Full Manual

Managed Switch

Instructions are continuously being developed. The latest version of the document can be found online on our website.

VIDEOR E. Hartig GmbH | Carl-Zeiss-Straße 8 | 63322 Rödermark | Germany | Tel. +49.6074.888-0 | Fax +49.6074.888-100 |
Amtsgericht Offenbach am Main | HRB 32047 | UIN DE 113592980 |
Geschäftsführer / Managing Directors: Lars Hagenlocher, Dominik Mizdrak

www.eneo-security.com | info@eneo-security.com

CONTENT / INHALT

ABOUT THIS DOCUMENT

This document provides a comprehensive description of a specific series of devices, which we have compiled with great care and accuracy to give you a deep insight into the general functions and features that characterize this series of devices.

However, you should be aware that the detailed characterization in this document refers to the general product line. The individual features of specific models or designs within this series may vary depending on the configuration.

The differences may result in an expanded or limited range of functions and performance, so that the actual specifications of individual products may differ in some respects from the descriptions provided in this document.

For this reason, we strongly recommend that you carefully read the specific data sheet for the product in question. The data sheet contains specific, detailed information tailored to the model in question. It is the primary reference document that provides the most authentic and accurate information about the individual functions and features of each specific product in our device series.

We appreciate your understanding and willingness to invest time in gaining accurate knowledge about the product you have selected from our product range. Please do not hesitate to contact us if you have any further questions or require additional information.

SAFETY INSTRUCTIONS

Read the safety instructions and operating instructions carefully before installing the product. Depending on the product type, individual points may be omitted.

Mounting and installation

- Ensure that the intended mounting location is suitable for the respective product (e.g. in terms of weight).
- Attach the products securely to the locations and surfaces recommended by the manufacturer to ensure stability and safety.
- Ensure that the products are weatherproof if they are installed outdoors and protect e.g. cameras from direct sunlight or extreme temperatures.
- Make sure that any ventilation slots are not blocked to ensure sufficient air circulation and cooling.
- Ensure that cameras, switches, etc. are installed at a safe distance from flammable materials, power sources, running water, etc.
- Installation, commissioning and maintenance may only be carried out by authorised specialist personnel in compliance with the relevant standards and directives.

Power supply & cabling

- To ensure a safe power supply, only use power supply units and cables recommended by the manufacturer.
- Ensure that the cables are properly routed and protected from tampering and damage (e.g. kinks) to prevent power failures or short circuits (e.g. due to moisture ingress).
- Ensure that the cables are not routed through doors, windows or other moving parts to avoid damage and tripping hazards.
- To disconnect the system from the power supply, only pull the cable by the plug and never directly by the cable.
- Wire end ferrules must be used when shortening flexible connection cables.

Operation

- The appliances may only be operated within the temperature and humidity ranges specified in the data sheet.
- Sufficient ventilation must be provided to prevent overheating. This applies in particular to devices such as recorders and switches, which can generate heat.
- Ensure that no lines of sight are blocked and that the accessories do not cover any areas used by other devices or people.
- Ensure that cameras are orientated so that they provide a clear view of the desired area without compromising people's privacy.

Security

- Use strong passwords for all cameras and devices to prevent unauthorised access.
- Keep device firmware up to date to minimise security vulnerabilities.
- Protect (remote) access to the devices using secure methods such as encrypted connections or VPN.

Cleaning and maintenance

- Clean the lenses and housing of the cameras regularly to ensure a clear view.
- Keep the ventilation slots clean and free of dust to ensure efficient cooling.
- Use a mild cleaning agent for cleaning. Harsh cleaning agents such as thinner or petrol can permanently damage the surface.
- Check the product regularly for damage and signs of wear.
- Only use original spare parts (e.g. connection cables) or accessories from VIDEOR E. Hartig GmbH.
- Any tampering by unauthorised persons will invalidate the warranty.
- Disconnect the power supply before opening the housing.

Warnings, data protection and legal information

- Make visitors aware that they are being recorded by means of clearly visible notices.
- If necessary, point out rules of behaviour.
- Ensure that the cameras are positioned in such a way that privacy is not violated, e.g. by recording neighbours or public areas.
- Observe the local laws and regulations on video surveillance and data protection (GDPR).

1 – INTRODUCTION

1.1 – Technical Data

The front panel of the Web Smart Switch has 8/16/24 adaptive 10/100M UTP ports and an LED display.

The 8/16/24 ports support devices with a bandwidth of 10/100 Mbit/s and auto-negotiation.

Each port has a LNK/ACT indicator.

1.2 – Precautions during installation

- Ensure that the surface on which the device is placed is sufficiently secure so that it cannot tip over.
- Ensure that the power outlet is no more than 1.8 m away from the device.
- Ensure that the device is securely connected to the power outlet with the power cord.
- Ensure that the device is well ventilated and that heat can dissipate easily.
- Do not place any heavy objects on the device.
- Use only the screws provided! This will prevent problems and ensure easy installation.

1.3 – Power supply

The switch can be used with an AC power supply of 100 to 240 V AC, 50 to 60 Hz. The switch's integrated power supply system automatically adjusts the operating voltage to the actual input voltage. The power connection is located on the back of the switch.

Disconnect the power cord by pulling the plug on the power switch on the rear panel and then pulling the other end out of a power outlet.

2 – STARTUP

You can use the web browser-based configuration to manage the Web Smart Switch. The Web Smart Switch to be configured via a web browser must be connected to at least one computer via an Ethernet connection. To do this, a PC/laptop can be connected to any RJ45 port.

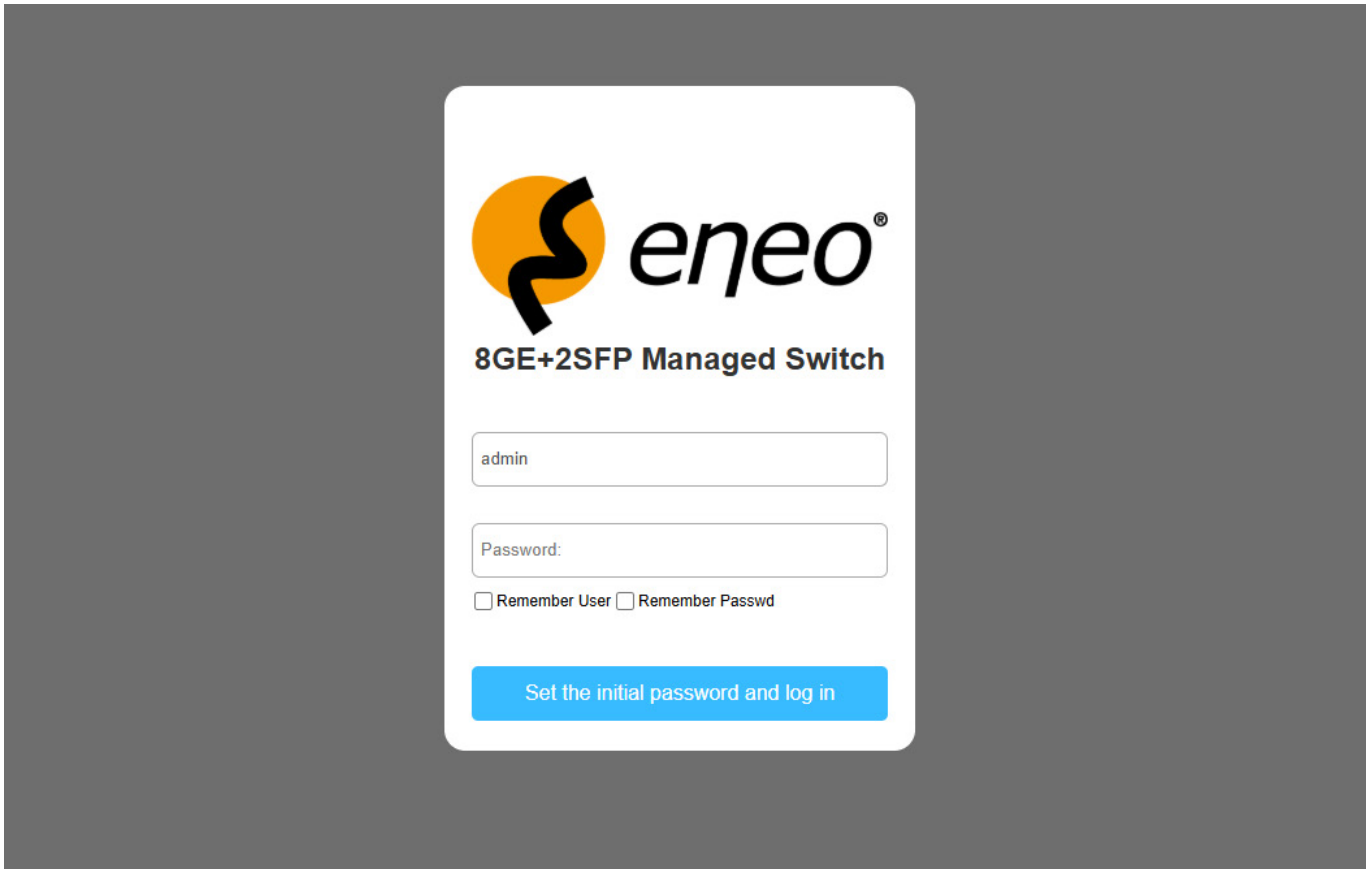
2.1 – Factory settings and login

The switches are delivered with the following factory settings:

IP address: 192.168.1.10
Subnet mask: 255.255.255.0

Username: admin
Password: You must first set a password for the first login. This must be at least eight characters long.

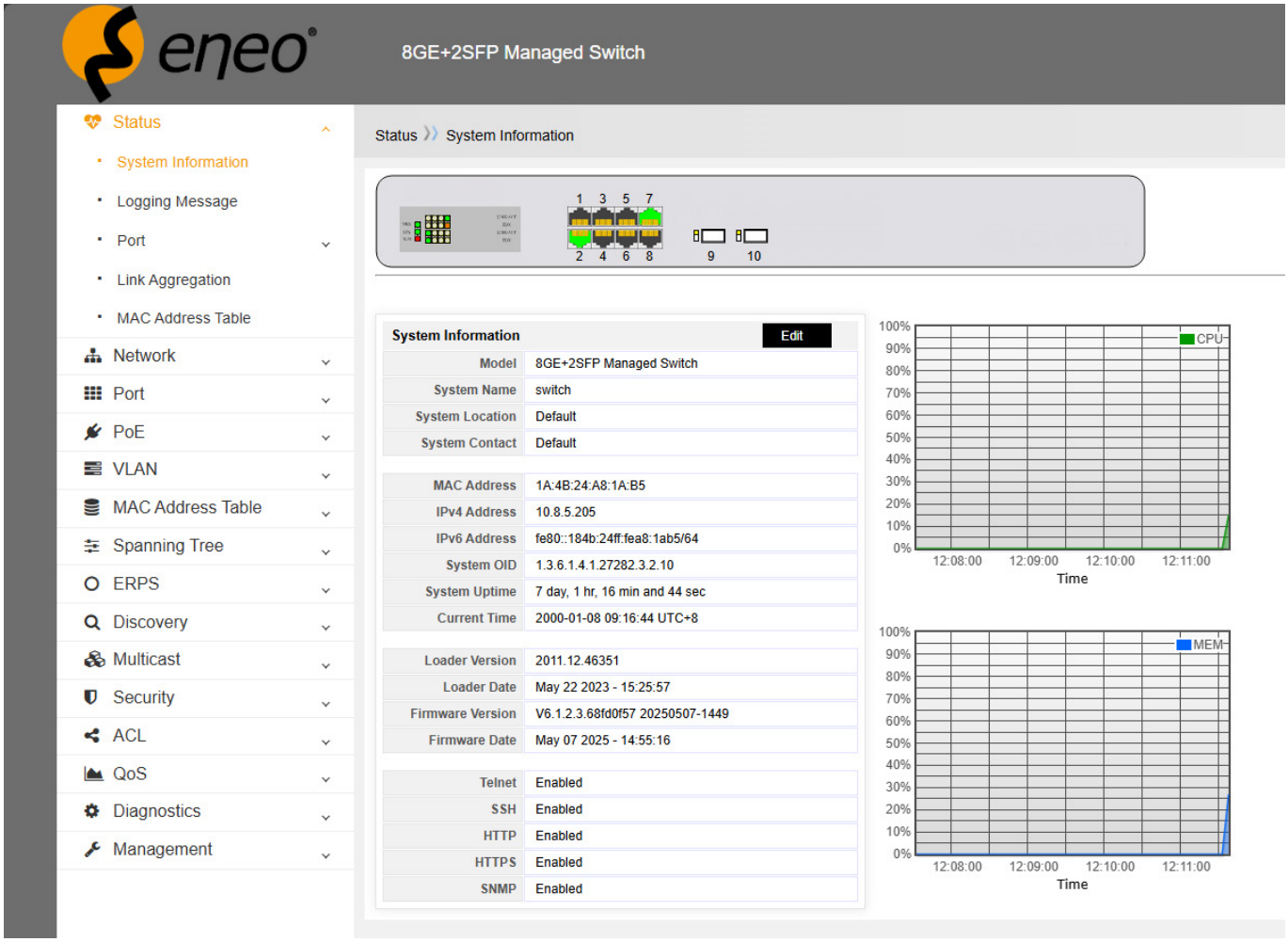
A connection to the switch can be established by entering the IP address of the switch (192.168.1.10) directly into a web browser.
To log in, the user simply enters the username and password listed above.



2.2 – System Information

After successful login, the "System Information" page is automatically displayed, showing the most important information about the switch.

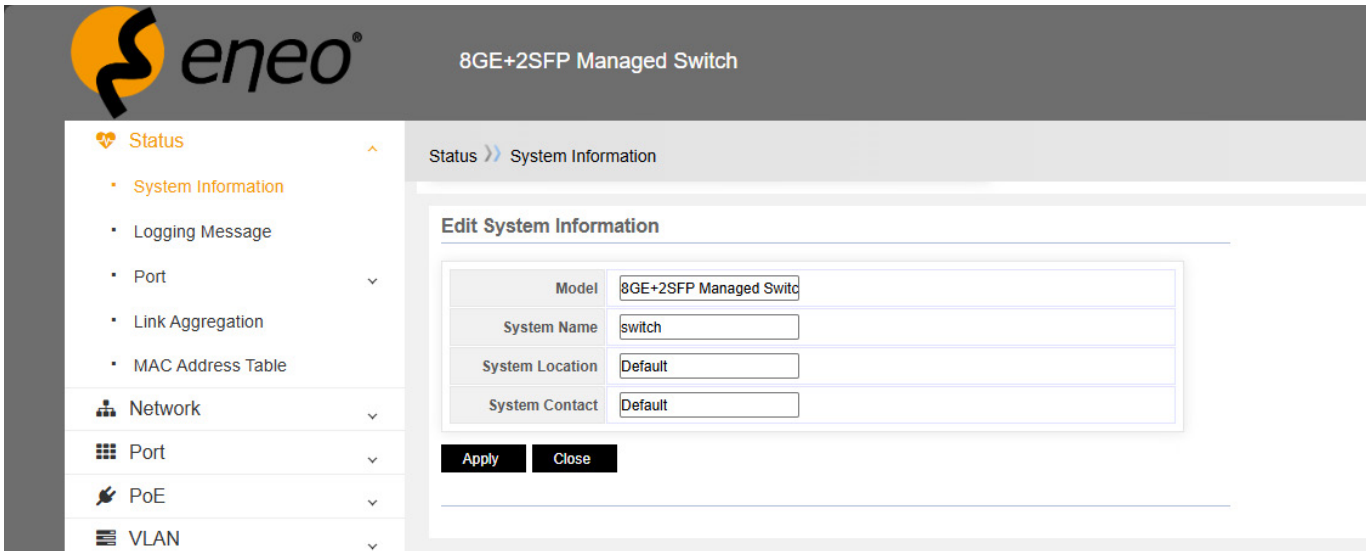
It displays the switch's system information, such as model name, MAC address, IP address, hardware and software version information.



Model: Model name of the device
System name: Name of the device. The default setting is "Switch".
System location: Location of the device.
System contact: Contact for the system.

2.2.1 – Edit

The "Edit" button allows you to edit some system information.



2.2.2 – Set static IP address or dynamic IP address

Static IP address

A static IP address is a manually assigned and fixed numerical identifier assigned to a device within a computer network. It remains unchanged and only changes if it is manually reconfigured. Static IP addresses are typically used for devices that require consistent and reliable network access.

Note!

If you select "Static," you must manually assign an IP address, subnet mask, default gateway, and DNS server (optional) to the switch. The IP address and gateway must be in the same network segment.

Dynamic IP address

A dynamic IP address is an IP address that is automatically assigned to a device by a DHCP server (Dynamic Host Configuration Protocol). Unlike a static IP address, a dynamic IP address can change over time. The DHCP server assigns IP addresses from a pool of available addresses, enabling efficient use of network resources.

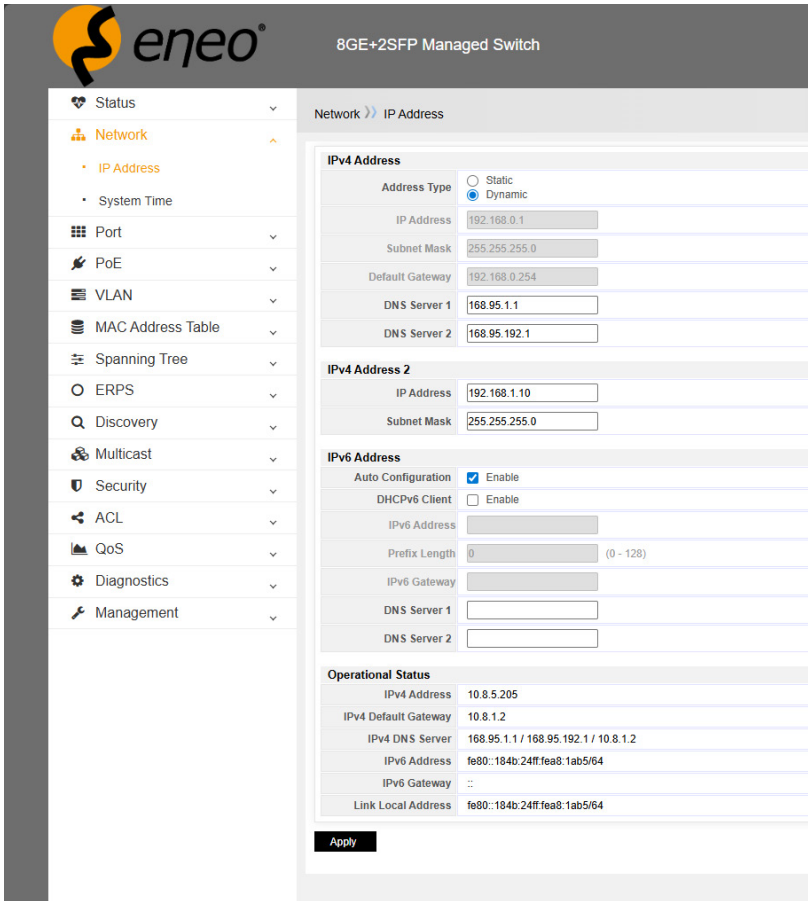
Note!

If you select "Dynamic," the DHCP server assigns an IP address within the predefined range to the switch. The subnet mask and NMS are automatically assigned by the DHCP server. However, the DNS server must still be set up manually.

On this page, you can manually set the IP address, subnet mask, gateway, and other information; you can also use your network, including a DHCP server that automatically assigns an IP address.

Note!

DHCP server (Dynamic Host Configuration Protocol Server) is a network server that automatically assign IP addresses and other network configuration parameters to devices in a network.



The **default IP address** of the switch is: 192.168.1.199

Default subnet mask: 255.255.255.0

Default gateway: 192.168.1.254

When you have finished editing, click "Apply" to complete the IP address settings.

Note!

Automatic IP address assignment: When a device (e.g., a computer, smartphone, or printer) connects to a network, the DHCP server assigns it an IP address. This IP address is essential for the device to communicate with other devices on the network and access the Internet.

Note!

Temporary leases: The IP addresses assigned by the DHCP server are usually assigned for a specific period of time (lease). After the lease expires, the device can request a new IP address or renew the existing one. This contributes to the efficient management of the limited number of IP addresses available in a network.

Note!

Subnet mask: The DHCP server also provides the device with the subnet mask. The subnet mask helps the device understand which part of the IP address refers to the network and which part refers to the host (the device) within the network.

Note!

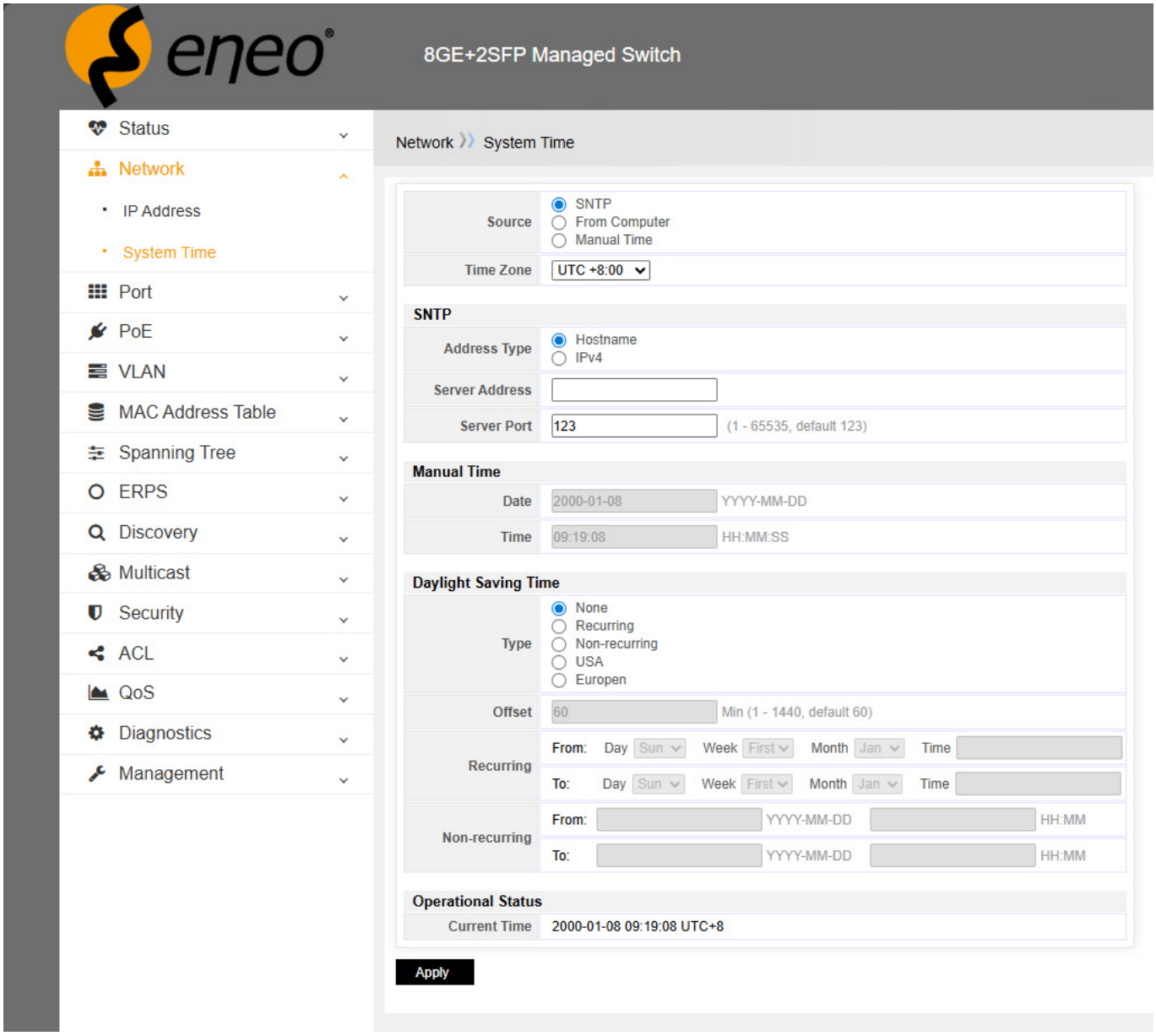
Default gateway: Assignes the default gateway address. The default gateway is the IP address of the router that connects the local network to other networks (such as the Internet). Devices use this gateway to send data to destinations outside their local network.

Note!

DNS server: The DHCP server informs the device about the DNS servers (Domain Name System). DNS servers translate domain names that are readable by humans (such as www.example.com) into IP addresses that devices can understand. This allows devices to easily access websites and other Internet resources.

2.3 – Time configuration

The system time of the switch can be retrieved via SNTP, the computer accessing the switch, and manual configuration.



2.3.1 – Source

2.3.1.1 – SNTP

SNTP (Simple Network Time Protocol) is a simplified version of NTP (Network Time Protocol), which is used to synchronize the clocks of devices in a network.

If no time source is available in your own network and the time is to be retrieved from an external source via the Internet, the data from the external NTP server can be entered directly, e.g. 213.209.109.45 at http://www.pool.ntp.org/de/

2.3.1.2 – From the computer

The system time is synchronized with the current computer time.

2.3.1.3 – Manual time

You can set any time manually.

2.3.2 – Time zone

A time zone is an area of the Earth where a uniform standard time applies for legal, economic, and social reasons. Time zones are usually based on the position of the sun relative to the Earth and generally differ by a certain number of hours (or in some cases by half hours) from Coordinated Universal Time (UTC). The standard time zone in Germany, for example, is UTC+1.

If the time is obtained via SNTP, you can enter the IPv4 address of the time server and 123 for the standard port directly. Make sure that the switch can actually reach the respective IP address.

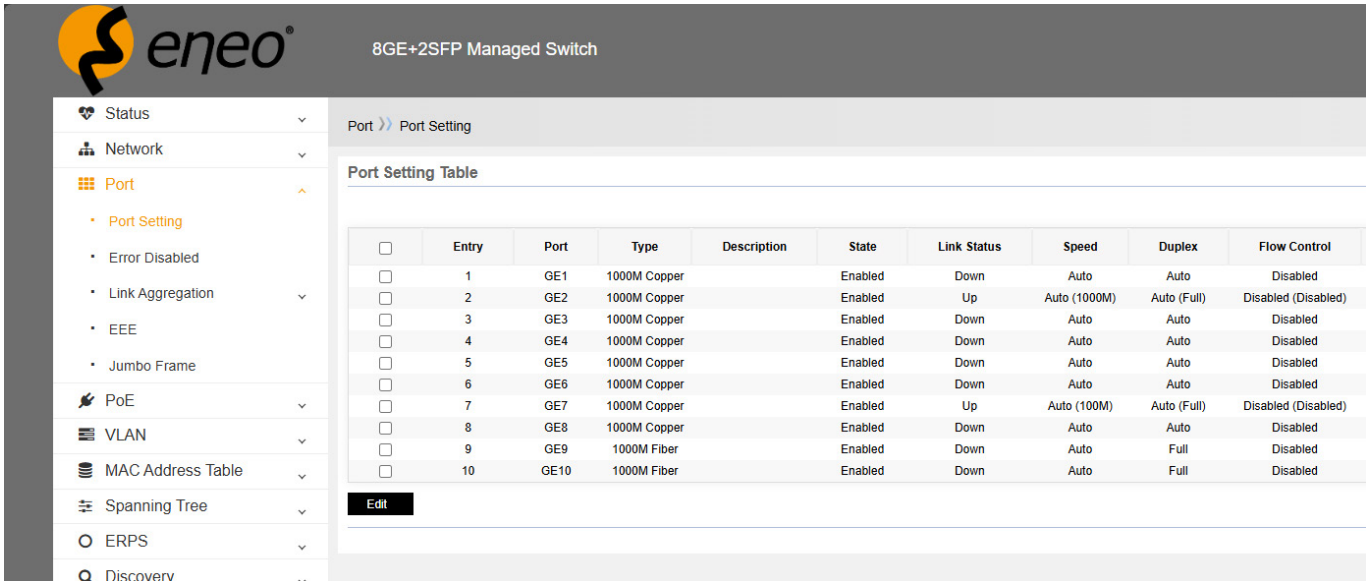
3 – PORT CONFIGURATION

On this page, you can set the descriptions, management status, speed, duplex mode, and flow control of the port. The ports are set to auto mode by default. Auto negotiation is a process that allows two connected Ethernet network ports to independently negotiate and configure the highest possible transmission speed and duplex mode. This process only applies to twisted pair cables—not fiber optic connections.

In some cases, however, the end device may not be recognized correctly. This sometimes occurs when using a camera with a 100 Mbps interface. In this case, the port must be set manually to 100 Mbps.

If a port is not to be used for security reasons, it can be completely disabled.

3.1 – Port settings



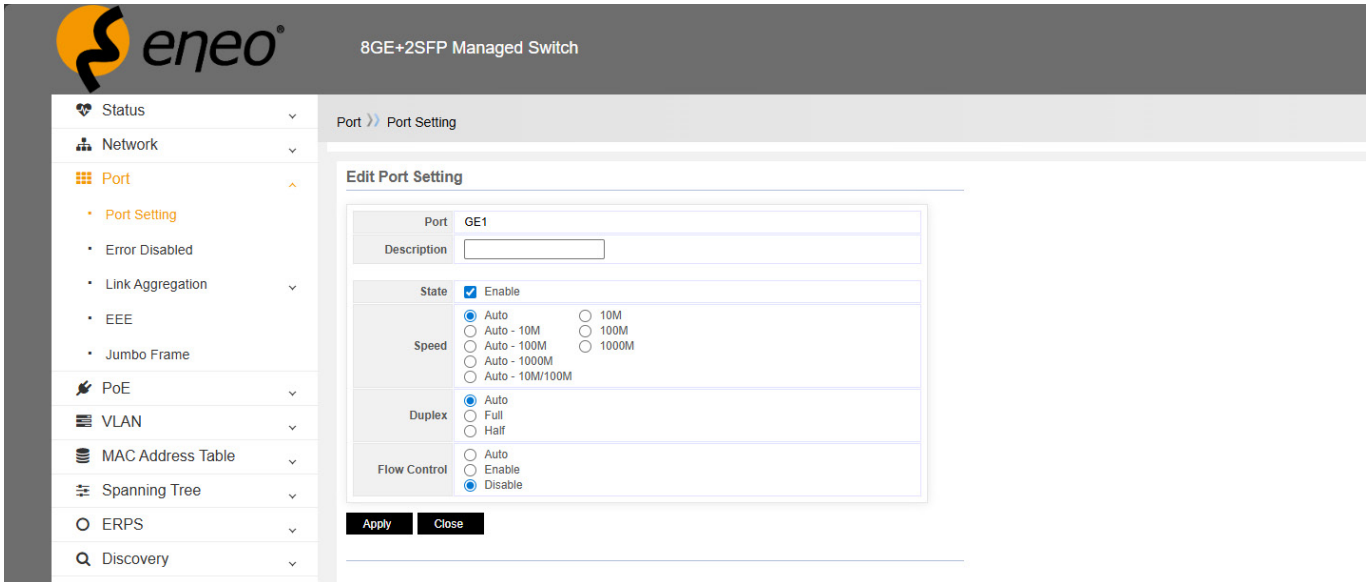
Entry: Entry number of the port

Port: The name of the port. GE stands for Gigabit Ethernet and refers to a network interface that supports data transfer rates of up to 1 gigabit per second (1 Gbps).

