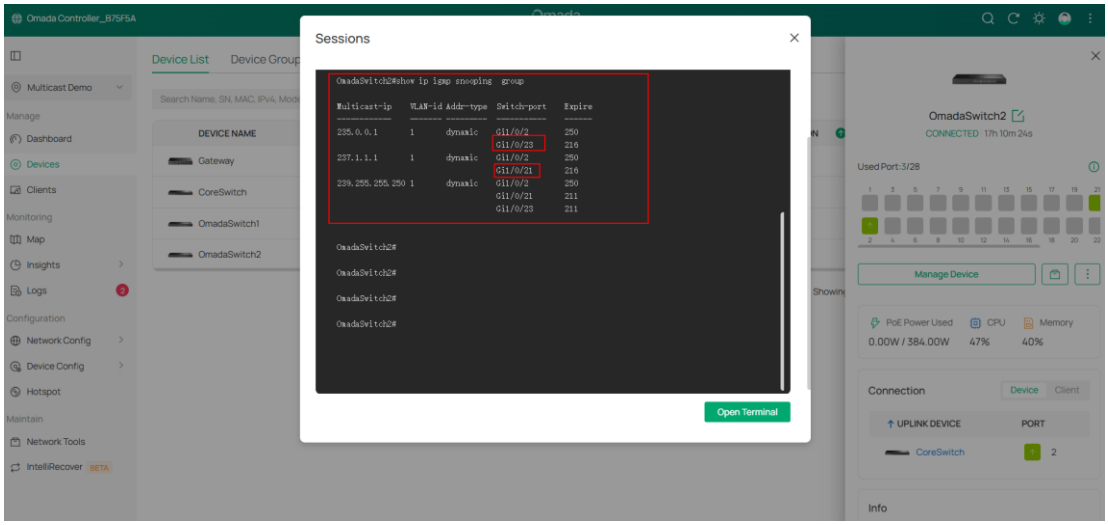


Receiver 2 packet capture shows multicast group data packets. The source address and destination port match the multicast source:

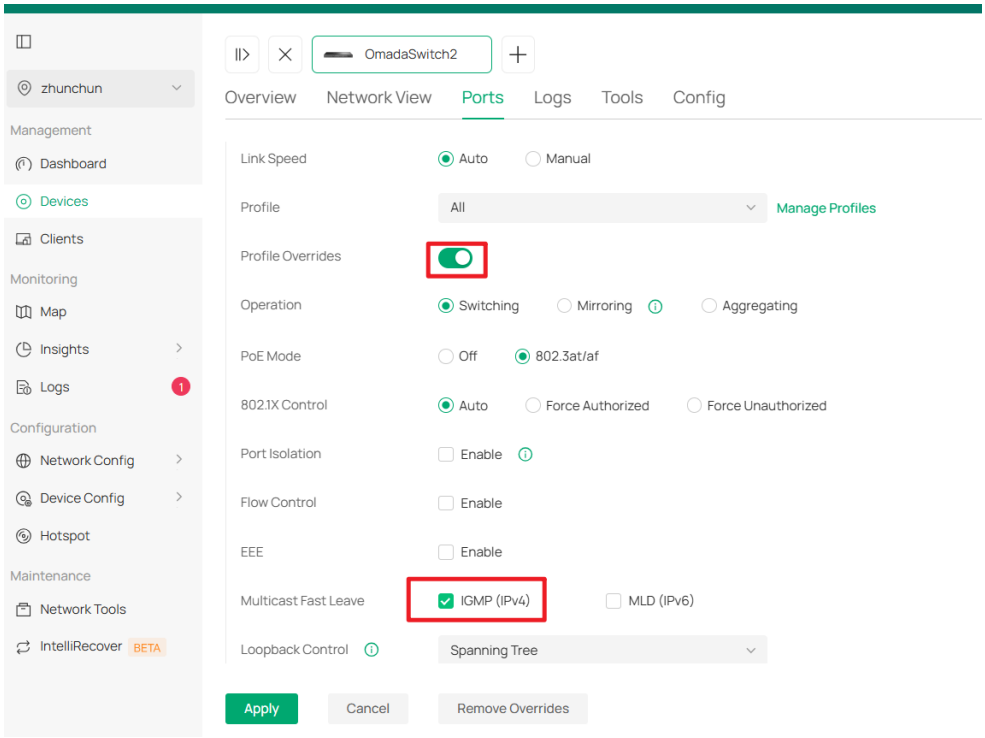
No.	Time	Source	Destination	Protocol	Length	Info
10	0.008297	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
11	0.016778	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
12	0.017100	192.168.0.103	237.1.1.1	MPEG TS	1358	59457 → 1234 Len=1316
13	0.017229	192.168.0.103	237.1.1.1	MPEG 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

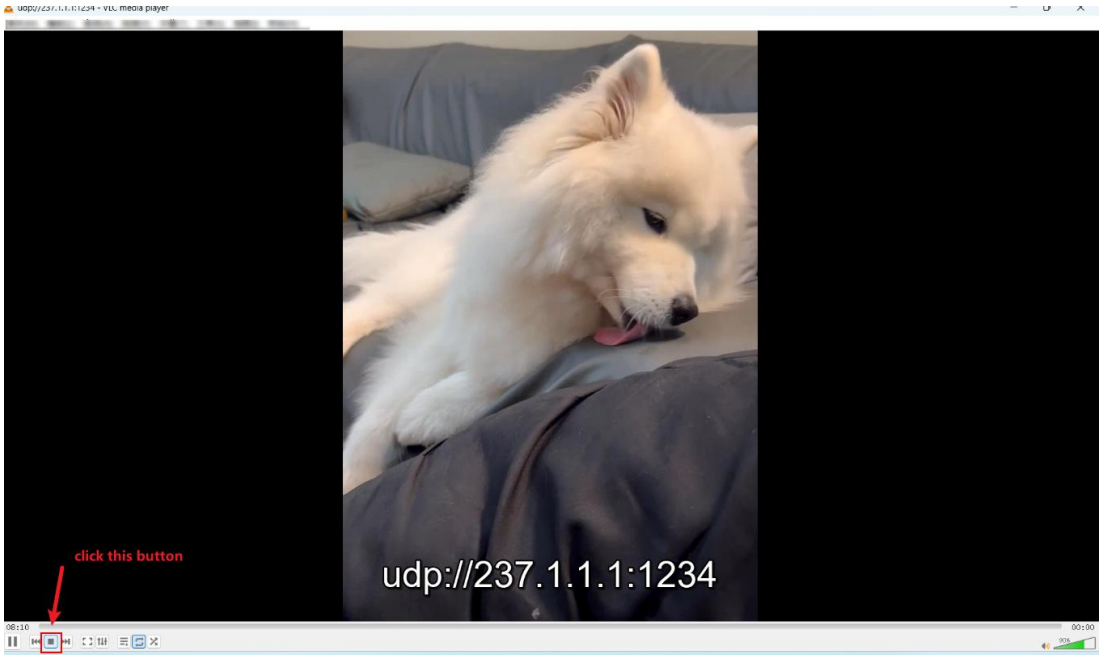
```
> Frame 1: 1358 bytes on wire (10864 bits), 1358 bytes captured (10864 bits) on interface \Device\NPF_{A8B17367-B912-4
> Ethernet II, Src: 58:11:22:0f:70:7e (58:11:22:0f:70:7e), Dst: IPv4mcast_01:01:01 (01:00:5e:01:01:01)
> Internet Protocol Version 4, Src: 192.168.0.103, Dst: 237.1.1.1
> User Datagram 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 2: Check the IGMP Snooping group status under Omada Switch 2: The ports connected to Receiver 1 and Receiver 2 have joined the corresponding multicast groups.

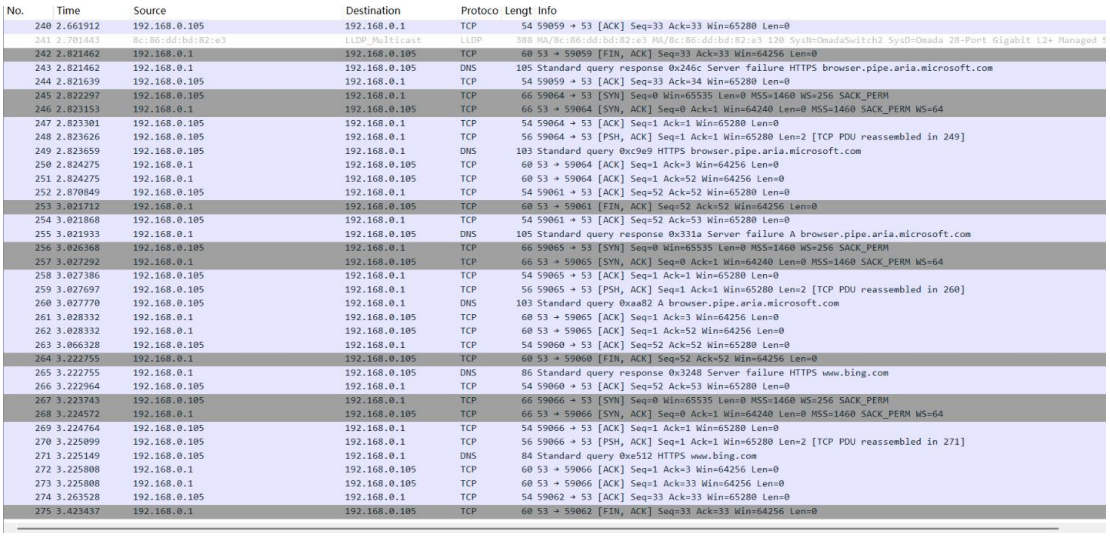


Step 3: Enable Fast Leave on the port connecting Receiver 2 to the switch. Receiver 2 clicks the stop button in the VLC (equivalent to sending a Leave message). Packet capture on Client 2 shows that no multicast video packets are received. Check the Omada Switch 2 IGMP Snooping multicast table: the entry for 237.1.1.1 is no longer present, confirming a successful Leave.



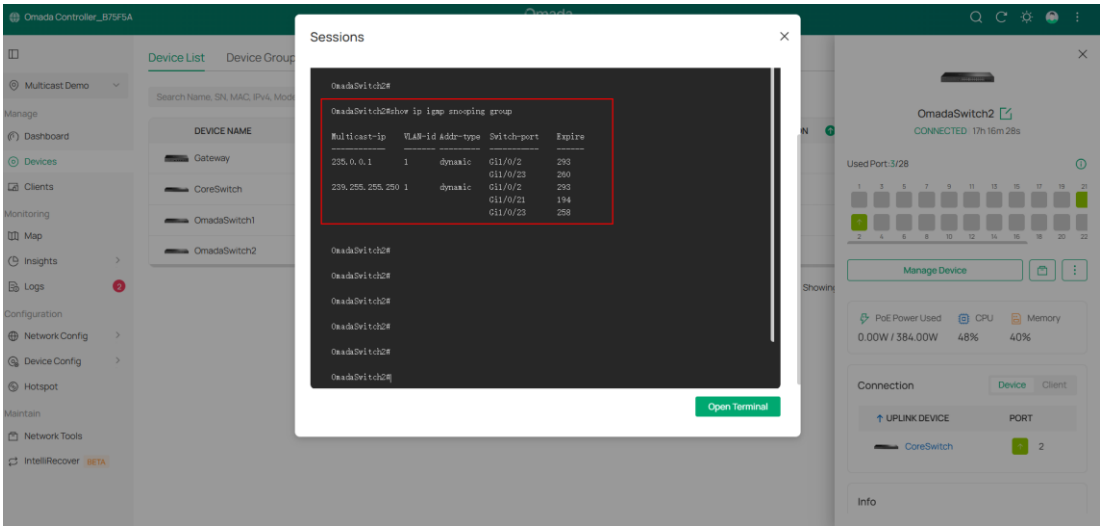


No multicast data packets detected:



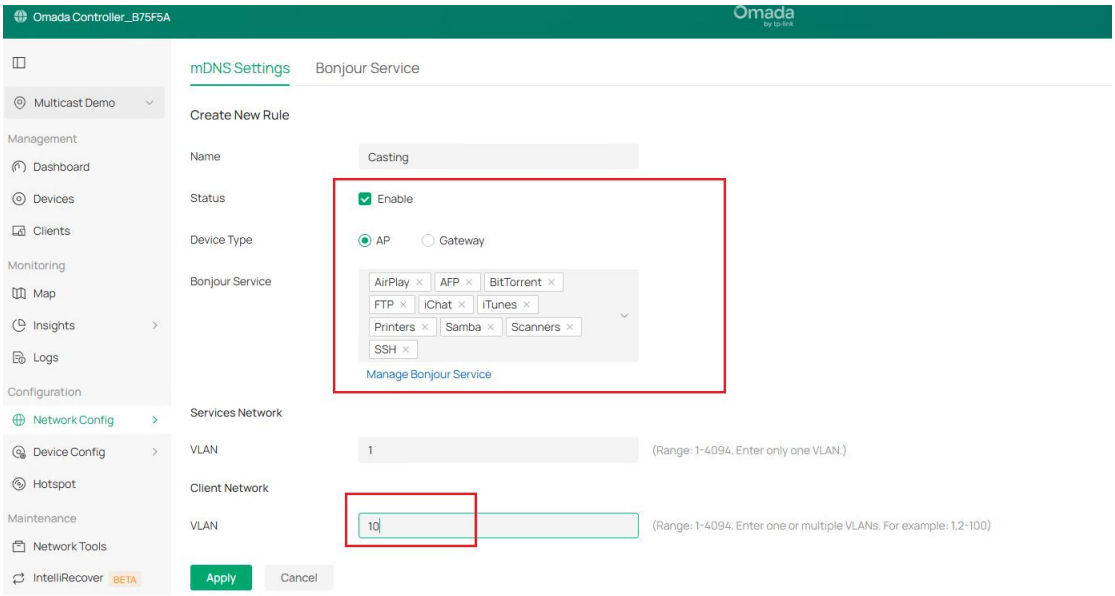
No.	Time	Source	Destination	Protoco	Lengt	Info
240	2.661912	192.168.0.105	192.168.0.1	TCP	54	59059 → 53 [ACK] Seq=33 Ack=33 Win=65280 Len=0
241	2.701443	8c:86:dd:bd:82:e3	LLDP_Multicast	LLDP	388	MA/8c:86:dd:bd:82:e3 MA/8c:86:dd:bd:82:e3 120 SysN=OmadaSwitch2 SysD=Omada 28-Port Gigabit L2+ Managed S
242	2.821462	192.168.0.1	192.168.0.105	TCP	60	53 → 59059 [FIN, ACK] Seq=33 Ack=33 Win=64256 Len=0
243	2.821462	192.168.0.1	192.168.0.105	DNS	105	Standard query response 0x246c Server failure HTTPS browser.pipe.aria.microsoft.com
244	2.821639	192.168.0.105	192.168.0.1	TCP	54	59059 → 53 [ACK] Seq=33 Ack=34 Win=65280 Len=0
245	2.822297	192.168.0.105	192.168.0.1	TCP	66	59064 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
246	2.823153	192.168.0.1	192.168.0.105	TCP	66	53 → 59064 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=64
247	2.823301	192.168.0.105	192.168.0.1	TCP	54	59064 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
248	2.823626	192.168.0.105	192.168.0.1	TCP	56	59064 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 249]
249	2.823659	192.168.0.105	192.168.0.1	DNS	103	Standard query 0xc9e9 HTTPS browser.pipe.aria.microsoft.com
250	2.824275	192.168.0.1	192.168.0.105	TCP	60	53 → 59064 [ACK] Seq=1 Ack=3 Win=64256 Len=0
251	2.824275	192.168.0.1	192.168.0.105	TCP	60	53 → 59064 [ACK] Seq=1 Ack=52 Win=64256 Len=0
252	2.870849	192.168.0.105	192.168.0.1	TCP	54	59061 → 53 [ACK] Seq=52 Ack=52 Win=65280 Len=0
253	3.021712	192.168.0.1	192.168.0.105	TCP	60	53 → 59061 [FIN, ACK] Seq=52 Ack=52 Win=64256 Len=0
254	3.021868	192.168.0.105	192.168.0.1	TCP	54	59061 → 53 [ACK] Seq=52 Ack=53 Win=65280 Len=0
255	3.021933	192.168.0.1	192.168.0.105	DNS	105	Standard query response 0x331a Server failure A browser.pipe.aria.microsoft.com
256	3.026368	192.168.0.105	192.168.0.1	TCP	66	59065 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
257	3.027292	192.168.0.1	192.168.0.105	TCP	66	53 → 59065 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=64
258	3.027386	192.168.0.105	192.168.0.1	TCP	54	59065 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
259	3.027697	192.168.0.105	192.168.0.1	TCP	56	59065 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 260]
260	3.027770	192.168.0.105	192.168.0.1	DNS	103	Standard query 0xaa82 A browser.pipe.aria.microsoft.com
261	3.028332	192.168.0.1	192.168.0.105	TCP	60	53 → 59065 [ACK] Seq=1 Ack=3 Win=64256 Len=0
262	3.028332	192.168.0.1	192.168.0.105	TCP	60	53 → 59065 [ACK] Seq=1 Ack=52 Win=64256 Len=0
263	3.066328	192.168.0.105	192.168.0.1	TCP	54	59060 → 53 [ACK] Seq=52 Ack=52 Win=65280 Len=0
264	3.222755	192.168.0.1	192.168.0.105	TCP	60	53 → 59060 [FIN, ACK] Seq=52 Ack=52 Win=64256 Len=0
265	3.222755	192.168.0.1	192.168.0.105	DNS	86	Standard query response 0x3248 Server failure HTTPS www.bing.com
266	3.222964	192.168.0.105	192.168.0.1	TCP	54	59060 → 53 [ACK] Seq=52 Ack=53 Win=65280 Len=0
267	3.223743	192.168.0.105	192.168.0.1	TCP	66	59066 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
268	3.224572	192.168.0.1	192.168.0.105	TCP	66	53 → 59066 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=64
269	3.224764	192.168.0.105	192.168.0.1	TCP	54	59066 → 53 [ACK] Seq=1 Ack=1 Win=65280 Len=0
270	3.225099	192.168.0.105	192.168.0.1	TCP	56	59066 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=2 [TCP PDU reassembled in 271]
271	3.225149	192.168.0.105	192.168.0.1	DNS	84	Standard query 0xe512 HTTPS www.bing.com
272	3.225808	192.168.0.1	192.168.0.105	TCP	60	53 → 59066 [ACK] Seq=1 Ack=3 Win=64256 Len=0
273	3.225808	192.168.0.1	192.168.0.105	TCP	60	53 → 59066 [ACK] Seq=1 Ack=33 Win=64256 Len=0
274	3.263528	192.168.0.105	192.168.0.1	TCP	54	59062 → 53 [ACK] Seq=33 Ack=33 Win=65280 Len=0
275	3.423437	192.168.0.1	192.168.0.105	TCP	60	53 → 59062 [FIN, ACK] Seq=33 Ack=33 Win=64256 Len=0

Receiver 2 successfully left the group:



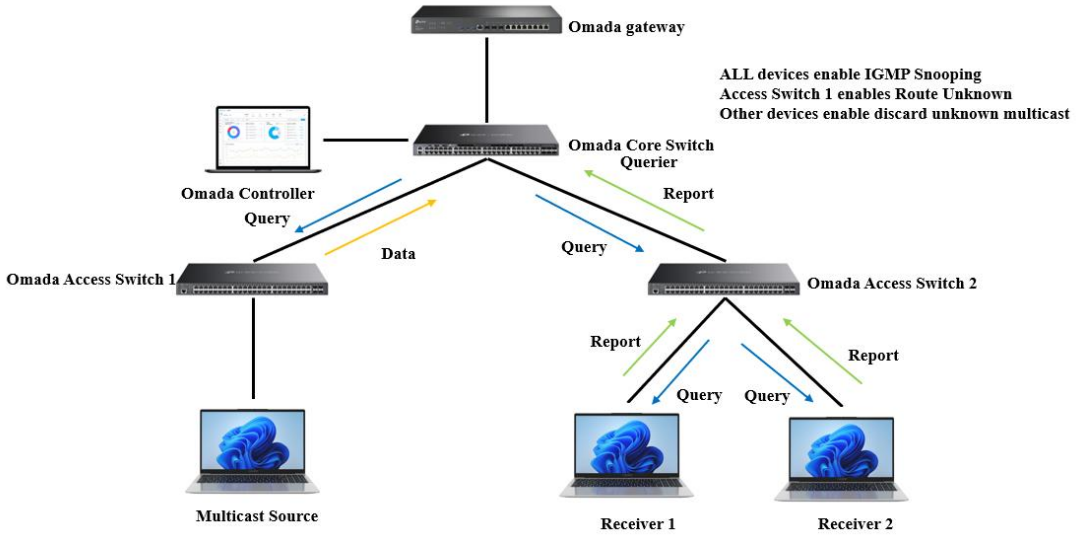
For screen casting, we currently support all 2-layer network screen casting. It is recommended that the client connected to the SSID and IPTV belong to the same network segment, and screen casting does not require external configuration.