Type: Type of transfer rate and medium.

Status: Enable/Disable. You can disable the port by changing the port status.

Link Status: If the port is properly connected, it is UP, otherwise it is DOWN.



The following steps show how to configure the port settings.

1. Select the port to be configured, e.g., Port 1-4.
2. Click on "Edit" at the bottom left.
3. Set the description, management status, speed, duplex mode, and flow control.
4. Click on "Apply" at the bottom left.

State: Enable/disable connection status. If you select "Enable," this port can be used normally. If you disable "Enable," this port cannot be used normally.

Speed: Set the default speed for automatic negotiation (5 types) and forced mode (3 types).

Duplex: Select from Auto, Duplex, and Half Duplex

Flow Control: Enable and disable automatic negotiation. Flow control is a mechanism for managing the amount of data sent over a network or communication link. It ensures that the sender does not overload the receiver with more data than it can process or buffer. This is crucial for maintaining reliable and efficient communication, especially in environments where the sender and receiver have different processing capacities or where network conditions vary.

Halbduplex-Modus: Two-way communication, but not simultaneously in both directions.

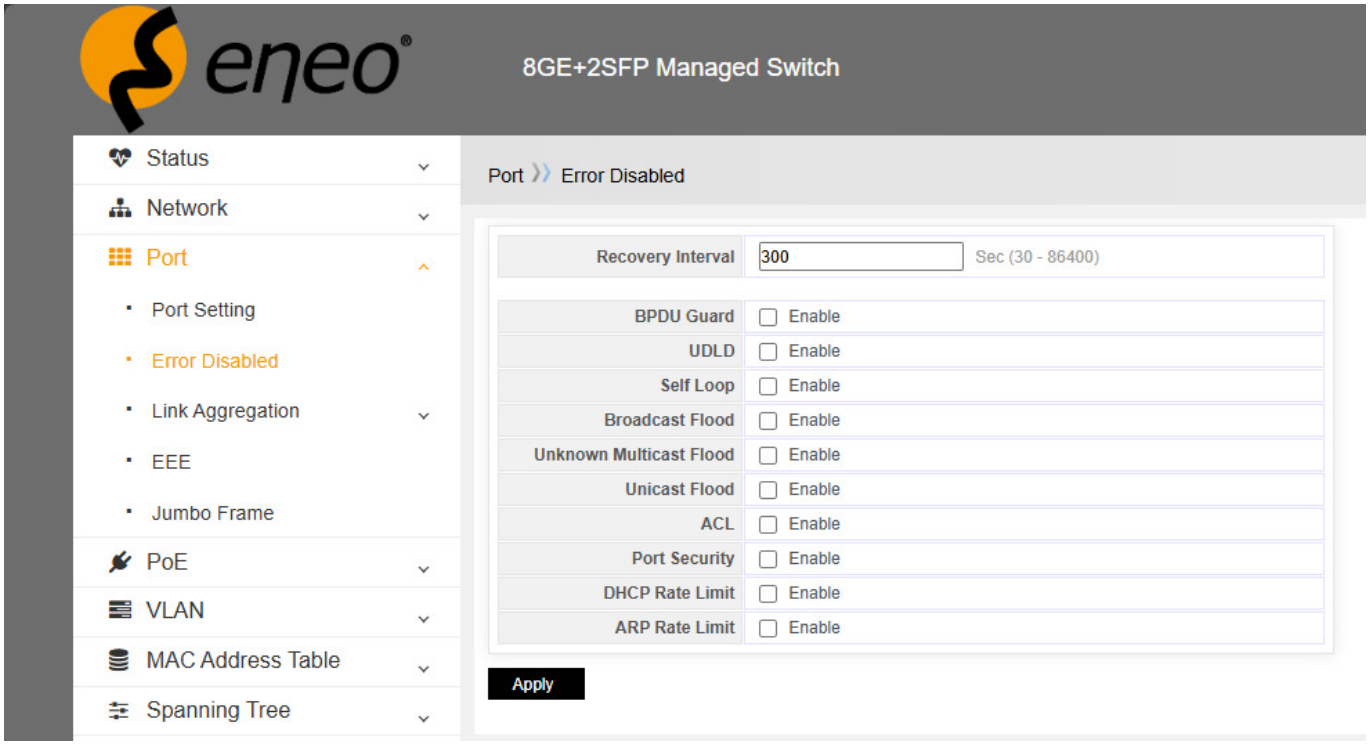
Vollduplex-Modus: Two-way communication, simultaneously in both directions.

3.2 – Error disabled

Troubleshooting for an error-related interface deactivation includes the following error symptoms: The line is blocked, the physical indicator is off or orange (the indicator status varies depending on the platform).

After a certain period of time (300 seconds by default), the system attempts to restore the interface that was disabled due to an error.

However, if the cause of the error deactivation has not been fundamentally resolved, the interface will be deactivated again as error-related after restoration.



From the list, we can identify common causes such as UDLD, DPUD Guard, port security, and loops. You can set the recovery interval and select the most common causes of deactivation

UDLD

UDLD stands for Unidirectional Link Detection. It is a data link layer protocol developed by Cisco Systems to monitor the physical configuration of cables and detect unidirectional connections.

A unidirectional connection is a connection that exists on both sides of the connection, but packets are only received from one side. This can lead to problems such as forwarding loops and traffic blackholing.

UDLD works by exchanging protocol packets between neighboring devices. Each switch port configured for UDLD sends UDLD protocol packets containing the device and port ID of the port and the neighbor device and port IDs detected by UDLD on that port. If a port does not see its own device and port ID in the incoming UDLD packets for a certain period of time, the connection is considered unidirectional. As soon as a unidirectional connection is detected, the corresponding port is disabled.

UDLD is a Cisco-specific protocol, but similar functions are available under different names in products from other vendors. HP, for example, calls its function Device Link Detection Protocol (DLDP), Extreme Networks calls it Extreme Link Status Monitoring (ELSM), and AVAYA calls it Link-State Tracking.

1. BPDU protection:

   Automatically disables a port when BPDU packets are detected, preventing unauthorized devices from interfering with the Spanning Tree Protocol (STP).

2. UDUL (UniDirectional Link Detection):

   Detects and blocks unidirectional fiber/copper connections to prevent network instability caused by one-way communication.

3. Self-loop detection:

   Identifies and blocks physical port loops (e.g., a cable connecting two ports on the same switch) to prevent traffic storms.

4. Broadcast flood control:

   Limits excessive broadcast traffic to prevent network congestion and performance degradation.

5. Unknown Multicast Flood Control:

   Restricts the flooding of unknown multicast frames, optimizing bandwidth utilization.

6. Unicast Flood Control:

   Blocks excessive flooding of unknown unicast traffic to reduce the risk of resource exhaustion.

7. ACL (Access Control List):

   Filters traffic based on predefined rules (e.g., IP/MAC addresses, ports) to enforce security policies.

8. Port security:

   Restricts port access to authorized MAC addresses, preventing unauthorized device connections.

9. DHCP rate limiting:

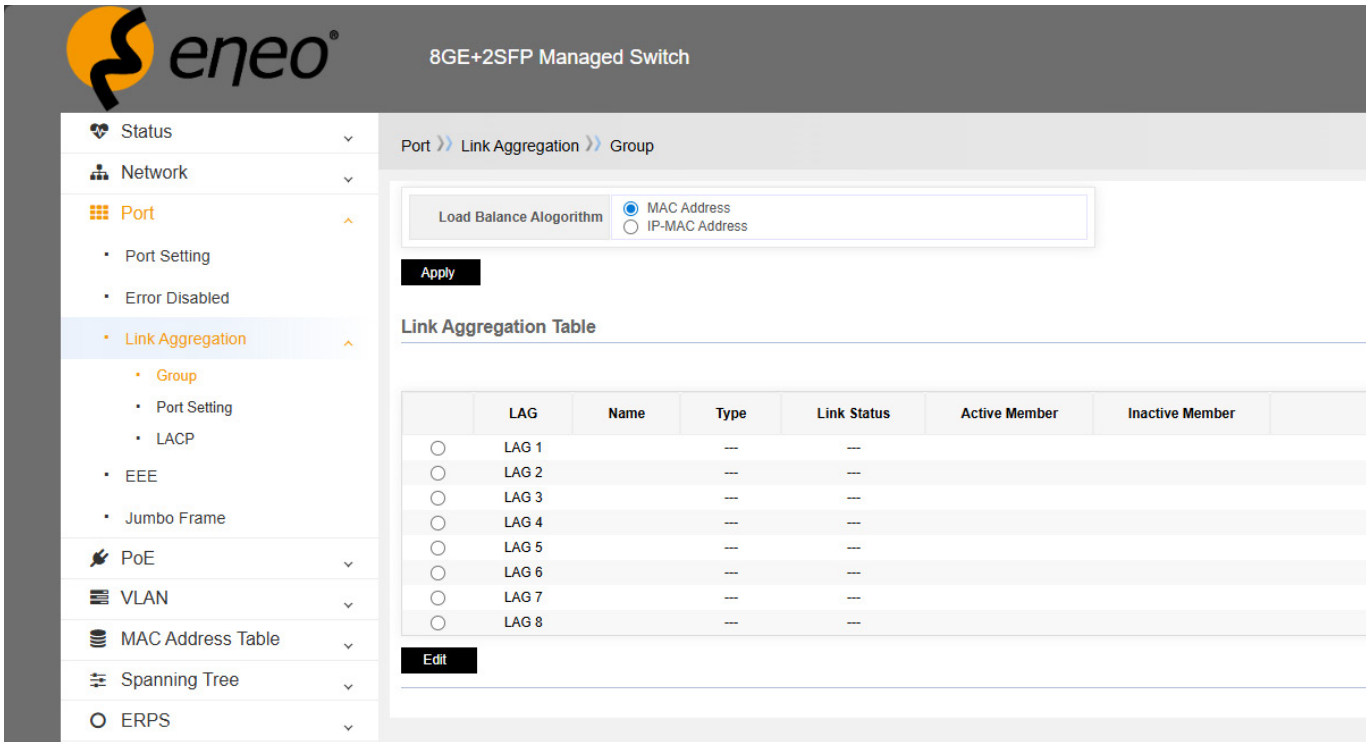
   Controls the number of DHCP requests per port to prevent DHCP exhaustion attacks.

10. ARP rate limiting:

    Throttles the frequency of ARP packets to prevent ARP spoofing or flooding attacks.

3.3 – Link aggregation

Link aggregation can combine multiple Ethernet ports into a logical aggregation group. At the layer entity, all physical connections in an aggregation group are a logical connection. Link aggregation is designed in an aggregation group to increase bandwidth by distributing the output/input load between the member ports. The link aggregation group also enables port redundancy to ensure connection reliability. A link aggregation consists of a maximum of eight properly configured Ethernet interfaces. All interfaces in the link aggregation must have the same speed and be configured as Layer 2 interfaces.



LAG (Link Aggregation Group): LAG refers to a group of physical Ethernet ports that are bundled together to increase throughput and ensure redundancy. This allows multiple physical connections to be treated as a single logical connection, improving network performance and reliability.

TYP: LAG can be set to static or LACP. Static is a common type of link aggregation. LACP is described in detail in ► „3.3.3 – LACP“.

Link status: If the port is properly connected, it is UP, otherwise it is DOWN.

3.3.1 – Define group and add ports

Load balancing algorithm:

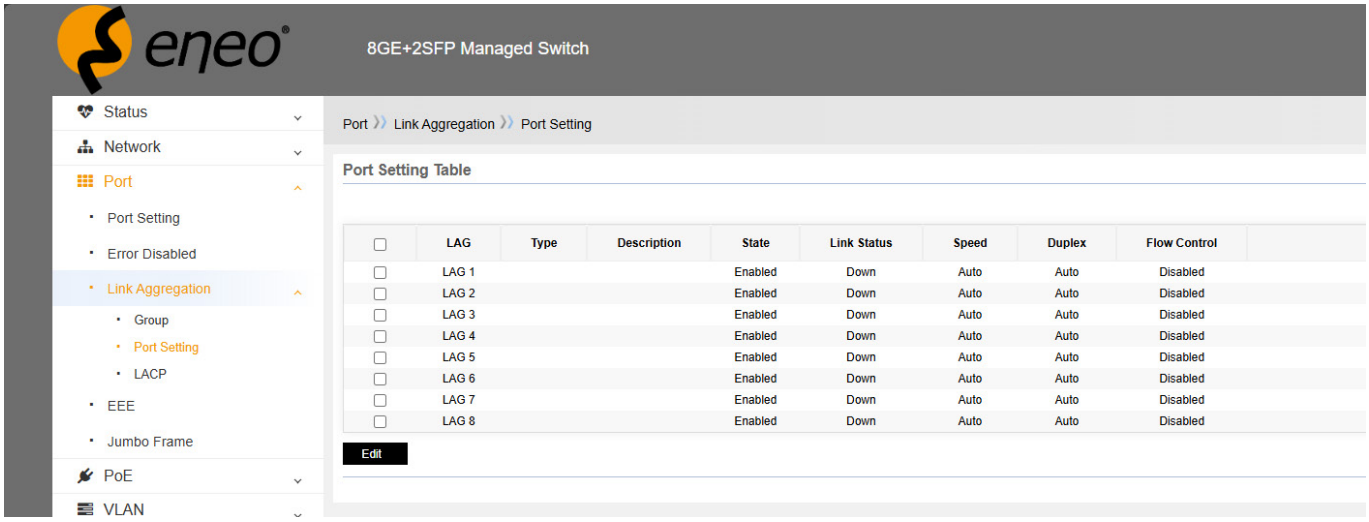
- MAC address (source MAC + destination MAC)
- IP-MAC address (source IP + destination IP + source MAC + destination MAC)

This is an aggregated routing algorithm.
The route of a message is selected based on its address

1. Select an aggregation group (1-8), LAG 1 ~ LAG 8
2. Click "Edit"
3. Select "Static" to add the port from the left field to the right field and add it to the aggregation group. A maximum of 8 aggregation groups and a maximum of 8 member ports per aggregation group are supported.

3.3.2 – Settings for aggregation port properties

Set the speed, duplex, and flow control of the aggregation port so that they match the port settings in ► „3.1 – Port settings“



Port: The name of the LAG.

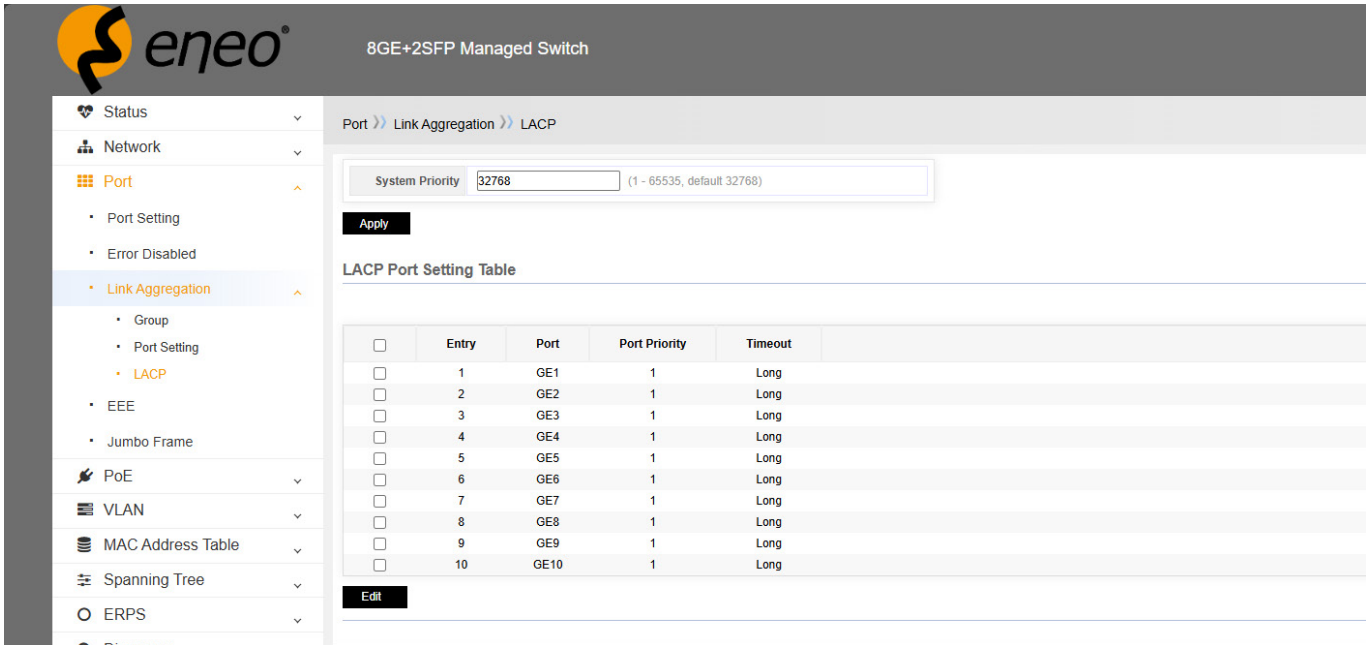
Description: Can be used to describe the use of a LAG port.

Status: Enable or disable. You can disable the port by changing the port status.

3.3.3 – LACP

LACP (Link Aggregation Control Protocol) is an industry-standard protocol defined in the IEEE 802.3ad standard. It is used to combine multiple physical connections into a single logical connection called a Link Aggregation Group (LAG) or EtherChannel. This aggregation helps increase bandwidth and provides redundancy, as traffic can be distributed across the member links and failover can occur if one link fails.

LACP operates at the data link layer and sends Link Aggregation Control Protocol Data Units (LACPDUs) between devices. These LACPDUs contain information such as the device's LACP system priority, MAC address, interface priorities, and interface numbers. Based on this information, the devices negotiate which connections are to be bundled and which are active for forwarding data traffic.



Set the system priority of LACP and ports.

The value is configured by default and can be changed by users as needed.

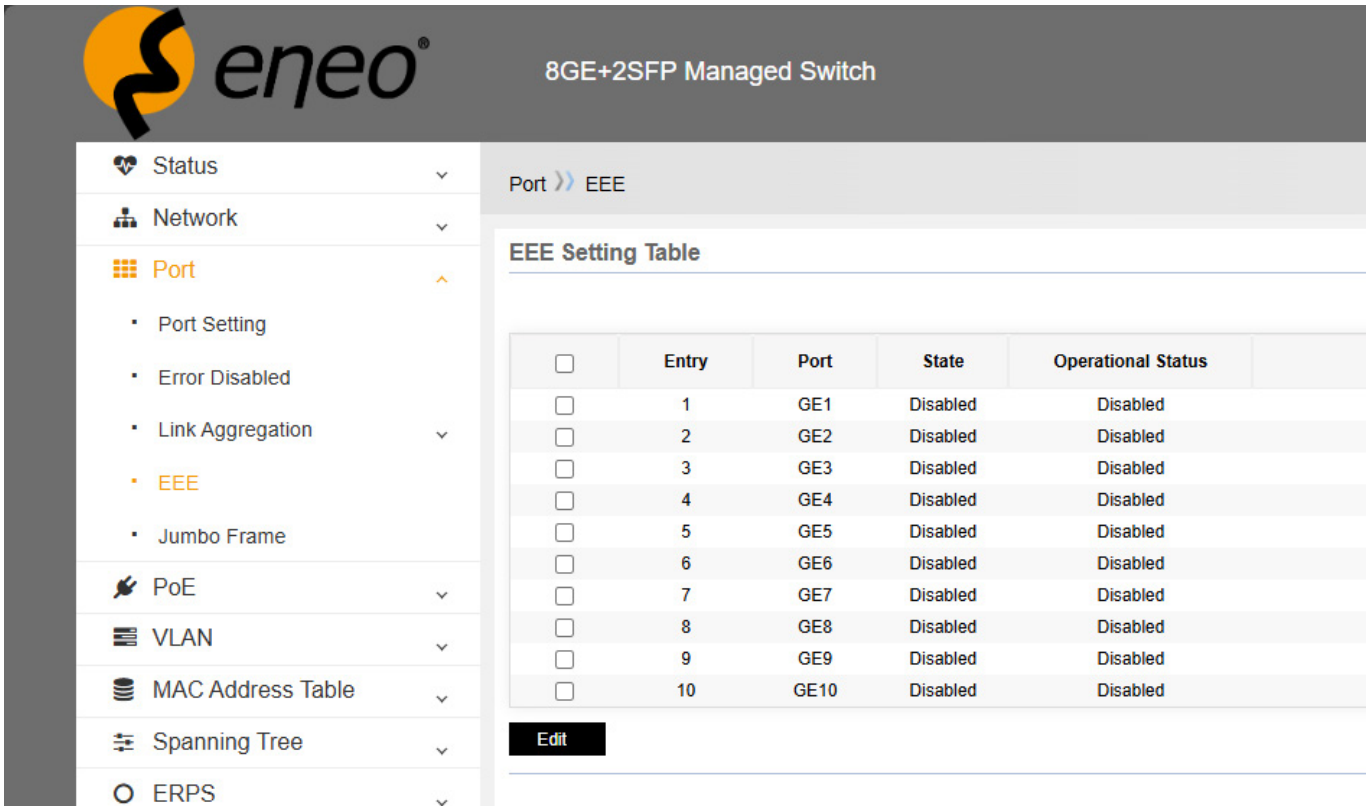
System priority: This parameter specifies the LACP priority. A smaller parameter value means a higher LACP priority.

Port priority: This parameter specifies the priority for joining LACP per port. The priority can be set between 1 and 65535, with the default value being 1. A smaller parameter value means a higher priority.

Time limit: Can be set to long or short.

3.4 – EEE

Energy Efficient Ethernet, or EEE for short, refers to "energy-efficient Ethernet technology" with the function of automatically reducing power consumption when the network card has no data traffic. The maximum power consumption can only be reached when the network is heavily loaded.



EEE is disabled for the port by default. If you require this function, simply enable it for the port.

3.5 – Jumbo Frame

A jumbo frame is an Ethernet frame with a length of more than 1522 bytes.
This is a standard format specified by the manufacturer for particularly long frames, which was developed specifically for Gigabit Ethernet. The length of jumbo frames varies between 9000 and 64000 bytes, depending on the manufacturer.
The jumbo frame can fully utilize the performance of Gigabit Ethernet and improve data transfer efficiency by 50% to 100%. The jumbo frame is extremely important in network storage environments.

As long as the jumbo frame is enabled, it supports transfer speeds of up to 10K.

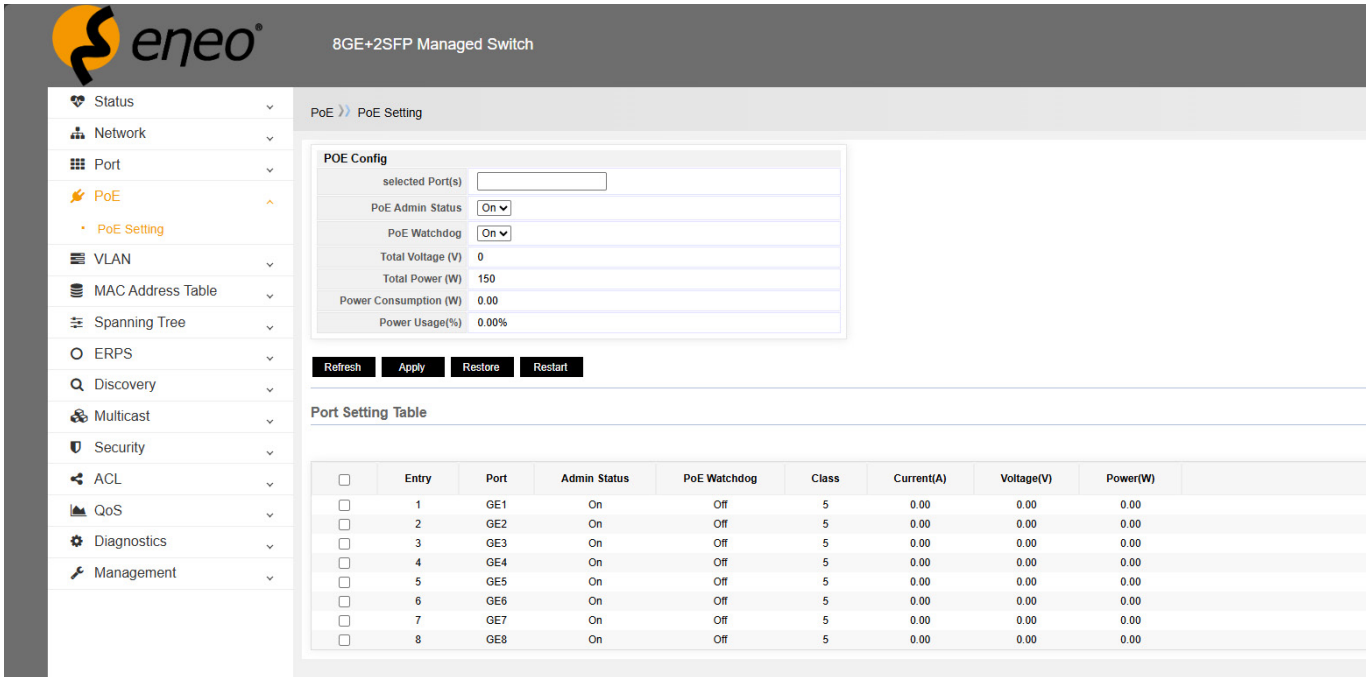
4 – POE

4.1 – PoE Configuration

Power over Ethernet (PoE) enables a network device to supply power to terminals via twisted pair cables. The device supports IEEE 802.3af and IEEE 802.3at.

IEEE 802.3af: A standard for Power over Ethernet (PoE) that enables the transmission of data and power over a single Ethernet cable and allows a maximum output power of 15.4 W per port.

IEEE 802.3at: Also known as PoE+ (Power over Ethernet Plus), is an extended standard for power supply via Ethernet cables. It allows a maximum output power of 30 watts per port from the Power Sourcing Equipment (PSE). At least 25.5 watts are available at the Powered Device (PD), taking into account power losses via the cable.



In the "Port Configuration" section, select the ports you want to configure and set the parameters. Click "Apply."

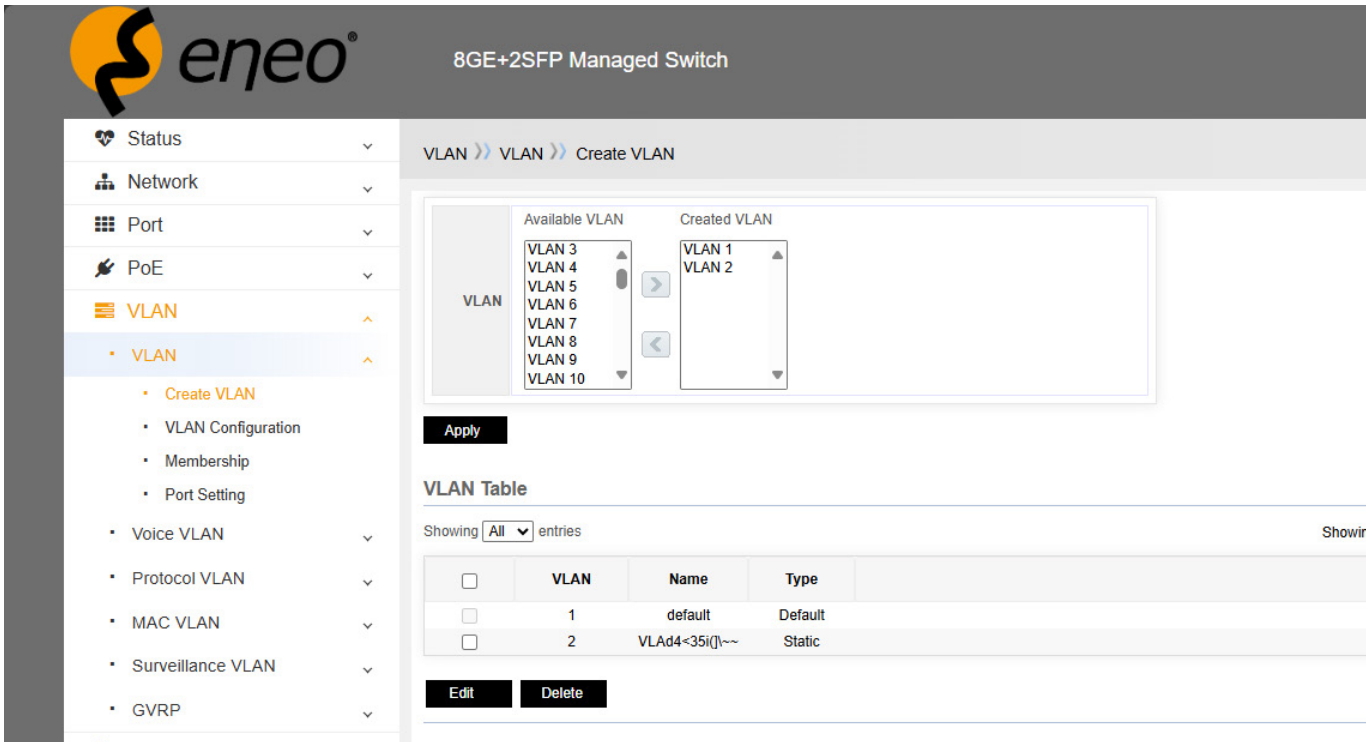
PoE Admin Status: Enable or disable the PoE function on the corresponding ports. A port can supply power to the PD when its status is enabled.

PoE Watchdog: If switch port communication fails, the corresponding PoE port automatically detects this, restarts, restores network communication independently, and reduces manual intervention and maintenance work.

5 – VLAN

VLAN (Virtual Local Area Network) is a network concept that enables the creation of multiple separate logical networks within a single physical network infrastructure.

5.1 – Create VLAN



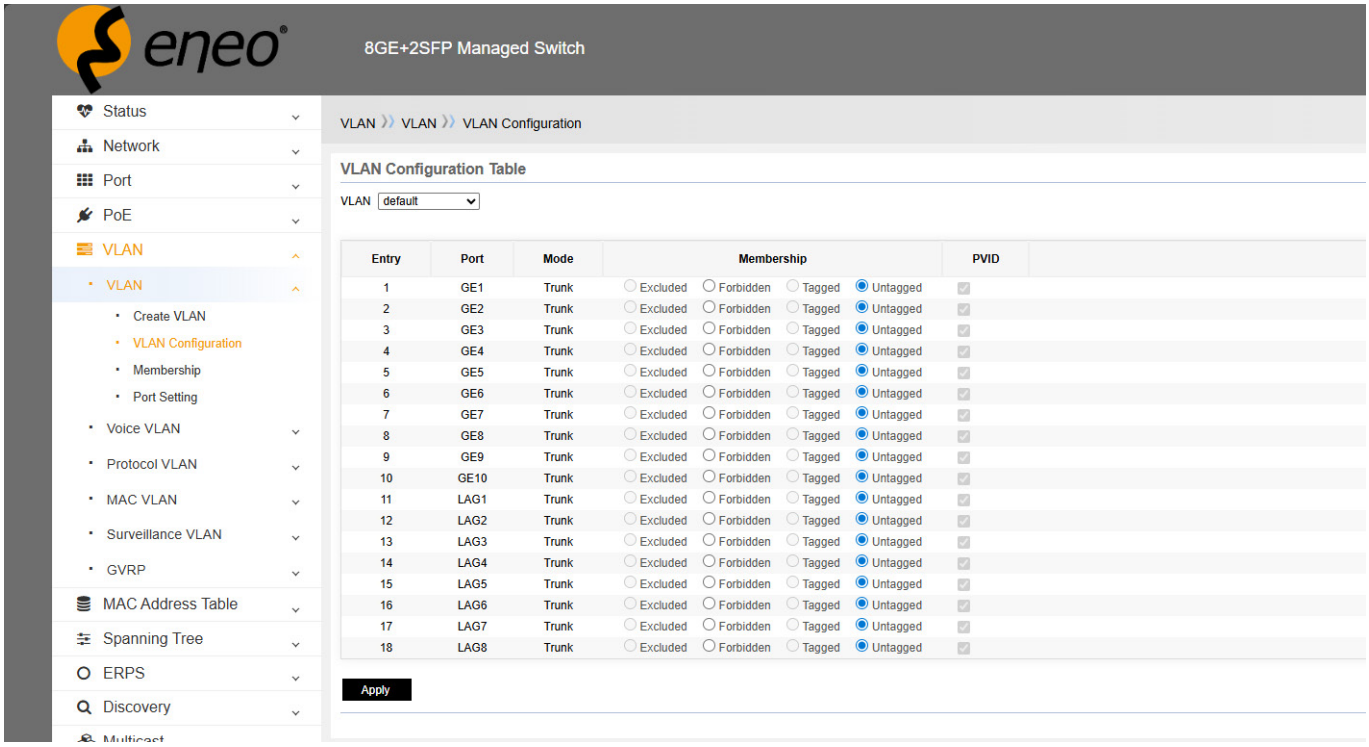
The total number of VLANs is 1-4094.

Select the VLAN number in the left field and add it to the right field to create a VLAN.

VLAN 1 is created by default and cannot be deleted. Therefore, the type of VLAN 1 is “Static” by default. You can edit and rename the VLAN.

5.2 – VLAN configuration

Configure 802.1Q_VLAN for the switch.

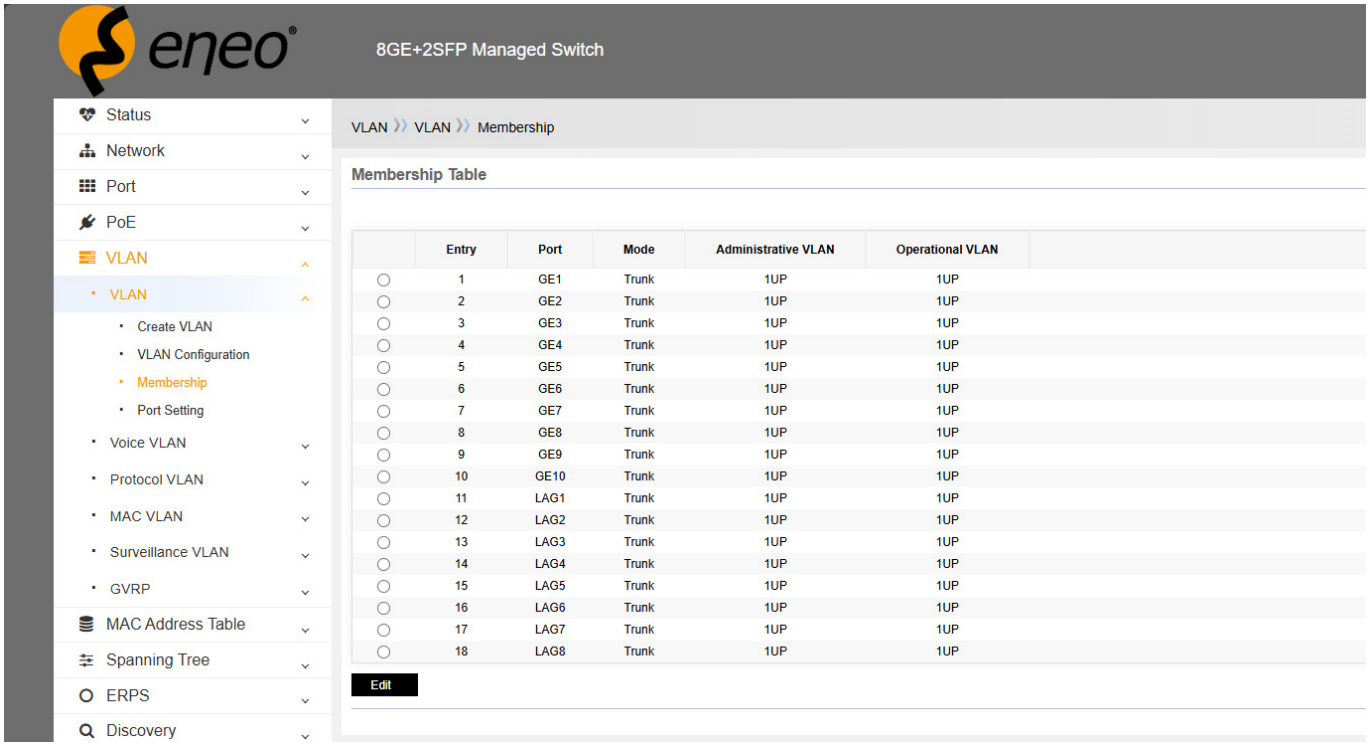


Default: Default means VLAN 1. It is clear that all ports belong to VLAN 1 and are not tagged, PVID=1.

If VLAN 2 is selected for VLAN, there are no members by default, so they can be set manually.

5.3 – Membership

VLAN configuration of the switch.



Administrative VLAN: VLAN setting of the port.

Operational VLAN: Indicates the properly functioning VLAN. If the settings are correct, this corresponds to the administrative VLAN.

In the next section, we will introduce the VLAN mode of the port.

5.4 – Port Settings

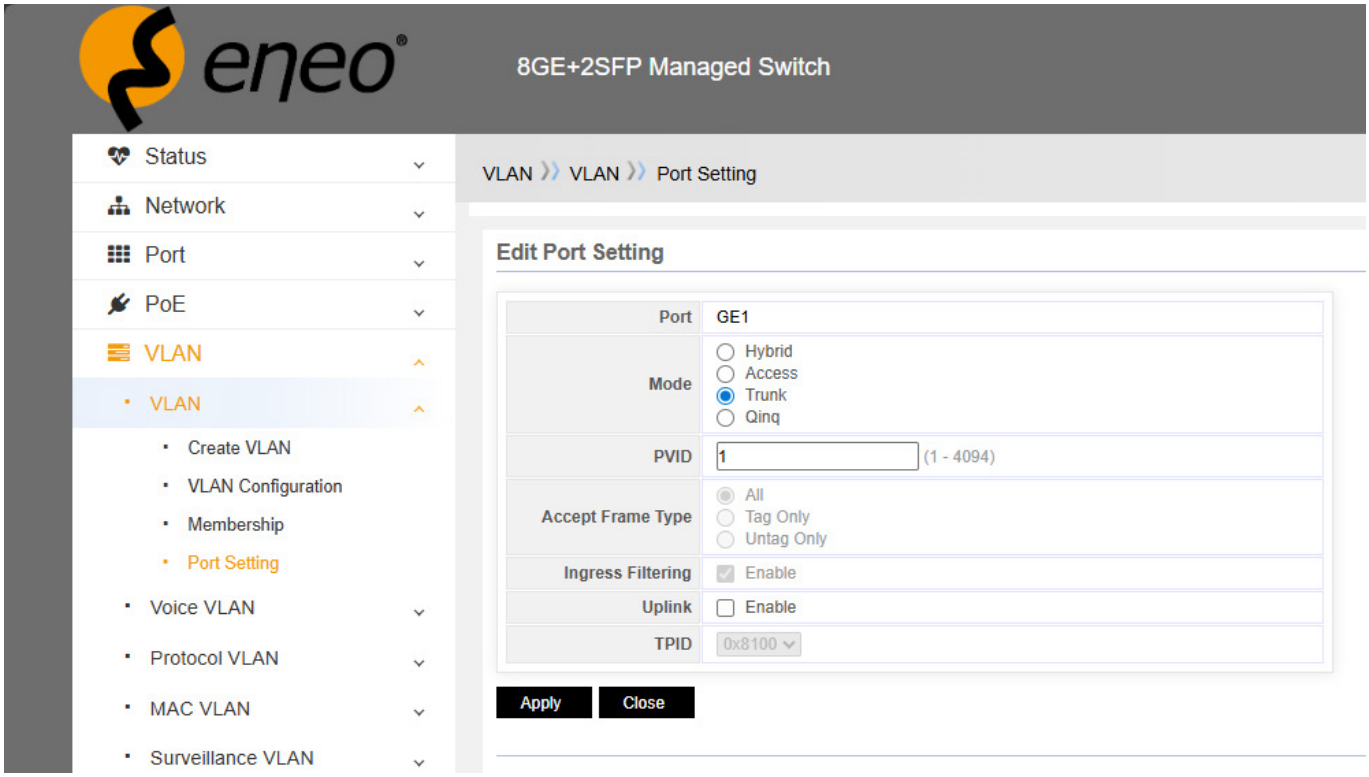
Configure the port mode, input detection function, and TPID function.

Input detection: If the port is a hybrid connection, tag messages, untagged messages, or all messages can pass through input detection.

TPID (Tag Protocol Identifier) is a field in the VLAN tag. According to the IEEE 802.1Q protocol, the value of this field is 0x8100. The default setting of the device is the TPID value specified in the protocol (0x8100). Some manufacturers set 0x9100 or other values as the TPID value that can be recognized by the device.

To be compatible with these devices, the device provides an adjustable function for the TPID value of global VLAN VPN messages, and users can configure the TPID value themselves. When the VLAN VPN uplink port forwards messages, it replaces the TPID value in the outer VLAN tag of the message with the value specified by the user and then sends it so that the VLAN VPN message sent to the public network can be recognized by devices from other manufacturers.

This allows these parameters to be configured according to customer requirements.



There are three VLAN modes: Access, Trunk, Hybrid

- **Access:** Connection to end devices (such as PCs, cameras, set-top boxes, etc.) and direct setting of PVID.
- **Trunk:** The port that is connected between switches. In general, many VLANs must be set to perform a tagging function.
- **Hybrid:** Mixed mode. It can perform tagging for many VLANs or untagging for other VLANs.

PVID: PVID is the default VLAN ID assigned to a port on a switch. When a switch port receives an untagged frame (i.e., a frame without a VLAN tag), it assigns the PVID to that frame, effectively placing it in the appropriate VLAN.

ACCEPT FRAME TYPE: You can only select this option if you have selected hybrid mode. Set the frame type to accept all frame types or only tagged/untagged frames.

As shown in the figure above, set the access mode for ports 5 and 6 at the same time and change the PVID value to 5.

Warning!

When setting the PVID value, VLAN must be added before the setting. VLAN2-4 was added in Chapter 6.1, so you can set 5. However, if the value is set to 9, the system reports an error and the setting is not successful. Under normal conditions, neither input detection filtering nor TPID is set. Apply the default value directly.

Note!

If you need to check the log information, visit the "Status Logging Message" page.

6 – MAC ADDRESS TABLE

6.1 – Introduction to MAC Addresses

6.1.1 – Introduction to the MAC Address Table

The main function of an Ethernet switch is to forward messages on the data link layer, i.e., to output the message to the appropriate port according to the MAC address of the recipient. The MAC address forwarding table is a 2-layer forwarding table that contains the corresponding relationships between MAC addresses and forwarding ports. It is the basis for the fast forwarding of Layer 2 messages by the Ethernet switch, which in turn is the basis for the fast forwarding of the above-mentioned 2-layer messages by the Ethernet switch. The entries in the MAC address forwarding table contain the following information:

- MAC destination address
- VLAN ID of the port
- Forwarding port number on the device

When the Ethernet switch forwards messages, it applies the following two forwarding methods according to the information in the MAC address table:

- **Unicast mode:** If the MAC address forwarding table contains a table entry that matches the MAC destination address of the message, the switch sends the message directly from the forwarding port of the table entry.
- **Broadcast mode:** If the switch receives messages with the destination address F or the MAC address forwarding table does not contain a table entry for the MAC address of the message recipient, the switch uses broadcast mode to forward the message to all ports except the receiving port.

6.1.2 – Introduction to the MAC address learning process

The entries in the MAC address forwarding table can be updated and maintained in two ways:

- Manual configuration mode
- MAC address learning mode

As a rule, most entries in the MAC address table are created and maintained using the MAC address learning function.

6.1.3 – Management of the MAC address forwarding table

6.1.3.1 – Aging mechanism of the MAC address forwarding table

The MAC address forwarding table of the Ethernet switch has a limited capacity. To maximize the use of the address forwarding table resources, the Ethernet switch uses an aging mechanism to update the MAC address forwarding table, i.e., when the system dynamically creates a table entry, it turns on the aging timer, and if it does not receive any MAC address messages from this table entry during the aging period, the switch deletes this MAC address table entry.

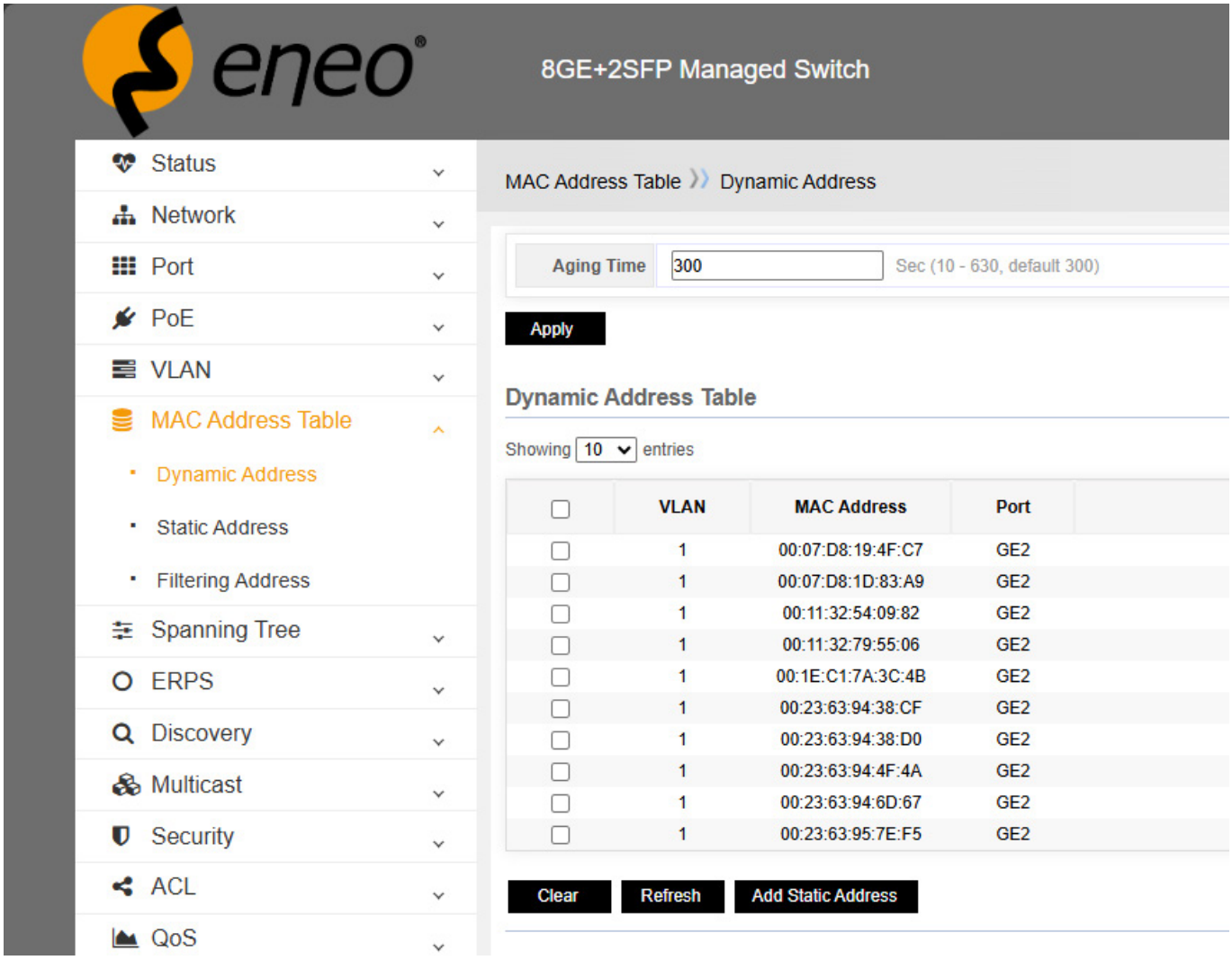
6.1.3.2 – Classification and characteristics of MAC address table entries

Depending on their characteristics and configuration methods, MAC address table entries can be divided into three categories:

- **Static MAC address table entry:** Also known as a "permanent address," it is added and deleted manually by the user and does not age over time. In a network with few device changes, broadcast traffic on the network can be reduced by manually adding static address table entries.
- **Dynamic MAC address table entry:** Refers to the MAC address table entry that expires according to the aging time specified by the user. The switch can add dynamic MAC address table entries via the MAC address learning mechanism or through manual setup by the user.
- **Black hole MAC address filtering:** Also known as "filtered MAC address filtering," this is a special MAC address that is manually configured by the user. When the switch receives a message whose source MAC address or destination MAC address is a black hole MAC address, it discards that message.

6.2 – Dynamic address

The MAC address is automatically learned by this switch, and the entries are as follows:



MAC address: automatically learned by this switch.

Port: transmits the learned MAC address to a specific port.

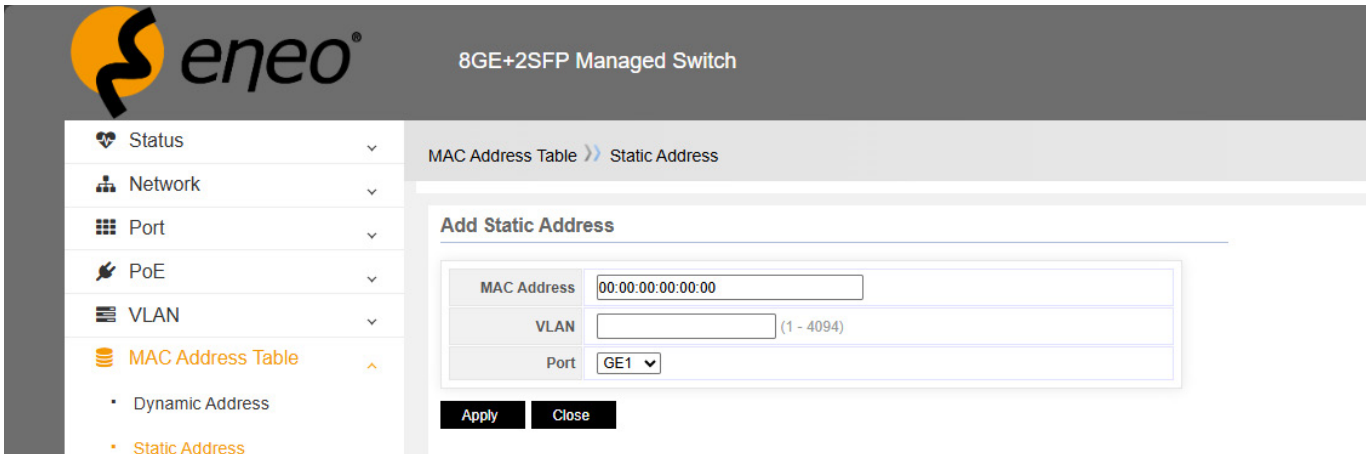
VLAN-ID (1-4094): transmission of the learned MAC address to a specific VLAN.

6.3 – Static address

6.3.1 – Set MAC address alignment

Depending on the actual situation, the administrator can manually add, change, or delete entries in the MAC address forwarding table. They can delete all MAC address table entries that refer to a specific port or delete specific types of MAC address table entries, such as dynamic table entries and static table entries.

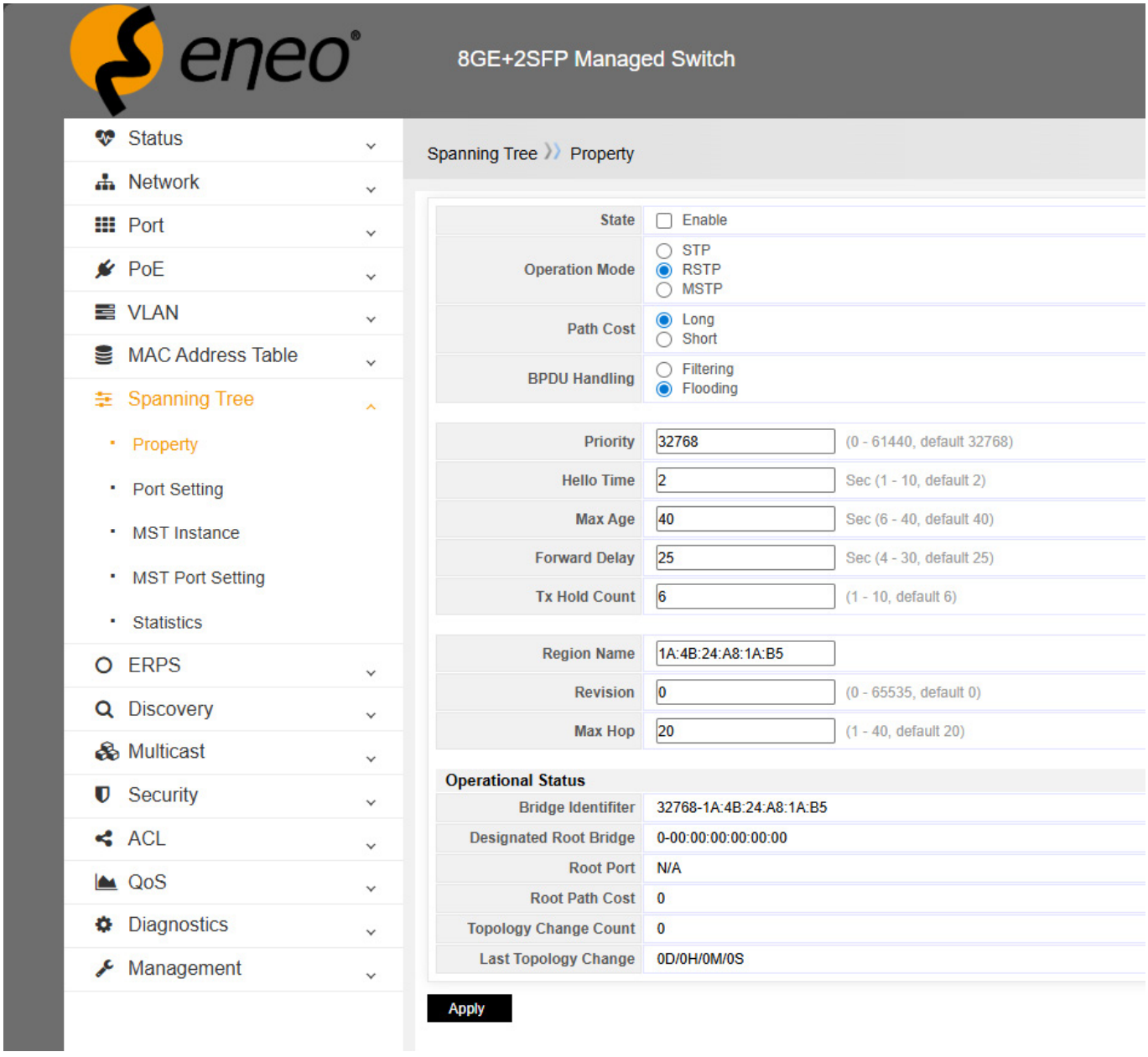
Users can add or delete static MAC address table entries on the page. This is also known as MAC address binding, i.e., linking the MAC address, port, and VLAN.



Example

Manually add the static MAC address 28:D2:44:80:B2:F0 to port GE 2.

1. Click "Add" to open the dialog box for adding a static MAC address.
2. Enter the MAC address, the VLAN number, and the port number to be bound.
3. Click "Apply."



The results of the binding configuration are as follows:

1. This MAC address can only communicate via port GE 2. If this MAC is connected to another port, it cannot receive messages whose destination address is this MAC. If the destination address received by this switch is the bound MAC address, this switch forwards the message only to this bound port.
2. After configuring the static MAC address, the address entry originally present in the dynamic MAC is deleted.

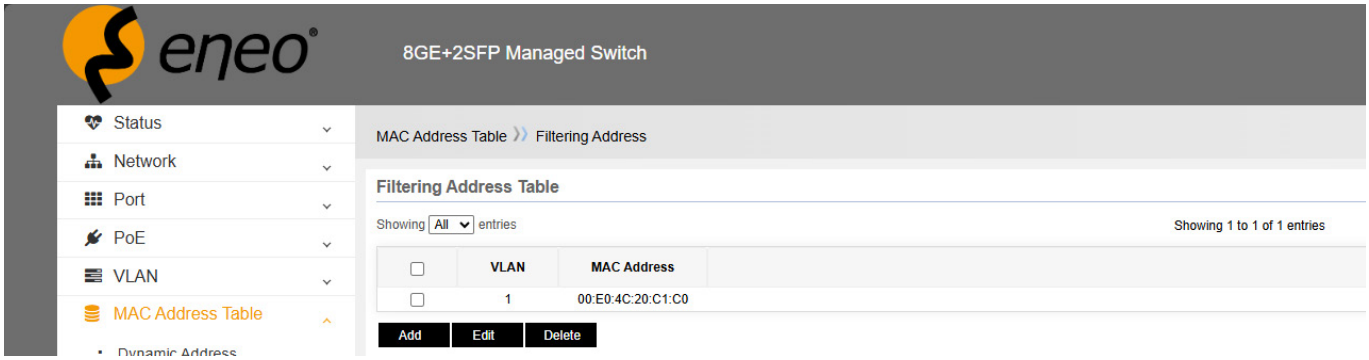
6.4 – MAC address filtering

If the entry for MAC address filtering is set in this switch, the message with this MAC address is discarded as soon as the switch receives it, regardless of whether it is in the source MAC or destination MAC.

Example

Add MAC address filtering: 00:E0:4C:20:C1:C0

1. Click "Add" to open the dialog box for adding a static MAC address.
2. Enter the MAC address and the VLAN to be assigned.
3. Click "Apply."

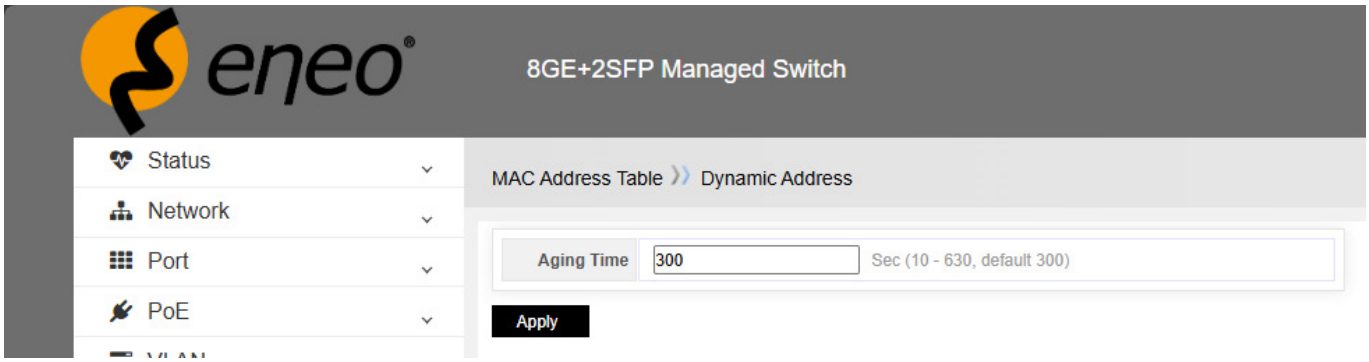


MAC Address: Enter the MAC address that should be rejected.

VLAN-ID (1-4094): Enter the VLAN of the rejected MAC address.

6.5 – MAC expiration time

Users can customize the expiration time for dynamic MAC address table entries. If the expiration time configured by the user is too long, the device may store many outdated MAC address table entries, which will exhaust the resources of the MAC address table and prevent the device from updating the MAC address table according to changes in the network. If the expiration time configured by the user is too short, the device may delete valid MAC address entries, which may cause the device to send a large number of data packets and affect performance. Therefore, users must configure an expiration time that suits the actual situation to use the MAC address expiration function effectively.



Enter the aging time and click "Apply."

The aging time of the dynamic MAC address table applies to all ports, and address aging only works for dynamic (learned by the device or dynamically configured by the user) entries in the MAC address table.

7 – SPANNING TREE PROTOCOL

7.1 – Introduction to STP

7.1.1 – Application of STP

STP (Spanning Tree Protocol) is a protocol based on the IEEE 802.1D standard that is used to eliminate physical loops on the data link layer in LANs. The devices running this protocol use mutual information to find loops in the network and selectively block some ports. Finally, the loop structure of the network is reduced to a tree-like network structure without loops to prevent continuous propagation and endless circulation of messages in the loop network and to avoid a reduction in packet processing capacity due to repeated reception of the same messages.

STP has two meanings. In a narrow sense, STP refers to the STP protocol defined in IEEE 802.1D, and in a broader sense, it refers to the STP protocol defined in IEEE 802.1D and various improved spanning tree protocols based on it.

7.1.2 – STP protocol messages

The protocol message in STP is BPDU (Bridge Protocol Data Unit), also known as a configuration message.

STP can determine the network topology by transmitting BPDUs between devices. BPDUs contain enough information to ensure that the device can complete the spanning tree calculation process.

BPDU can be divided into two types in the STP protocol

- **Configuration BPDU:** A message used to calculate the spanning tree and maintain the spanning tree topology.
- **TCN-BPDU** (Topology Change Notification BPDU): When the topology changes, this message is used to inform devices connected to the network topology about the changes.

7.2 – Basic concept of STP

7.2.1 – Root Bridge

The tree structure of a network must have a root, so STP introduces the concept of the root bridge. There is only one root bridge in the entire network, and the root bridge changes with the network topology, so the root bridge is not fixed.
After the network has converged, the root bridge generates the configured BPDU at specific time intervals and sends it. Other devices transmit the configured BPDU to ensure the stability of the topology.

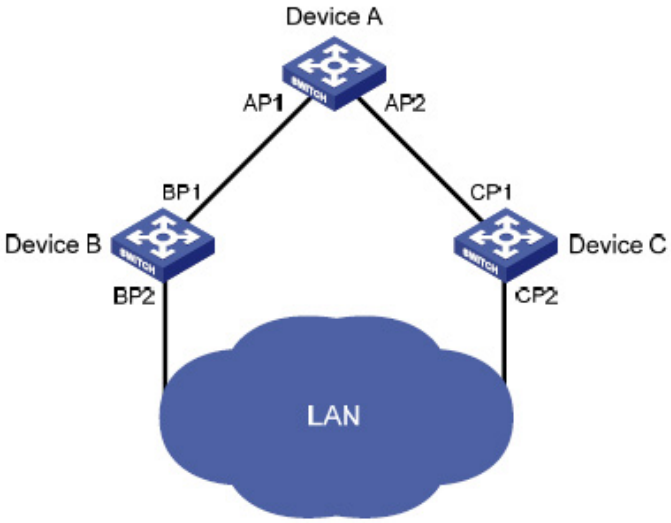
7.2.2 – Root Port

The root port is the port on a non-root bridge device that is closest to the root bridge. The root port is responsible for communicating with the root bridge. There is only one root port on a non-root bridge device. There is no root port on the root bridge.