If it is not on the same network segment as IPTV, such as connecting an EAP on Omada Access Switch 2, configure a PPSK SSID with VLAN 10. By configuring mDNS Service and Client VLAN on the gateway or EAP, it can achieve three-layer screen casting based on the mDNS discovery protocol. The configuration is as follows:



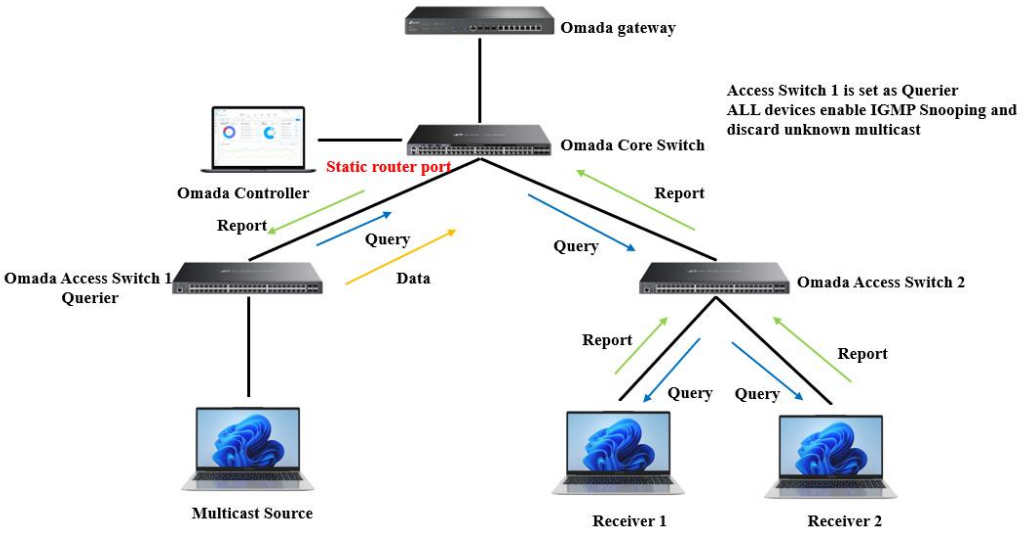
4.1.2 Solution 2

Solution 2 is the same as Solution 1 in terms of networking, with slight differences in configuration. The configuration is that the Omada Core Switch is set as the Querier and all devices enable IGMP Snooping. The switch connecting to the multicast source chooses Route Unknown for unknown multicast, while other devices choose Discard.



4.1.3 Solution 3

The configuration of Solution 3 is that the switch connecting to the multicast source is set as the Querier and all devices enable IGMP Snooping. All devices choose Discard for unknown multicast.



4.2 Recommended All-Optical Network IPTV Deployment Solution

4.2.1 Solution 1

4.2.1.1 Prerequisites

This configuration guide assumes that the devices are managed by the Omada Controller. Therefore, before performing the subsequent configuration steps, make sure the following requirements are met:

1. The recommended Omada Controller version is 6.0 or above.

2. Switch firmware must be upgraded to the latest version available on the official website. Note that some switches may not support the Querier function (for details, refer to the user guide for the corresponding model on the official website). We recommend using an Omada Smart/L2+/L3 switch as the Querier.

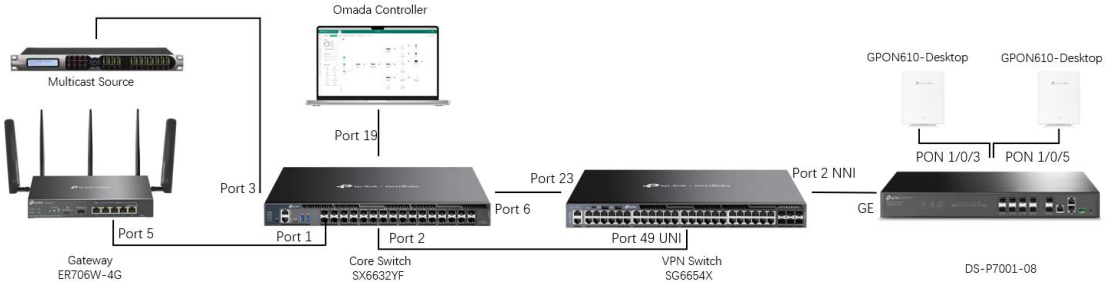
3. There are no specific functional requirements for the gateway. However, in real customer scenarios, ER8411 is commonly used. Other Omada gateway models may be used in this deployment solution.

4. For Omada EAPs, only GPON APs are used in real customer scenarios.

5. A VPN switch that supports QinQ is required.

6. This solution recommends configuring more than 30 VLANs.

4.2.1.2 Topology



This topology applies to most all-optical network scenarios. Two links are built between the core switch and the VPN switch: one for management and the other for service traffic. The following briefly explains why this design is required:

In hotel and MDU scenarios, PPSK is typically used for wireless services. If many VLANs are configured (more than 30), limitations may apply to OLT PON ports. Therefore, a QinQ networking approach is used. QinQ is configured on both the OLT and the VPN switch so that wireless traffic from different VLANs is tagged with the same outer VLAN tag. Since the OLT and VPN switch process only a single VLAN tag by default in this case, wireless traffic from different VLANs is treated as the same VLAN (i.e., the outer tag) on both the VPN switch and the OLT. As a result, the VLAN limitation on the OLT PON port no longer applies.

4.2.1.3 Configuration Steps

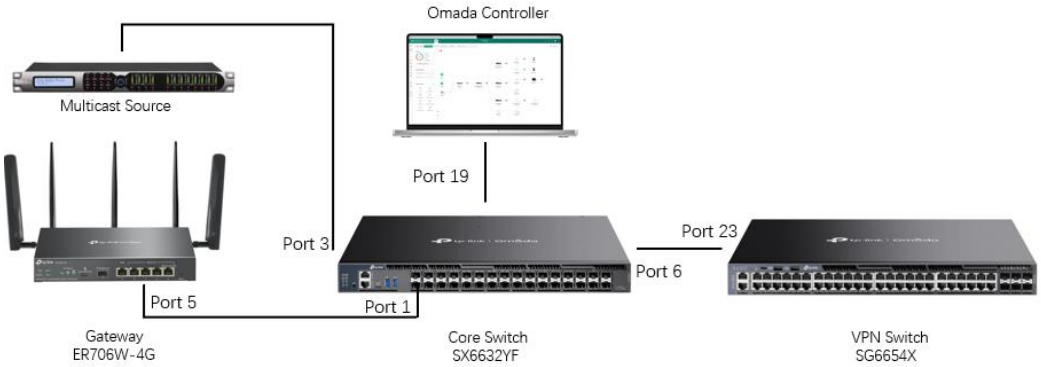
The Management VLAN on the VPN switch is VLAN 200. The Management VLAN for the other devices is VLAN 1. The VLAN for the multicast source and IPTV is VLAN 227. The VLANs for the PPSK service are VLAN 10 and VLAN 11.

Step 1: Construct the topology, configure relevant VLANs, and change the management address and VLAN of VPN SW.

To realize the configuration in the above figure, configure the OLT and switch respectively.

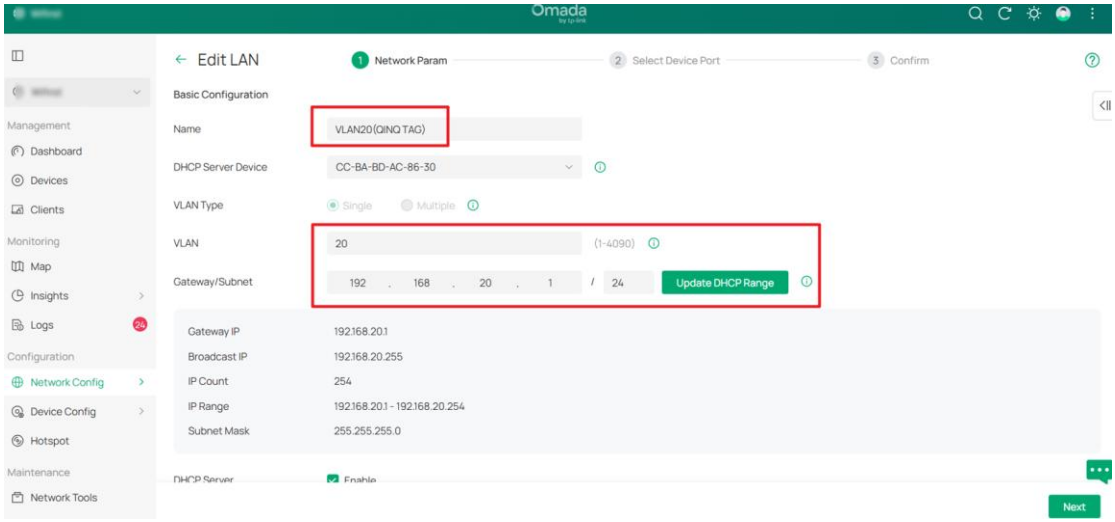
First, establish the management link between the VPN Switch and Controller. The topology is as follows:

Gateway ER706W-4G is connected to Port 1 of Core Switch SX6632YF v1.0 through LAN Port 5, and SX6632YF is connected to Port 23 of VPN Switch SG6654X through Port 6.

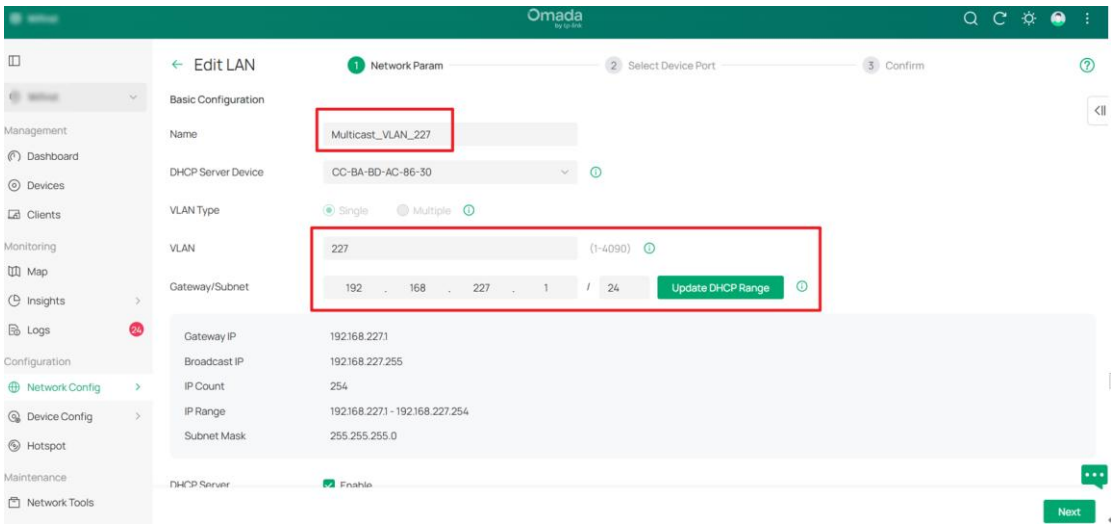


After connecting the topology, go to **Settings > Wired Networks > LAN > Networks** and create VLAN Interface 20 and 227.

Create VLAN 20:

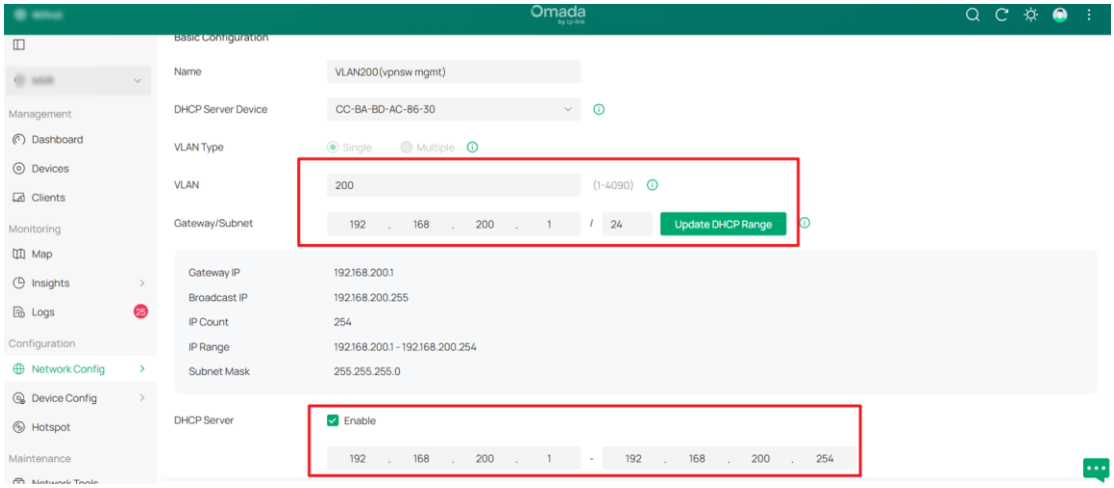


Create VLAN 227:

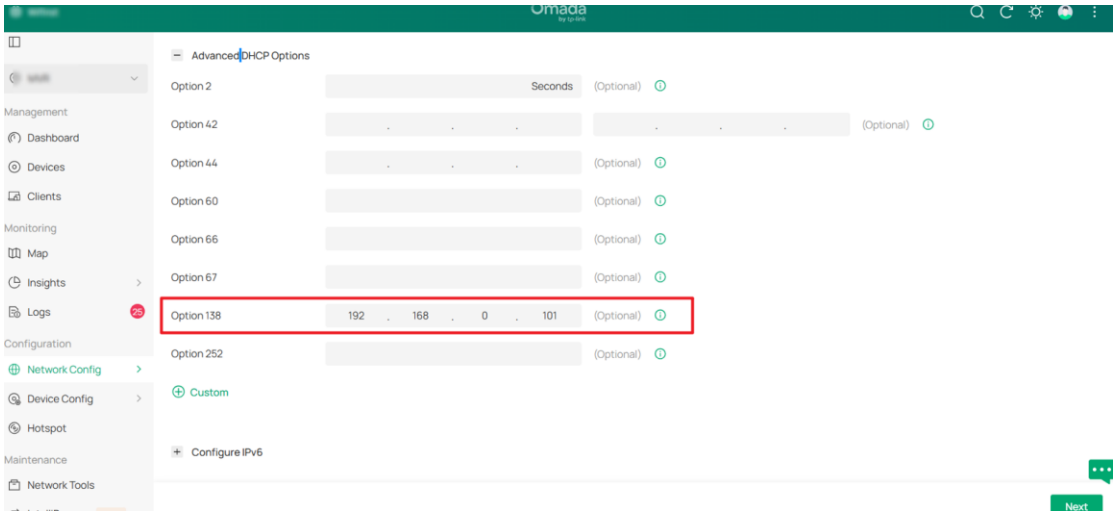


Go to **Settings > Wired Networks > LAN > Networks** and create VLAN Interface 200 for

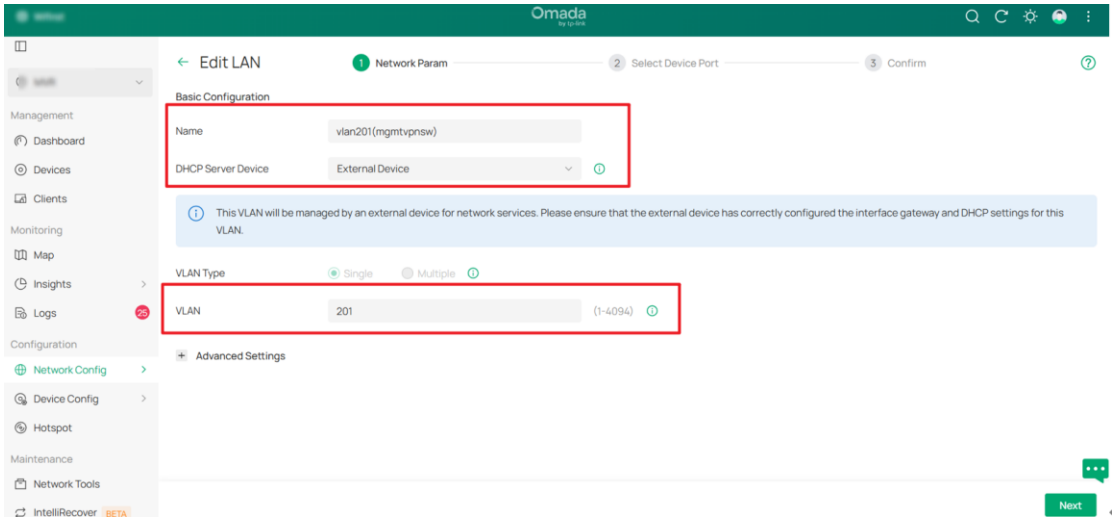
managing the VPN Switch.



After the configuration is complete, the VPN Switch will be managed by the Controller through the L3 network, so you need to configure DHCP Option 138 to the IP address of the Controller.



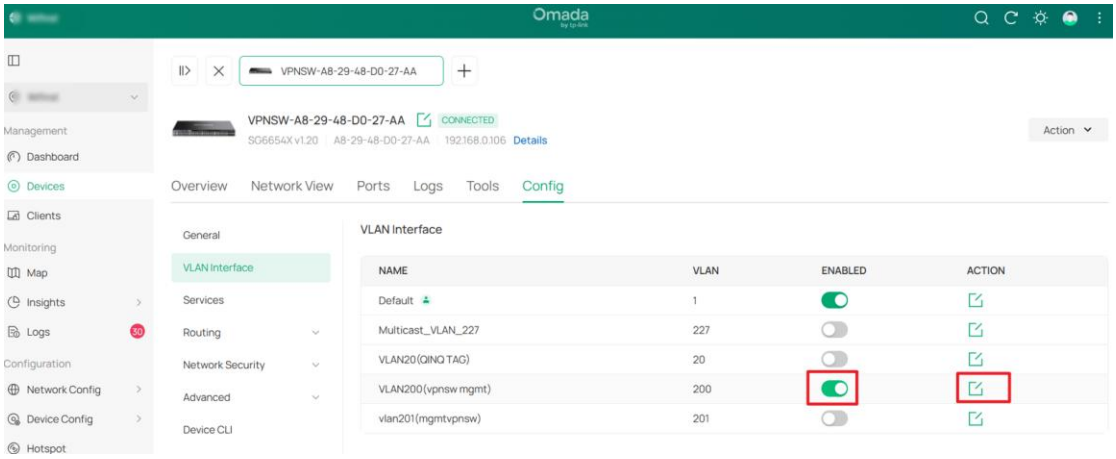
Configure VLAN 201 for VPN Switch management.