7.2.3 – Specified bridge and specified port

The definitions of specified bridge and specified port can be found in this table.

Type	Specified bridge	Specified port
For one device	This device is directly connected to the local computer and is responsible for transmitting configuration messages to the local computer.	This port transmits configuration messages from the specified bridge to the local computer.
For LAN	This device is responsible for transmitting configuration messages to the local segment.	This port transmits configuration messages from the specified bridge to the local computer.



The figure shows the specified bridge and port, where AP1, AP2, BP1, BP2, CP1, and CP2 are the ports of device A, device B, and device C, respectively.

- When device A sends configuration messages to device B via port AP1, the specified bridge of device B is device A and the specified port is AP1.
- Two devices are connected to the LAN: device B and device C. When device B is responsible for transmitting configuration messages to the LAN, the specified bridge of the LAN is device B and the specified port is BP2.

7.2.4 – Path costs

Path costs are the reference value of the STP protocol for connection selection. STP calculates the path costs to select the stronger connection and block the redundant connection, reducing the network to a tree structure without loops.

7.3 – Basic principle of STP

STP can determine the network topology by transmitting BPDUs between devices. The configuration messages contain sufficient information to ensure that the device can complete the calculation process for creating trees, including several important pieces of information such as the following:

- Root Bridge ID: consists of the priority and MAC address of the root bridge;
- Root Path Cost: Path cost to reach the root bridge;
- Specified Bridge ID: Consists of the priority and MAC address of the specified bridge.
- Specified Port ID: Consists of the priority and port name of the specified port.
- Lifetime of configuration messages distributed on the network: Message age.
- Maximum lifetime of configuration messages stored in the device: Max. age.
- Cycle of transmission of configuration messages: Hello time;
- Delay of port status migration: Forwarding delay.

7.3.1 – Specific process of STP algorithm implementation

- Initial state

  At the beginning, each port of each device generates a configuration message, considering itself as the root bridge. The root path costs are 0. The specified bridge ID is the device's own ID and the specified port is the device's own port.

- Selection of the optimal configuration message

  Each device sends its own configuration messages to the outside and receives the configuration messages sent by other devices.
  The selection process for the optimal configuration message is shown in the following table.

Step	Contents
1	After receiving the configuration message, each port proceeds as follows: • If the priority of the configuration message received by the port is lower than that of the port configuration message, the device discards the received configuration message without further processing. • If the priority of the configuration message received by the port is higher than that of the port, the device replaces the contents of the port configuration message with the received configuration message.
2	The device compares the configuration messages of all ports to select the optimal one.

7.3.1.1 – Selecting a root bridge

During network initialization, all STP devices in the network consider themselves to be the "root bridge," with the root bridge ID corresponding to their own device ID. By exchanging configuration messages, the root bridge IDs are compared between the devices and the device with the smallest root bridge ID in the network is selected as the root bridge.

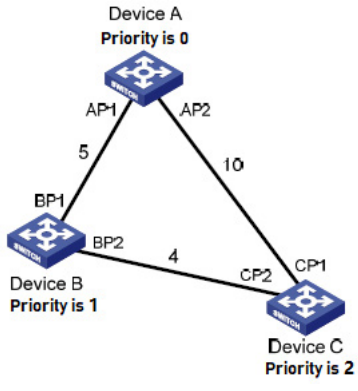
7.3.1.2 – Selecting a root port and a designated port

The selection process for root ports and designated ports is shown in the following table.

Step	Contents
1	The non-root bridge device sets the port that receives the optimal configuration message as the root port.
2	Based on the configuration message and the path overhead of the root port, the device calculates a specific port configuration message for each port: • Replace the root bridge ID with the root bridge ID in the root port configuration message. • Replace the root path overhead with the root path overhead of the root port configuration message plus the path overhead corresponding to the root port. • Replace the specified bridge ID with your own device ID. • Replace the specified port ID with your own port ID.
3	The device compares the calculated configuration messages with the configuration messages at the port whose role must be determined and selects different processing methods based on the comparison results: • If the calculated configuration message is superior, the device sets the port as the designated port, and the configuration message at this port is replaced by the calculated configuration message and sent regularly. • If the configuration message at the port is superior, the device does not update the configuration message of this port and blocks it. The port no longer forwards any data, but only receives the configuration message without sending it.

Once the root bridge, root port, and specified port have been successfully selected, the entire tree topology is constructed.

The following example illustrates the calculation process of the STP algorithm. The priority of device A is 0, that of device B is 1, and that of device C is 2. The path overhead of all connections is 5, 10, and 4, respectively.



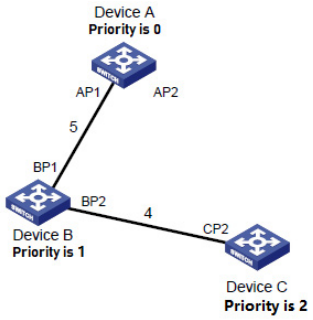
Device	Port name	Port configuration message
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP1}

7.3.1.3 – Comparison procedure and results for all devices

Device	Comparison process	Port configuration message after comparison
Device A	• Port AP1 receives the configuration message {1, 0, 1, BP1} from device B. Device A determines that this port configuration message {0, 0, 0, AP1} is higher-level than the received configuration message and therefore discards the received message. • Port AP2 receives the configuration message {2, 0, 2, CP1} from device C. Device A determines that this port configuration message {0, 0, 0, AP1} is higher-level than the received configuration message and therefore discards the received message. • If device A determines that the root bridge and the designated bridge are included in the configuration message of its own ports, it considers itself to be the root bridge without changing the configuration messages of all ports, and then sends configuration messages to the outside regularly.	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	• Port BP1 receives the configuration message {0, 0, 0, AP1} from device A. Device B determines that the received configuration message is better than its own configuration message {1, 0, 1, BP1} for this port and therefore updates the configuration message of port BP1. • Port BP2 receives the configuration message {2, 0, 2, CP2} from device C. Device B determines that the configuration message {1, 0, 1, BP2} of this port is better than the received configuration message and therefore discards the received configuration message.	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	• Device B compares the configuration messages of all ports and selects the configuration message from port BP1 as the optimal one. It then sets port BP1 as the root port without changing its configuration message. • Device B calculates a specific port configuration message {0, 5, 1, BP2} for port BP2 based on the configuration message and path overhead 5 of root port BP. • Device B compares the calculated configuration message {0, 5, 1, BP2} with the configuration message on port BP2. The comparison result is that the calculated configuration message is better, so device B sets port BP2 as the specified port and replaces its configuration message with the calculated one, which is sent regularly to the outside world.	Root-Port BP1: {0, 0, 0, AP1} Designated Port BP2: {0, 5, 1, BP2}
Device C	• When port CP1 receives the configuration message {0, 0, 0, AP2} from device A, device C determines that the received configuration message is better than the configuration message {2, 0, 2, CP1} of this port, so it updates the configuration message of port CP1. • Before the update, port CP2 receives the configuration message {1, 0, 1, bp2} from BP2 from device B. Device C determines that the received configuration message is better than the configuration message {2, 0, 2, CP2} of this port and therefore updates the configuration message of port CP2.	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	After comparison: • The configuration message from port CP1 is selected as the optimal configuration message, and port CP1 is set as the root port without changing its configuration message. • After comparing the calculated configuration message {0, 10, 2, CP2} of the specified port with the configuration message of port CP2, port CP2 is converted to the specified port and its configuration message is replaced by the calculated configuration message.	Root-Port CP1: {0, 0, 0, AP2} Designated Port CP2: {0, 10, 2, CP2}

Device	Comparison process	Port configuration message after comparison
Device C	• Port CP2 then receives the updated configuration message {0, 5, 1, bp2} from device B. Since the received configuration message is better than the original one, device C triggers the update process. • At the same time, port CP1 receives the configuration message sent regularly by device A. After comparison, device C does not trigger the update process.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	After comparison: • The root path overhead 9 of port CP2 (root path overhead 5 of the configuration message + path overhead 4 of port CP2) is smaller than the root path overhead 10 of port CP1 (root path overhead 0 of the configuration message + path overhead 10 of port CP1), Therefore, the configuration message from port CP2 is selected as the optimal one, and port CP2 is set as the root port without changing its configuration message. • After comparing the configuration message from port CP1 with the calculated configuration message of the specified port, port CP1 is blocked without changing its port configuration message and does not receive any data forwarded from device A until a new condition triggers the spanning tree calculation, e.g., when the connection from device B to device C is interrupted.	Blocked Port CP1: {0, 0, 0, AP2} Root-Port CP2: {0, 5, 1, BP2}

After the comparison in the table above, a spanning tree is formed that uses device A as the root bridge.



7.3.2 – Transmission mechanism of the SPT configuration message

- When the network is initialized, all devices consider themselves to be the root bridge and generate configuration messages in which they specify themselves as the root in order to send these messages at regular intervals with the Hello Time.
- If the port receiving the configuration message is the root port and the received configuration message is better than that of the port, the device increases the message age in the configuration message according to certain rules, starts a timer to calculate the time for the configuration message, and forwards it from the specified port of the device.
- If the priority of the configuration message received from the designated port is lower than that of the port, the port immediately sends its own better configuration message in response.
- If a path fails, the root port on that path no longer receives new configuration messages, and the old ones are discarded due to a timeout. The device regenerates the configuration message, using itself as the root, and sends it out, causing the spanning tree to be recalculated to obtain a new path that replaces the failed connection and restores the network.

However, the newly calculated configuration message is not immediately transmitted to the entire network, so the old root port and designated port continue to forward data via the original path because they do not recognize the change in the network topology. If the newly selected root port and designated port immediately start forwarding data, this can lead to a temporary loop.

7.3.3 – STP-Timer

Three important time parameters must be used in the STP calculation: forward delay, hello time, and max age.

- Forward delay refers to the delay time of device state migration. A connection failure causes the network to recalculate the spanning tree and change its structure accordingly. However, the newly calculated configuration message is not immediately transmitted to the entire network. If the newly selected root port and the designated port immediately start forwarding data, this can lead to a temporary loop. For this reason, STP uses a state change mechanism. The newly selected root port and designated port can only forward data after two forward delays, ensuring that the new configuration message has been transmitted throughout the network.
- The Hello Time is used to detect whether a connection to the device exists. At each Hello time interval, the device sends a Hello message to the surrounding devices to confirm whether the connection is established.
- The "Max Age" parameter is used to determine whether the storage period of configuration messages in the device has "expired." The device discards the expired configuration messages.

7.4 – MSTP Introduction

7.4.1 – MSTP Background

7.4.1.1 – Shortcomings of STP and RSTP

STP cannot migrate quickly. Even with a point-to-point connection or an edge port (i.e., this port is directly connected to the user's end device without any connection to other devices or a common network segment), it must wait twice the forward delay time before migrating to the forwarding state.

RSTP (Rapid Spanning Tree Protocol) is an optimized version of the STP protocol, where "rapid" means that when selecting a port as the root port and designated port, the delay time for entering the forwarding state is significantly reduced under certain conditions in order to shorten the time required for the network to achieve final topological stability.

- In RSTP, the condition for the rapid change of the root port status is that the old root port on that device has stopped forwarding data and the upstream designated port has started forwarding data.
- In RSTP, the condition for fast change of the designated port status is that the designated port is an edge port or a designated port connected to the point-to-point connection. If the designated port is an edge port, this port can enter forwarding status directly; if the designated port is connected to a point-to-point connection, this device can establish a connection with the downstream device and enter forwarding status immediately after receiving the response.

RSTP can converge quickly, but has similar shortcomings to STP: All bridges in the LAN share a spanning tree, so redundant connections cannot be blocked according to VLAN and all VLAN packets are forwarded along a spanning tree.

7.4.1.2 – Features of MSTP

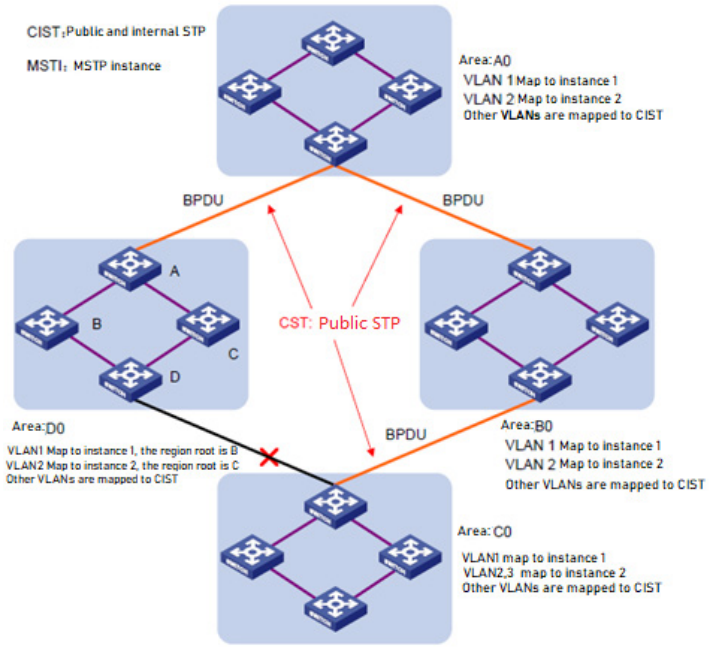
MSTP (Multiple Spanning Tree Protocol) can compensate for the shortcomings of STP and RSTP. It can converge quickly and forward traffic in different VLANs via their own paths, providing a better load distribution mechanism for redundant connections. For information on introducing VLAN, see "VLAN Configuration" in the "Access Volume" section.

- MSTP can define a VLAN mapping table (a table showing the corresponding relationships between VLAN and spanning tree) to connect VLAN and spanning tree. By adding the concept of "instance" (integration of many VLANs into a set), many VLANs are bundled into one instance to reduce communication overhead and resource utilization.
  MSTP divides a switched network into many areas in which there are many independent spanning trees.

- MSTP prunes the ring network to a tree network without loops to prevent the propagation and endless circulation of packets in the ring network. At the same time, many redundant paths are provided for data forwarding to achieve load balancing of VLAN data during data forwarding.
- MSTP is compatible with STP and RSTP.

7.4.2 – Basic concept of MSTP

In this figure, each device is running MSTP. Some basic concepts of MSTP are explained using the following diagrams.



7.4.2.1 – MST area

The MST area (Multiple Spanning Tree area) consists of many devices in a switched network and the network segments between them. These devices have the following characteristics:

- They have the same area name.
- They have the same assignment configuration from VLAN to Spanning Tree instance.
- They have the same MSTP revision configuration.
- They are physically connected to each other.

For example, in area A0 in the previous figure, all devices in this area have the same MST area configuration:

- Same area name;

- Same mapping relationship between VLAN and spanning tree instance (VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, and other VLANs are mapped to CIST, where CIST is spanning tree instance 0);
- Same MSTP revision level (not shown in the figure above).

There are many MST areas in a switched network. Users can divide many devices into an MST area using MSTP configuration commands.

7.4.2.2 – WLAN assignment table

The VLAN assignment table is an attribute of the MST area that is used to describe the assignment relationship between VLAN and spanning tree instance.

In the previous figure, for example, the VLAN mapping table for area A0 is as follows: VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, and other VLANs are mapped to CIST. MSTP can achieve load distribution based on the VLAN mapping table.

7.4.2.3 – IST

IST (Internal Spanning Tree) is a spanning tree in an MST area.

IST and CST (Common Spanning Tree) form the spanning tree CIST (Common and Internal Spanning Tree) of the entire switched network. IST is the fragment of CIST in the MST area.
In the figure, for example, CIST has a fragment in each MST area that corresponds to the IST in the respective area.

7.4.2.4 – CST

CST is a single spanning tree that connects all MST areas in a switched network. If each MST area is considered a "device," CST is a spanning tree generated by these "devices" through STP protocol and RSTP protocol calculation.

For example, the red line in the figure is CST.

7.4.2.5 – CIST

CIST is a single spanning tree that connects all devices in a switched network and consists of IST and CST.

In the figure, for example, the IST in each MST area and the CST between the MST areas form the CIST of the entire network.

7.4.2.6 – MSTI

An MST domain can generate many spanning trees that are independent of each other via MSTP. Each spanning tree is referred to as an MSTI (Multiple Spanning Tree Instance).
In the figure, for example, there are many spanning trees in each domain, with each spanning tree corresponding to the corresponding VLAN. These spanning trees are referred to as MSTIs.

7.4.2.7 – Area root

The root bridge of IST and MSTI in the MST area is the area root. The topology of each spanning tree in the MST area is different, so the area root can also be different.
In the figure, for example, the domain root of spanning tree instance 1 in domain D0 is device B, and the domain root of spanning tree instance 2 is device C.

7.4.2.8 – Common root bridge

The common root bridge refers to the root bridge of CIST.
In the figure, for example, the common root bridge is a device in area A0.

7.4.2.9 – Area boundary port

The area boundary port is the port at the edge of the MST area through which different MST areas, MST areas and areas in which STP is running, as well as MST areas and areas in which RSTP is running, are connected to each other.
For example, in the figure, if a device in region A0 is connected to the first port of a device in region D0 and the common root of the entire switched network is in A0, the first port of this device in region D0 is the area boundary port of region D0.
The role of the area boundary port on the spanning tree instance is the same as that of the CIST, with the exception of the master port, whose role is the CIST root port on other instances but is the master port on other instances.

7.4.2.10 – Port role

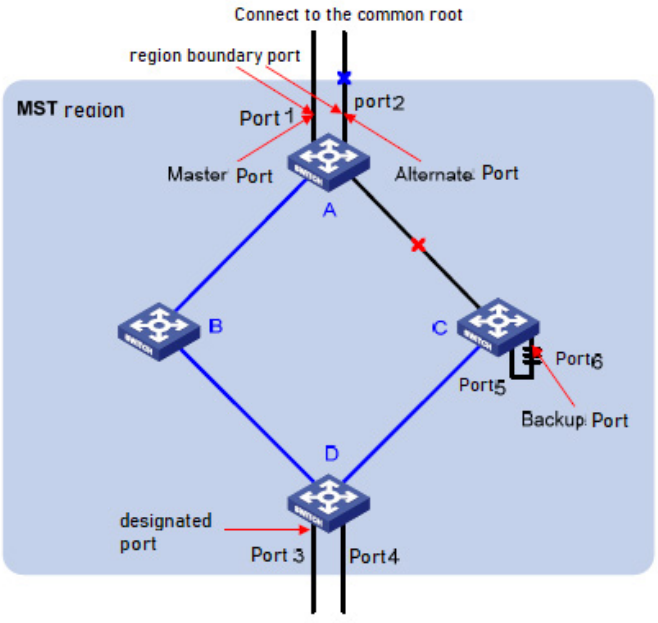
In the MSTP calculation process, port roles mainly include root port, designated port, master port, alternate port, backup port, and so on.

- Root port: Forwarding data to the root bridge.
- Designated port: Forwarding data to downstream network segments or devices.
- Master port: Connects the MST area to the common root, which is located on the shortest path from the entire area to the common root. From the perspective of CST, the master port is a "root port" of the area (if the area is considered a node). The role of the master port in IST/CIST is root port, in other instances it is master port.
- Alternative port: Backup port of the root port and master port. If the root port or master port is blocked, the alternative port becomes the new root port or master port.
- Backup port: Designated port of the backup port. If the designated port is blocked, the backup port quickly becomes a new designated port and forwards data without delay.
  If two ports of a device with MSTP are open and connected to each other, a loop is created. In this case, the device blocks one of the ports, and the backup port is the blocked port.

Ports play different roles in different spanning tree instances.

The above concepts are illustrated in the following figure.

- Devices A, B, C, and D form an MST domain.
- Port 1 and port 2 of device A are connected to the common root.
- Port 5 and port 6 of device C form a loop.
- Port 3 and port 4 of device D are connected to other MST domains downstream.



7.4.2.11 – Port status

In MSTP, the status of a port can be divided into the following three types depending on whether it learns MAC addresses and forwards user traffic:

- **Forwarding status:** MAC addresses are learned and user traffic is forwarded.
- **Learning status:** MAC addresses are learned, but user traffic is not forwarded.
- **Discard status:** Neither MAC addresses are learned nor is user traffic forwarded.

There is no necessary connection between the port status and its role. The following table shows the port status of different port roles ("√" means that this port role can have this status; "--" means that this port role cannot have this status).

Port Role / Port Status	Root-Port/ Master-Port	Specific Port	Alternative Port	Backup Port
Forwarding	√	√	--	--
Learning	√	√	--	--
Discard	√	√	√	√

7.4.3 – Basic principle of MSTP

MSTP divides the entire two-layer network into multiple MST areas, and CST is generated by calculation between the areas; multiple spanning trees are generated by calculation within the area, and each spanning tree is referred to as multiple spanning tree instances, where instance 0 is IST and other multiple spanning tree instances are MSTI. Like STP, MSTP uses configuration messages to calculate the spanning tree, but the configuration message contains the configuration information of the MSTP device.

7.4.3.1 – Calculation of the CIST spanning tree

After comparing the configuration messages, a device with the highest priority in the entire network is selected as the root bridge of the CIST. In each MST area, MSTP generates an IST by calculation. At the same time, MSTP treats each MST area as a single device and generates a CST between the areas by calculation. CST and IST form the CIST of the entire network.

7.4.3.2 – Calculation of MSTI

In an MST area, MSTP generates different spanning tree instances for different VLANs according to the assignment relationship between VLANs and spanning tree instances. Each spanning tree is calculated independently. The calculation process is similar to that of STP.

In MSTP, a VLAN message is transmitted via the following path:

- In the MST area, it is transmitted along the corresponding MSTI.
- Between MST areas, it is transmitted along the CST.

7.4.4 – Implementation of MSTP on devices

MSTP is compatible with STP and RSTP. Messages from the STP and RSTP protocols can be identified by MSTP devices and used to calculate the spanning tree.

In addition to the basic functions of MSTP, this device offers many special functions that are practical for administration from the user's point of view, including:

- Root bridge maintenance
- Root bridge backup
- Root protection function
- BPDU protection function
- Loop protection function
- Protection against attacks by TC-BPDU messages

7.5 – Protocol

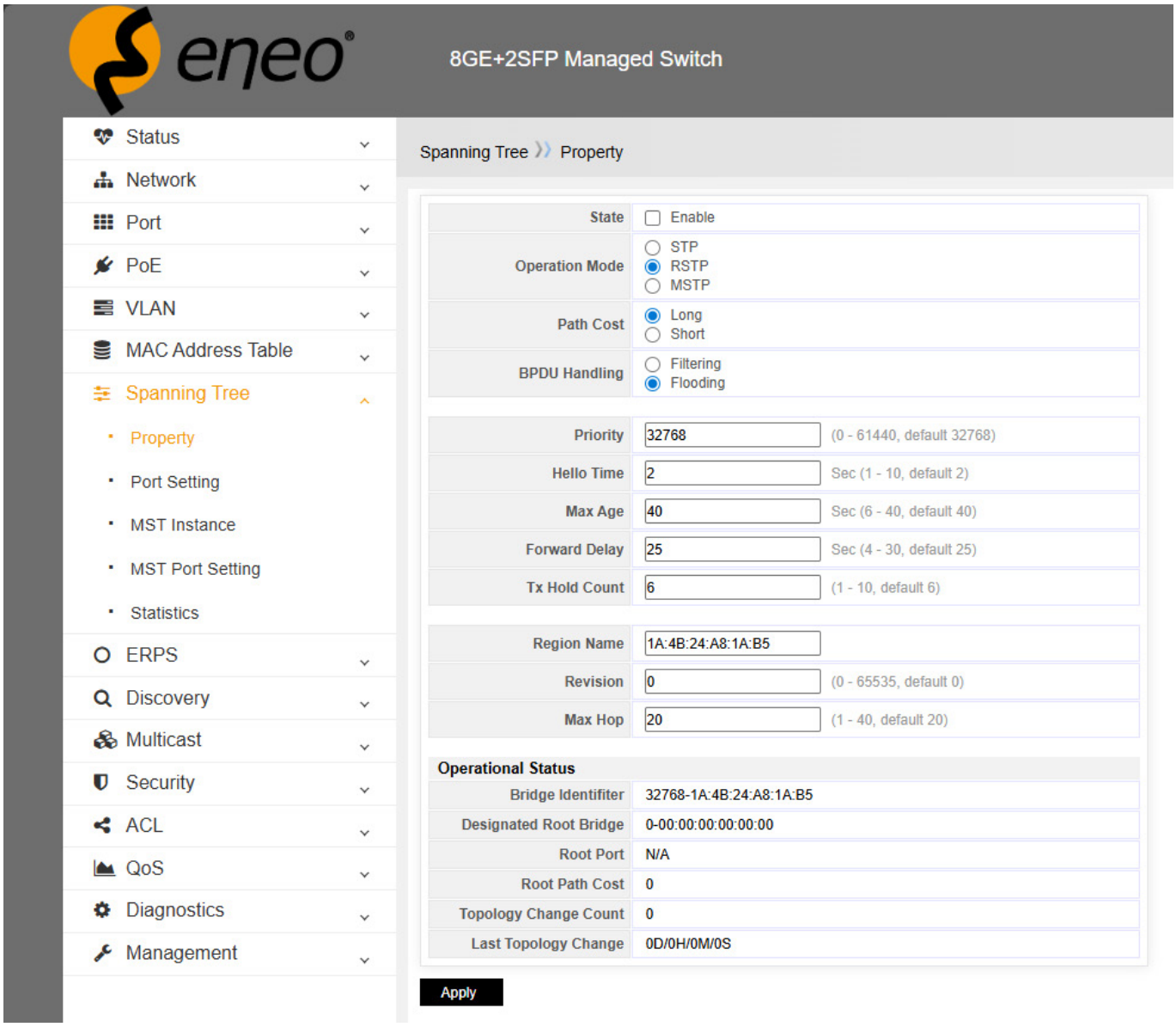
Relevant protocols:

- **IEEE 802.1D:** Spanning Tree Protocol (STP)
- **IEEE 802.1w:** Rapid Spanning Tree Protocol (RSTP)
- **IEEE 802.1s:** Multiple Spanning Tree Protocol (MSTP)

7.6 – Property

Status: Enable (complete switch spanning tree configuration, select to enable, deselect to disable)

Operation mode: STP/RSTP/MSTP (three modes to choose from)



Path cost: Long/Short (the value range is a short integer (short: 1-65535) (long: 1-200000000))

BPDU handling: Filtering/Flooding (filtering or flooding of BPDU messages)

Priority: Configure the priority for the switch. The value range is between 0 and 61440. It is increased by a multiple of 4096. The default value is 32768.

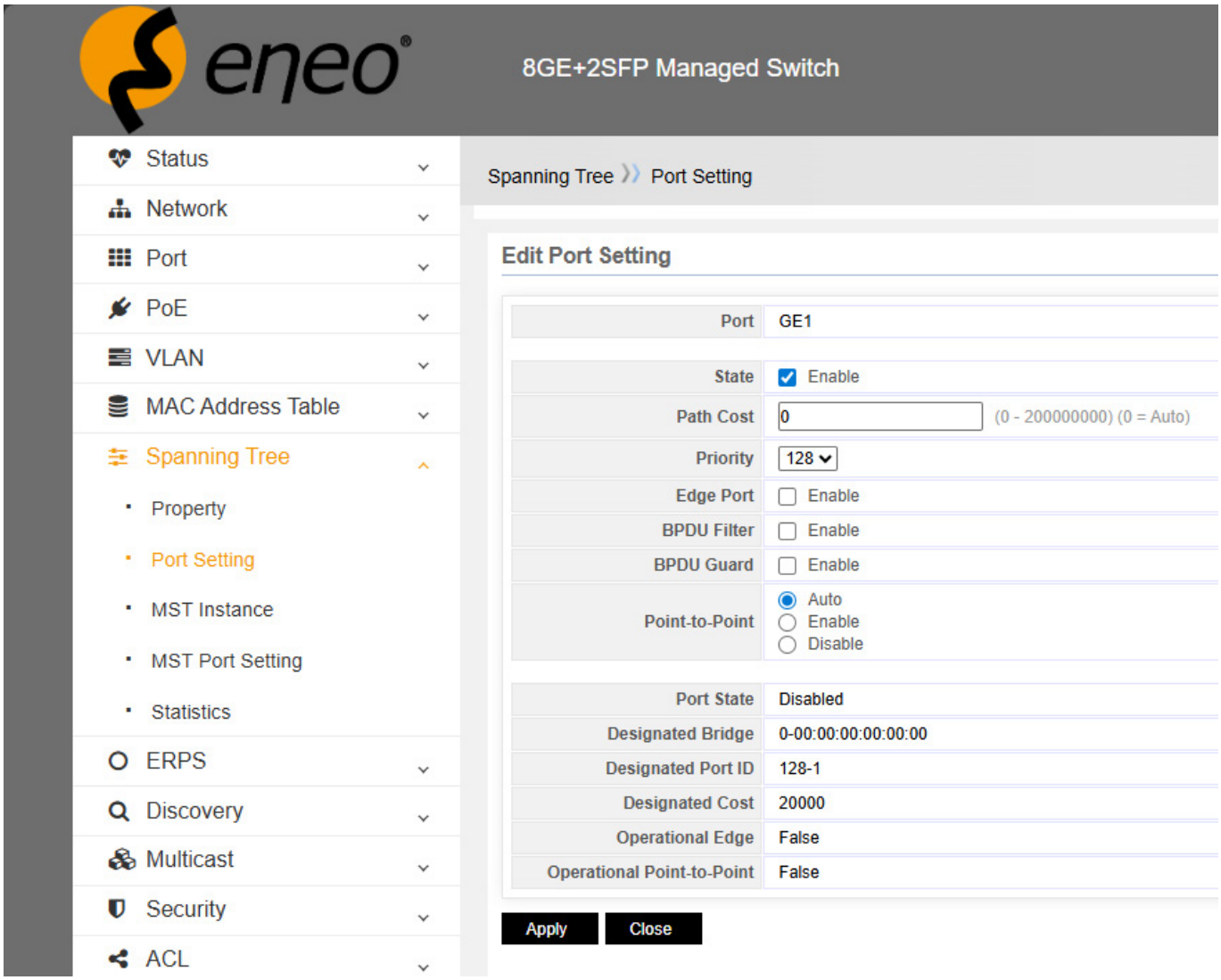
Hell Time: Configure the time interval for transmitting BPDU messages for the switch. The default value is 2 seconds.

Maximum lifetime: Configure the maximum lifetime of BPDU messages. The default value is 20 seconds.

Forward Delay: Configure the time interval for changing the port status. The default value is 15 seconds.

TX Hold Count: Configure the maximum number of BPDUs transmitted per second. The default value is 3.

7.7 – Port settings



Status: Enable (as spanning tree configuration of the switch port; select to enable, deselect to disable)

Path cost: Long/Short (the value range is a short integer (short: 1-65535) (long: 1-200000000))

Priority: Configure the priority of the switch port in the range from 0 to 240.

Edge-Port: A port configured as an edge port can change the port status directly to "Forwarding" when it is active.

BPDU-Filter: If the BPDU filter is configured on the port, the interface no longer sends or receives BPDU messages.

BPDU protection: If BPDU protection is configured on the port, the interface is immediately disconnected as soon as a BPDU packet that should not be present is received on a specific interface, causing it to enter the "Soft Close Err disabled" state. This method is more robust than the BPDU filter.

Point to point: If BPDU filtering is configured on the port, the interface no longer sends or receives BPDU messages.

8 – ERPS (G.8032)

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops on Layer 2. It implements the convergence of carrier-class reliability standards and enables communication between all ERPS-enabled devices in a ring network.

8.1 – Introduction

8.1.1 – Definition

Since the standard number is ITU-T G.8032/Y1344, ERPS is also referred to as G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) and protection switching mechanisms.

ERPS is available in two versions: ERPSv1, published by ITU-T in June 2008, and ERPSv2, published in August 2010. EPRSv2 is fully compatible with ERPSv1 and offers the following enhanced features:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on virtual channels (VCs) and non-virtual channels (NVCs) in subrings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

8.1.2 – Purpose

In general, redundant links are used in an Ethernet switching network, such as a ring network, to provide link backup and increase network reliability.
However, the use of redundant connections can lead to loops, which cause broadcast storms and make the MAC address table unstable.
As a result, communication quality deteriorates and communication services may even be interrupted.
The following table describes the ring network protocols supported by the devices.

ring network protocol	Pro	Con
STP / RSTP / MSTP	• Applies to all Layer 2 networks. • This is a standard IEEE protocol that enables communication between Huawei devices and devices from other manufacturers.	• Offers low convergence in a large network that cannot meet carrier-class reliability requirements.
ERPS	• Offers fast convergence and carrier-class reliability. • Is an ITU-T standard protocol that enables Huawei devices to communicate with devices from other manufacturers. • Supports single-ring and multi-ring topologies in ERPSv2.	• The network topology must be planned in advance. • The configuration is complex.

Ethernet networks require faster protection switching. STP does not meet the requirements for fast convergence. RRPP and SEP are proprietary ring protocols from Huawei that cannot be used for communication between Huawei and non-Huawei devices in a ring network.

ERPS, an ITU-T standard protocol, prevents loops in ring networks. It optimizes detection and ensures fast convergence. ERPS enables communication between all ERPS-enabled devices in a ring network.

8.1.3 – Advantages

- Prevents broadcast storms and implements fast traffic transfer in a network with loops.
- Offers fast convergence and carrier-class reliability.
- Enables communication between all ERPS-enabled devices in a ring network.

8.2 – Principles

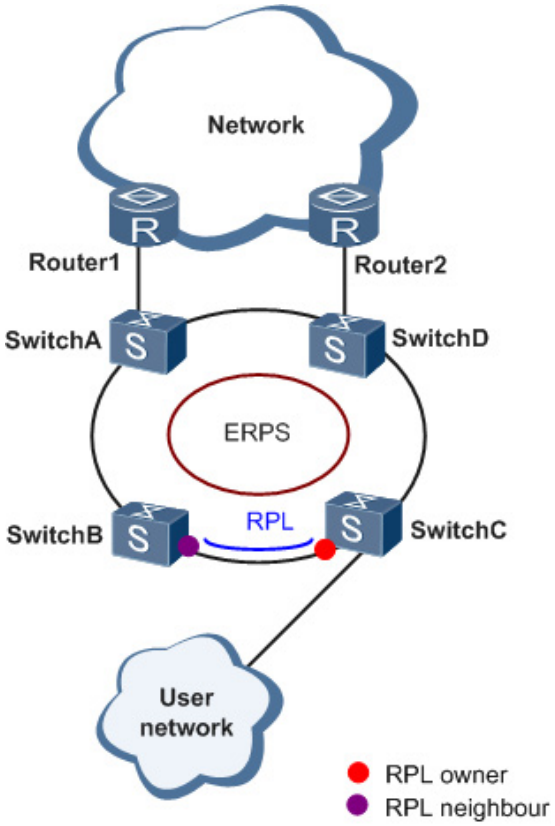
This section describes the implementation of ERPS.

8.2.1 – Basic ERPS concepts

ERPS eliminates loops on the link layer of an Ethernet network. ERPS works for ERPS rings. There are multiple nodes in an ERPS ring. ERPS blocks the RPL owner port and controls common ports to switch the port status between forwarding and discarding to avoid loops. ERPS uses the control VLAN, the data VLAN, and the Ethernet Ring Protection (ERP) instance.

In the network shown in the following figure, SwitchA to SwitchD form a ring and are double-bundled with the upstream network. This access mode results in a loop throughout the network. To eliminate redundant connections and ensure connection connectivity, ERPS is used to prevent loops.

8.2.1.1 – ERPS ring



An ERPS ring consists of interconnected Layer 2 switching devices that are configured with the same control VLAN.

8.2.1.2 – Port role

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- **RPL owner port**

  An RPL owner port is responsible for blocking traffic via the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.
  When the node on which the RPL owner port is located receives a RAPS PDU indicating a link or node failure in an ERPS ring, the node releases the RPL owner port lock. The RPL owner port can then send and receive traffic to ensure uninterrupted traffic forwarding.
  The link on which the RPL owner port is located is the RPL.

- **RPL neighbor port**

  An RPL neighbor port is directly connected to an RPL owner port.
  Both the RPL owner port and the RPL neighbor ports are blocked in normal situations to prevent loops.
  If an ERPS ring fails, both the RPL owner port and the neighbor ports are unlocked.
  The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port is located.

- **Common port**

  Common ports are ring ports that are not RPL owner or neighbor ports.
  A common port monitors the status of the directly connected ERPS connection and sends RAPS PDUs to inform the other ports of changes in the connection status.

8.2.1.3 – Port status

In an ERPS ring, an ERPS-enabled port has two statuses:

- **Forwarding:** Forwards user traffic and sends and receives RAPS PDUs.
- **Discard:** Only sends and receives RAPS PDUs.

8.2.1.4 – Control VLAN

A control VLAN is configured in an ERPS ring to transmit RAPS PDUs. Each ERPS ring must be configured with a control VLAN. After a port is added to an ERPS ring that is configured with a control VLAN, the port is automatically added to the control VLAN. Different ERPS rings must use different control VLANs.

8.2.1.5 – Data VLAN

Unlike control VLANs, data VLANs are used to transmit data packets.

8.2.1.6 – ERP instance

On a Layer 2 device running ERPS, the VLAN in which RAPS PDUs and data packets are transmitted must be assigned to an Ethernet Ring Protection (ERP) instance so that ERPS forwards or blocks the packets based on configured rules. If the assignment is not configured, the preceding packets can cause broadcast storms in the ring network. This results in the network becoming unavailable.

8.2.1.7 – Timer

- **Guard-Timer**

  After a faulty connection or node has been restored or a deletion process has been carried out, the device sends RAPS No Request (NR) messages to inform the other nodes that the connection or node has been restored and starts the guard timer. Before the guard timer expires, the device does not process RAPS (NR) messages to avoid receiving outdated RAPS (NR) messages. If the device still receives a RAPS (NR) message after the guard timer expires, the local port enters the forwarding state.

- **WTR-Timer**

  If an RPL owner port is unlocked due to a connection or node error, the affected port cannot go up immediately after the connection or node is restored. Blocking the RPL owner port can lead to network flapping. To avoid this problem, the node containing the RPL owner port starts the WTR (Wait to Restore) timer after receiving a RAPS (NR) message. If the node receives a RAPS Signal Fail (SF) message before the timer expires, it stops the WTR timer. If the node does not receive a RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends a RAPS (no request, root blocked) message. Upon receiving this RAPS (NR, RB) message, the nodes set their restored ports in the ring to forwarding state.

- **Holdoff-Timer**

  In Layer 2 networks where EPRS is used, there may be different requirements for switching protection. In a network where multi-layer services are provided, users may need some time to fix a server failure after it occurs so that clients do not detect the failure. You can set the holdoff timer. If the failure occurs, it is not sent to ERPS until the holdoff timer expires.

8.3 – Configuration examples

This section contains configuration examples for ERPS, including network requirements, configuration roadmap, configuration procedure, and configuration files.

8.3.1 – Example of ERPS multi-instance configuration

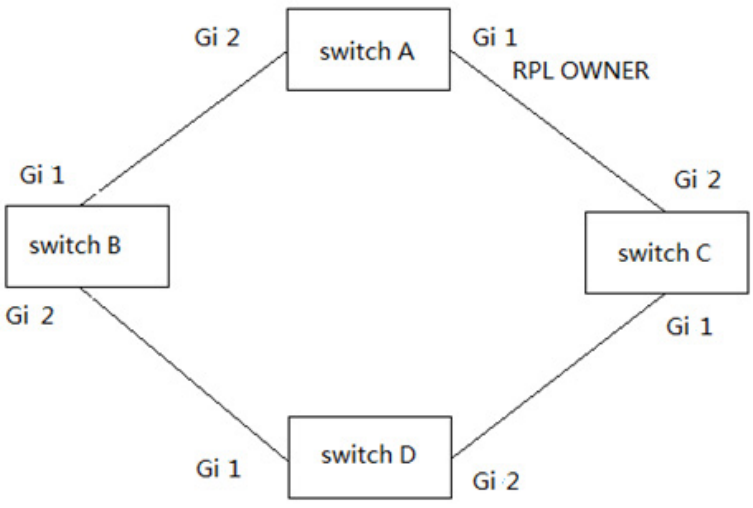
This section contains an example of configuring multiple instances of ERPS.

8.3.1.1 – Network requirements

In general, redundant links are used in an Ethernet switching network to provide link backup and increase network reliability. However, the use of redundant links can cause loops, which cause broadcast storms and make the MAC address table unstable. As a result, communication quality deteriorates and communication services may even be interrupted.

To prevent loops caused by redundant links, enable ERPS on the nodes of the ring network. ERPS is a Layer 2 loop interruption protocol defined by ITU-T that enables fast convergence of carrier-class reliability standards.

The following figure shows a network in which an ERPS ring with multiple instances is used. SwitchA to SwitchD form a ring network at the aggregation layer to implement service aggregation at Layer 2 and process Layer 3 services. ERPS is used in the ring network to provide protection circuits for redundant Layer 2 connections. ERPS Ring 1 and ERPS Ring 2 are configured on SwitchA to SwitchD. P1 on SwitchB is a blocked port in ERPS Ring 1, and P2 on SwitchA is a blocked port in ERPS Ring 2, implementing load balancing and link backup.



8.3.1.2 – Configuration roadmap

The configuration roadmap is as follows:

1. Configure the connection type of all ports to be added to ERPS rings as trunk.
2. Create ERPS rings and configure control VLANs and Ethernet Ring Protection (ERP) instances in the ERPS rings.
3. Add Layer 2 ports to ERPS rings and define port roles.
4. Configure the guard timers and WTR timers in the ERPS rings.
5. Configure Layer 2 forwarding on SwitchA to SwitchD.

8.3.1.3 – Adding a Layer 2 port to an ERPS ring and configuring the port role

After ERPS has been configured, add Layer 2 ports to an ERPS ring and configure the port roles so that ERPS functions properly.
You can add a Layer 2 port to an ERPS ring in one of the following ways:

- In the ERPS ring view, add a specific port to the ERPS ring and configure the port role.
- In the interface view, add the current port to the ERPS ring and configure the port role.

The web page configuration is as follows:

1. Configure port 1 and port 2, both tagged with "VLAN200."
2. Configure SwitchA to enable ERP, then configure the VLAN ID of the control VLAN to 200, and then configure port 1 for RTL owner mode and port 2 for ring mode.
3. Click the "Apply" button to complete the configuration of SwitchA.
4. If you need to configure SwitchB~D, everything else is the same, just configure the port mode to "Ring".

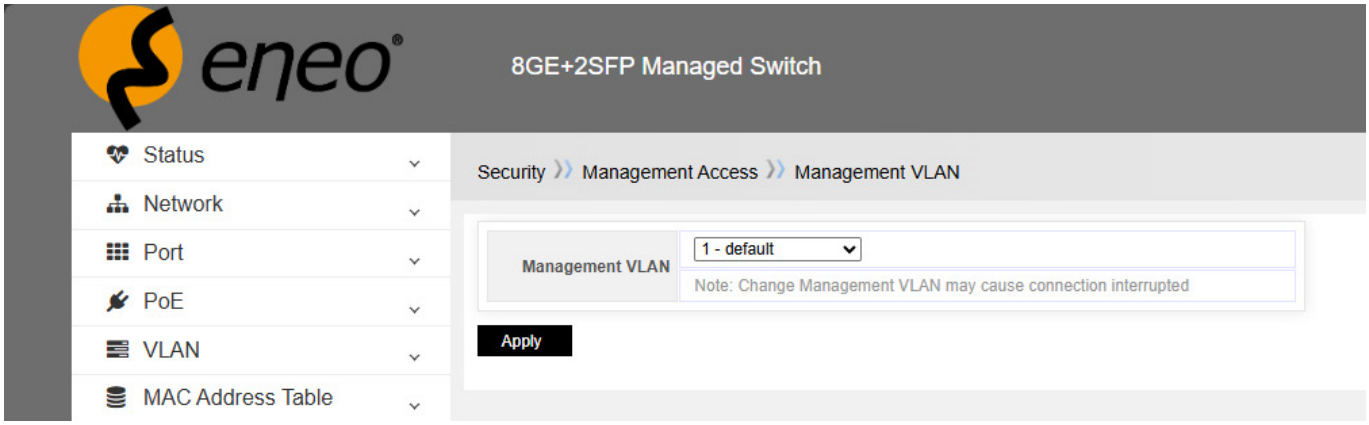
9 – SECURITY

9.1 – Management access

9.1.1 – VLAN management

VLAN management means that only the VLAN on the port can communicate with the switch CPU and manage the switch system.

By default, member ports of VLAN1 can manage member ports of switches.

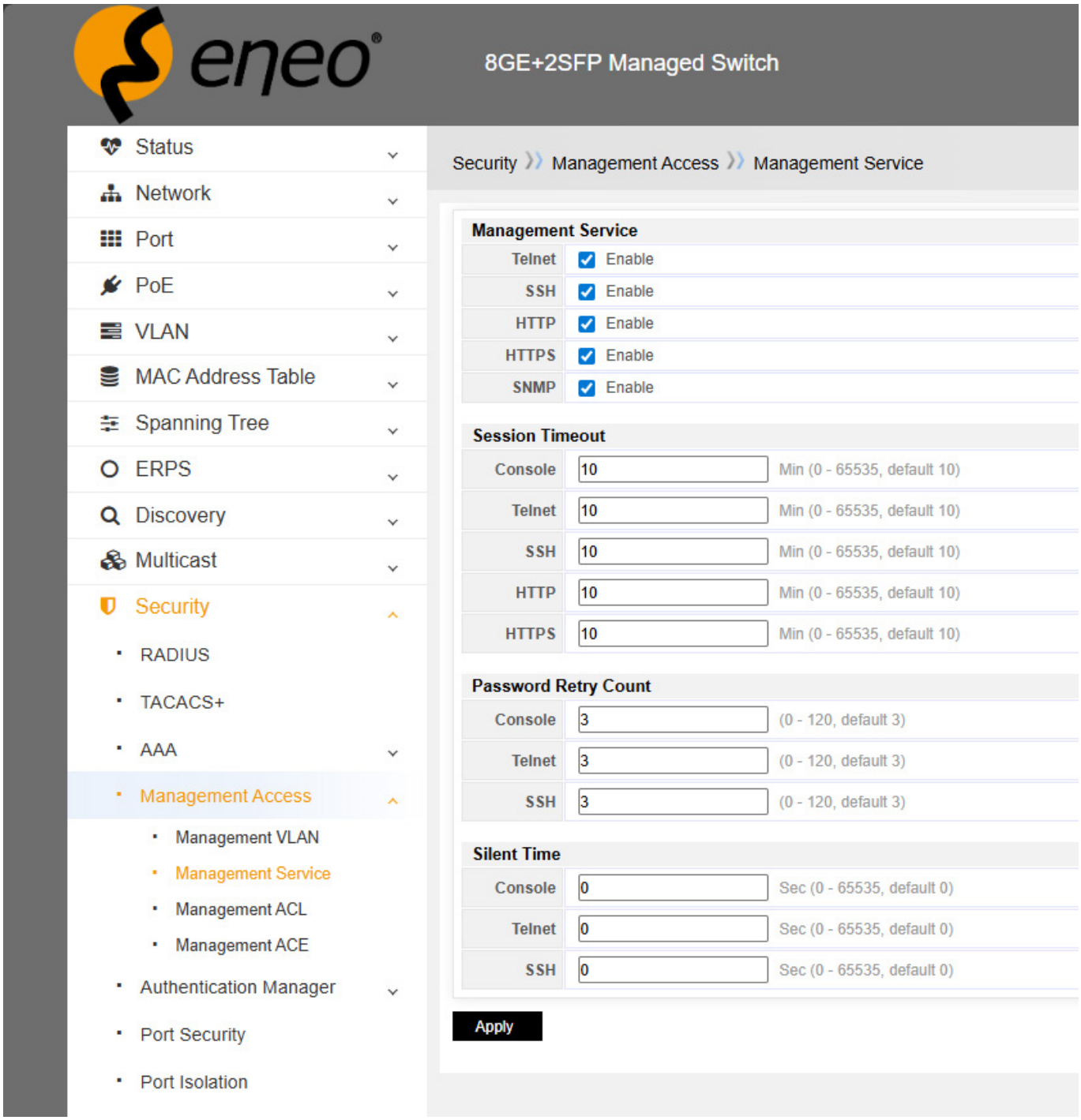


Depending on user requirements, you can select any VLAN to manage the switch system. However, the selected VLAN must have been set up beforehand.

Example

1. Add a VLAN, e.g., VLAN100
2. Add port 5 to VLAN 100
3. Set VLAN100 as the managing VLAN
4. Connect the PC to port 5 to manage the switch.

9.1.2 – Management Service



Telnet: Telnet is a network protocol used on the Internet or local networks to enable bidirectional, interactive, text-oriented communication via a virtual terminal connection, allowing network administrators to remotely access and manage network devices such as routers, switches, and servers. For example, an administrator can log on to a router from a remote location via Telnet and configure its settings, such as IP addresses, routing protocols, and access control lists.

SSH (Secure Shell): SSH is a cryptographic network protocol for the secure operation of network services over an unsecured network. The standard TCP port for SSH is 22. Similar to Telnet, SSH is used for remote login and management of network devices. However, it offers a significantly higher level of security. When an administrator uses SSH to log in to a device, the data transmitted between the client (the computer on which the administrator is working) and the server (the network device) is encrypted. This encryption protects sensitive information such as passwords and configuration details from being disclosed.

HTTP (Hypertext Transfer Protocol): HTTP is the basis of data communication on the World Wide Web. It is an application layer protocol for transferring hypermedia documents such as HTML. This interface allows the administrator to view the device status, configure settings, and perform various management tasks such as updating the firmware.

HTTPS (Hypertext Transfer Protocol Secure): HTTPS is an extension of HTTP. The data transferred between the web browser and the network device is encrypted using SSL/TLS (Secure Sockets Layer/ Transport Layer Security) protocols. This ensures that sensitive information such as login details and configuration changes are protected from interception and manipulation.

SNMP (Simple Network Management Protocol): SNMP is an Internet standard protocol for managing devices on IP networks. It is used to monitor network devices for conditions that require administrative attention. SNMP is often used in network management systems to collect information from network devices. Network devices such as routers, switches, and servers can be configured to act as SNMP agents. These agents collect data about the device's performance, such as CPU usage, memory usage, interface status, and traffic statistics. The SNMP manager, which is usually network management software, can then query the agents to obtain this information. For example, a network administrator can use SNMP to monitor the bandwidth usage of a router's various network interfaces in real time.

Timeout: Depending on user requirements, you can select the switches to be supported.

Session Timeout: For example, after logging in to the website, if no action is taken for 10 seconds, the system will automatically exit the website. The user must re-enter their name and password to manage the switch.

Number of password retries: If the number of incorrect password entries exceeds the set value, the user must wait a few moments and re-enter the password to prevent brute force attacks.

10 – MULTICAST

10.1 – Introduction to Multicast

The multicast method, which exists alongside unicast and broadcast, is an effective solution to the problem of point-to-multipoint data transmission. Through highly efficient point-to-multipoint data transmission over a network, multicast significantly saves network bandwidth and reduces network load.

With multicast technology, a network operator can easily offer new value-added services, such as live webcasting, web TV, distance learning, telemedicine, web radio, real-time video conferencing, and other bandwidth- and time-critical information services.

10.2 – IGMP snooping – overview

Internet Group Management Protocol Snooping (IGMP snooping) is a multicast restriction mechanism that runs on Layer 2 devices to manage and control multicast groups.

10.2.1 – When a general query is received

The IGMP querier sends general IGMP queries at regular intervals to all hosts and routers (224.0.0.1) in the local subnet to find out if there are any active multicast group members in the subnet.

After receiving a general IGMP query, the switch forwards it to all ports in the VLAN except the receiving port and performs the following for the receiving port:

- If the receiving port is a router port that exists in its router port list, the switch resets the aging timer for that router port.
- If the receiving port is not a router port that is present in its router port list, the switch adds it to its router port list and sets an aging timer for this router port.

10.2.2 – When receiving a membership report

A host sends an IGMP report to the multicast router under the following circumstances:

- After receiving an IGMP query, a host that is a member of a multicast group responds with an IGMP report.
- When a host wants to join a multicast group, it sends an IGMP report to the multicast router to indicate that it is interested in the multicast information intended for that group.

After receiving an IGMP report, the switch forwards it via all router ports in the VLAN, resolves the address of the reported multicast group, and performs the following:

- If there is no entry for the reported group in the forwarding table, the switch creates an entry, adds the port as a member port to the list of outgoing ports, and starts a member port aging timer for that port.
- If there is an entry in the forwarding table for the reported group, but the port is not included in the list of outgoing ports for this group, the switch adds the port as a member port to the list of outgoing ports and starts a member port aging timer for this port.
- If there is an entry in the forwarding table for the reported group and the port is included in the list of outgoing ports, which means that this port is already a member port, the switch resets the member port aging timer for this port.

10.2.3 – When receiving a leave group message

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave group message to the multicast router.

When the switch receives a group-specific IGMP leave group message on a member port, it first checks whether there is an entry for this group in the forwarding table and, if so, whether the outgoing port list contains this port.

- If the entry does not exist in the forwarding table or if the list of outgoing ports does not contain this port, the switch discards the IGMP leave-group message instead of forwarding it to a port.
- If the entry is in the forwarding table and the list of outgoing ports contains the port, the switch forwards the Leave-Group message to all router ports in the VLAN. Since the switch does not know whether other hosts connected to the port are still listening to this group address, it does not immediately remove the port from the list of outgoing ports in the forwarding table entry for this group, but resets the member port aging timer for the port.

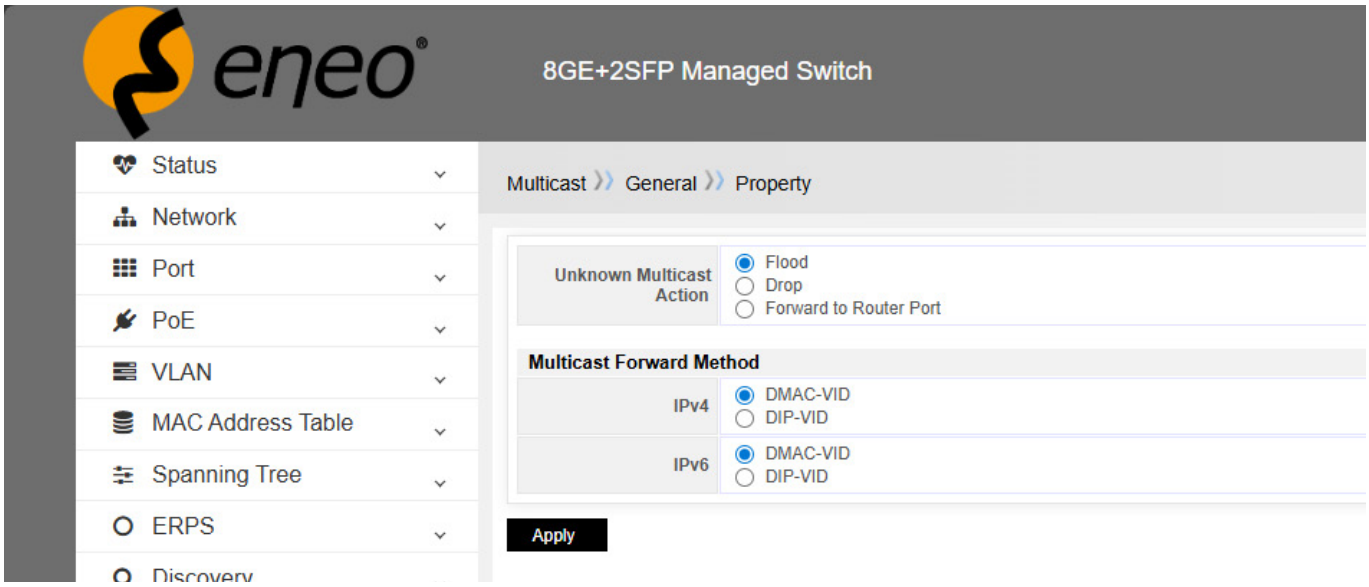
After receiving the IGMP leave group message from a host, the IGMP querier determines the address of the multicast group that the host has just left from the message and sends an IGMP group-specific query to this multicast group via the port that received the leave group message. After receiving the IGMP group-specific query, the switch forwards it to all its router ports in the VLAN and all member ports for this multicast group and performs the following:

- If an IGMP report is received in response to the group-specific query before the aging timer expires on a member port, this means that a host connected to the port is receiving or expecting multicast data for this multicast group. The switch resets the aging timer of the member port.
- If no IGMP report is received in response to the group-specific query on a member port before the aging timer expires, this means that no hosts connected to the port are listening to this group address: The switch removes the port from the list of outgoing ports in the forwarding table entry for this multicast group when the aging timer expires.

10.3 – IGMP snooping configuration

10.3.1 – Processing unknown multicast packets

For processing unknown multicast packets, you can choose whether to treat them as flooding, discard them, or forward them to the routing port.



IGMP (Internet Group Management Protocol) is used to manage multicast group memberships. In the context of IGMP, the terms "flood," "drop," and "forward" refer to specific actions performed by network devices (e.g., switches) when handling multicast traffic. Here is an explanation of each term:

Here is an explanation of each term:

Flood

Definition: When a switch "floods" multicast traffic, it sends the multicast packets to all ports within a VLAN, except for the port from which the packet was received. This is similar to the processing of broadcast packets.

Scenario: This happens when the switch does not know which ports are receivers for a particular multicast group. For example, if "Flood Unknown Multicast" is enabled and the switch has not received any IGMP reports for a multicast group, the multicast traffic is forwarded to all ports in the VLAN.

Drop

Definition: "Dropping" multicast traffic means that the switch discards the multicast packets without forwarding them to a port.

Scenario: This can occur if the switch has not received any IGMP reports for a multicast group and "Flood Unknown Multicast" is disabled. In this case, the switch assumes that there are no interested recipients and discards the multicast traffic.

Forward

Definition: "Forwarding" multicast traffic means that the switch only sends the multicast packets to the ports where it knows there are interested recipients.

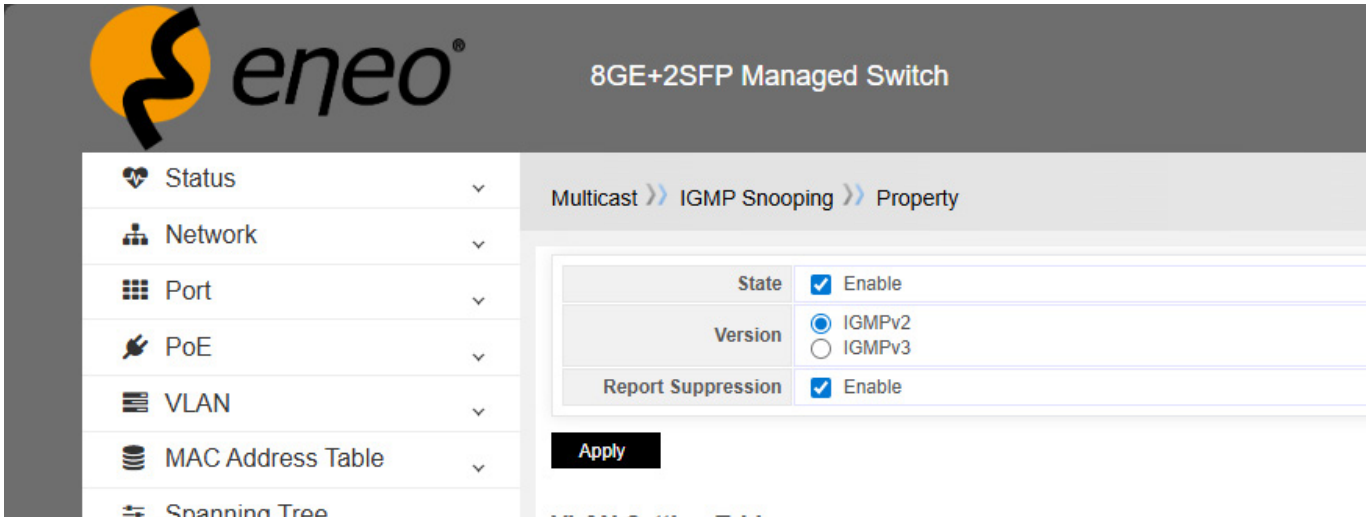
Scenario: This happens when the switch has received IGMP reports from hosts that signal their interest in a multicast group. The switch then forwards the multicast traffic only to those ports. For example, if a switch receives an IGMP report from a host on a specific port, it forwards the multicast traffic for that group to that port.

10.3.2 – Enable IGMP snooping

The default status of IGMP snooping on the switch is enabled, which serves as a global toggle for enabling or disabling IGMP snooping on the switch. By default, the switch supports IGMPv2, which is predominantly used in versions v1 and v2 on the market. Of course, this switch also supports v3.

However, the default status of IGMP snooping for VLANs on the switch is disabled, so IGMP snooping must be enabled for each individual VLAN in order for it to take effect.

To enable the IGMP snooping function of VLAN1:



Status: Enable or disable IGMP snooping.

Version: Select IGMPv2 or IGMPv3. The following is a comparison of the features:

IGMP v2:

- Manages membership in multicast groups.
- Allows hosts to join or leave multicast groups.
- Introduces an explicit exit mechanism to reduce unnecessary traffic.
- Provides efficient query and reporting mechanisms for managing group membership.