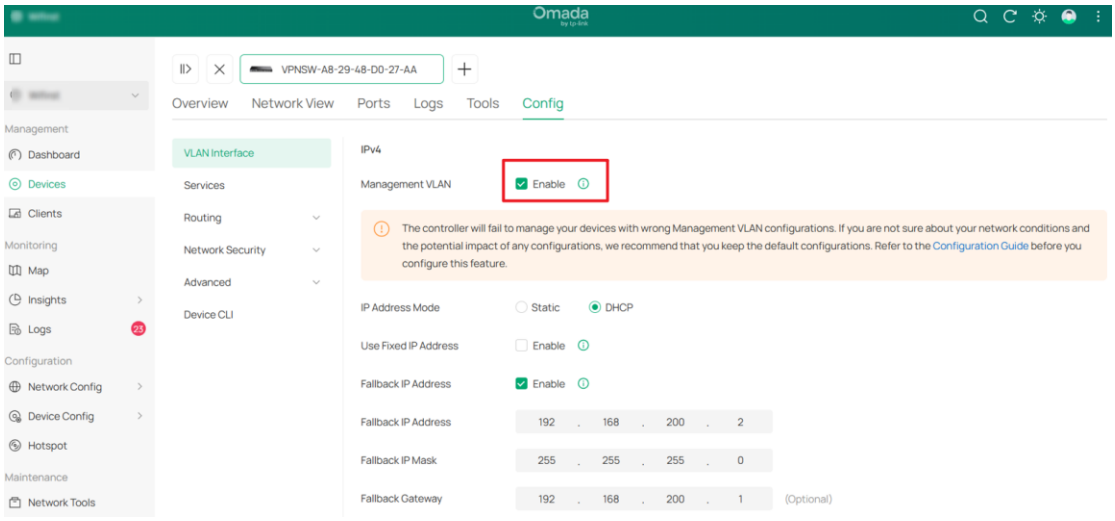
Configure the Management VLAN on the VPN Switch details page as follows:

First, go to **Config > VLAN Interface** and enable VLAN Interface 200.

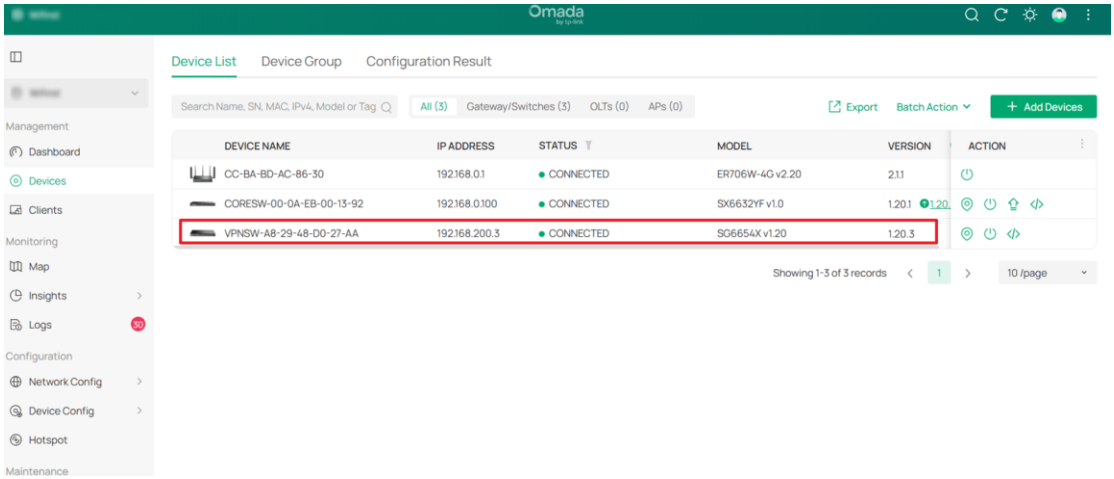
Click to edit VLAN Interface 200.



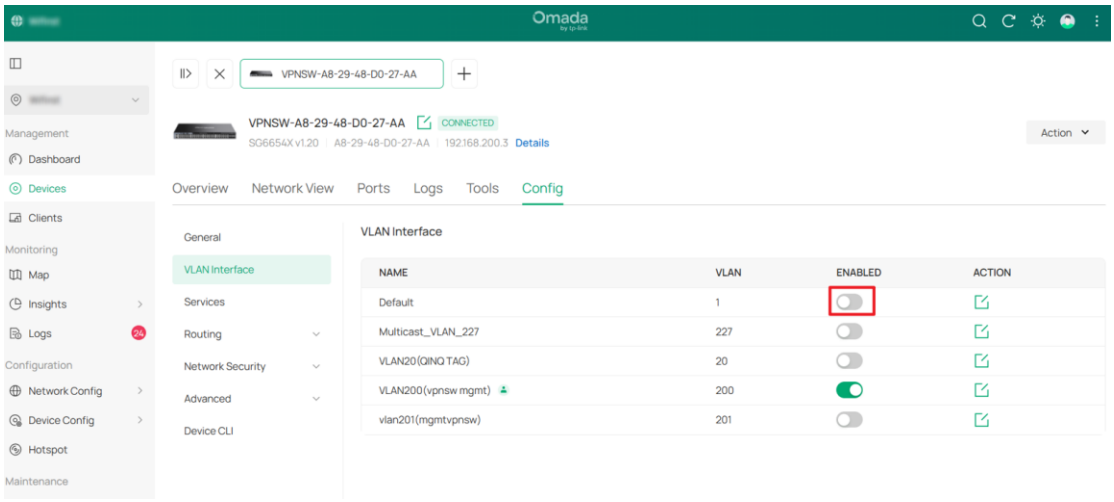
Enable **Management VLAN**, set **Fallback IP Address** to 192.168.200.2 (corresponding to Network Segment 200), and set **Fallback Gateway** to 192.168.200.1. Apply the settings.



Wait until the IP address of the VPN Switch changes to Network Segment 200 and remains in the **CONNECTED** state.

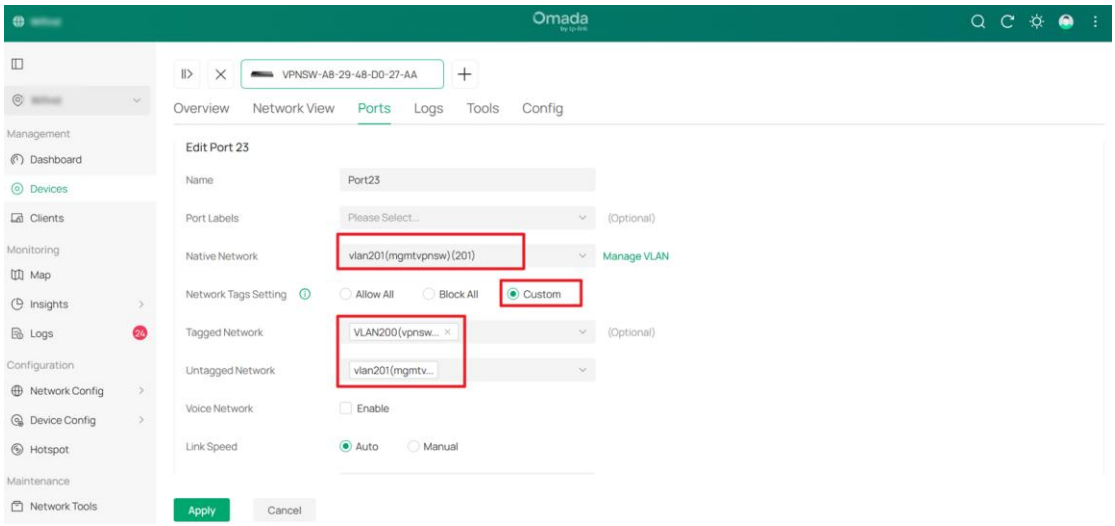


After switching the Management VLAN, turn off VLAN 1 in the VLAN interface on the VPN Switch details page.

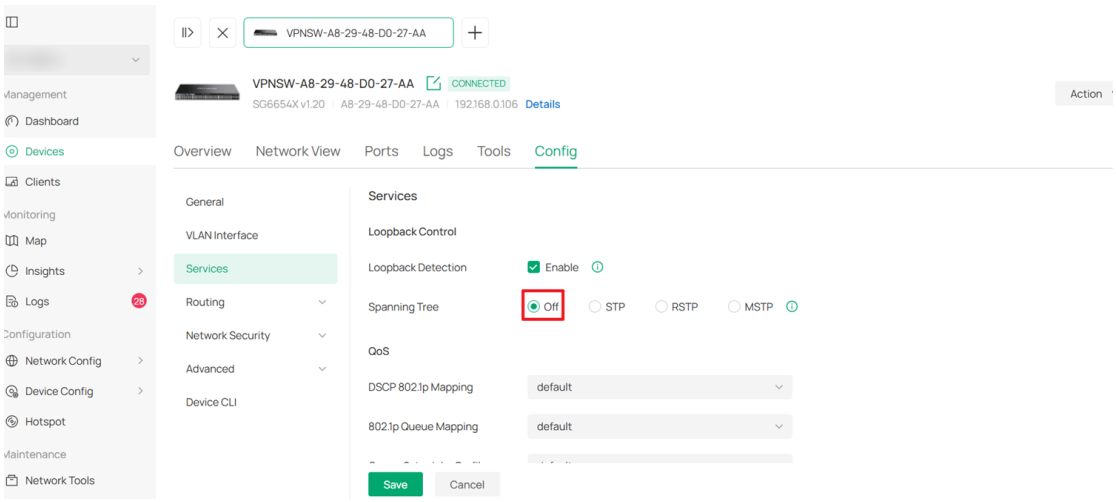


After VLAN 1 is turned off, the corresponding button will turn gray and the device will remain **CONNECTED**.

Edit Port 23 for the Controller to manage the VPN Switch through the Layer 3 network. Select VLAN Interface 200 for Tagged Networks, and select VLAN Interface 201 for the Native Network. The Native / Untagged Network (VLAN 201) must differ from the switch's MGMT VLAN (VLAN 200) and from any other VLAN in use. VLAN 201 is just for Port 23.



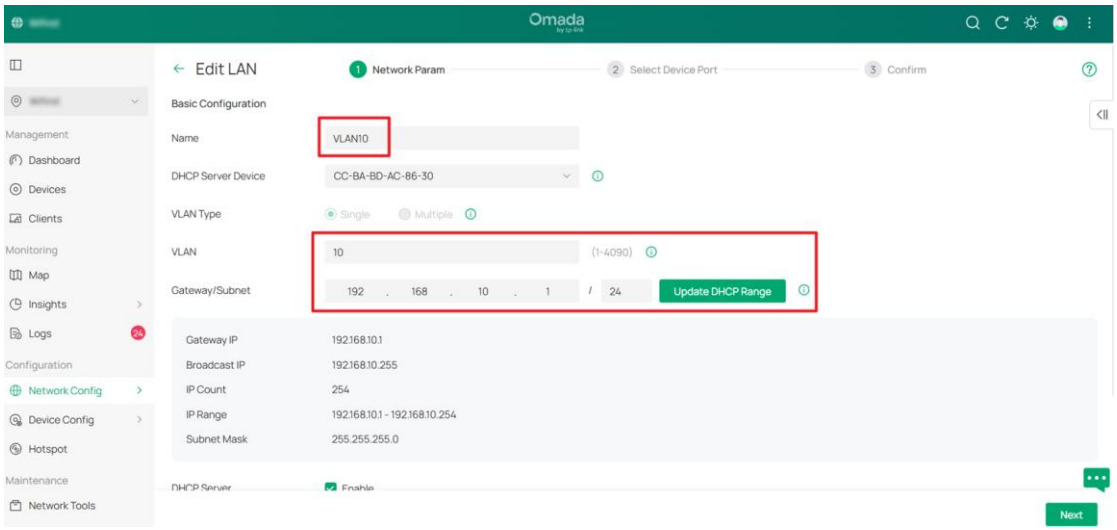
Then, close **Spanning Tree on VPN Switch**:



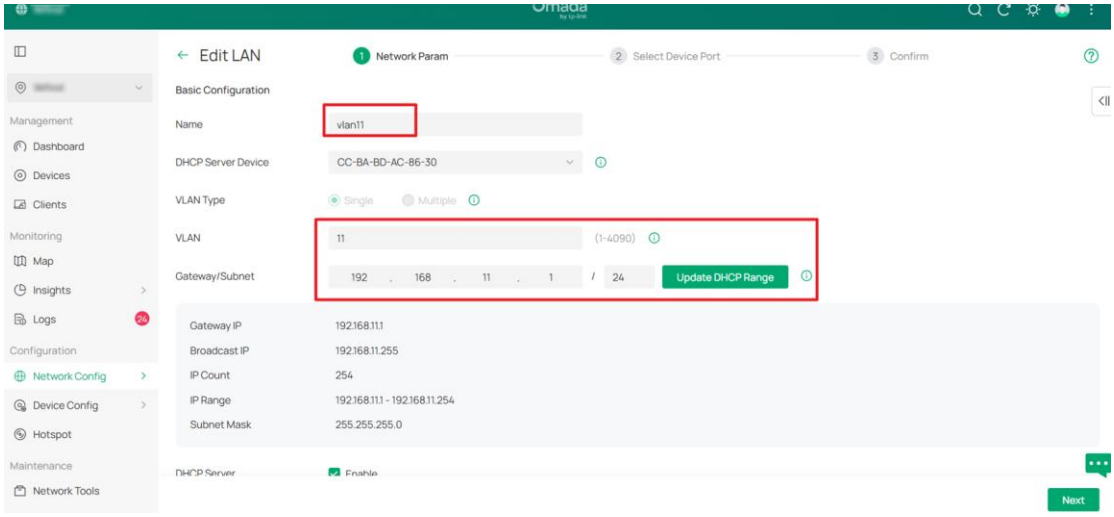
Now, you have successfully established the management link from the Controller to the MGMT VLAN 200 of the VPN Switch. Next, you can establish the VLAN VPN channel of the VPN Switch.

This section uses VLAN 10/VLAN 11 as the IPTV VLAN. First, create a new VLAN in **Site > Wired Networks > LAN > Networks** in VLAN 10/VLAN 11.

Create VLAN 10:



Create VLAN 11:



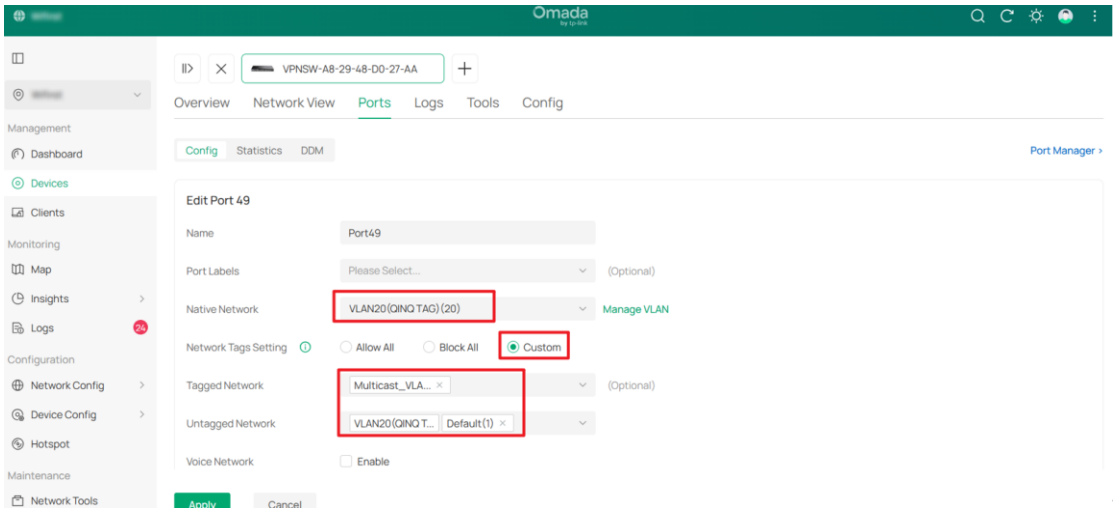
Step 2: Configure QinQ.

The next step is to configure the specific application port of the VLAN VPN.

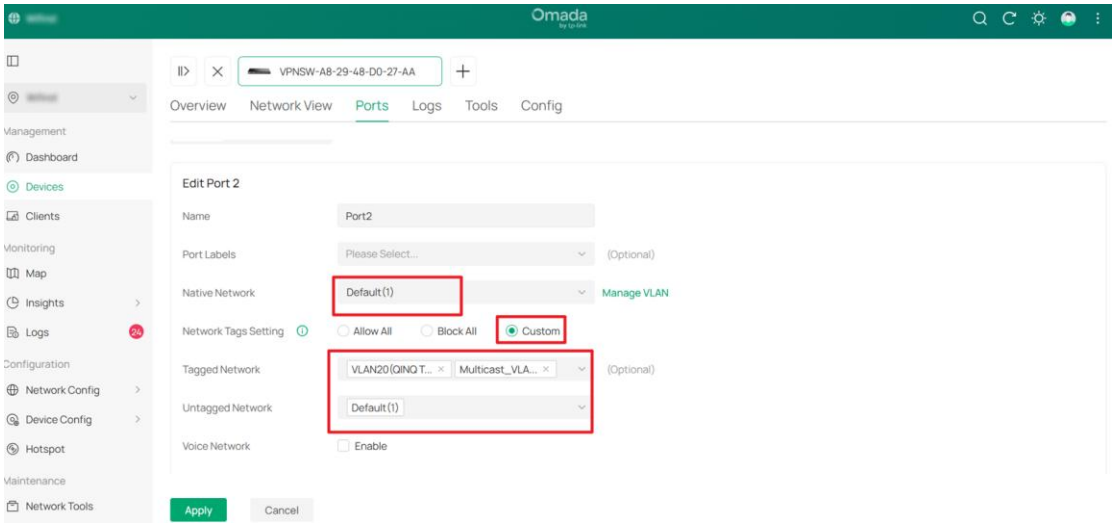
Use Port 49 of the VPN Switch as the uplink port (i.e., UNI Port). It will connect to the uplink core switch.

Use Port 2 of the VPN Switch as the downlink port (i.e., NNI Port). It will be downlinked to the OLT.

For VPN UNI, select VPN 20 for the Native Network, select VPN 20 and Default (1) for Untagged Networks and select VLAN 227 for Tagged Networks. Go to the **VPN Switch details page > Ports** to edit Port 49.



For VPN NNI, select Default (1) for the Native Network, select VLAN 227 and VPN 20 for Tagged Networks, and select Default (1) for Untagged Networks. Go to the **VPN Switch details page > Ports** to edit Port 2.

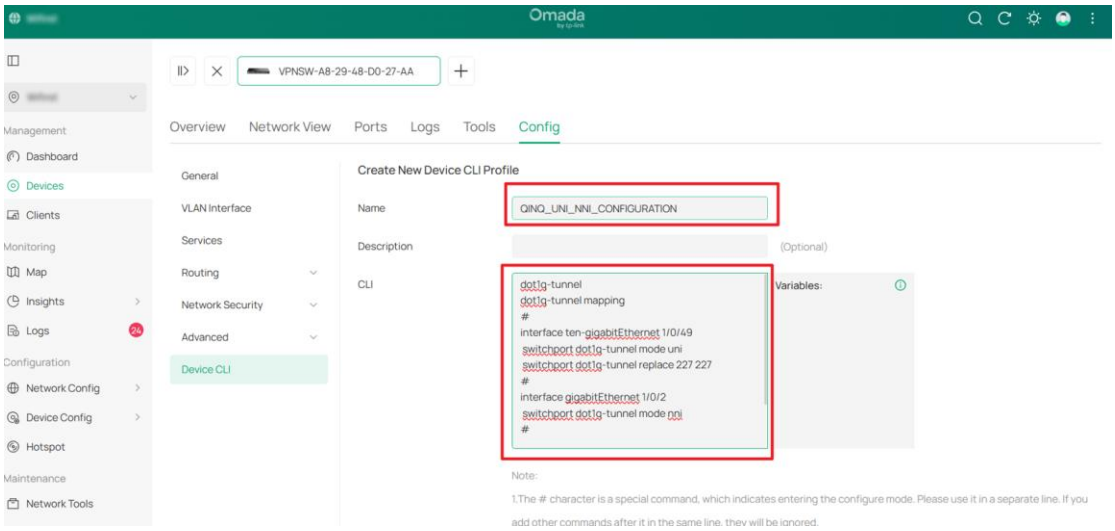


Finally, enable the global VPN VLAN function of the VPN Switch as follows:

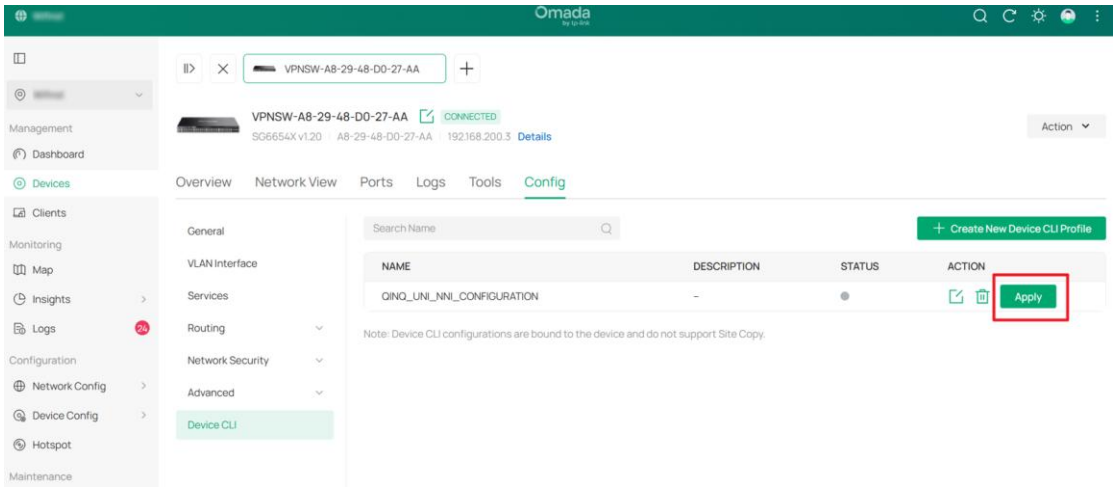
Go to **VPN Switch** to create a Device CLI profile.

Enter the following CLI command and click **Next**. The command is used to turn on the global VLAN-VPN QinQ function, set Port 49 as a UNI port, and set Port 2 as an NNI port. The "#" in the command is used to return to the configure view.

```
#
dot1q-tunnel
dot1q-tunnel mapping
#
interface ten-gigabitEthernet 1/0/49
 switchport dot1q-tunnel mode uni
 switchport dot1q-tunnel replace 227 227
#
interface gigabitEthernet 1/0/2
 switchport dot1q-tunnel mode nni
#
```

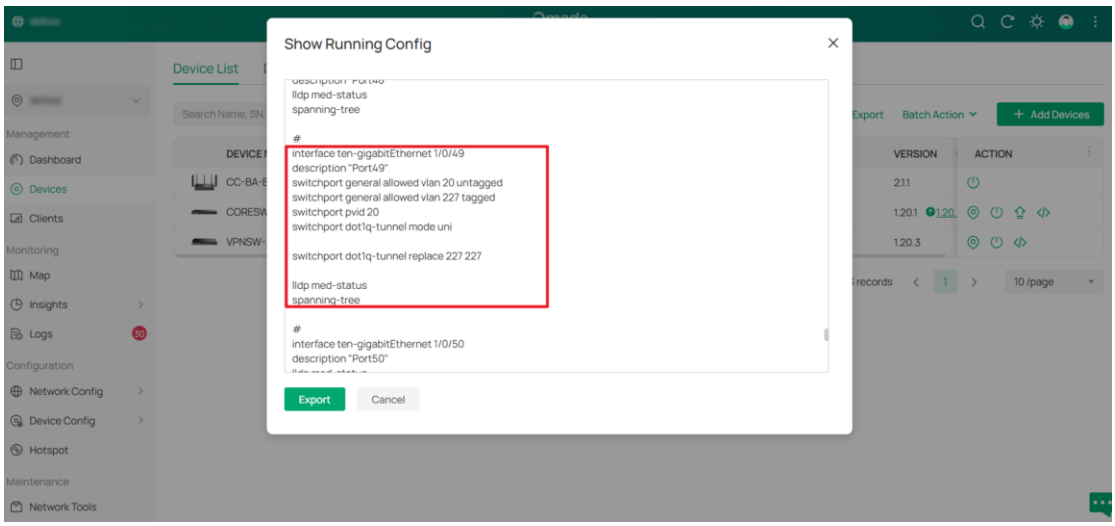


Apply the CLI profile.



You can also go to the **Device List** and click **Show Running Config** for the VPN SW to check its configuration.

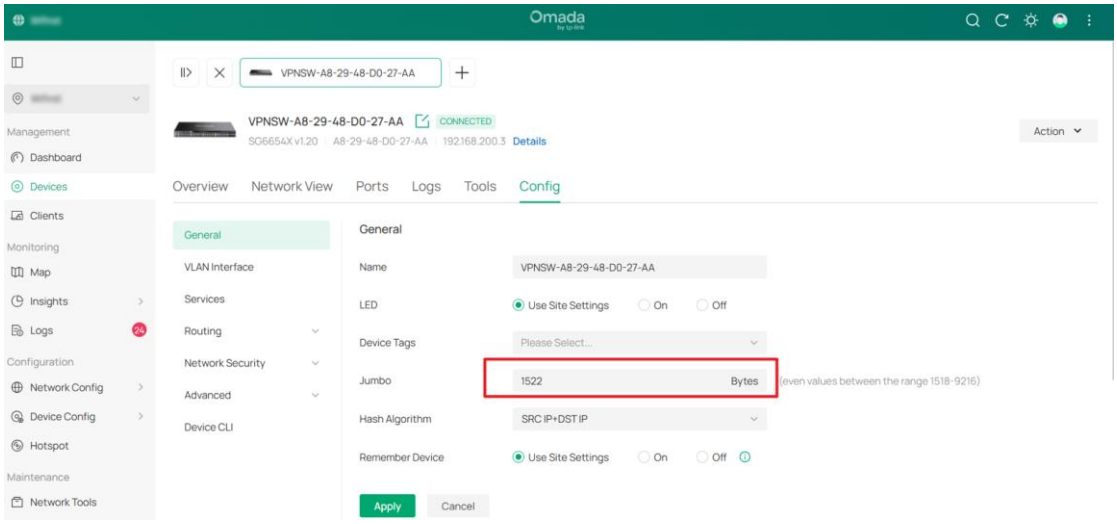
The displayed configuration of Port 49 UNI and Port 2 NNI is as shown in the figure, which means the configuration is complete.



Note: The VLAN VPN Switch processes double-tagged VLAN packets. During transmission, this can cause the Jumbo frame size to exceed 1518 bytes; for example, when a GPON AP adds a VLAN and VLAN tag packets require processing. In this case, increase the Jumbo frame size from 1518 to 1522 on both the OLT and the VLAN VPN Switch. A 1518-byte frame accommodates a single VLAN tag, while 1522 bytes support dual VLAN tags.

You can configure it on the **Device details page > Config > General**.

Change the Jumbo frame length to 1522.



Now you have completed configuring the VPN Switch and can proceed to configuring the OLT.

Step 3: Change the Management VLAN of the OLT.

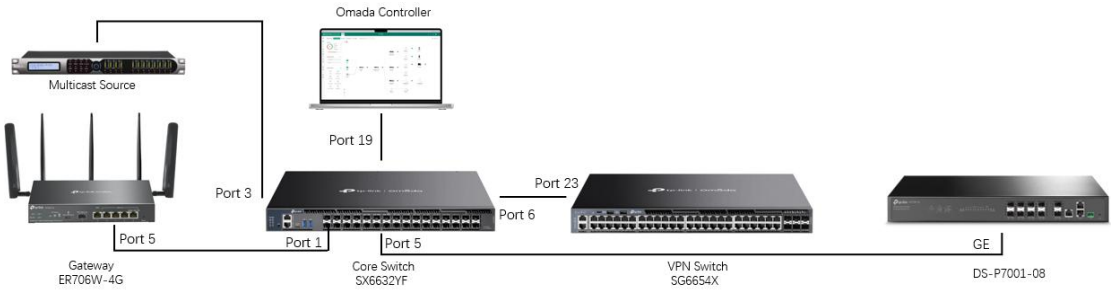
In order to cooperate with the VPN Switch to establish a dual-layer VLAN path for VLAN 20, the OLT needs to be connected to the uplink core switch of the VPN Switch first. The VLAN 20 Interface and the VLAN 20 MGMT Interface need to be configured on the OLT's

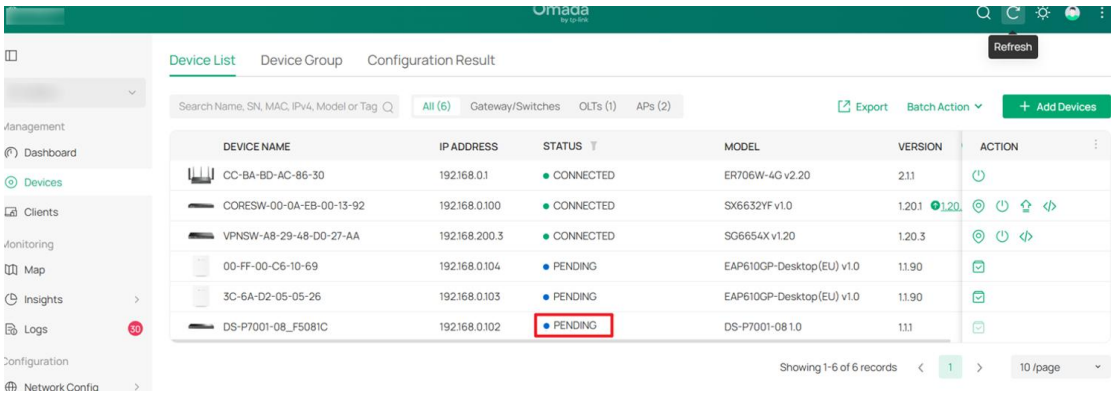
webpage. In this way, the OLT establishes communication with the VPN Switch through the VLAN 20 Interface.

The topology is as follows:

Gateway ER706W-4G is connected to Port 1 of Core Switch SX6632YF through the LAN port, and SX6632YF is connected to Port 23 of VPN Switch SG6654X through Port 6.

SX6632YF is connected to the GE port of the OLT through Port 5.





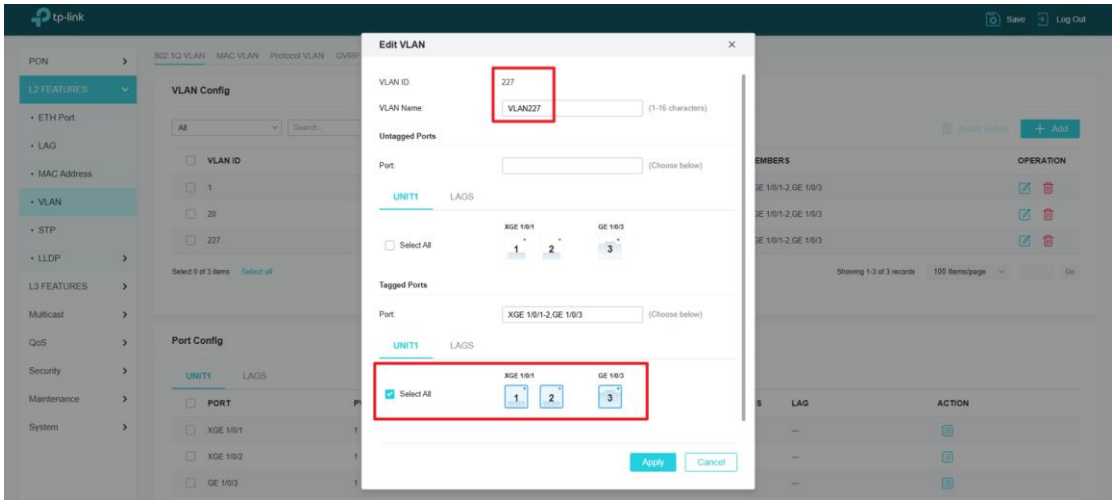
Since the Omada management of some functions used in this part is still being adapted, this section configures the functions on the OLT's web page.

Since the current Controller does not support some OLT configuration items, we will configure the following OLT-related configurations in Standalone mode. Access the IP address of the OLT and log in. The initial username and password are **admin/admin**.

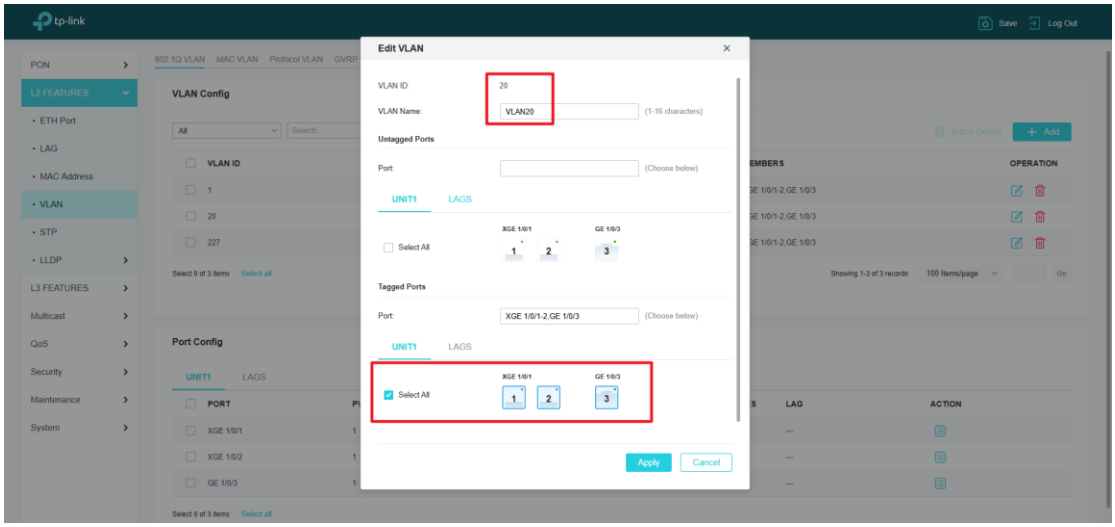
Change the password. The OLT will be adopted and managed by the Controller subsequently.

Go to the **L2 Feature > VLAN** page, create VLAN 227 and VLAN 20, and select the uplink port in **Tagged Ports**. VLAN 227 is the multicast VLAN, and VLAN 20 is the outer VLAN of the VLAN VPN.

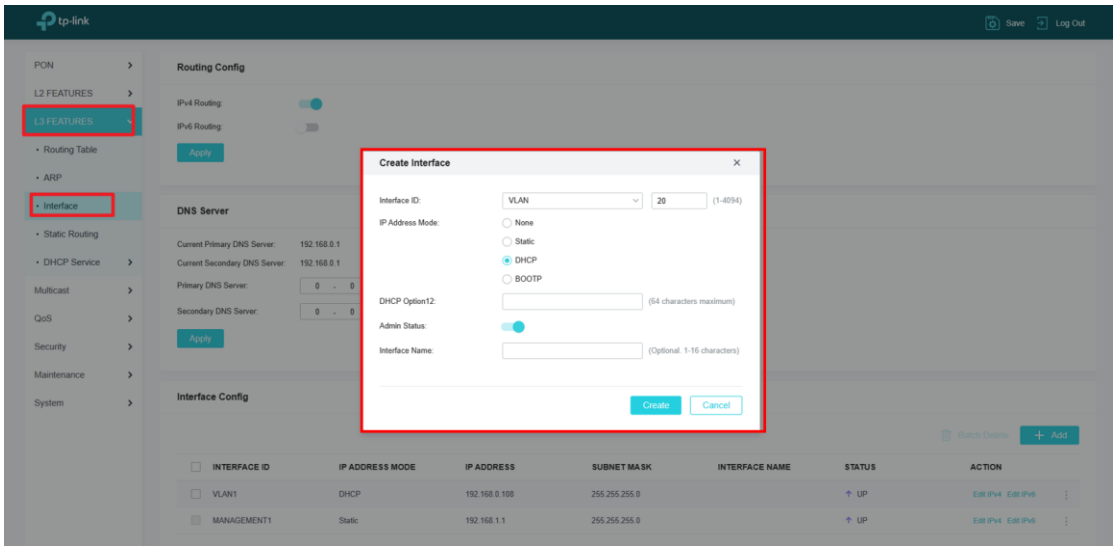
Set **VLAN ID** to 227, and in **Tagged Ports** select the uplink port.



Set **VLAN ID** to 20, and in **Tagged Ports** select the uplink port.



Go to **L3 FEATURES > Interface**. Add the VLAN 20 Interface for VPN VLAN transmission, and change the **IP Address Mode** to DHCP.



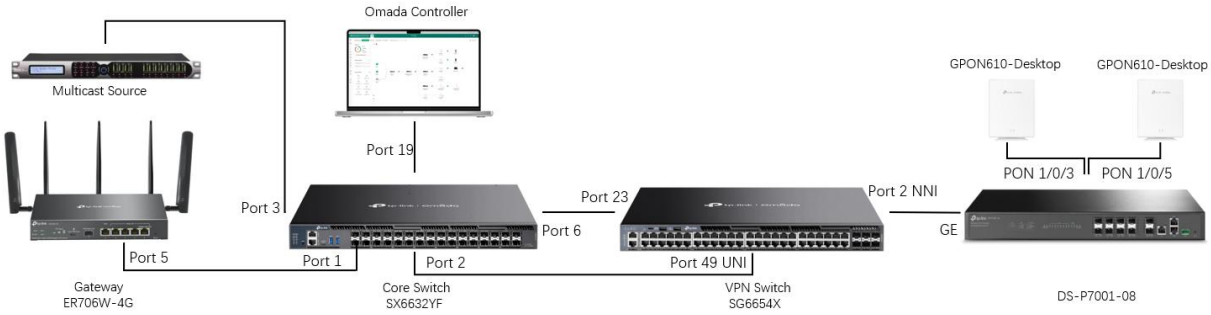
Step 4: Configure QinQ on the OLT.

Now you have set up the channel for the OLT to cooperate with VPN VLAN 20. You can connect the OLT to the NNI port (Port 2) of the VPN Switch and connect another line from the UNI port (Port 49) of the VPN Switch to the uplink core switch.