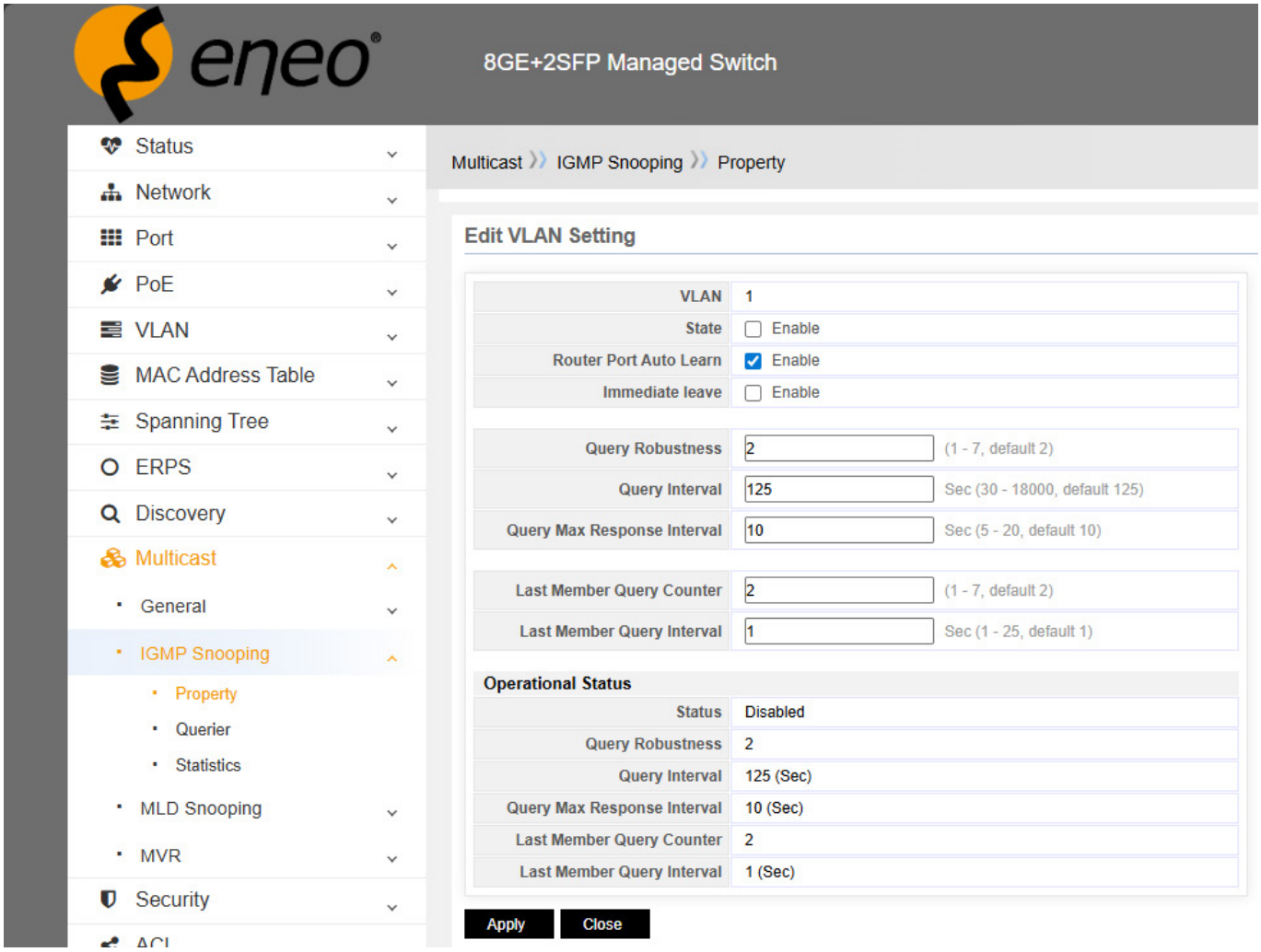
IGMP v3:

All features of IGMP v2 plus:

- Supports Source-Specific Multicast (SSM), which allows hosts to specify both the multicast group and the desired sources.
- Provides more detailed control over multicast traffic through improved membership reports and source-specific queries.

Report suppression:

Report suppression is a mechanism that reduces the number of IGMP report messages in a network. This helps to minimize network congestion and the processing load on devices.



VLAN: The VLAN ID to be configured (here VLAN 1).

Status: Use this check box to enable or disable the VLAN. When "Enable" is selected, the VLAN is enabled; when it is deselected, the VLAN is disabled.

Router Port Auto Learn: When this option is enabled, the switch can automatically detect and register devices connected to ports configured as router ports.

Immediate leave: When this option is enabled, the switch immediately sends a leave message to the router when a device leaves a multicast group, instead of waiting until the end of the poll interval.

Query Robustness: This value indicates the robustness of IGMP queries, i.e., the system's tolerance to lost IGMP queries due to network problems. A higher value means greater tolerance to losses.

Query Interval: This value defines the time interval between IGMP queries sent by the router in seconds. A shorter interval allows for faster detection of changes in multicast group membership, but increases network traffic.

Query Max Response Interval: This value defines the maximum time a member of a multicast group has to respond after receiving an IGMP query, measured in seconds.

Last Member Query Counter: This value defines how often the router sends IGMP queries after the last member of a multicast group has left the group. This mechanism ensures that all members have actually left the group.

Last Member Query Interval: This value defines the time interval between IGMP queries sent by the router after the last participant in a multicast group has left the group, measured in seconds.

"Operating Status" section

Status: Displays the current status of the VLAN, which in this case is "Disabled," indicating that the VLAN is currently inactive.

Query Robustness: Displays the current value of the IGMP query robustness, which is 2.

Query Interval: Displays the current time interval between IGMP queries, which is 125 seconds.

Query Max Response Interval: Displays the maximum time that a member of a multicast group has to respond after receiving an IGMP query, which is 10 seconds.

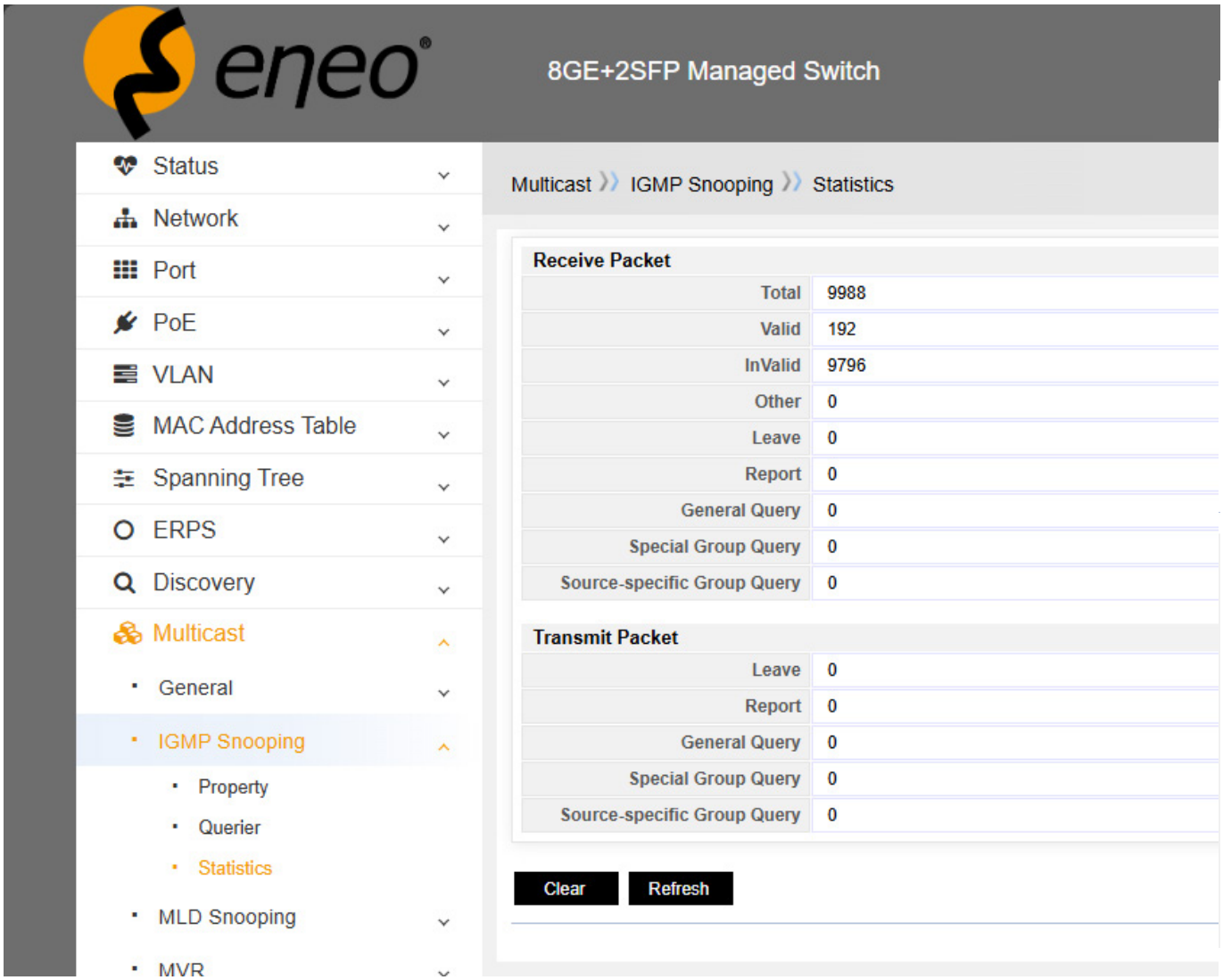
Last Member Query Counter: Shows how many times the router sends IGMP queries after the last member of a multicast group has left. The value is 2.

Last Member Query Interval: Shows the time interval between IGMP queries sent by the router after the last member of a multicast group has left. The value is 1 second.

Note!

The default aging time for multicast is 260 seconds. If it needs to be increased, the query interval time can be changed to 18000, which results in an aging time of 36010 seconds.

10.3.3 – IGMP protocol packet statistics



10.3.3.1 – Package received

Total: The total number of IGMP packets received by the switch.

Valid: The number of valid IGMP packets received. Valid packets are those that are properly formatted and processed correctly by the switch.

InValid: The number of invalid IGMP packets received. These are packets that are either incorrectly formatted or cannot be processed correctly.

Other: The number of IGMP packets that do not fall into the "Valid" or "Invalid" categories. These may include packets that are not relevant to the current IGMP snooping configuration.

Leave: The number of IGMP leave group messages received. These messages are sent by hosts when they want to leave a multicast group.

Report: The number of IGMP membership report messages received. These messages are sent by hosts to indicate that they want to receive multicast traffic from a specific group.

General Query: The number of IGMP general query messages received. These are sent by multicast routers to determine which hosts are members of which multicast groups.

Special Group Query: The number of IGMP special group query messages received. These are sent to specific multicast addresses to determine the members of these groups.

Source-specific Group Query: The number of IGMP messages received for source-specific group queries. These are used in source-specific multicast (SSM) to query members who are interested in traffic from specific sources to a multicast group.

10.3.3.2 – Transmit packet

Leave: The number of IGMP leave group messages transmitted by the switch.

Report: The number of IGMP membership report messages transmitted by the switch.

General Query: The number of IGMP general query messages transmitted by the switch.

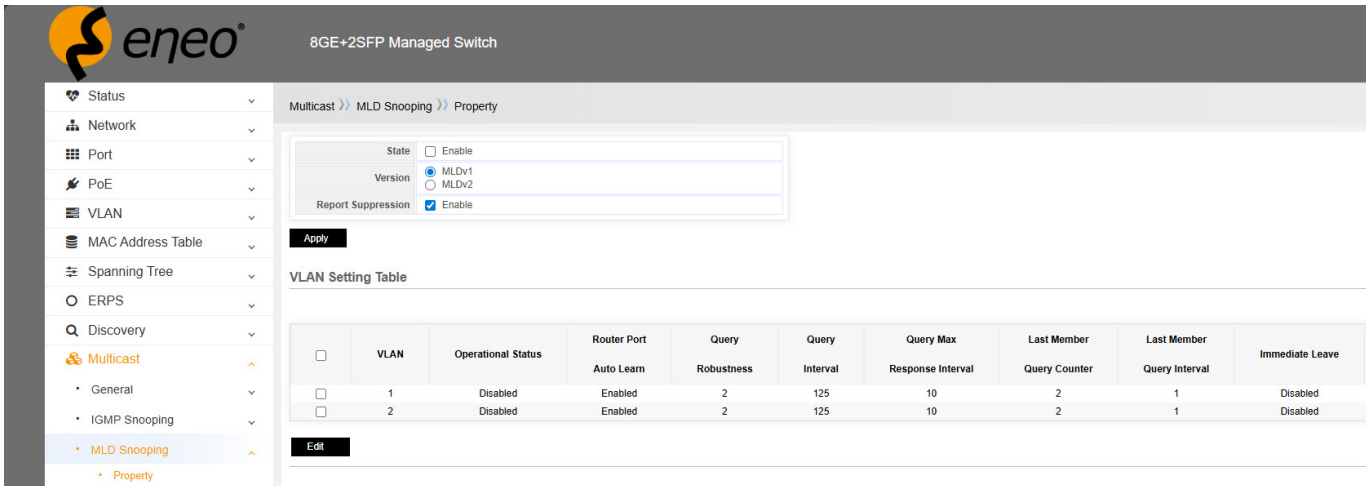
Special Group Query: The number of IGMP special group query messages transmitted by the switch.

Source-specific Group Query: The number of IGMP source-specific group query messages transmitted by the switch.

- **Locate problem source:** In the event of a network error, the IGMP protocol message statistics can provide detailed information about the messages and help network administrators quickly find the cause of the problem.
- **Analyze protocol interactions:** By statistically analyzing the interactions of IGMP protocol messages, we can evaluate the compatibility and stability between network protocols and thus resolve communication problems caused by protocol incompatibilities.

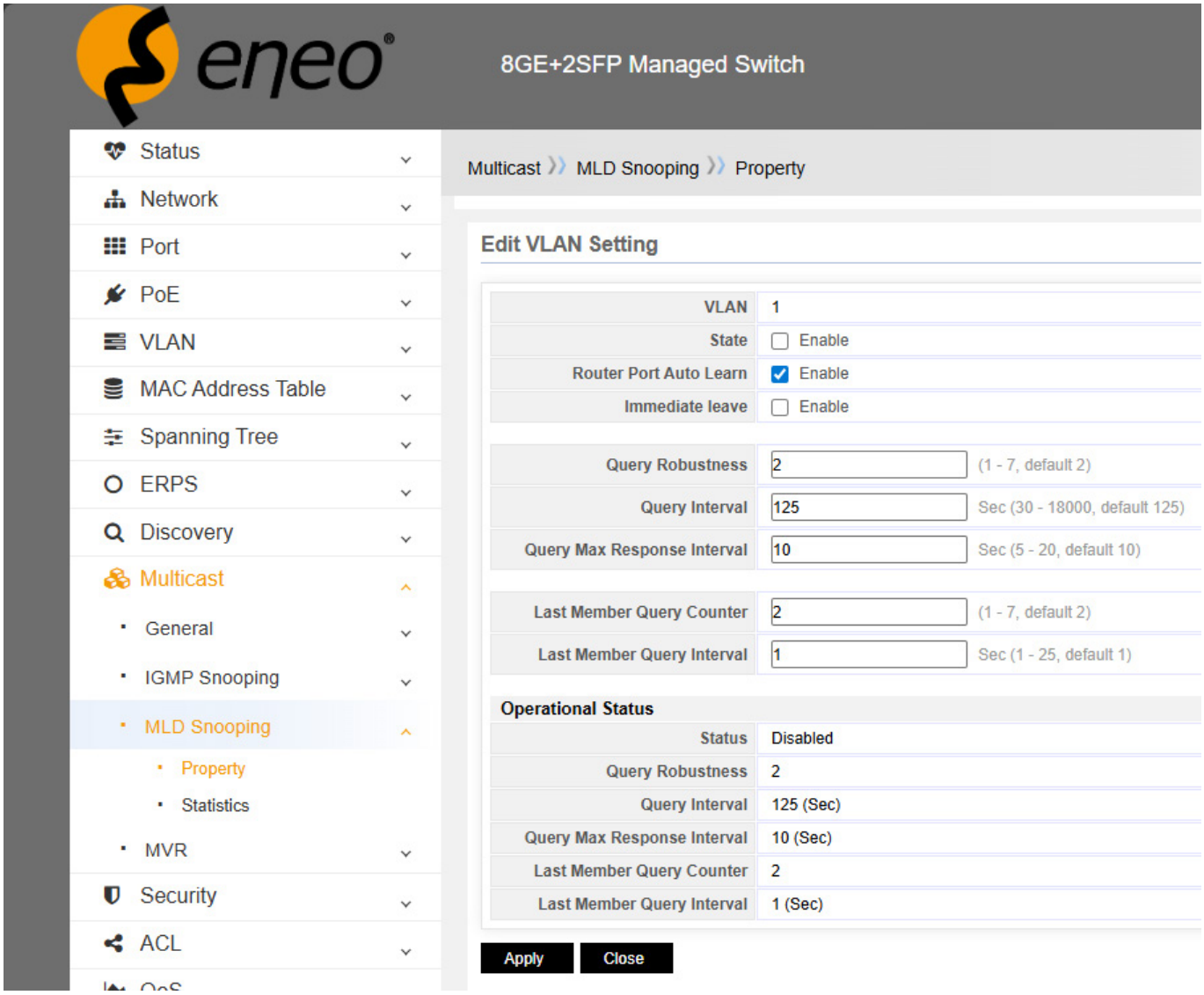
10.3.4 – MLD-Snooping

MLD Snooping, short for Multicast Listener Discovery Snooping, is a feature that is primarily used on Layer 2 devices in IPv6 multicast networks. It serves as a mechanism for managing and controlling IPv6 multicast groups by analyzing the received MLD messages (Multicast List Discovery). Specifically, a mapping between ports and MAC multicast addresses is established and IPv6 multicast data is forwarded based on this mapping.



- Users must set the MLD snooping status to "enabled" and select whether MLDv1 or MLDv2 should be supported.
- In addition, VLAN-based MLD snooping must be set to "enabled".

Check the MLD snooping entry option for VLAN1 and click on the "Edit" button.

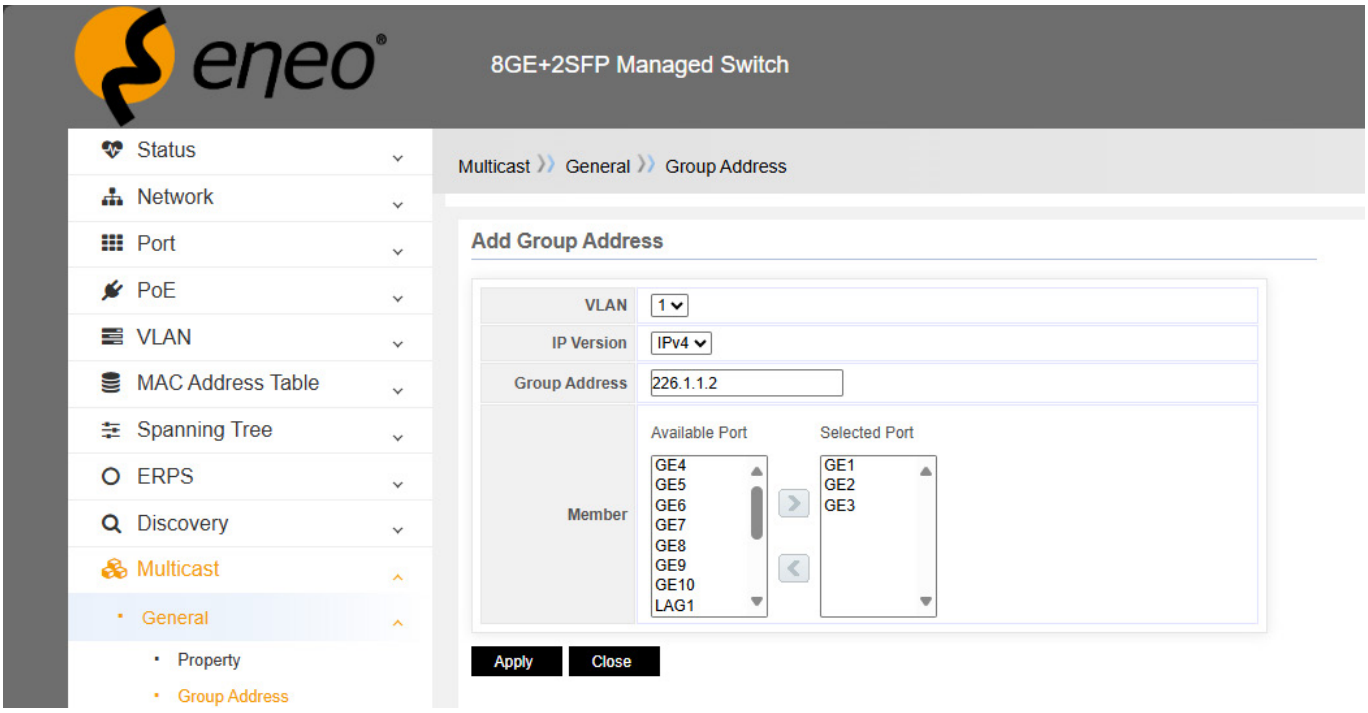


- **MLD-Snooping status:** Set the IGMP snooping status, enable or disable it (must be enabled).
- **Automatic learning of routing ports:** Specifies whether the switch learns a port as a routing port when it receives an IGMP query (must be enabled).
- **Immediate Leave:** Specifies whether the switch immediately removes a member from the multicast group when it receives an IGMP leave message and whether fast leave should be enabled (set according to user requirements).

10.3.5 – IGMP group address table

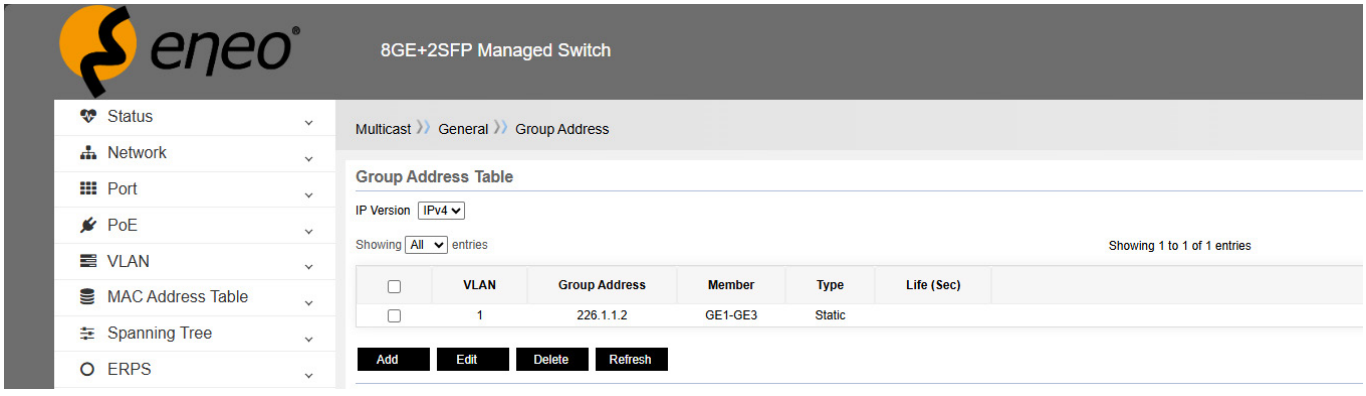
When the corresponding port of the switch receives an IGMP protocol message, it creates a multicast address table based on the content.

If necessary, the user can also manually add a multicast address table by clicking the 'Add' button and then entering the configuration interface.



After you have set up the VLAN, IP version, multicast address and member ports, click the Apply button to complete the configuration.

Finally, you will see in the group address table that the static multicast group for 226.1.1.2 has been set up with member ports 1-3.



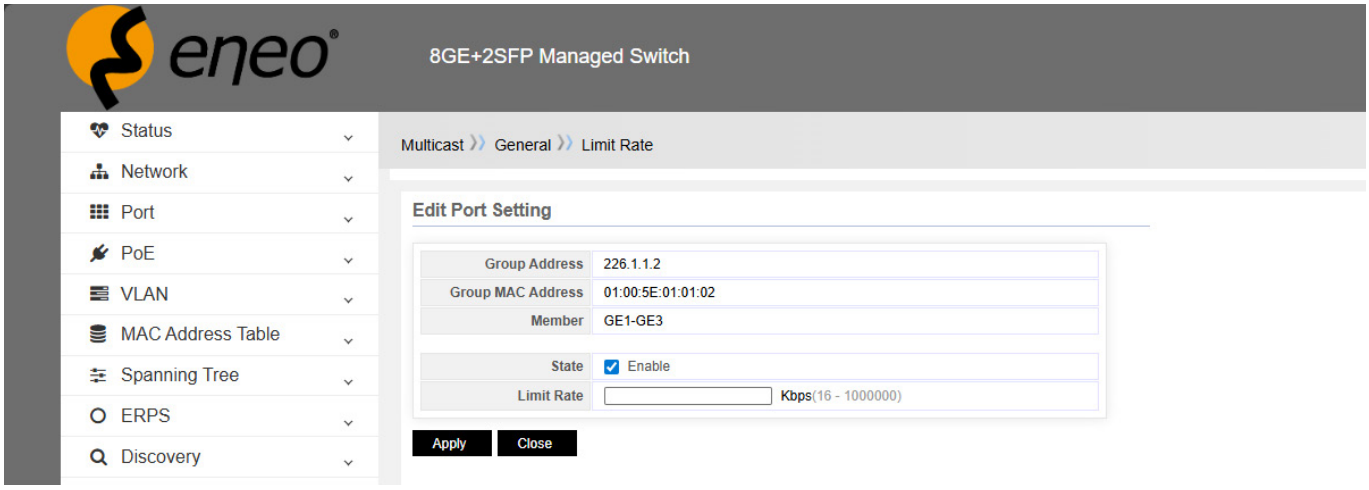
10.3.6 – IGMP multicast rate limiting

There are several advantages:

- **Fine-tuned traffic control:** With the transmission rate limiting feature, network administrators can precisely control the traffic of specific multicast groups and adjust bandwidth allocation to actual demand to meet different network requirements in various application scenarios.
- **Improved user experience:** By implementing appropriate rate limits, critical applications or services can be prioritised for data transmission, improving the user experience.
- **Defence against malicious traffic attacks:** Multicast group rate limiting can also serve as a defence mechanism against malicious traffic attacks by limiting the bandwidth consumed by attack traffic, thereby reducing its impact on the network.

Select the multicast group for which rate limiting is required, click the 'Edit' button and continue with the configuration.

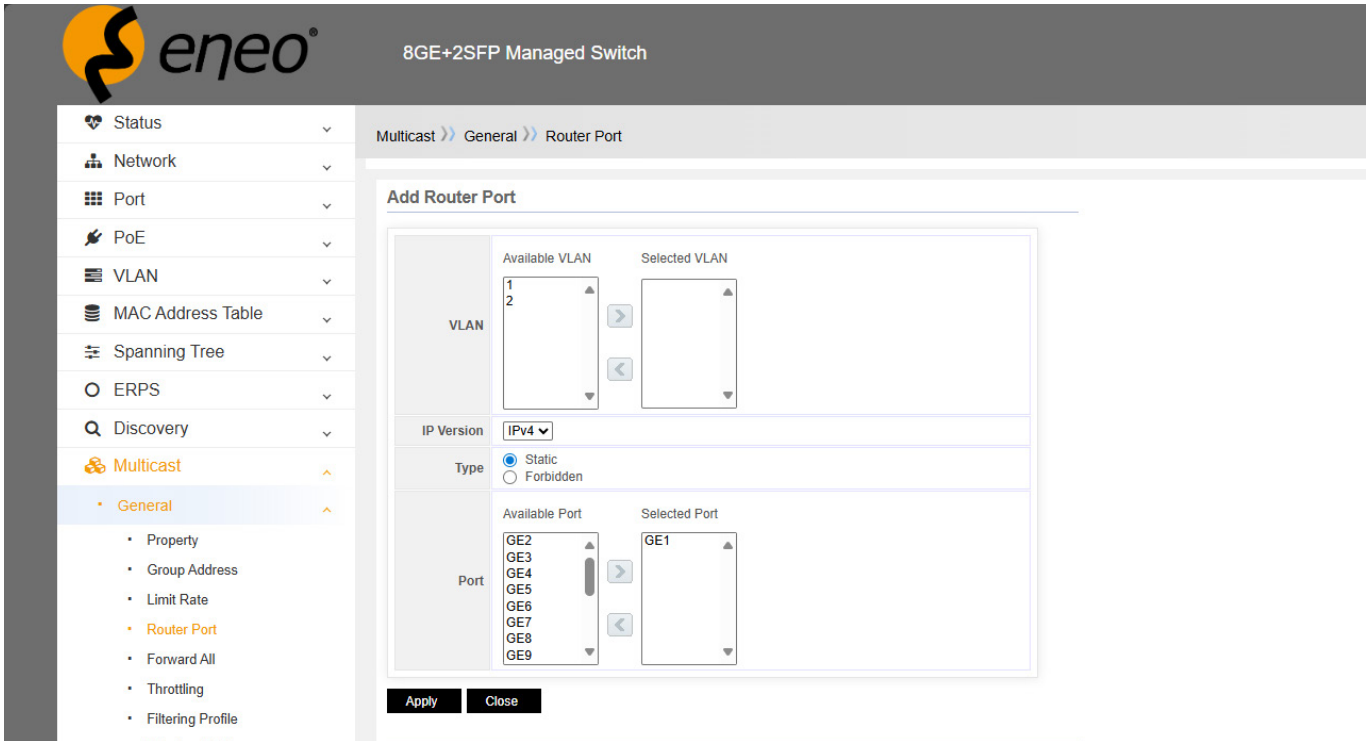
Select the status by ticking the checkbox, then enter the value for the rate limit and finally click 'Apply' to complete the process.



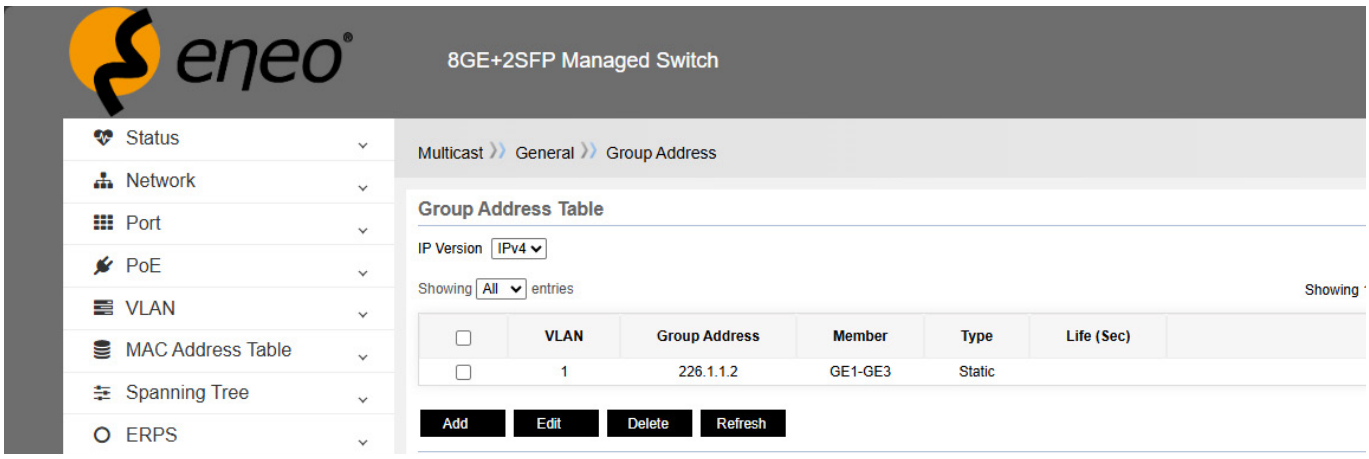
10.3.7 – IGMP router port

IGMP routing ports are divided into two types: dynamic and static. When a switch receives an IGMP query, it automatically recognises this port as a dynamic routing port. Users can also manually configure static routing ports, which have the same function as dynamically recognised routing ports.