The topology is as follows:

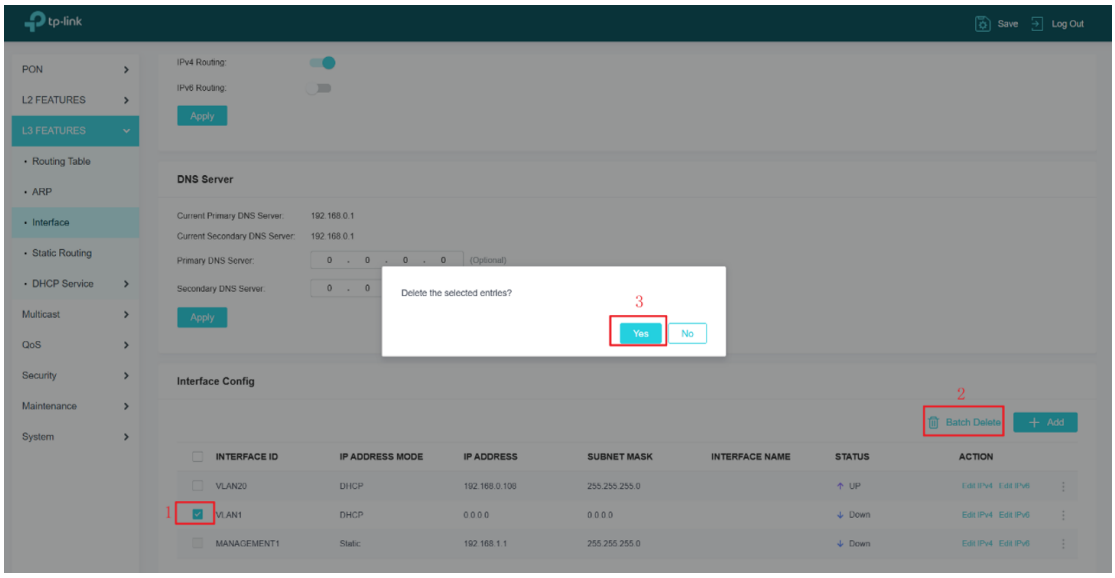
Gateway ER706W-4G is connected to Port 1 of Core Switch SX6632Y through the LAN port, and SX6632Y is connected to Port 23 of VPN Switch SG6654X through Port 6.

SX6632Y is connected to Port 49 UNI of VPN Switch SG6654 through Port 2, VPN Switch SG6654X is connected to the GE port of the OLT through Port 2 NNI, and the OLT PON3 and PON5 ports are connected to the ONU through the OLT optical module.

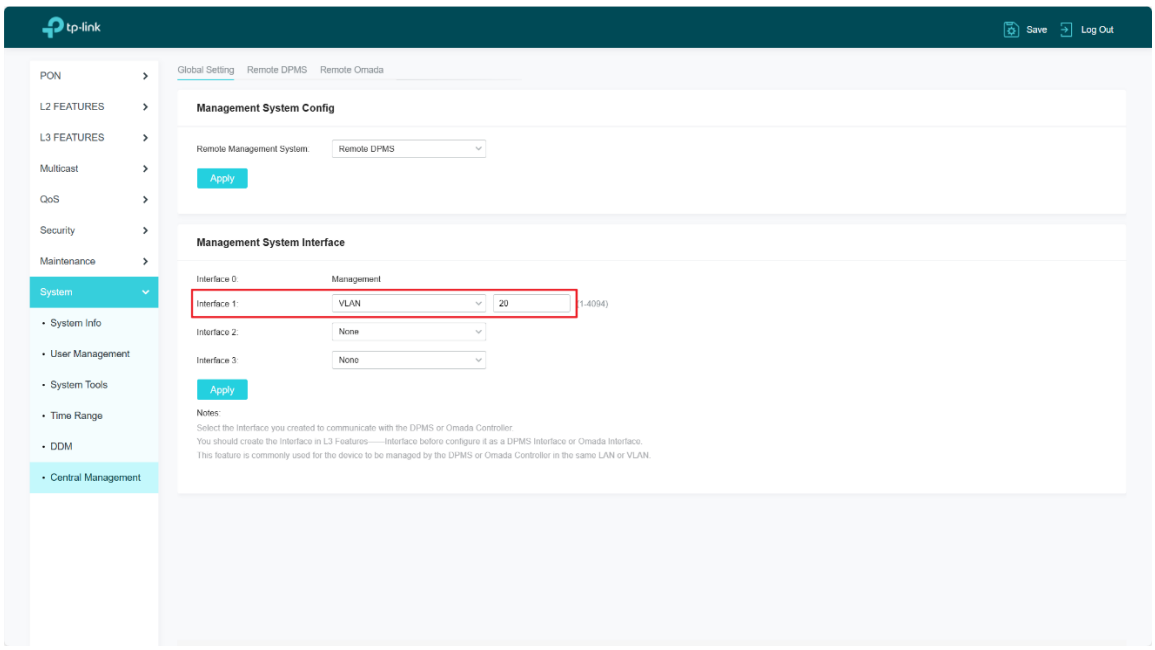


Under this topology, the VLAN 1 interface of the OLT will be unable to obtain an IP, while the VLAN 20 interface will obtain an IP from VLAN 1 of the ER706W-4G.

You can choose to delete the VLAN 1 interface.



Go to **System > Central Management**. Change the Management System Interface (VLAN 20) for VPN VLAN transmission.

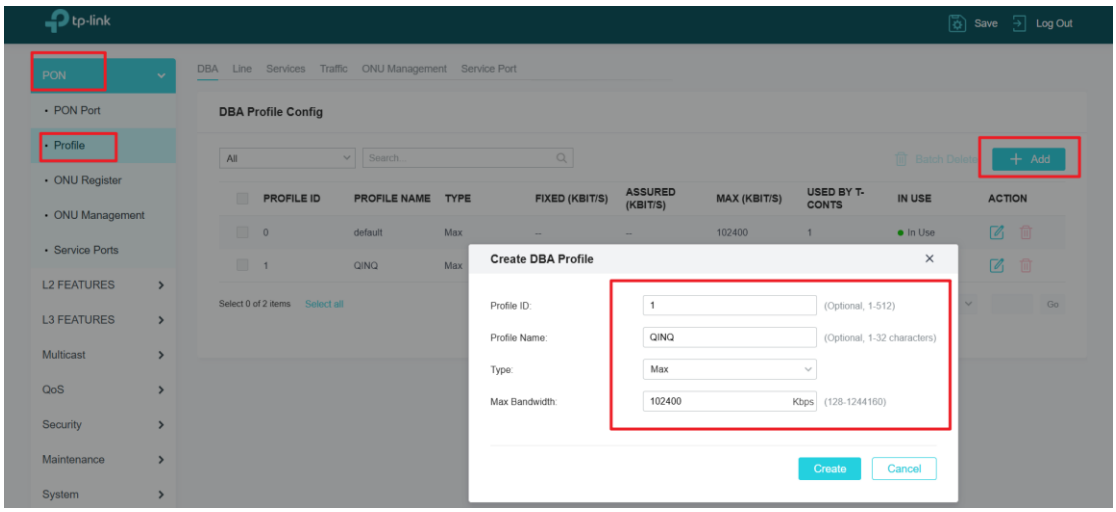


We recommend completing the relevant VLAN configuration of the OLT before adopting the GPON AP.

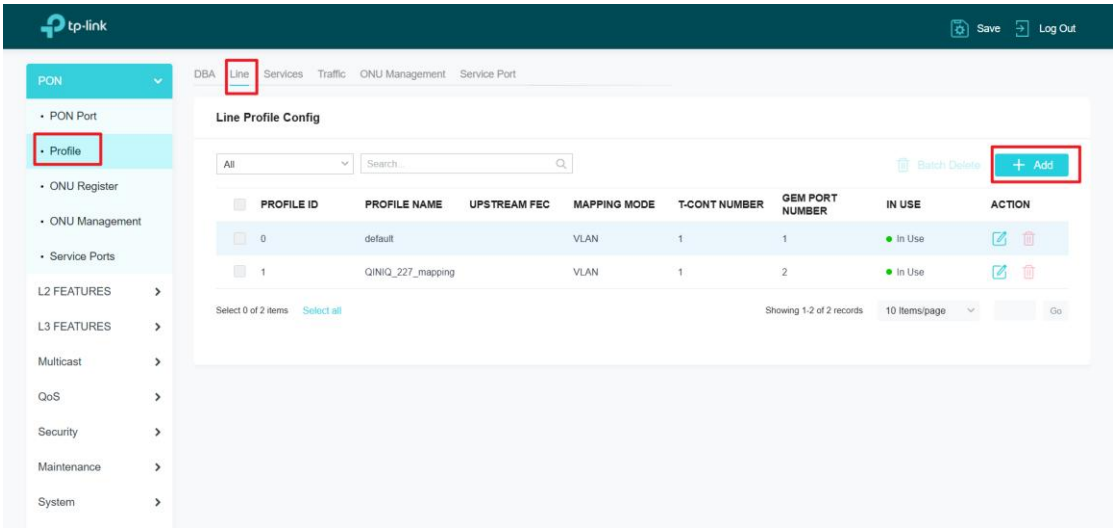
First, go to **OLT Settings** to configure the line profile and service port.

(Optional) Go to **OLT Settings > PON > Profile > DBA** to create a DBA profile for the GPON AP's bandwidth allocation.

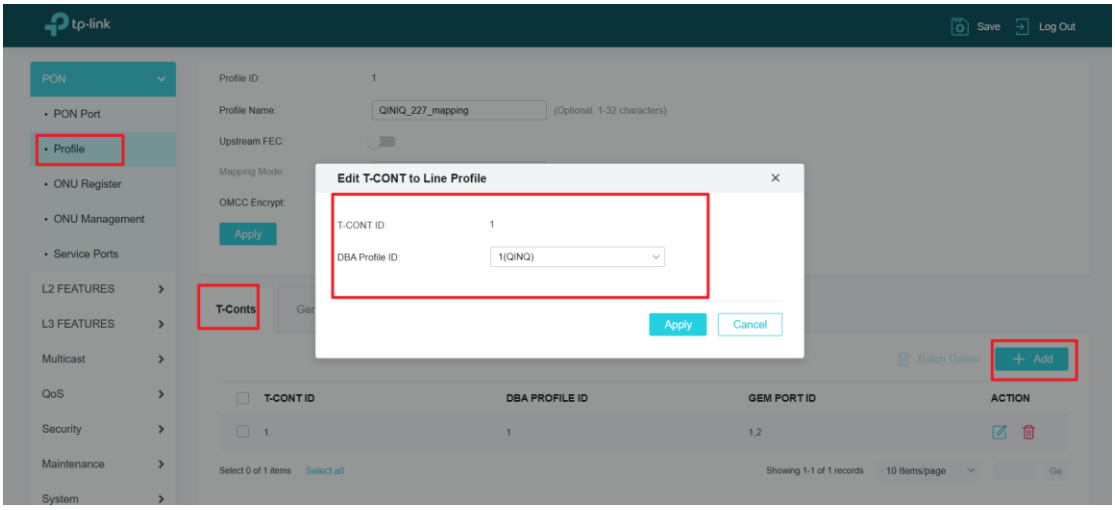
DBA (Dynamic Bandwidth Allocation) improves the efficiency of GPON upstream bandwidth by dynamically adjusting the bandwidth among the ONUs. DBA profiles are applied to T-CONTs, which are created in a line profile, to determine the desired bandwidth allocation for certain GPON lines.



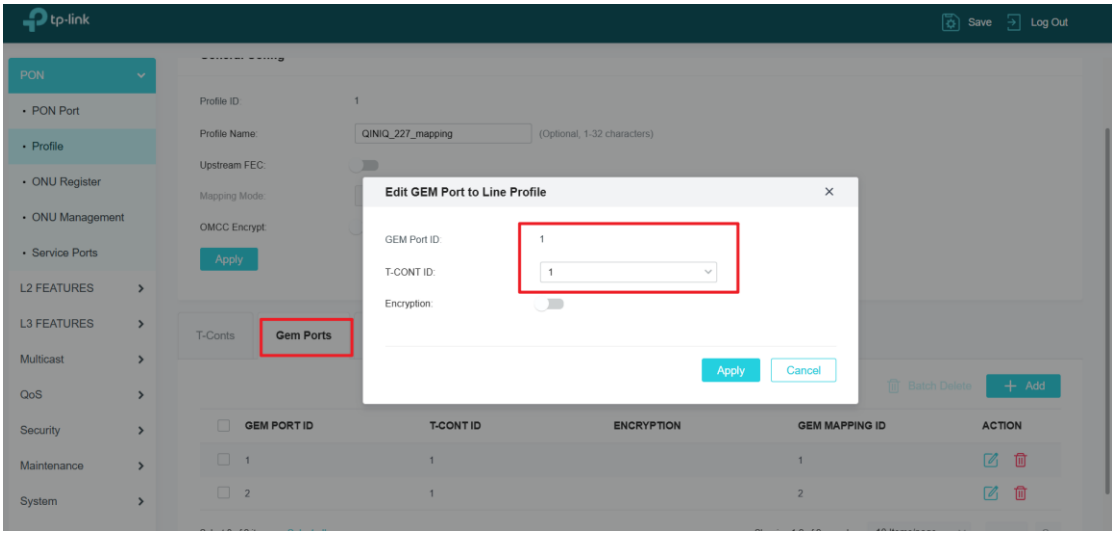
Create a Line Profile corresponding to the function of both QinQ and multicast VLAN 227.

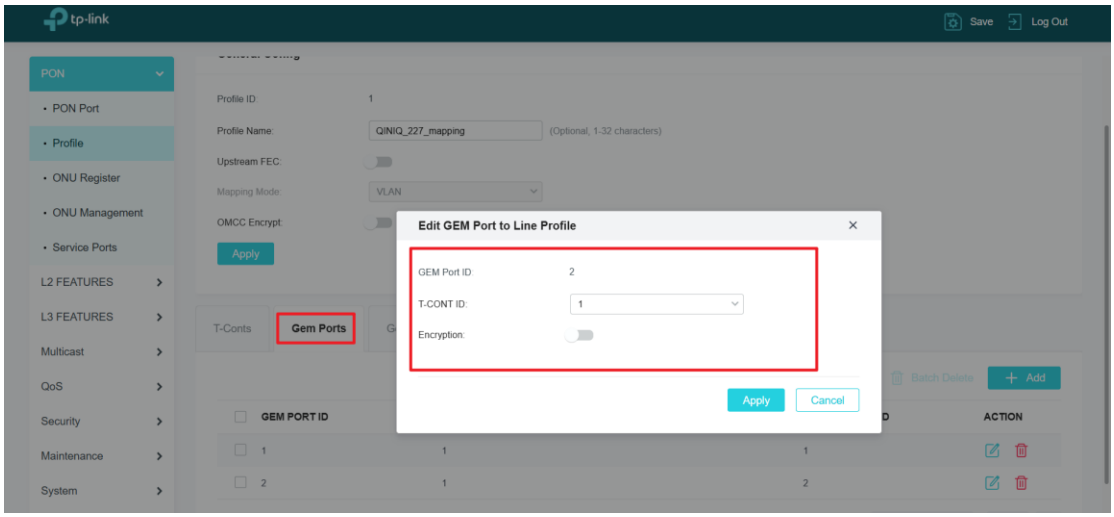


Create the T-Conts corresponding to the DBA Profile of QinQ.



Create two GEM Port entries corresponding to T-Conts ID 1.

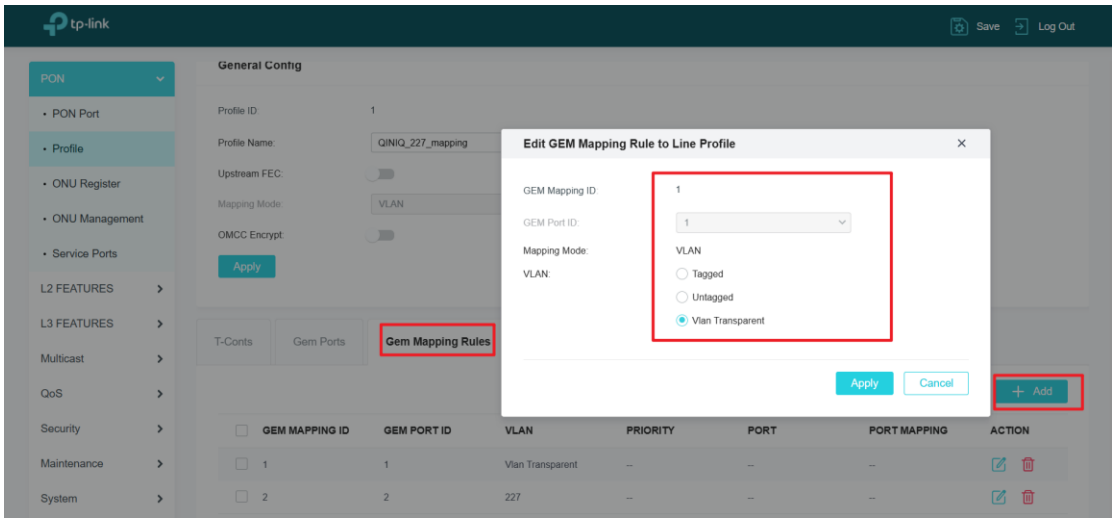


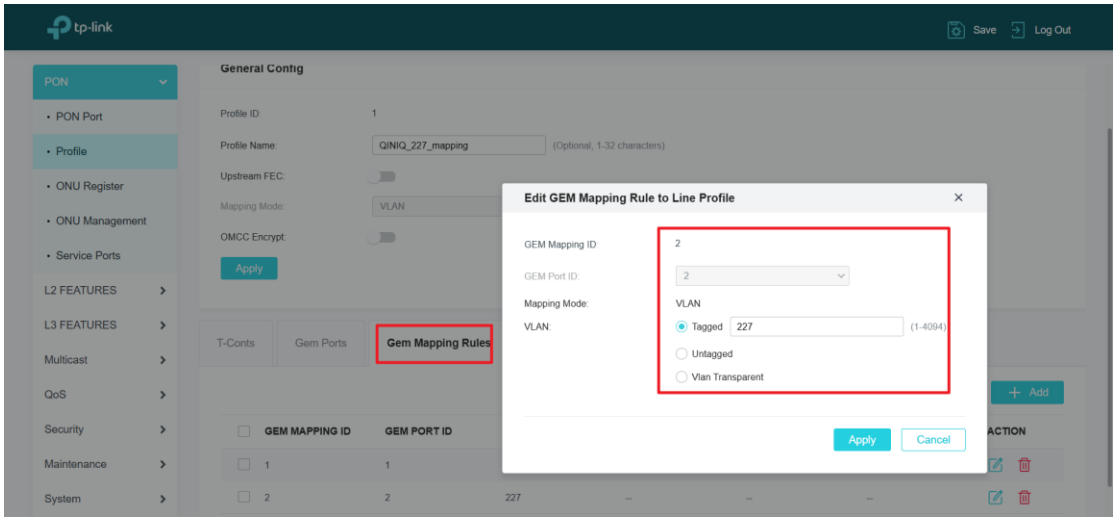


Create two GEM Mapping Rules. The mapping relationship is as follows:

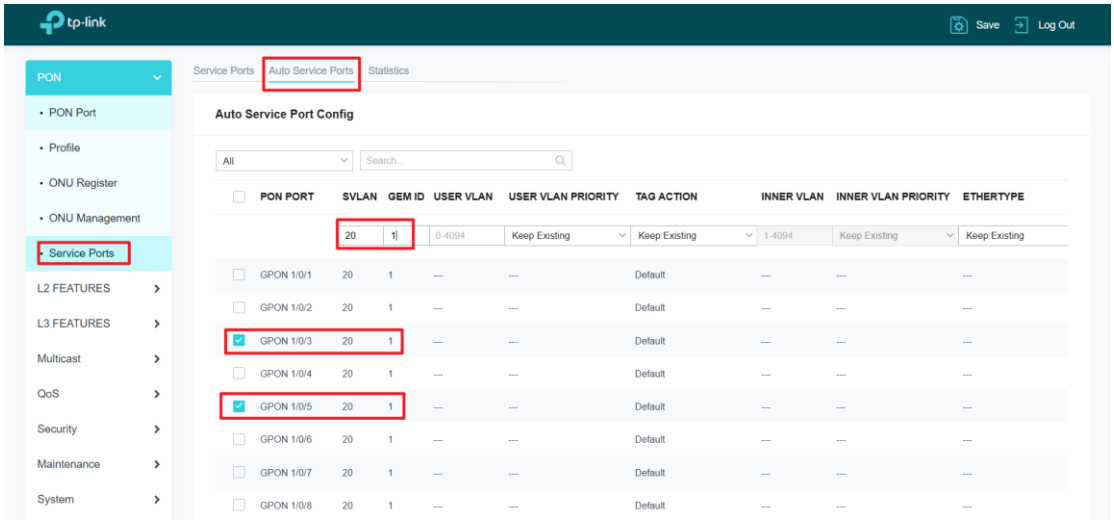
- GEM mapping ID 1_GEM Port ID1_ VLAN transparent
- GEM mapping ID 2_GEM Port ID2_ VLAN 227 tagged

These configurations are for multicast VLAN services.



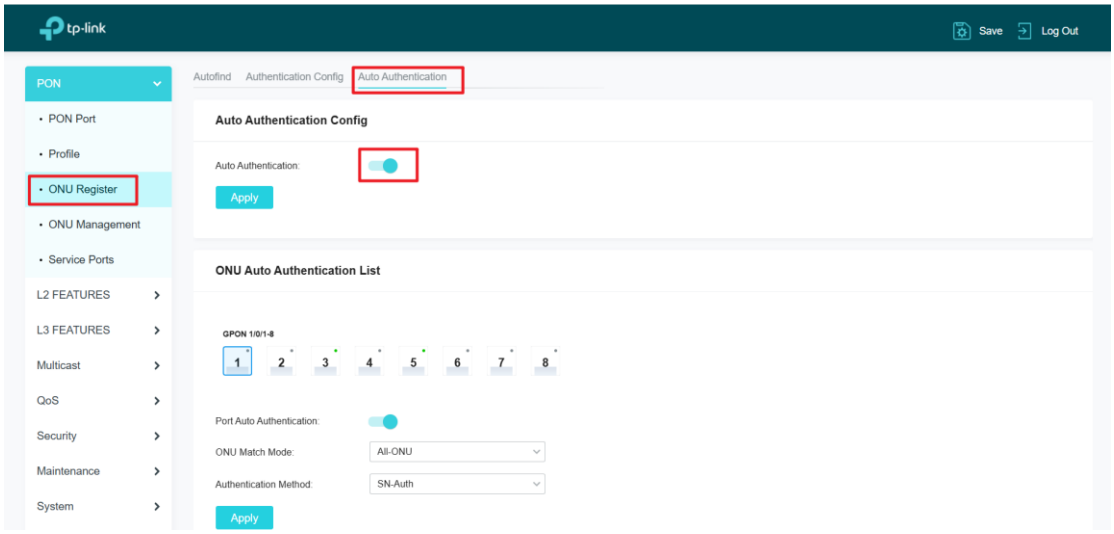


Configure the Auto Service Port on the **PON > Service Ports** page. The SVLAN is the same as the outer VLAN of the front-end switch's VLAN VPN. Configure SVLAN as VLAN 20, GEM ID as 1, and other default Settings. This is the QinQ configuration on the OLT.

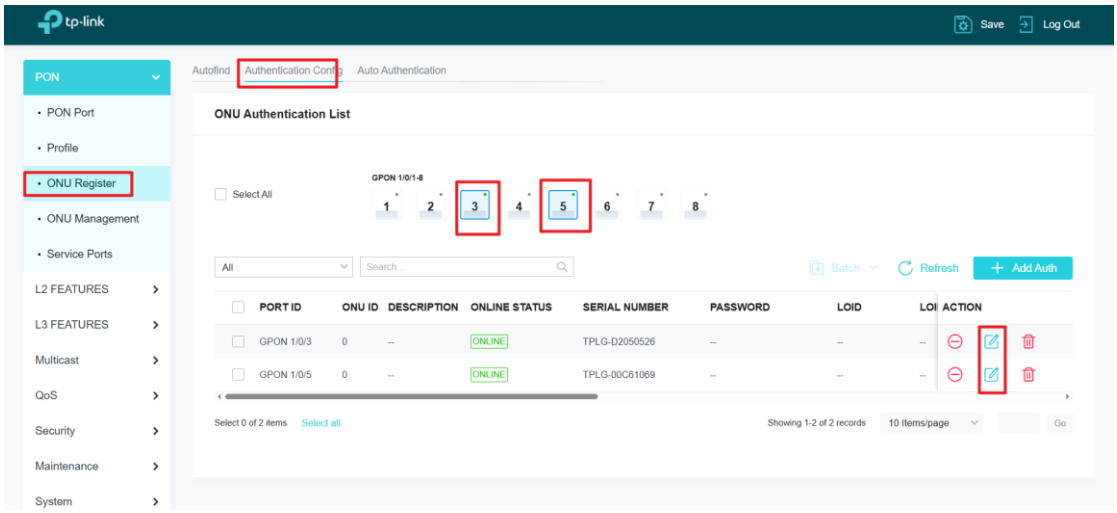


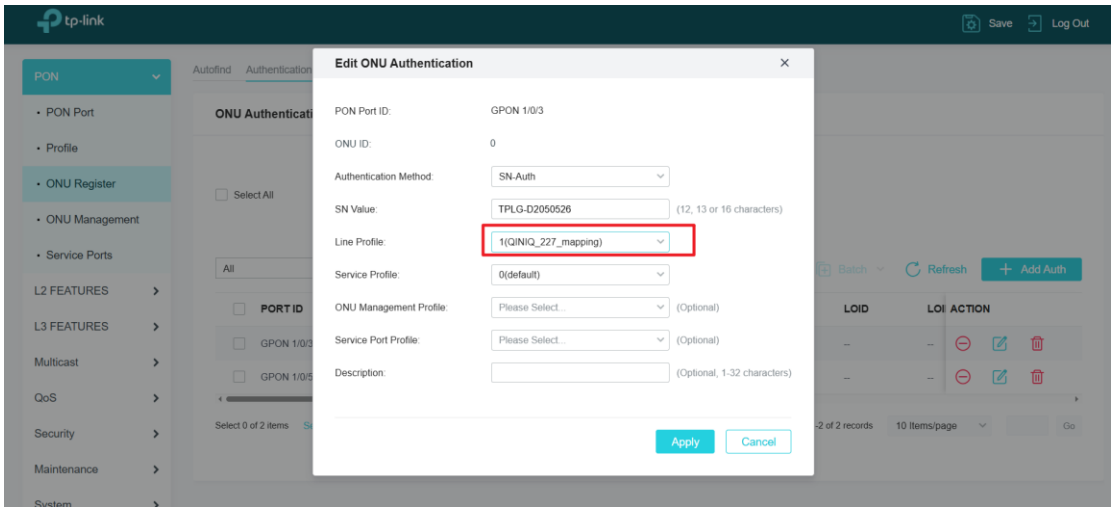
Now, you can modify the Profile of the registered ONU on the **PON > ONU Register > Auto Authentication** page.

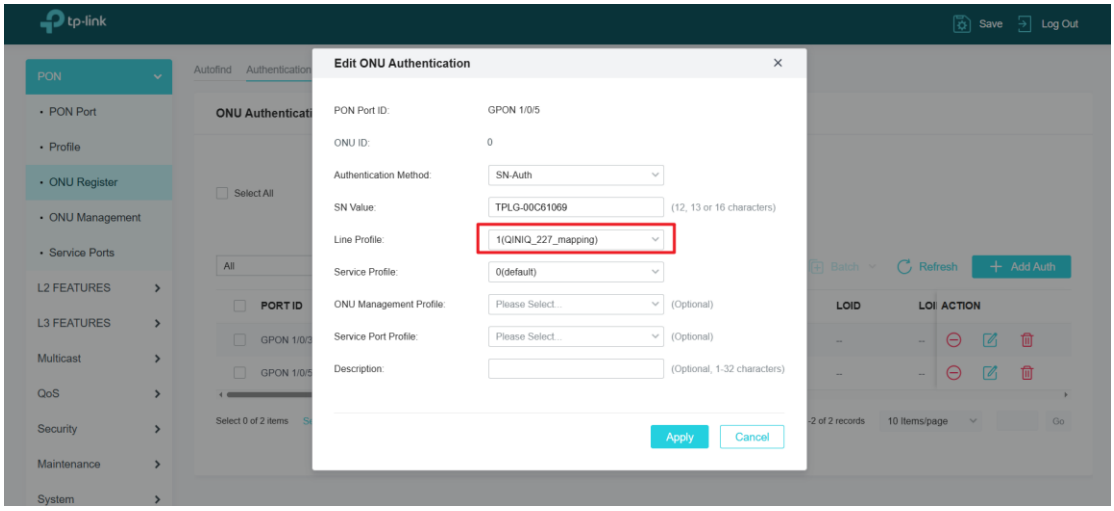
Enable auto authentication:



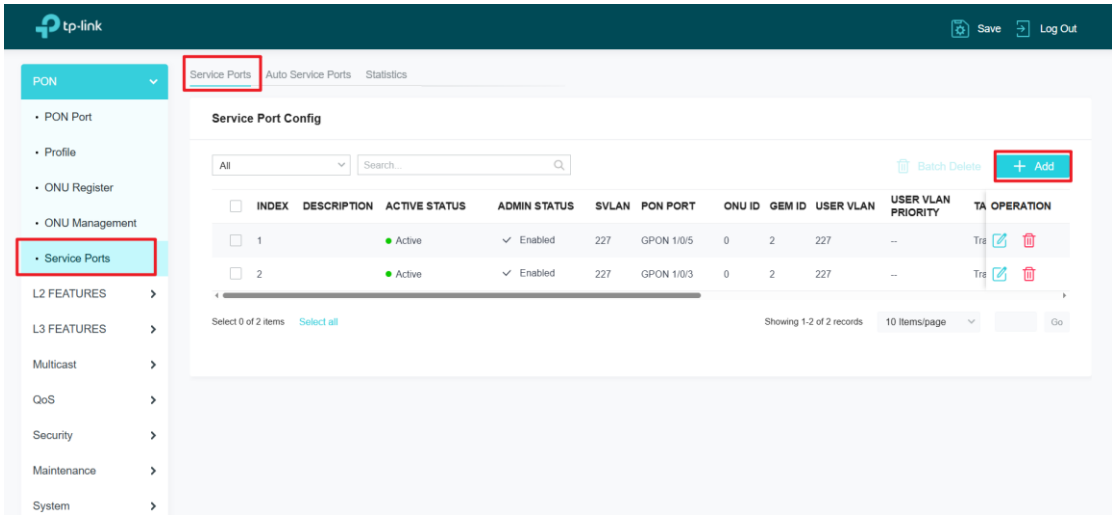
On the **Authentication Config** page, edit ONU Authentication, and choose line profile QinQ_227_mapping.

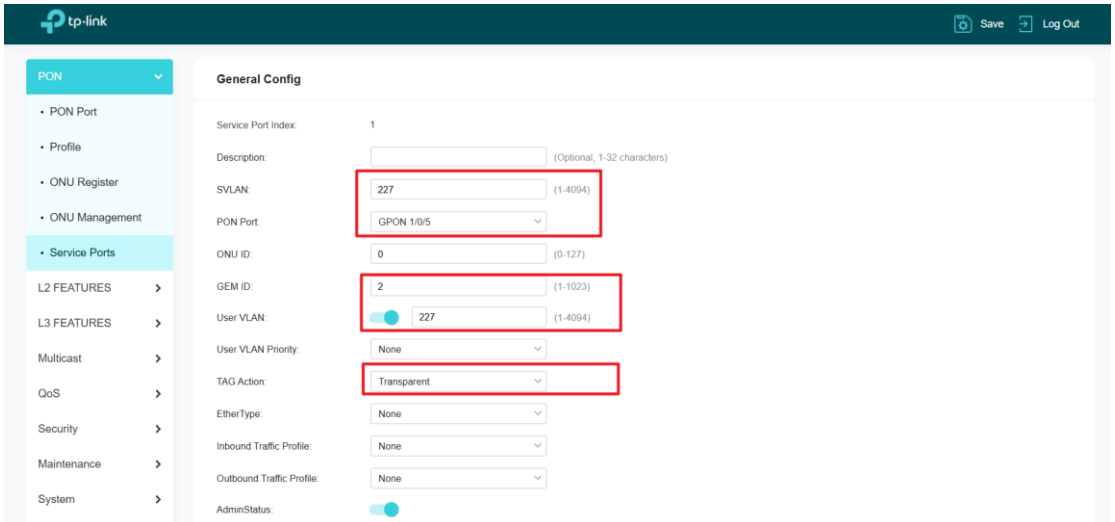


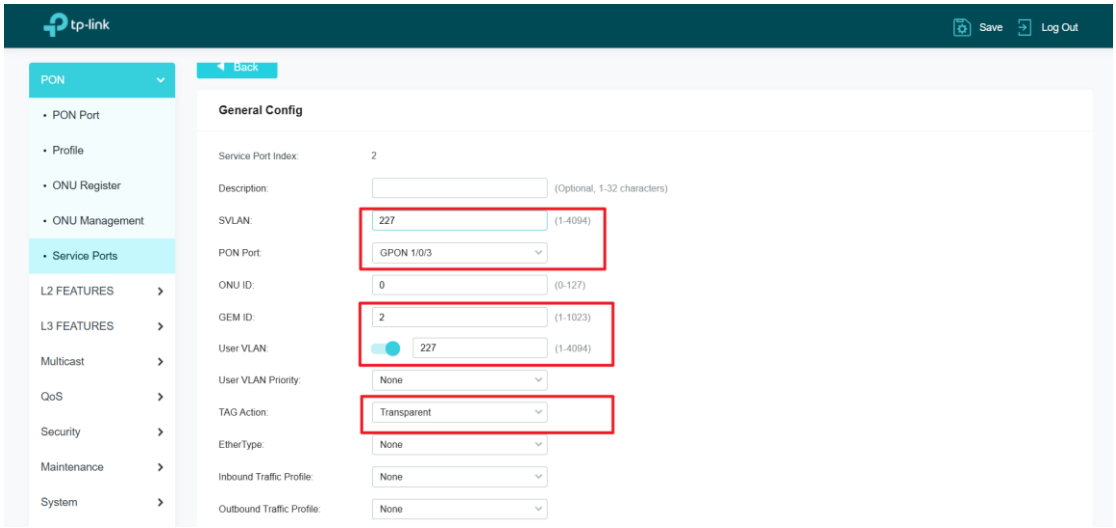




Go to the **PON > Service Ports** page and configure the rules for each ONU.

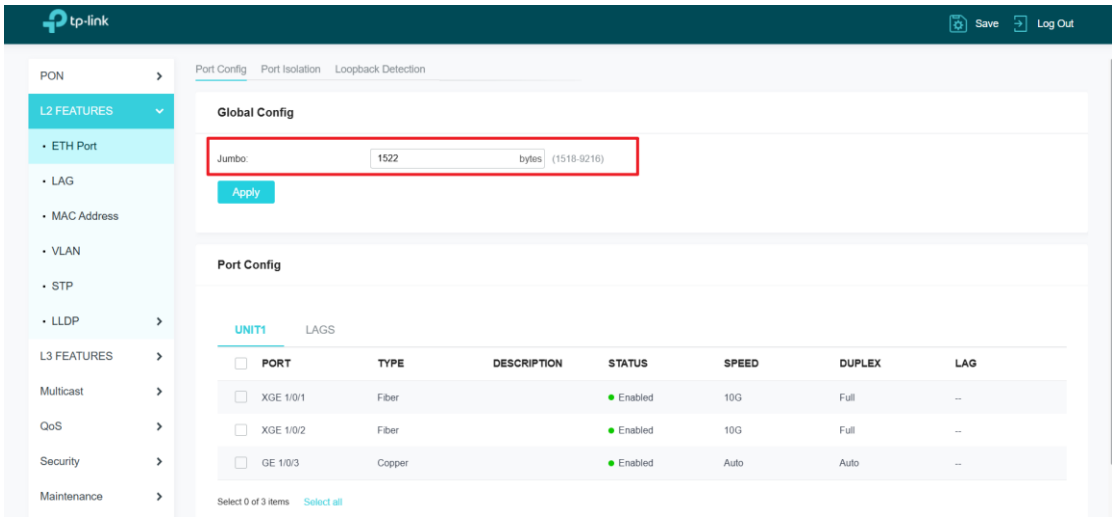






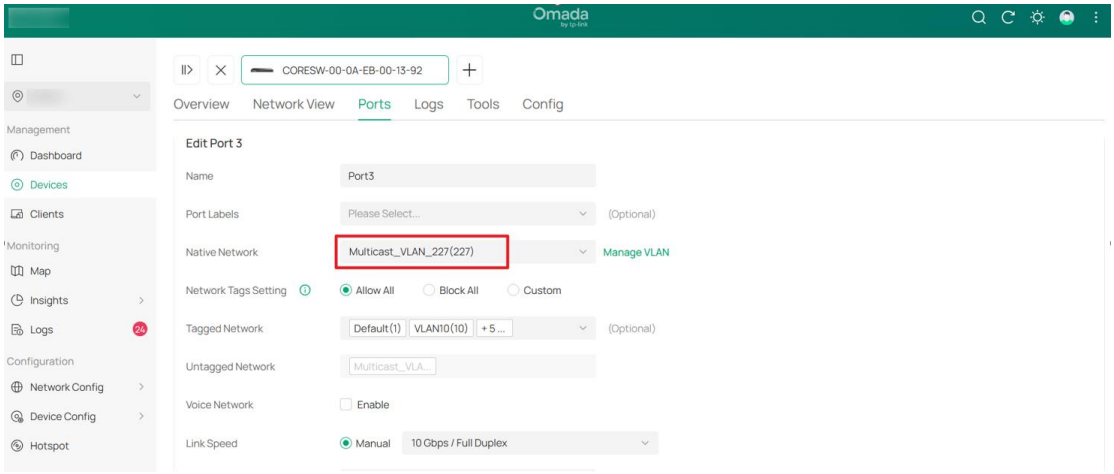
Note: Because the VLAN configured on the OLT's GEM Port is processed as VLAN Transparent, Jumbo frames may exceed 1518 bytes, such as when a GPON AP adds a VLAN and VLAN tag packets require processing. In this case, increase the Jumbo frame size from 1518 to 1522 on both the OLT and the VLAN VPN Switch. A 1518-byte frame accommodates a single VLAN tag, while 1522 bytes support dual VLAN tags.

Change the Jumbo frame length to 1522.