For example, to set the GE1 port as the selected port, click the 'Apply' button and you're done.

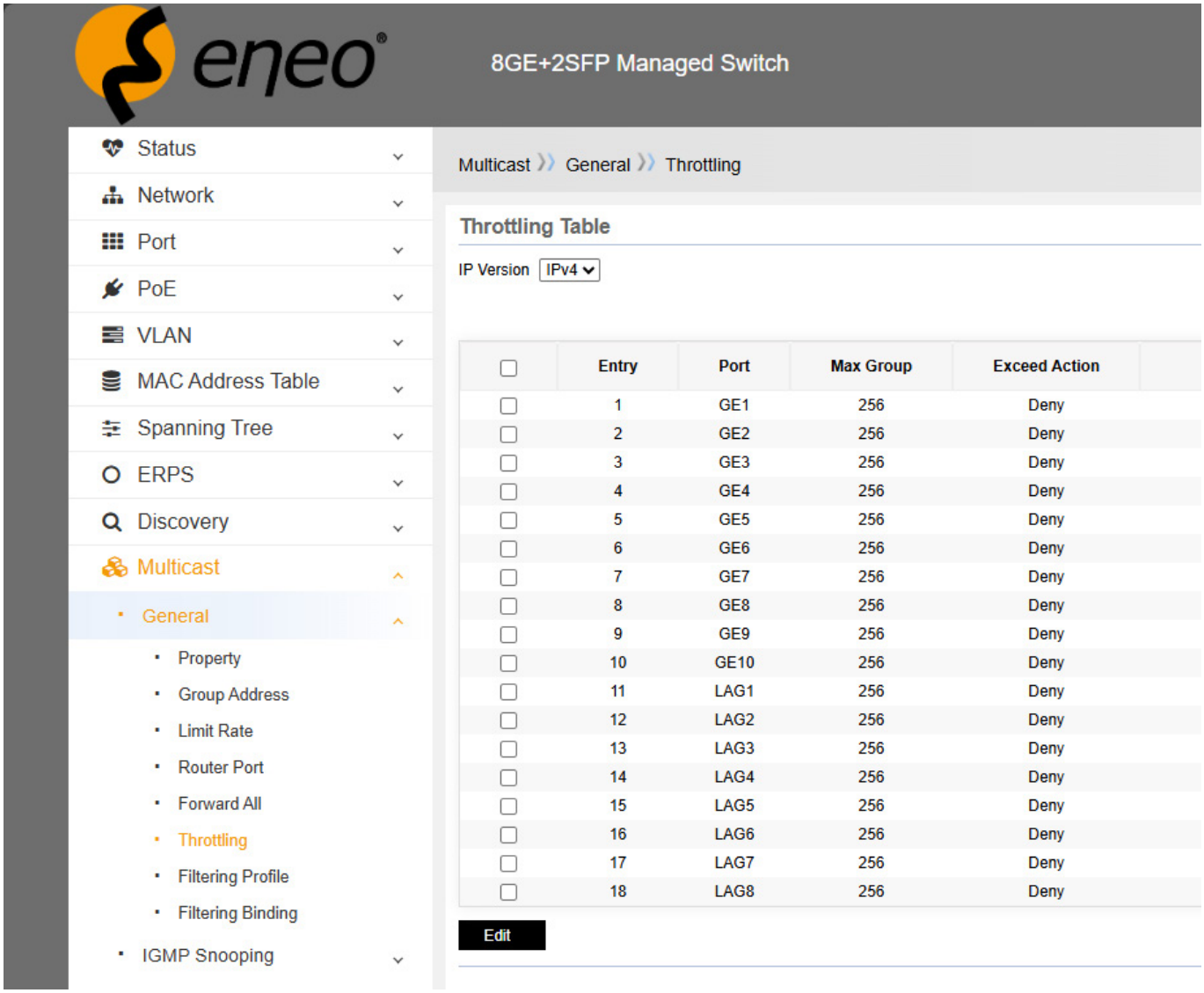


As you can see, GE1 has been configured as a routing port, and it also shows that GE1 is a static routing port.

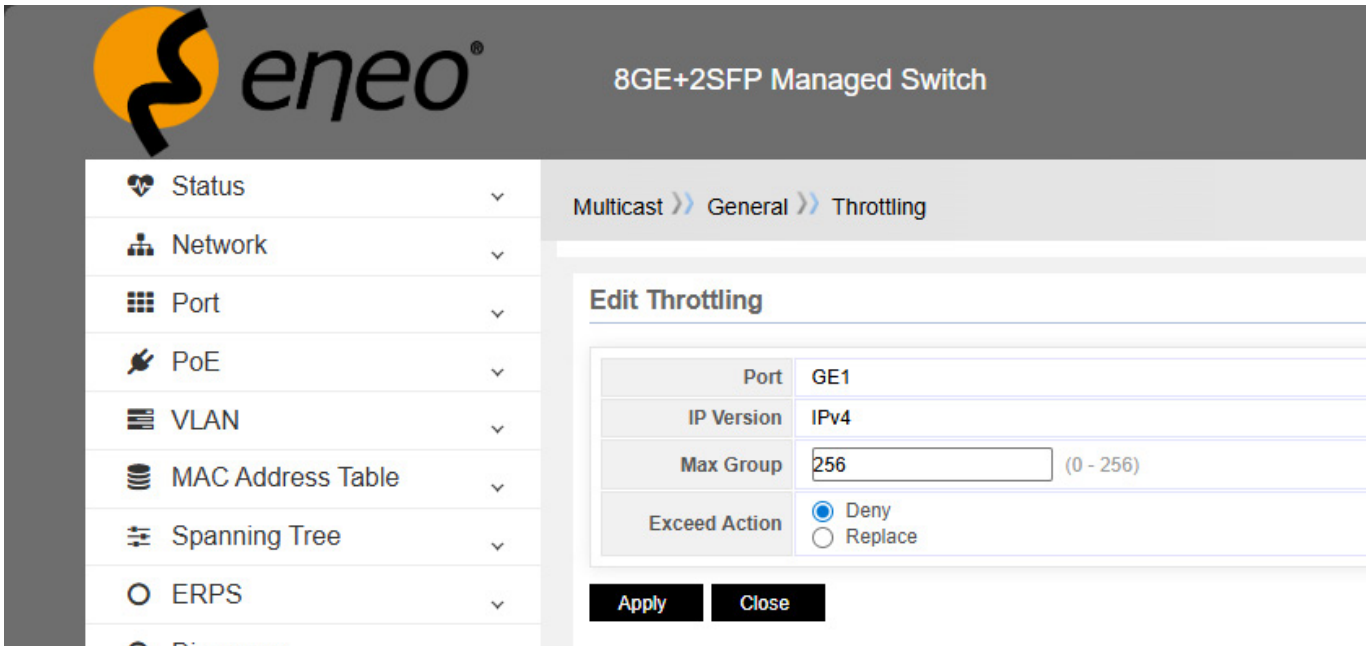


10.3.8 – Maximum number of ports that can be added to multicast groups

By default, an IGMP member port can join up to 512 multicast groups, but users can limit the number of multicast groups it can join. For example, a user can restrict the port so that it can only join one multicast group.



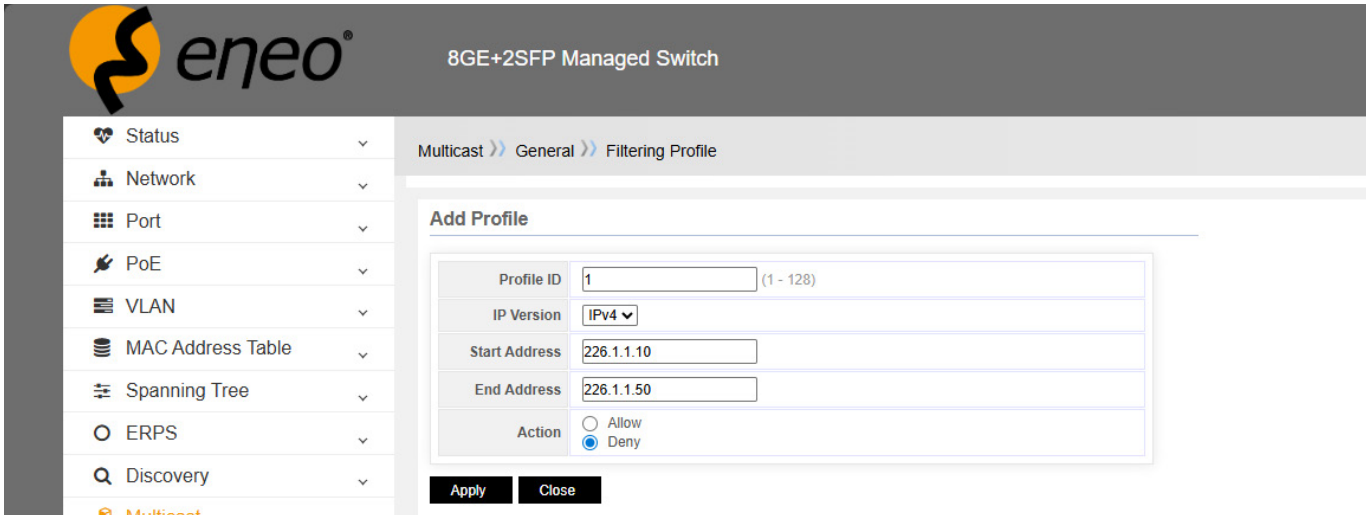
Select the port that you want to restrict. For example, if the maximum group limit is set to 1, this port can only join one multicast group. For all other multicast groups, you have the option of either rejecting or replacing them. Reject means that no new groups will be joined, while Replace means that the existing multicast group will be replaced by a new one, but the port will still only be a member of one multicast group at a time.



10.3.9 – IGMP filter table

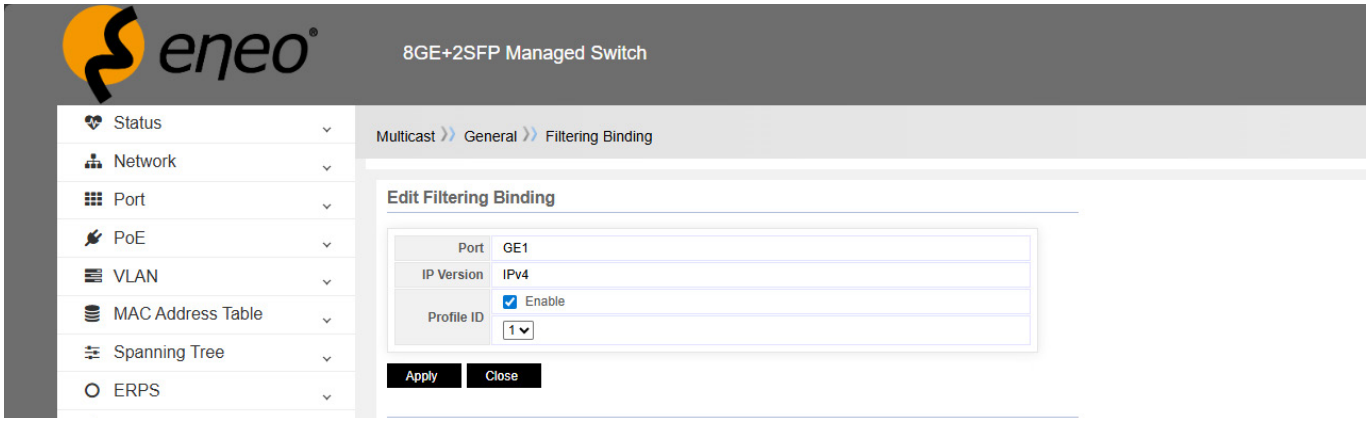
The function of IGMP filtering is usually to filter a specific port or multiple ports that have joined the multicast group. Users can filter some multicasts and some ports according to their actual requirements to meet user needs.

Therefore, the IGMP filter table and the IGMP filter port must be used together.



For example, to add a filter rule, select 'IPv4' as the IP version information, set the start address to '226.1.1.10' and the end address to '226.1.1.50', and set the action to 'Reject'.

Link the filter rule to the specified ports as shown in the following figure:



Then bind this rule to port 1 and port 3. This will prevent the multicast stream sent by the server to this group from being forwarded to ports 1 and 3, even if ports 1 and 3 have joined multicast group 226.1.1.22.

10.3.10 – MVR

The MVR (Multicast VLAN Registration) function is an essential component for multicast environments. It primarily facilitates the replication of multicast streams across VLANs.

With MVR, client PCs can remain in their individual VLANs and still access shared multicast streams. This is particularly useful in scenarios where multicast resources need to be shared across different VLANs, such as video conferencing or live TV broadcasts over the network.

How MVR works

In a multicast scenario, multicast data sent from a multicast source is replicated to all hosts that are interested in that multicast group. However, in traditional VLAN configurations, VLANs are isolated from each other, so multicast data cannot be transmitted directly across VLANs.

MVR solves this problem with a registration mechanism. When a host within a VLAN expresses interest in a particular multicast group, that VLAN registers its interest with the switch. The switch then replicates the multicast data for that group to all VLANs that have expressed interest, enabling cross-VLAN sharing of multicast data.

Application scenarios for MVR

MVR is crucial in scenarios that require large-scale deployment of multicast applications. In enterprise networks, for example, it may be necessary to share video conferences or live TV broadcasts across different departments or floors. By enabling MVR, these resources can be easily shared across VLANs without having to provide separate multicast sources in each VLAN.

Configuring MVR

When configuring the MVR function, there are two types of MVR ports: source ports and receive ports.

- **Source port:** A source port is the port through which multicast streams are transmitted in a multicast VLAN.
- **Receiving port:** This is the port of a switch that is connected to a multicast-listening host. It can be placed in any VLAN other than the multicast VLAN or in a VLAN-less state (VLAN-less usually refers to VLAN1, where traffic is not tagged). This means that with MVR enabled, the switch performs a VLAN tag exchange and replaces the VLAN tag of the multicast receiving port with the VLAN tag of the source port.

Multicast VLAN refers to a dedicated VLAN for MVR that must be manually configured in a specific network. It must be explicitly configured for all source ports.
It is often used to transmit multicast streams in the network while avoiding the duplication of multicast streams in different VLANs.

MVR has two configuration modes: compatible mode and dynamic mode

- **Compatible mode:** In compatible mode, the CPU of the MVR switch normally forwards queries from routers and processes report messages from clients to create a dynamically learned multicast forwarding table. However, the CPU does not forward report messages to router ports, so the parent router does not receive the underlying report messages, which means that router data cannot be forwarded to the switch normally. In this mode, the router's multicast forwarding table must be configured manually to forward data to the switch.
- **Dynamic mode:** The only difference between dynamic mode and compatible mode is that in dynamic mode, the CPU can forward report messages to router ports, allowing parent routers to learn the multicast forwarding table dynamically without having to manually configure the router's multicast forwarding table to forward data to the switch.

11 – ACL

11.1 – ACL Overview

Due to the increasing size and traffic of networks, security controls and bandwidth allocation are playing an increasingly important role in network management. By filtering packets, unauthorised users can be effectively prevented from accessing the network, network traffic can be controlled and network resources can be saved. Access control lists (ACLs) are commonly used to configure matching rules for packet filtering.

When a message is received, the switch compares the message with the ACL rules applied to the current port to allow or reject the message.

An ACL rule can be used by other IP and MAC type classification references. An ACL uses a set of conditions, called rules, to classify packets. Conditions can be based on the packet type, source address, destination address, and port number contained in the packet.

ACLs are divided into the following three types according to their intended use:

- **MAC-based ACL:** Rules are created based solely on the source MAC address and destination MAC address.
- **IPv4-based ACL:** Rules are created based on information from layers 3 and 4, such as source and destination IP addresses, protocol type transported by the IP, detailed protocol characteristics, etc.
- **IPv6-based ACL:** Rules are created based on information from layers 3 and 4, such as source and destination IP addresses, protocol type transported by the IP, detailed protocol characteristics, etc.

11.2 – Understanding access control parameters

Before configuring an ACL on a switch, you must have a good understanding of access control parameters (ACP). ACP in the CLI output of a switch includes masks.

Each ACE has a mask and a rule. The classification domain or mask is the domain in which you want to perform an action. Specifying a value and a specific mask is called a rule.

Messages can be classified into these domains of layers 2, 3, and 4:

Layer 2:

- Source MAC address (specify all 48 bits)
- Destination MAC address (specify all 48 bits)
- Ether type (16-bit Ether type field)

You can use some or all of these domains to define a stream.

Layer 3:

- **IP source address**

  (Specify all 32-bit IP source addresses to define the stream, or specify a user-defined subnet. There are no restrictions on the specified IP subnet.)

- **IP destination address**

  (Specify all 32-bit IP destination address bits to define the stream, or specify a user-defined subnet. There are no restrictions on the specified IP subnet.)

You can define a stream using some or all of these domains.

Layer 4:

- TCP (you can specify TCP, source port, destination port or both)
- UDP (you can specify UDP, source, destination port number or both)

11.3 – Example ACL configuration

Name ACL

When creating MAC ACLs, IPv4 ACLs, and IPv6 ACLs, users must first specify a name for the ACL. Each ACL type can have multiple names. Named ACLs allow users to identify an ACL by its name and perform appropriate operations. When creating an ACL, users must first configure the name. Once an ACL has been created, users can delete it but cannot change it.

ACL matching order

An ACL can contain multiple rules, each of which specifies different options for packet matching. These rules can be duplicated or contradictory. Which rules should be used when a packet matches the rules of an ACL? The order of the matching rules must be determined.

The following principles apply to determining the priority of an ACL

Configuration order: The rules are matched in the order of the user configuration rules and also in the order of the ACL serial numbers.

Number of ACL entries

Based on MAC, IPv4, and IPv6, the total number of entries is 1000, which can be assigned by users.

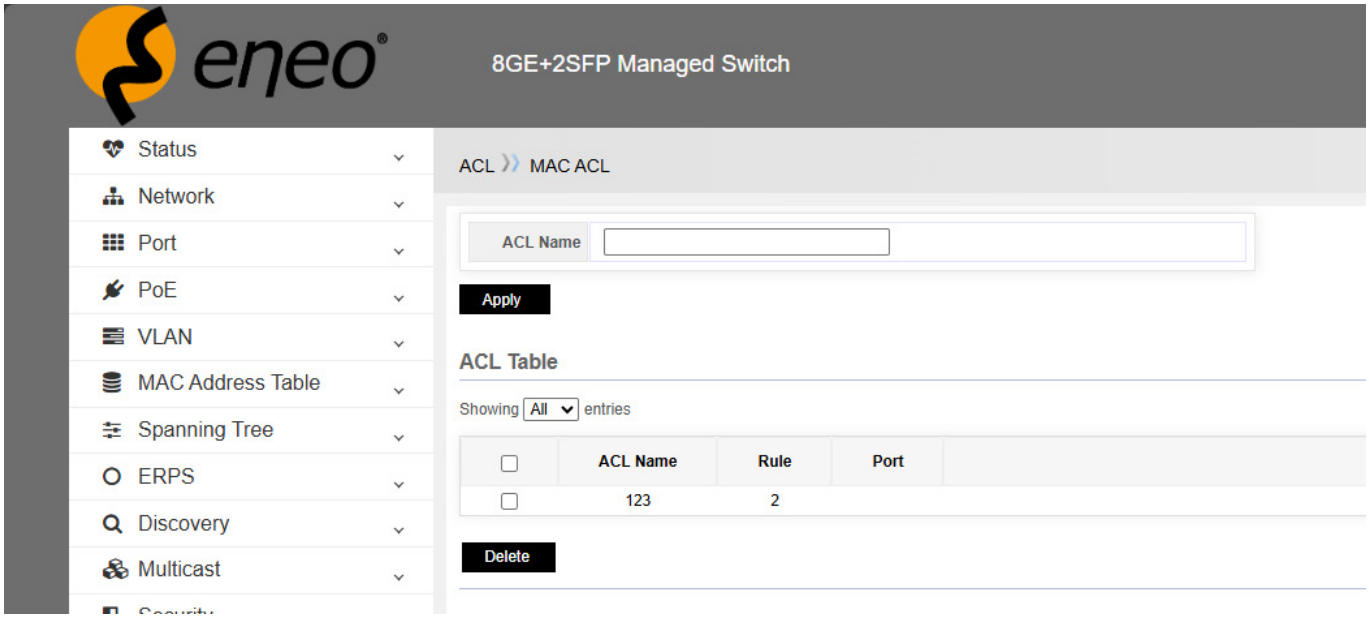
For port binding ACL entry rules

ACL entries can be bound to a specific port, which can individually match MAC, IPv4, and IPv6 ACL. However, if they match at the same time, only MAC ACL + IPv4 ACL or MAC ACL + IPv6 ACL can match.

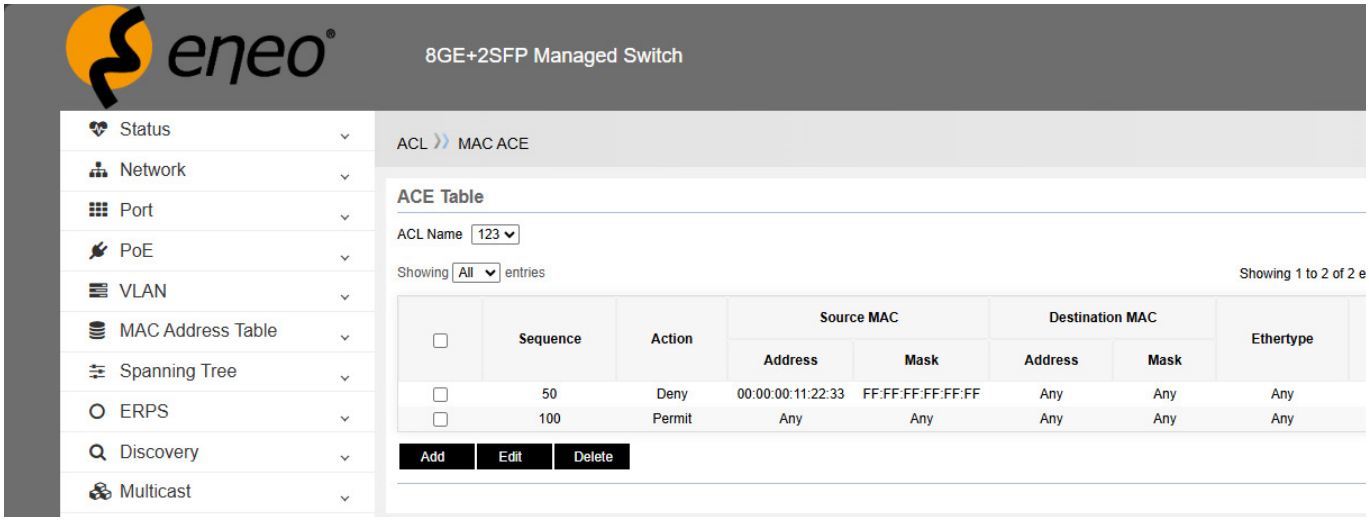
This means that IPv4 can, for example, define multiple name ACL rules, port 1 can match one of them, port 2 can match another rule.

MAC ACL

An entry with ACL 123 is configured



Two rules were then added to the MAC ACE rules

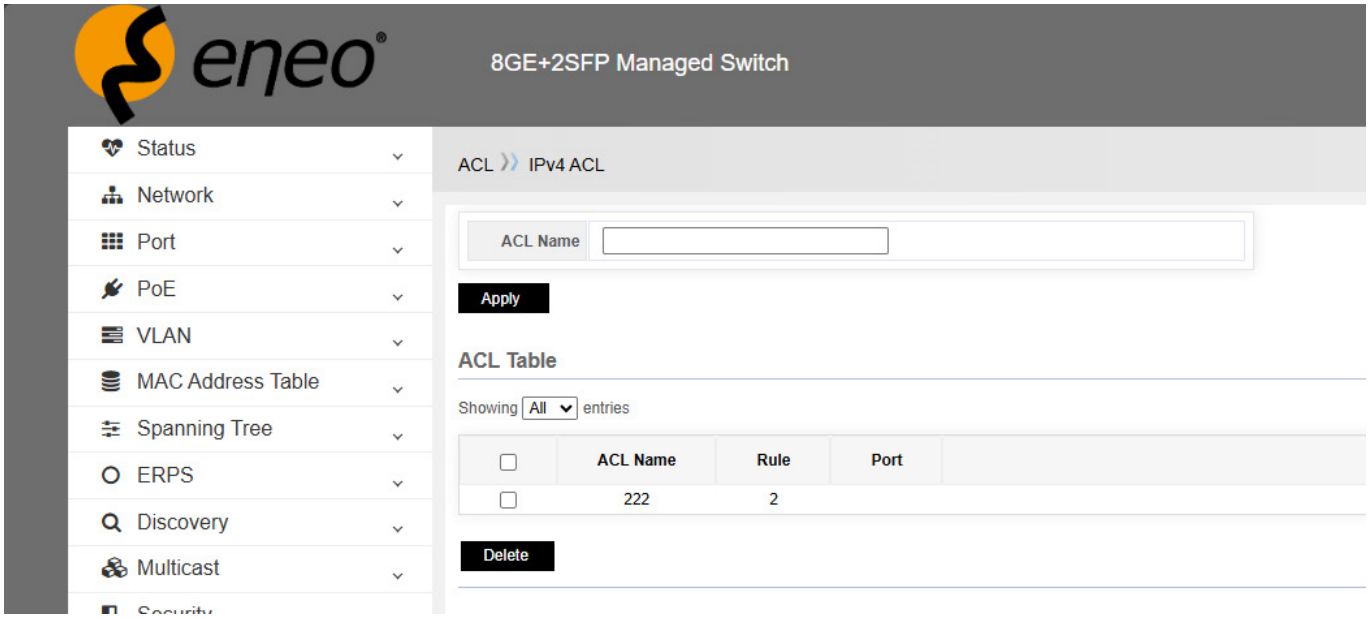


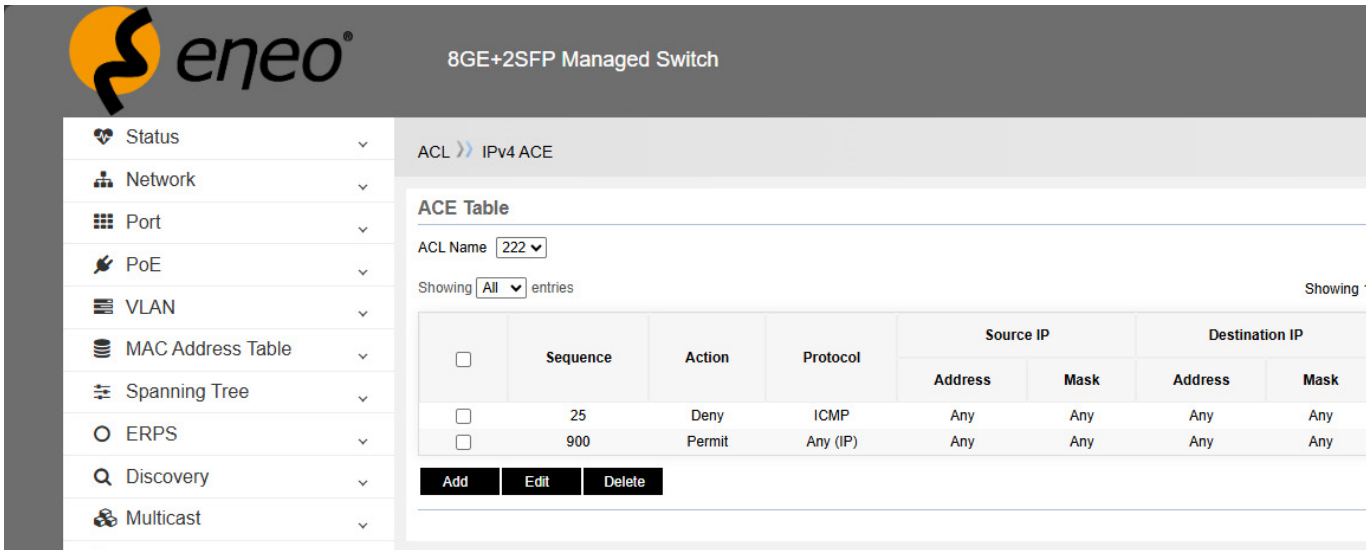
Configuring the MAC ACL rules

- The first rule rejects messages with the MAC address 00:00:00:11:22:33.
- The second rule allows all messages based on the MAC address to pass.

IPv4 ACL

An entry with ACL 222 is configured.