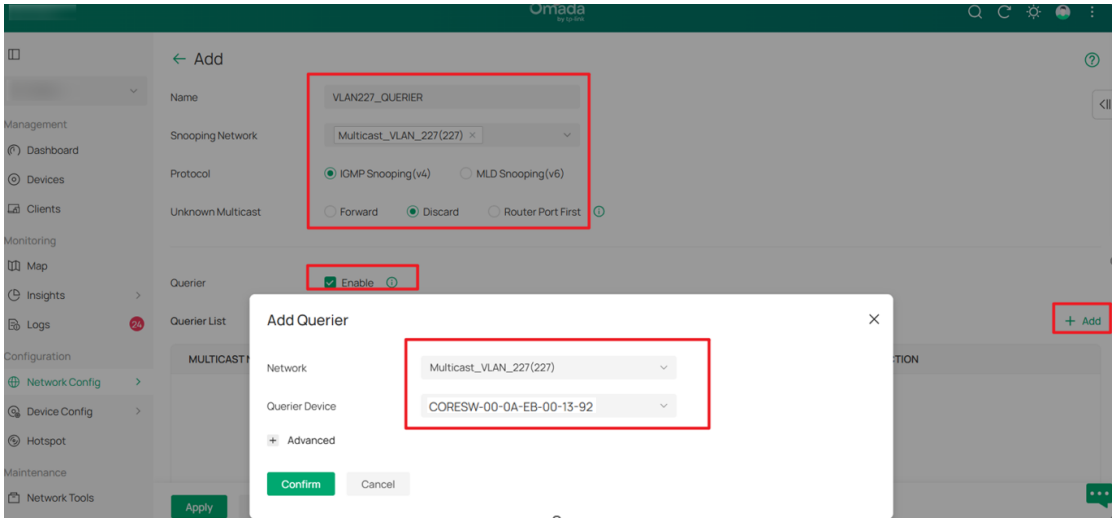


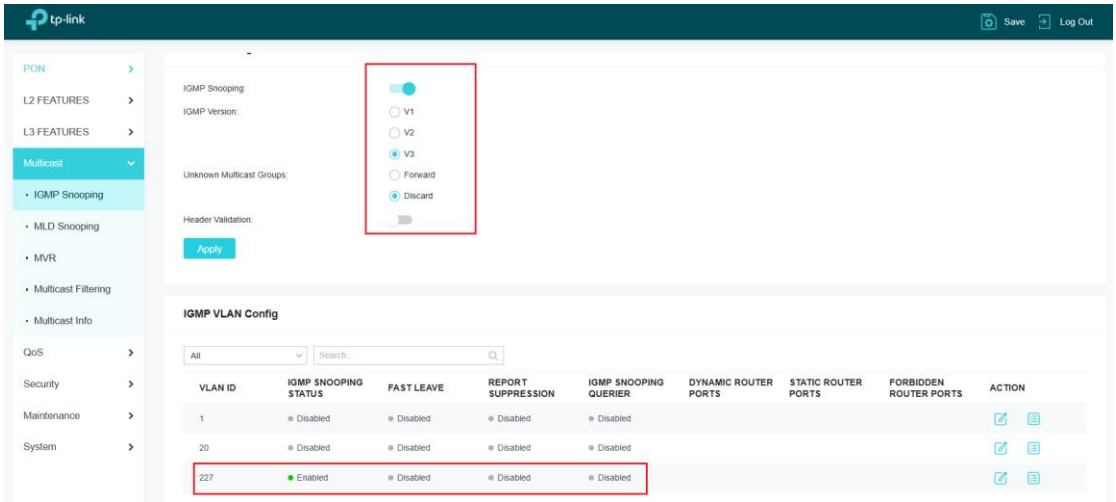
Step 5: Configure multicast on Controller.

The last configuration concerns multicast and PPSK on the Controller. In this topology, Port 3 of CORE SW is connected to the multicast source, so we need to change this port's VLAN PVID.



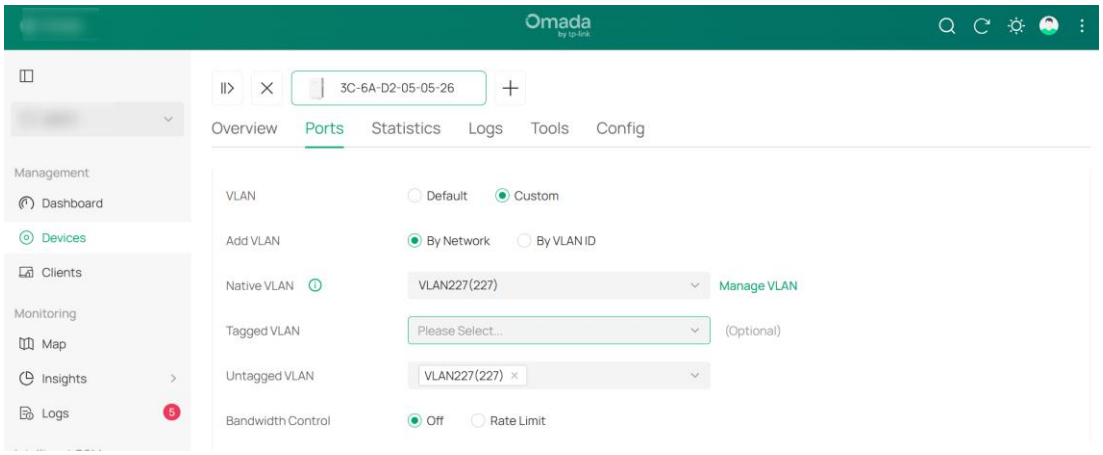
Set the CORE SW as Querier and configure IGMP Snooping on OLT.



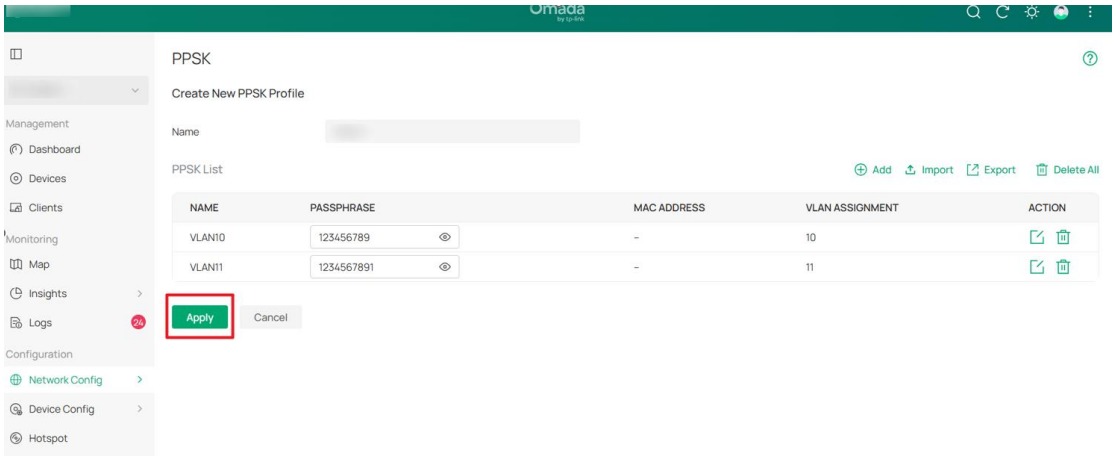


Step 6: Configure on the GPON AP.

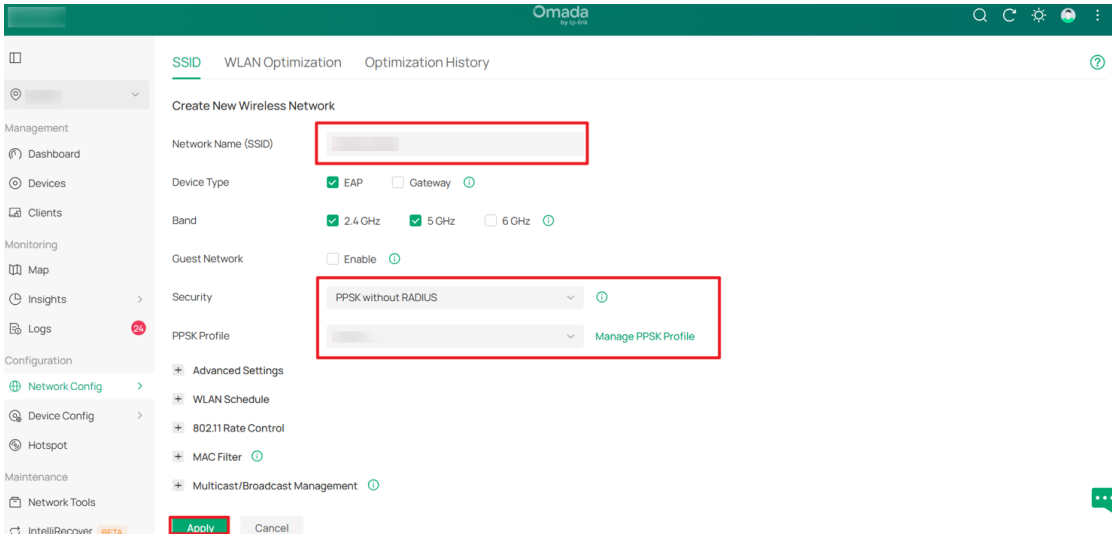
Finally, we need to change the LAN port of the GPON AP to ensure the IPTV can obtain the correct address of VLAN 227.



Step 7: Configure PPSK.



Configure the WLAN SSID and choose **PPSK without RADIUS**.



So far, all configurations have been completed.

4.2.1.4 Verify Configuration

Please refer to section 4.1.1.4.

4.2.2 Solution 2

4.2.2.1 Prerequisites

This configuration guide assumes that the devices are managed by the Omada Controller. Therefore, before performing the subsequent configuration steps, make sure the following requirements are met:

1. The recommended Omada Controller version is 6.0 or above.

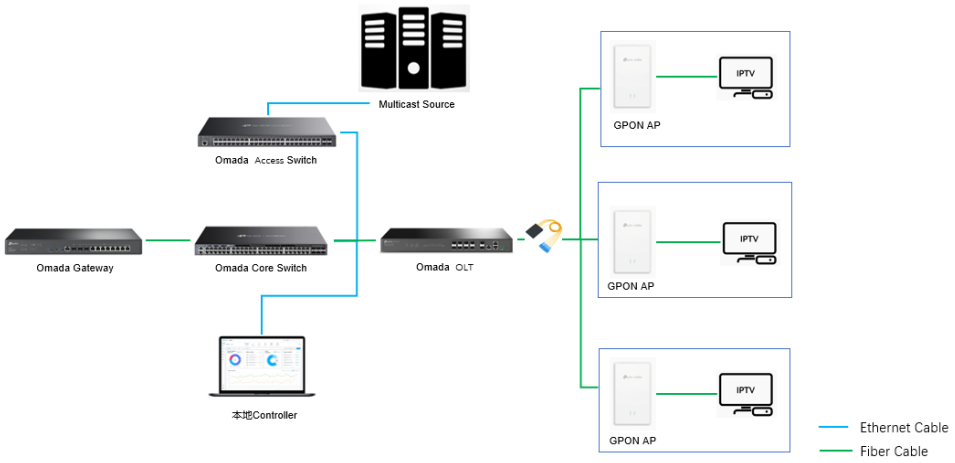
2. Switch firmware must be upgraded to the latest version available on the official website. Note that some switches may not support the Querier function (for details, refer to the user guide for the corresponding model on the official website). We recommend using an Omada Smart/L2+/L3 switch as the Querier.

3. There are no specific functional requirements for the gateway. However, in real customer scenarios, ER8411 is commonly used. Other Omada gateway models may be used in this deployment solution.

4. For Omada EAPs, only GPON APs are used in real customer scenarios.

5. This solution recommends configuring fewer than 30 VLANs.

4.2.2.2 Topology



4.2.3.3 Configuration Steps

Same as 4.1.1.1, PPSK VLAN is VLAN 10, multicast VLAN is VLAN 1.

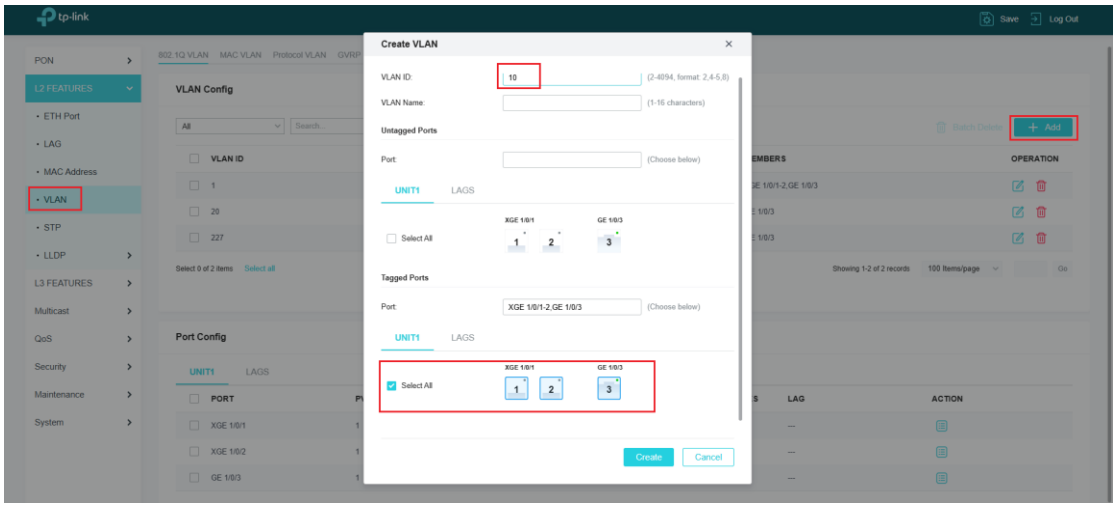
Unlike switches, OLT devices require a separate configuration. Here, OLT devices need to be configured with the following content:

1. VLAN 10 (VLAN 1 is the default configuration)

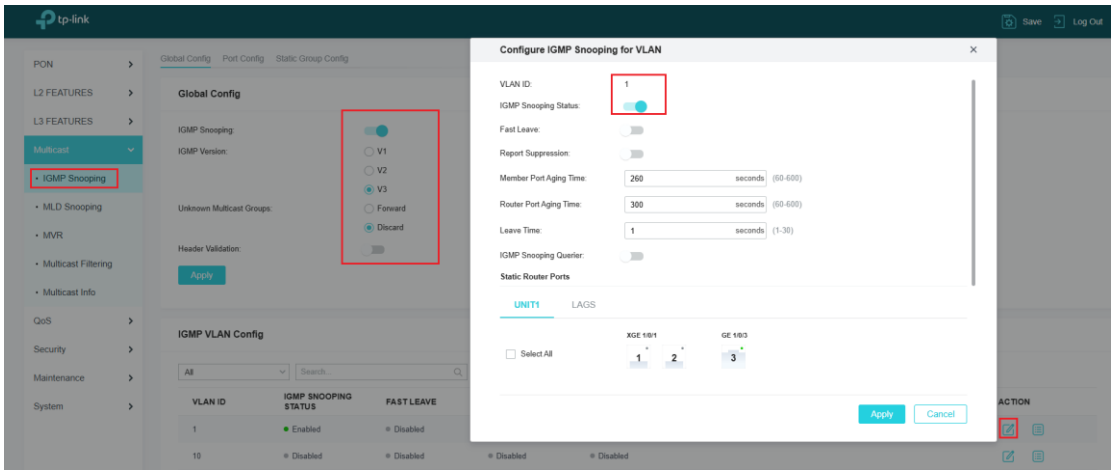
2. IGMP Snooping for VLAN 1

3. It is necessary to set VLAN 10 tagged on both the Ethernet and PON ports of the OLT

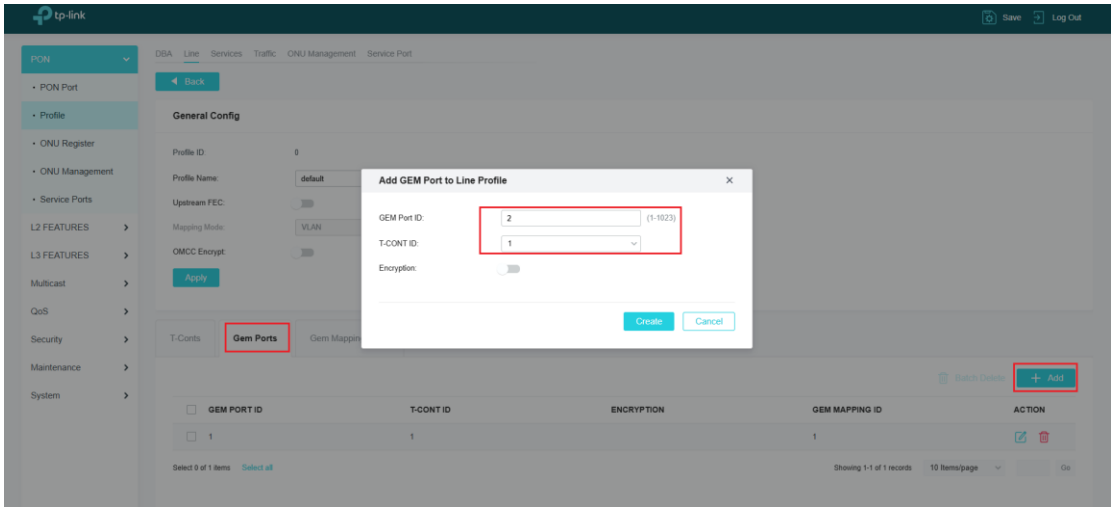
Step 1: Create VLAN 10 and set it tagged on the Ethernet port.

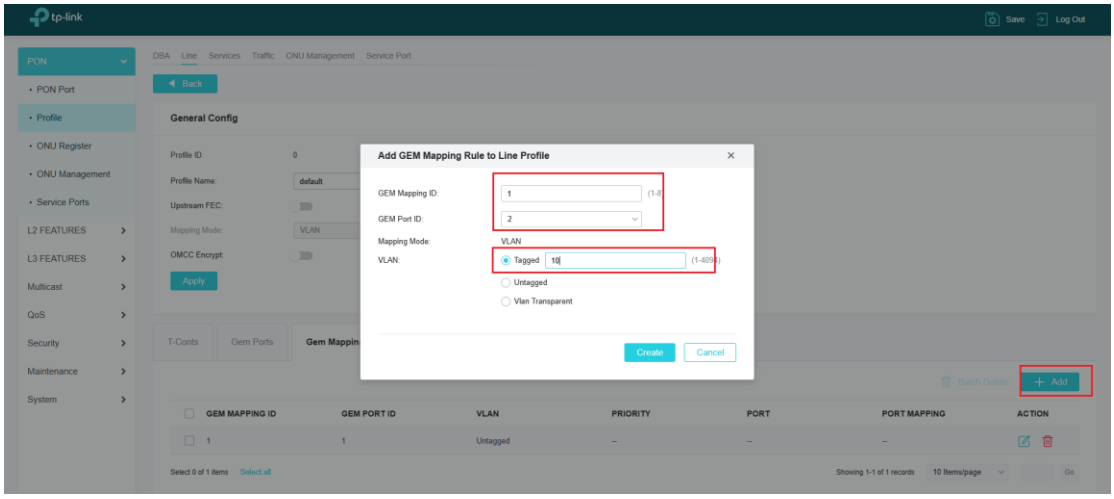


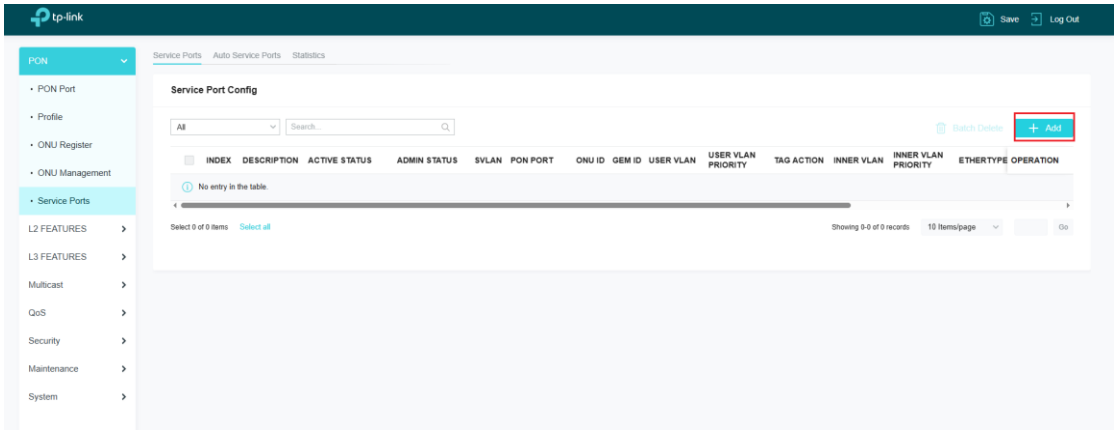
Step 2: Enable IGMP Snooping for VLAN 1.

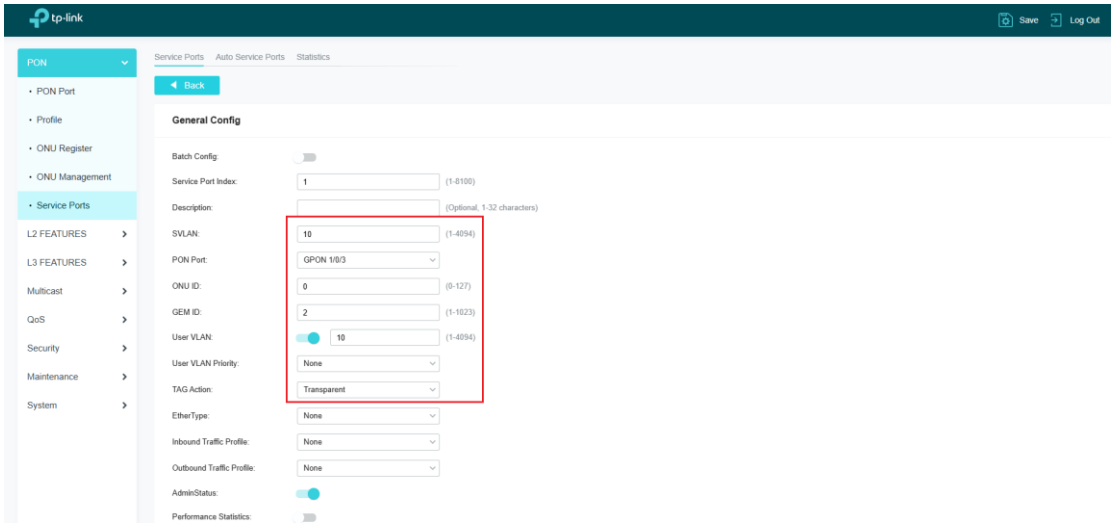


Step 3: Set VLAN 10 tagged on the PON port.









The remaining multicast and screen casting configurations can be fully referenced in section 4.1.1.1.

4.2.3.4 Verify Configuration

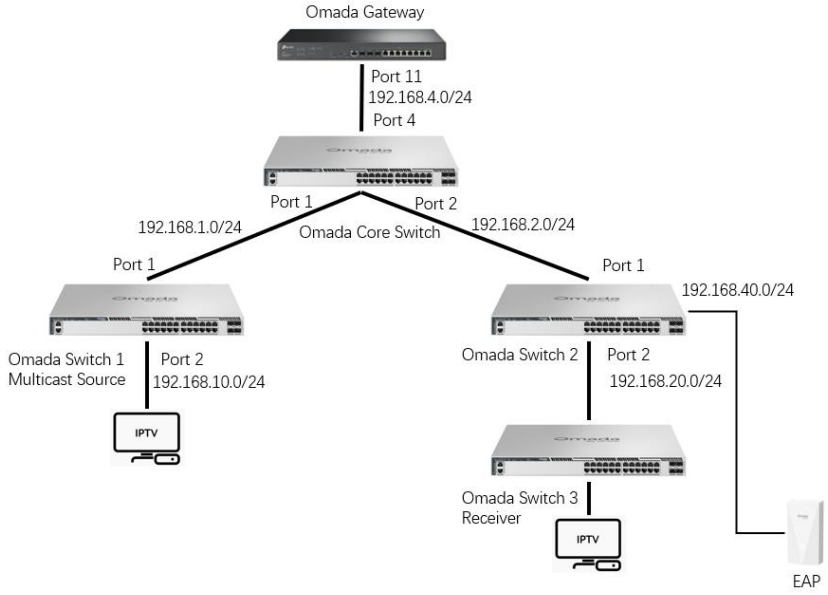
Please refer to section 4.1.1.4.

4.3 Recommended L3 Ethernet IPTV Deployment Solution

4.3.1 Prerequisites

Currently, we only support the PIM solution on L3 switches. This solution is typically used when interfacing with third-party devices, where the peer's network design is configured as an L3 network for PIM multicast. At present, our PIM commands are only supported for configuration via CLI.

4.3.2 Topology



As it is a three-tier network, the networking types are diverse. As shown in the figure above, all networks are in different segments. IPTV routes are connected via OSPF through L3 switches, and PIM multicast is enabled. The Omada Switch 2 connects to the downstream network as an L2 network. Switch 2 needs to enable IGMP, while Switch 3 requires IGMP Snooping.

4.3.3 Configuration Steps

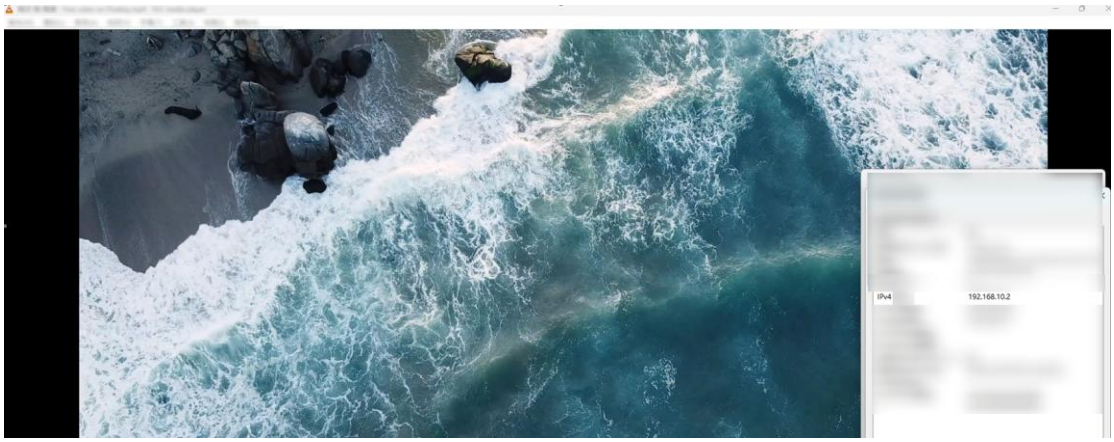
The main core configuration commands are as follows

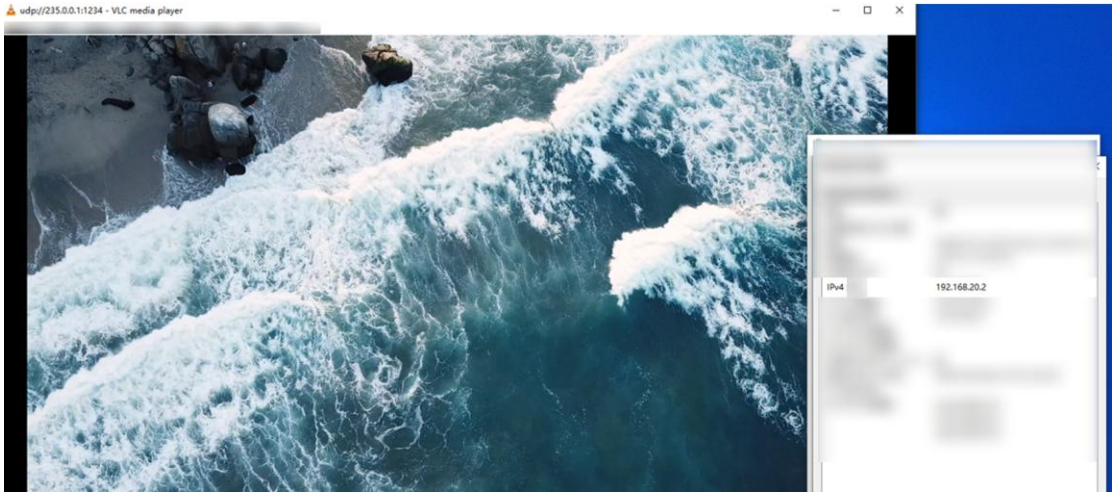
Omada Core Switch	Omada Switch 1	Omada Switch 2	Omada Switch 3
# vlan 2-4,10,20,30 # hostname "Omada_Switch" # # # ip multicast-routing ip pim dense-mode no snmp-server # # interface vlan 1 ip address 192.168.1.1 255.255.255.0 ipv6 enable ip pim # interface vlan 2 ip address 192.168.2.1 255.255.255.0 ipv6 enable ip pim #	# vlan 2-4,10,20,30 # hostname "Omada_Switch 1" # ip multicast-routing ip pim dense-mode no snmp-server # # interface vlan 1 ip address 192.168.1.2 255.255.255.0 ipv6 enable ip pim # interface vlan 10 ip address 192.168.10.1 255.255.255.0 ipv6 enable ip pim # #	# vlan 2-4,10,20,30 # hostname "Omada_Switch 2" # ip multicast-routing ip pim dense-mode no snmp-server # # interface vlan 2 ip address 192.168.2.2 255.255.255.0 ipv6 enable ip pim # interface vlan 20 ip address 192.168.20.1 255.255.255.0 ipv6 enable ip igmp ip pim #	# vlan 2-4,10,20,30 # hostname "Omada_Switch 3" # Ip igmp snooping vlan-config 20

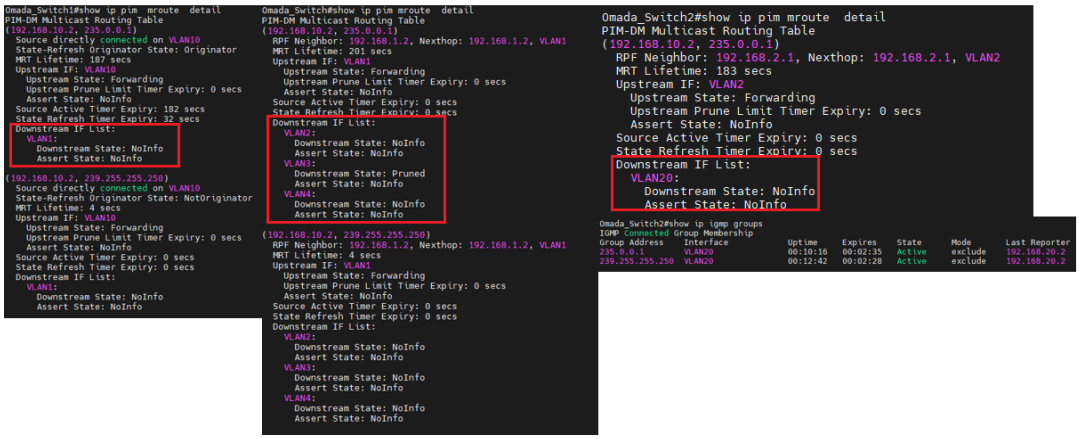
interface vlan 3 ip address 192.168.3.1 255.255.255.0 ipv6 enable ip pim # interface vlan 4 ip address 192.168.4.1 255.255.255.0 ipv6 enable ip pim # interface gigabitEthernet 1/0/1 switchport general allowed vlan 2-4,10,20,30 tagged # interface gigabitEthernet 1/0/2 switchport general allowed vlan 2 untagged switchport general allowed vlan 1,3-4,10,20,30 tagged switchport pvid 2 # interface gigabitEthernet 1/0/3 switchport general allowed vlan 3 untagged switchport general allowed vlan 1-2,4,10,20,30 tagged switchport pvid 3 # interface gigabitEthernet 1/0/4 switchport general allowed vlan 4 untagged switchport general allowed vlan 1-3,10,20,30 tagged switchport pvid 4 # router ospf 1 network 192.168.1.0 255.255.255.0 area 0 network 192.168.2.0 255.255.255.0 area 0 network 192.168.3.0 255.255.255.0 area 0 network 192.168.4.0 255.255.255.0 area 0	interface gigabitEthernet 1/0/1 switchport general allowed vlan 2-4,10,20,30 tagged # interface gigabitEthernet 1/0/2 switchport general allowed vlan 10 untagged switchport general allowed vlan 1-4,20,30 tagged switchport pvid 10 # router ospf 1 network 192.168.1.0 255.255.255.0 area 0 network 192.168.10.0 255.255.255.0 area 0	# interface gigabitEthernet 1/0/1 switchport general allowed vlan 1,3-4,10,20,30 tagged switchport general allowed vlan 2 untagged switchport pvid 2 # interface gigabitEthernet 1/0/2 switchport general allowed vlan 20 untagged switchport general allowed vlan 1-4,10,30 tagged switchport pvid 20 # router ospf 1 network 192.168.2.0 255.255.255.0 area 0 network 192.168.20.0 255.255.255.0 area 0	

4.3.4 Verify Configuration

After configuring the above commands, use VLC to pull the stream, such as using a PC under Omada Switch 1 as the multicast source and a PC under Omada Switch 3 as the receiver for multicast pull experiments.







From the above routing table, it can be seen that in addition to the 235.0.0.1 multicast address, the SSDP discovery protocol 239.255.255.250 has also been integrated into the PIM network, allowing for direct screen casting based on the SSDP protocol.

5 Recommended Models

Here is a brief introduction to some commonly used models. For more models, please visit the official website or consult local sales representatives.

S7500-24Y4C

Omada S7500-24Y4C is a high-performance L3 managed switch tailored for the aggregation and core layer, featuring L3 routing, ultra-fast 100 Gbps wired speeds, stacking options, and redundant power supply modules. It includes 24× 25 Gbps SFP28 slots, 4× 100 Gbps QSFP28 slots, physical stacking ability, and centralized management. Integrating strong security, easy O&A, and extensive management features, S7500-24Y4C offers a dependable networking solution for hotels, enterprises, campuses, and ISPs.

Features abundant L3 routing protocols that support a scalable network, such as OSPF, BGP, IS-IS, VRF, VRRP, PIM-SM/PIM-DM/PIM-SSM, ECMP, and PBR. In complex large-scale network environments, dynamic routing protocols automatically adapt to changes in network topology and select the best transmission path based on real-time network conditions to maintain stability.

SG3428XMPP

The Omada SG3428XMPP Enterprise Managed PoE Switch, belonging to the Omada Access Plus series, is a high-performance PoE switch designed for medium-to-large network scenarios.

There are 16 PoE+ ports that support the 802.3af/at standard, with a maximum power of 30W per port, suitable for devices such as Wi-Fi 6 APs and regular IP cameras. Among them, there are 8 PoE++ ports, supporting the 802.3bt standard, with a maximum power of 90W per port, which can supply power to high-power devices such as video conferencing terminals, PTZ pan/tilt cameras, and high-power wireless APs.

Omada SG3428XMPP provides 10 Gbps upstream bandwidth and can be connected to fiber-optic modules, providing high-speed uplinks for core switches or backbone links while avoiding gigabit ports becoming bottlenecks.

Omada SG3428XMPP supports enterprise-level features such as VLAN, QoS, link aggregation, IGMP Snooping, and ring network protection to meet complex network architecture requirements.

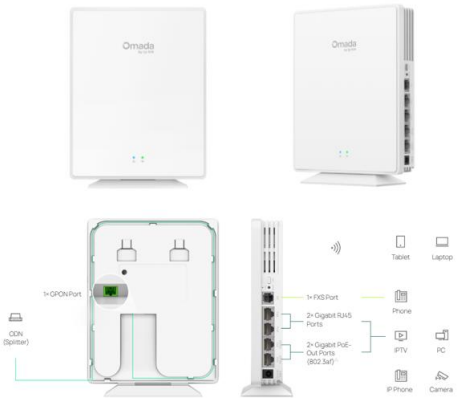
EAP725-Wall

Omada EAP725 Wall is an indoor AP that supports the latest Wi-Fi 7 (802.11be) standard. It supports both 2.4 GHz (2×2 MIMO) and 5 GHz (2×4 MIMO) dual-band simultaneous service, with 4 spatial streams and speeds of up to 5 Gbps. Equipped with a built-in smart antenna, the signal moves with the user, and the new Wi-Fi 7 technology greatly enhances the user's wireless network experience. Suitable for indoor coverage scenarios such as small and medium-sized enterprise offices, hotels, retail, and more.

This AP provides a combination of dual 2.5G PoE ports and dual Gigabit ports, achieving dual capabilities of high-speed Wi Fi 7 wireless coverage and multi-device wired access.

Multiple wired ports can simultaneously connect multiple devices, such as phones and IPTV. At the same time, PoE power supply and transparent transmission design greatly simplify the wiring and deployment process, making it an ideal choice for hotels and apartments.

EAP650GPON-Desktop



Omada EAP650GP-Desktop is a desktop/wall-mounted three-in-one access point that integrates GPON ONU, Gigabit wired, and Wi-Fi 6 wireless, designed specifically for

scenarios such as hotels, apartments, and offices. It supports AX3000 Wi-Fi 6 (dual-band, up to 2402 Mbps in the 5 GHz band and up to 574 Mbps in the 2.4 GHz band) and provides high-speed and stable wireless coverage.

Omada EAP650GP-Desktop integrates a Gigabit GPON ONU module, which can be directly connected to fiber optic networks without the need for additional optical modem devices. A single fiber-optic cable simultaneously supports wired networks, Wi-Fi, and multiple services such as voice over internet protocol (VoIP) and IPTV, reducing deployment costs. The AP also seamlessly integrates with the Omada SDN platform and achieves centralized configuration, monitoring, and upgrades with OLTs, switches, and other APs, making it suitable for unified operation and maintenance across multiple sites.

Omada EAP650GP Desktop supports 4× Gigabit RJ45 Ethernet ports, including two regular Gigabit ports, which can be connected to devices such as computers, set-top boxes, IPTV boxes, etc. The other two are 802.3af PoE output ports, which can directly power low-power PoE devices such as cameras and IP phones. The maximum power output per port is 15.4W, and the total PoE output power is 22.4W.

6 Appendix

6.1 Terminology

Term	Description
DR	Designated Router
IGMP	Internet Group Management Protocol
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
RP	Rendezvous Point
RPT	Rendezvous Point Tree
SPT	Shortest Path Tree
IGMP Snooping	Internet Group Management Protocol Snooping
IPTV	Internet Protocol Television
IGMP Snooping	Internet Group Management Protocol Snooping
MBGP	Multicast BGP

Term	Description
MSDP	Multicast Source Discovery Protocol

6.2 References

[1] B. Haberman, Ed., " IANA Considerations for Internet Group Management Protocols," RFC 9778, BCP57, Mar. 2025.

[2] B. Haberman, Ed., "Internet Group Management Protocol, Version 3," RFC 9776, STD 100, Mar. 2025.

[3] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, R. Parekh, Z. Zhang, and L. Zheng, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)," RFC 7761, STD 83, Mar. 2016.