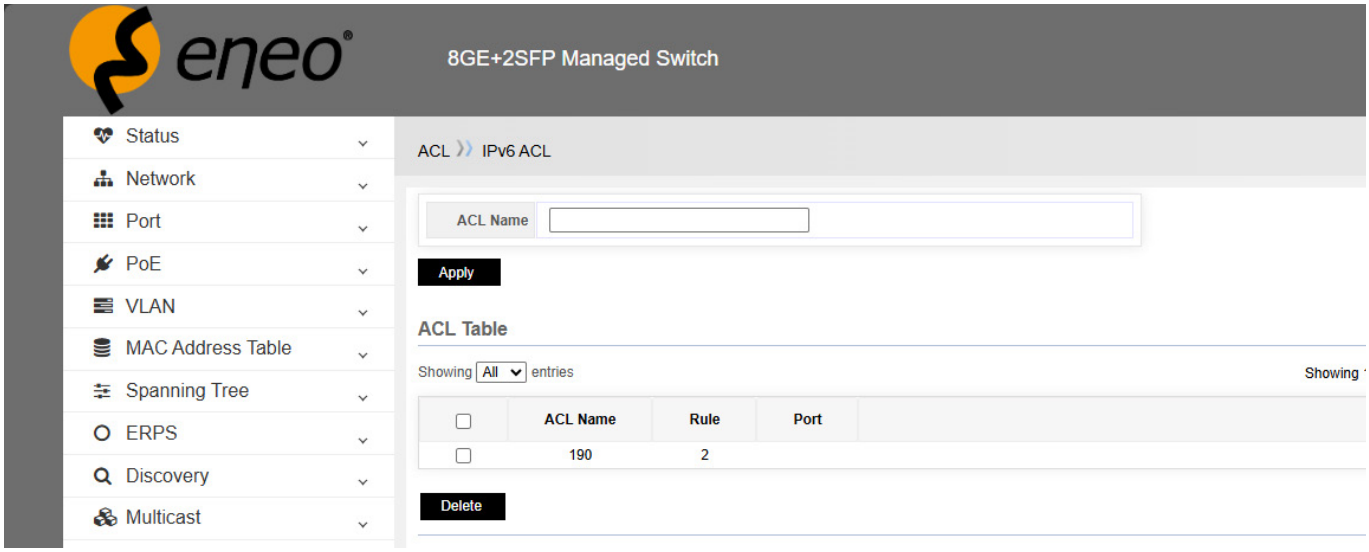


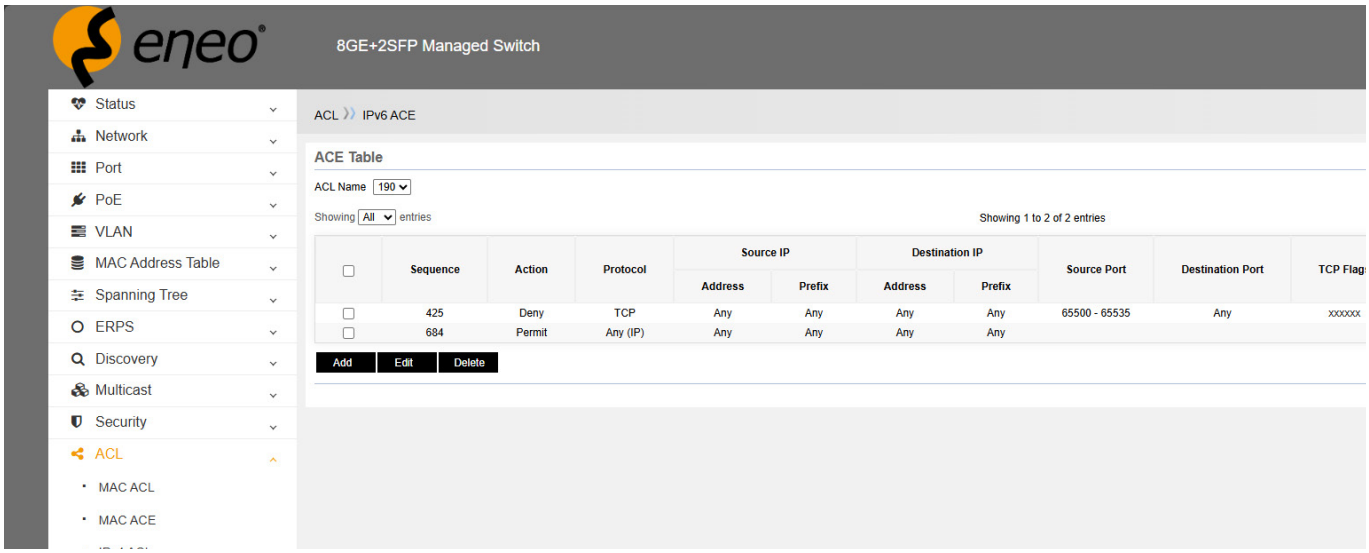
Configuring the IPv4 ACL rules

- The first rule rejects ICMP IPv4 packets.
- The second rule allows all IPv4-based packets to pass through.

IPv6 ACL

An entry with ACL 333 is configured.



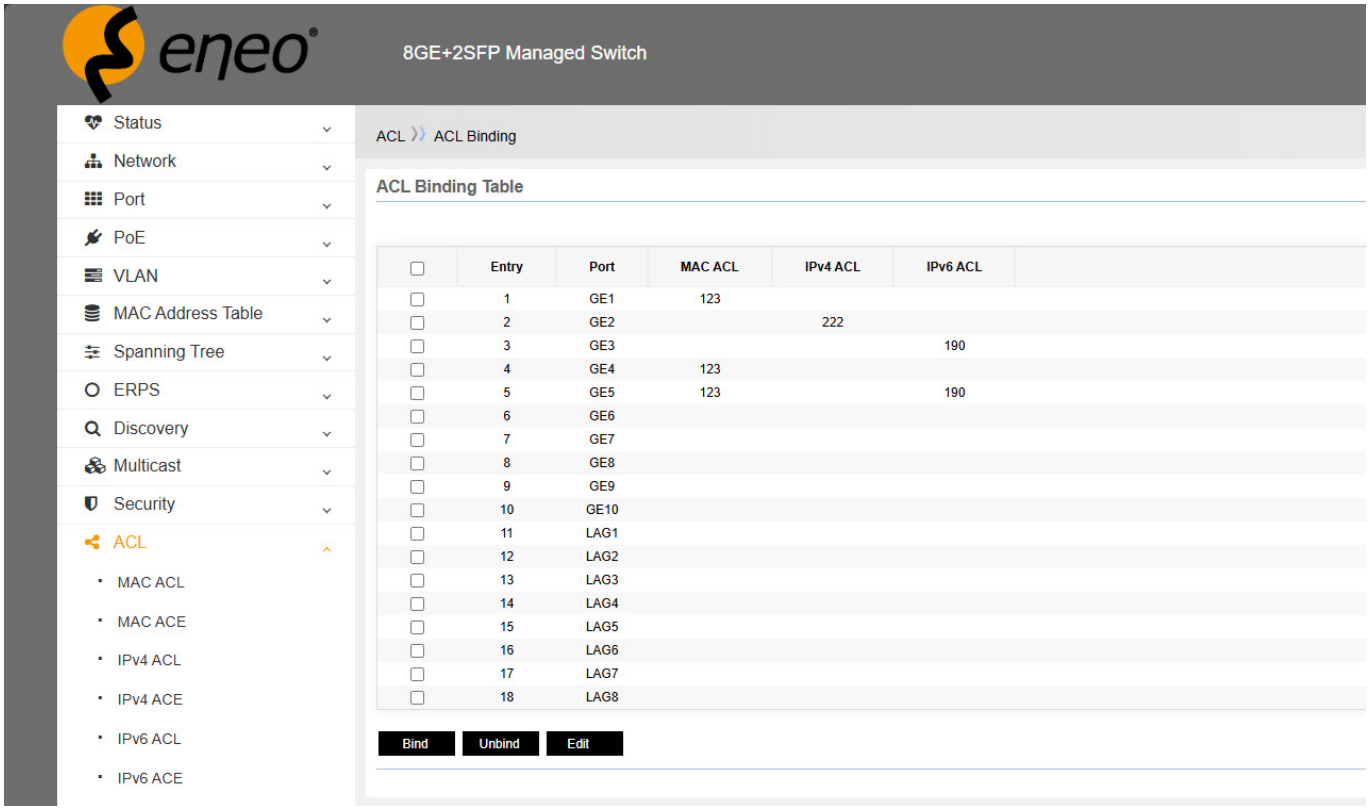


Configuring the IPv6 ACL rules

- The first rule rejects IPv6 packets whose TCP port number is between 65500 and 65535.
- The second rule allows all IPv6-based packets to pass through.

ACL-Binding

Link ACL rules to the corresponding ports.



As can be seen here:

- 1 is linked to rule 123
- 2 is linked to rule 222
- 3 is linked to rule 190
- 4 is bound to rules 123+222
- 5 is bound to rules 123+190

Rules can be defined in a variety of ways depending on user requirements and then bound to the appropriate port. For example, in MAC ACL, you can define a rule entry with the value 111 and then bind it to another port.

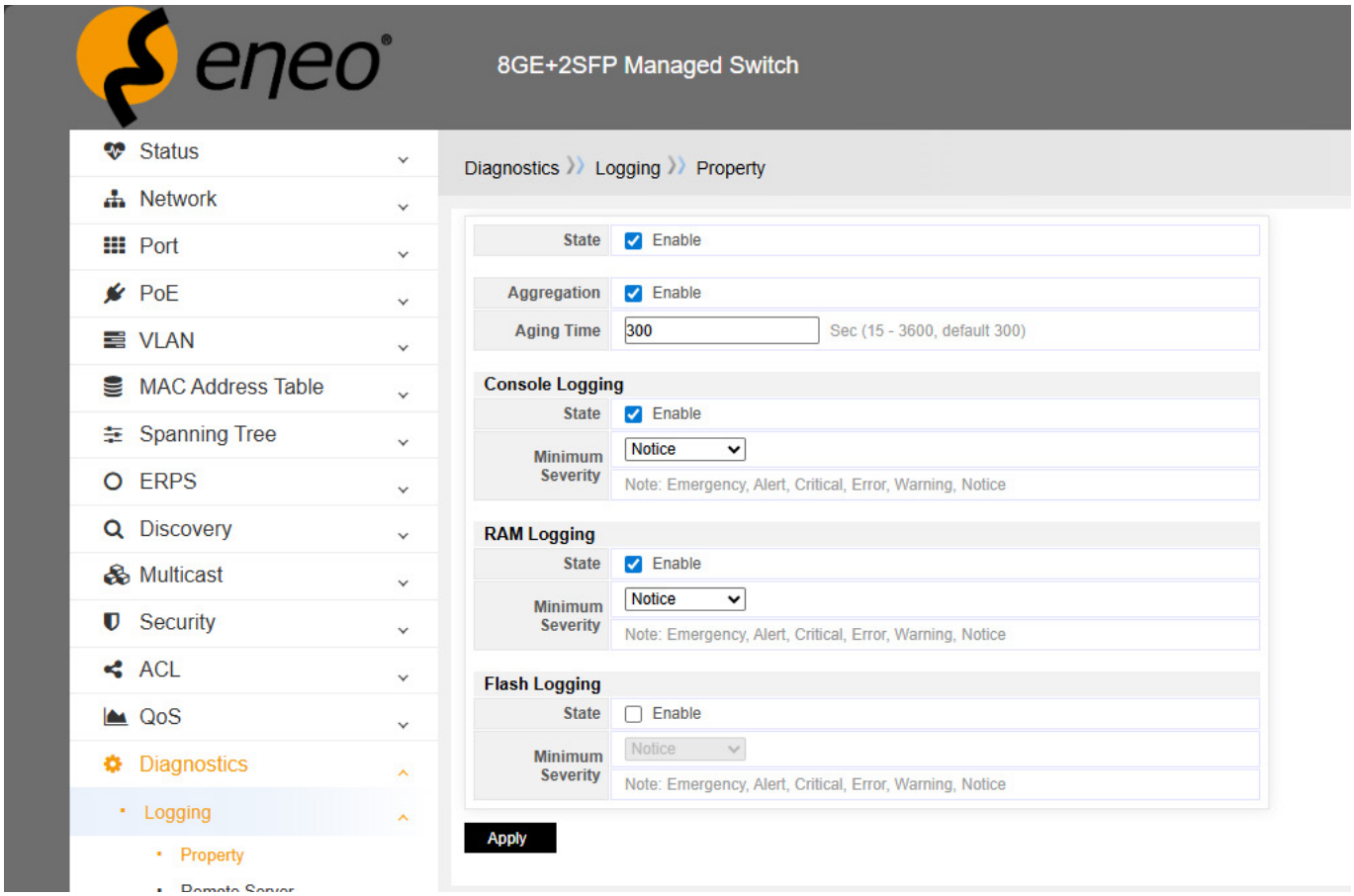
Note!

If you want to delete an ACL entry rule, you must first remove it before you can delete it. If this entry is already linked to the port, you cannot delete it.

12 – DIAGNOSTICS

12.1 – Logging

12.1.1 – Property



Status: Information about logging, on/off.

Aggregation: Specifies whether log entries are displayed combined, on/off.

Aging Time: How often the log information is updated. The default value is 300 seconds.

Console logging: Display log information on the console.

RAM logging: Display log information in RAM.

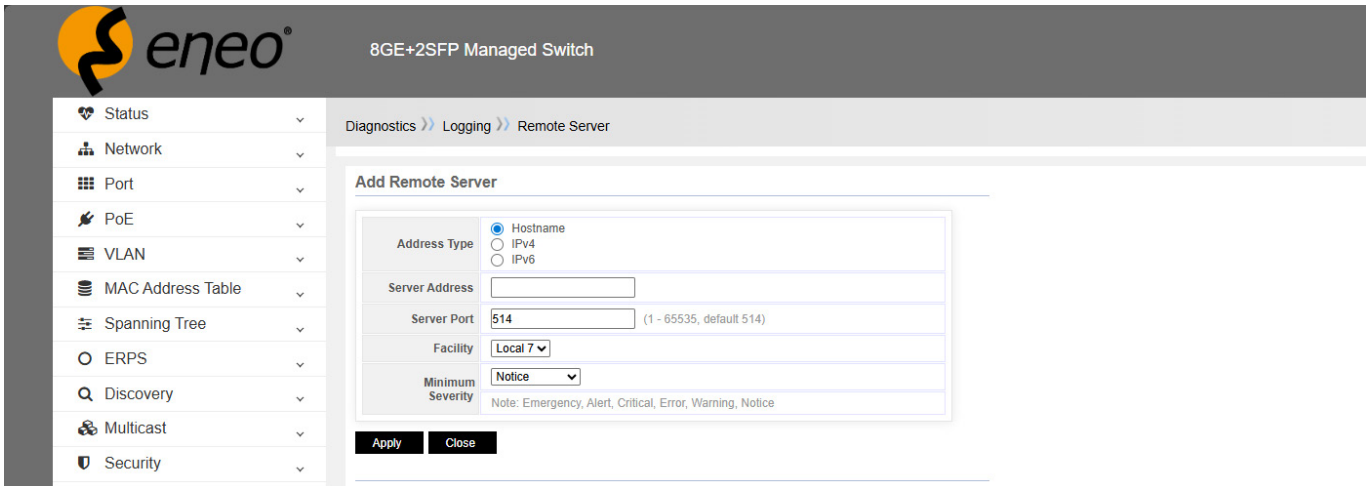
Flash logging: Display log information in flash.

Minimum severity: Log level, divided into 8 types: Emergency, Warning, Critical, Error, Note, Information, Debug.

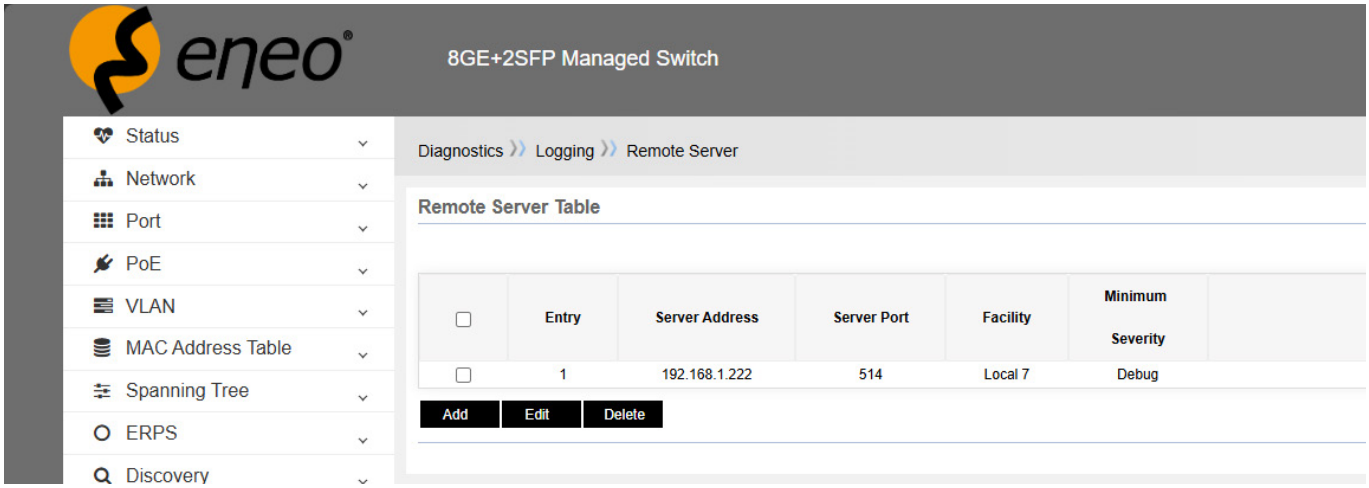
12.1.2 – Setting for outputting information about switching to a log server

The switch's log information can be sent to the log server, which stores all log information without gaps. This is convenient for users to query.

Add information about the log server, including the server address and minimum severity option.



After completing the configuration, it will look like the following figure:



The log server can receive the log records sent by the switch and display detailed log information.

12.2 – Mirroring

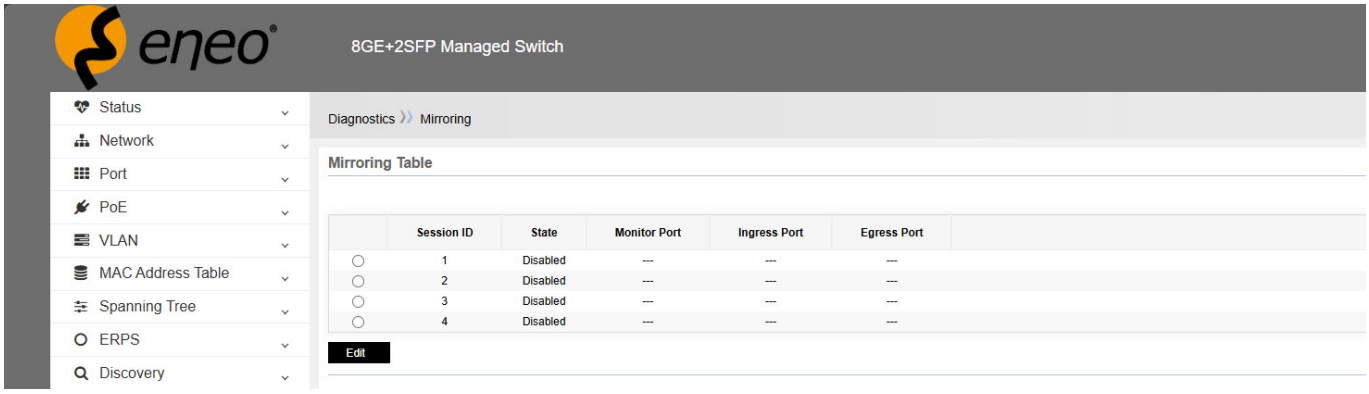
Supports 4 mirroring sessions.

Data capture settings:

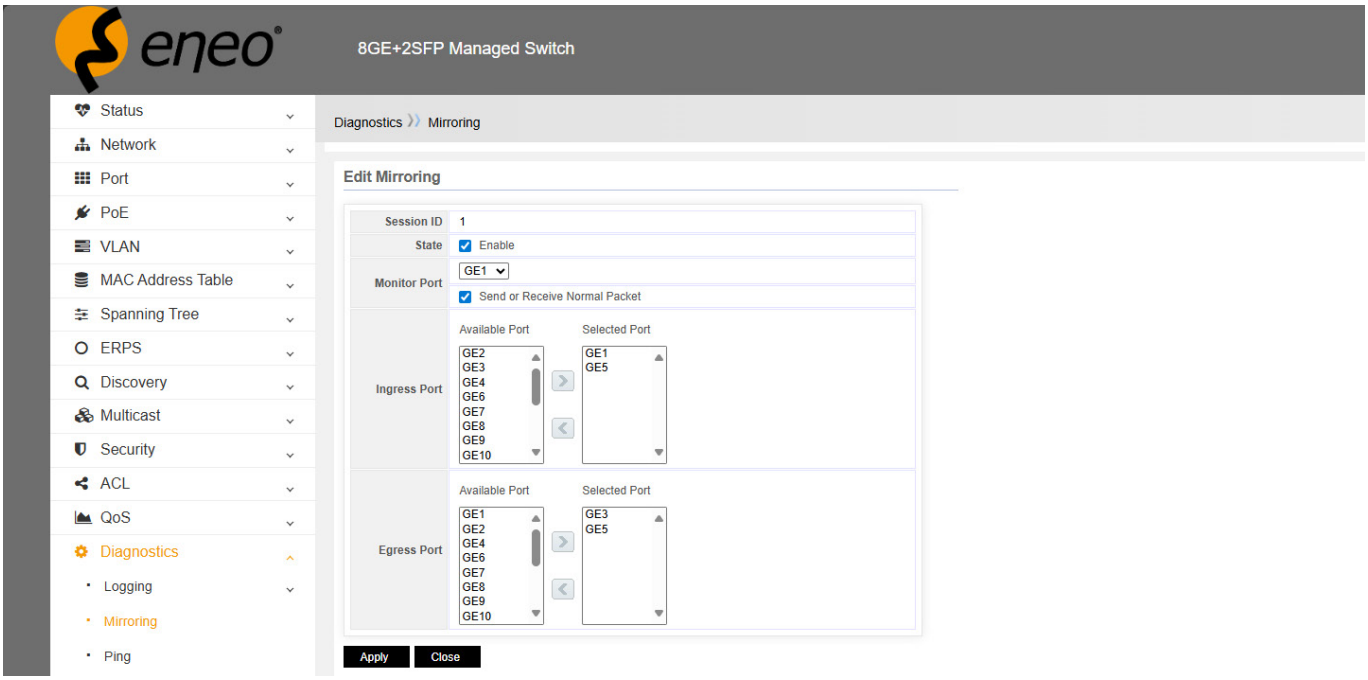
Capture status: Set the port mirroring status, on/off

Capture port: Select a capture port, i.e. mirror messages received on the captured port to this port

Captured port: Capture incoming messages, outgoing messages or all messages.



Select a mirroring session and click 'Edit'.



Status: Activate

Monitor port: Select some ports whose messages are to be mirrored on this port.

Note!

Enable 'Send or receive normal packet' to control the switch via the PC connected to this port after configuration. Otherwise, this port cannot be used to control the switch.

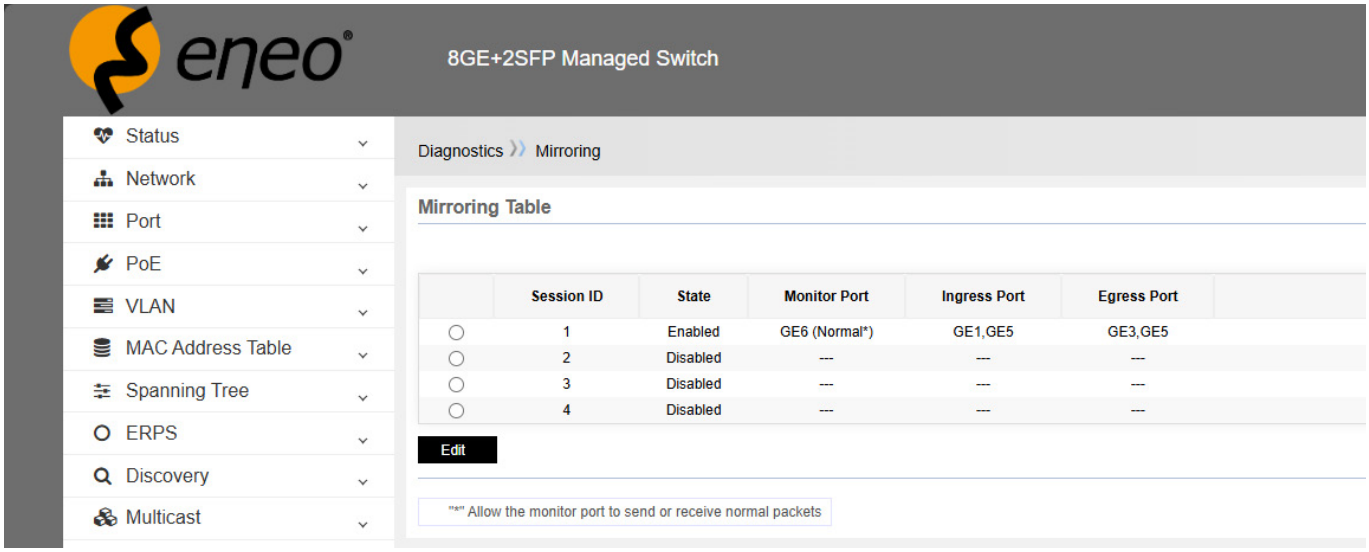
Input port: Messages sent to this port

Progress port: Messages sent from this port

As shown in the example:

- Mirror the input messages of the GE2 port to the GE6 port
- Mirror the output messages of the GE3 port to the GE6 port
- Mirror the input and output messages of the GE5 port to the GE6 port

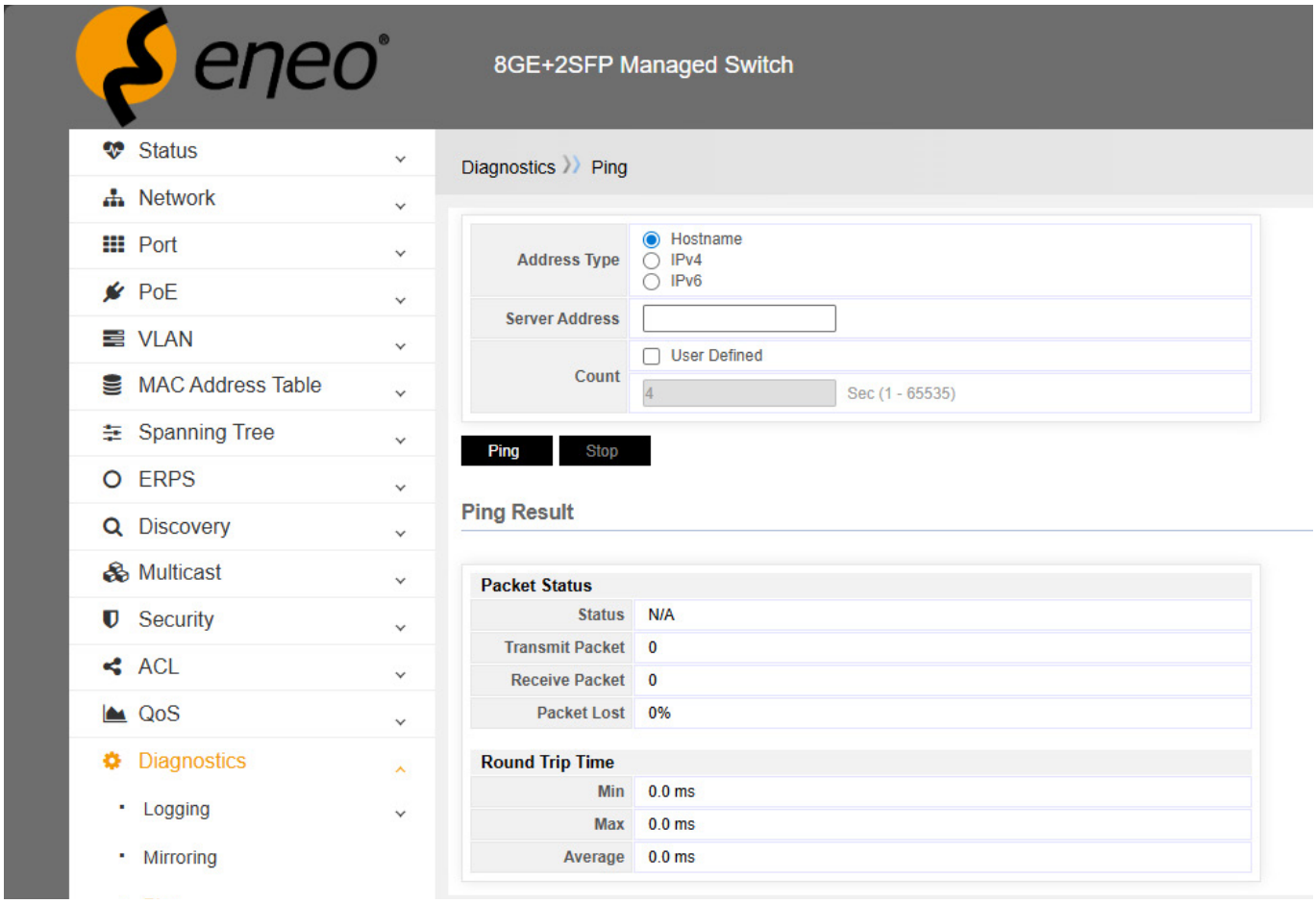
Check the details of the mirror configuration.



12.3 – PING

PING (Packet Internet Groper) is used to test the network connection. Ping is a service command that runs in the application layer of the TCP/IP network architecture and is mainly used to send an ICMP ECHO request message to a specific destination host to test whether that destination host is reachable and to understand its relevant status.

PING is used to ensure that the local host can successfully exchange (send and receive) packets with another host. Based on the returned information, we can deduce whether the TCP/IP parameters are set correctly, the process is running normally, and the network is free of interference.



Address type: Host name, IPv4, IPv6

Service address: The destination address for PING must be entered here.

Number: The number of messages for PING in succession. The default value is 4. You can also enter the number of messages for PING manually.

Ping result

Status: Passed or failed

Packet transmitted: How many ping messages were sent?

Packet received: How many ping messages were received?

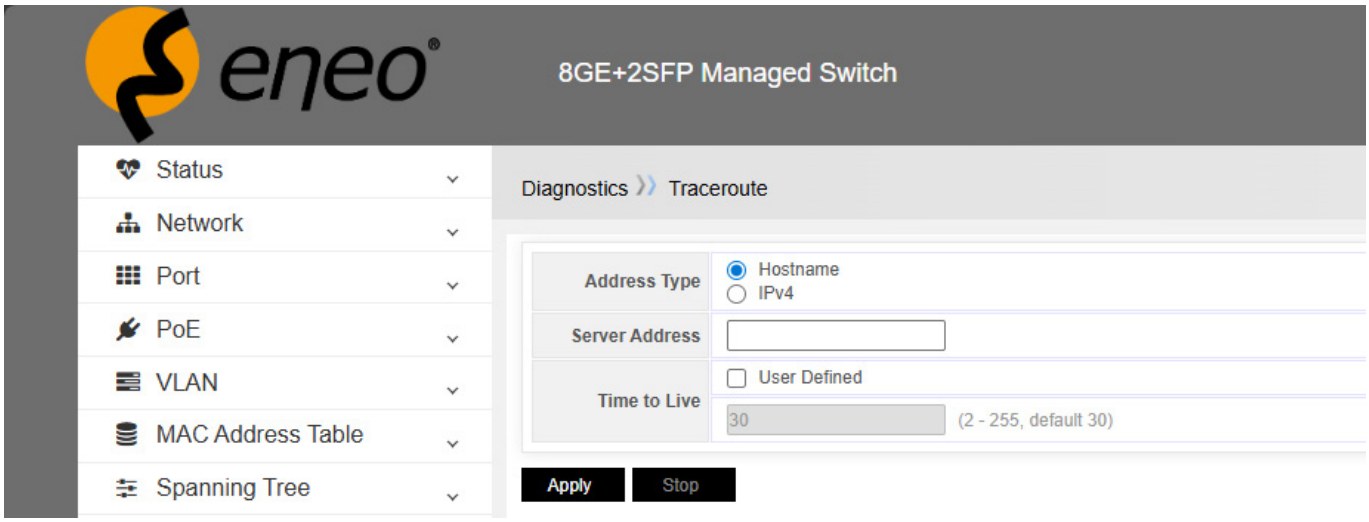
Packet lost: Compare the data of the sent and received messages to determine the percentage of lost messages.

12.4 – Traceroute

The traceroute command uses the ICMP protocol to locate all routers between the terminal device and the destination terminal device. The TTL value can reflect the number of routers or gateways that the data packet has passed through. By controlling the independent ICMP to retrieve the TTL value of messages and observe the discarded return information of this message, the traceroute command can traverse all routers on the packet transmission path.

This programme will increase the TTL value to perform its functions. The programme performs its function by increasing the TTL value. Each time a packet passes through a router, its lifetime is reduced by 1. When its lifetime is 0, the host terminates the packet and sends an ICMP TTL packet to the sender of the original packet.

The TTL values of the first three packets sent by the programme are 1, the next three are 2, and so on, so that the programme obtains a series of packet paths. Note that IP does not guarantee that each packet will take the same path.



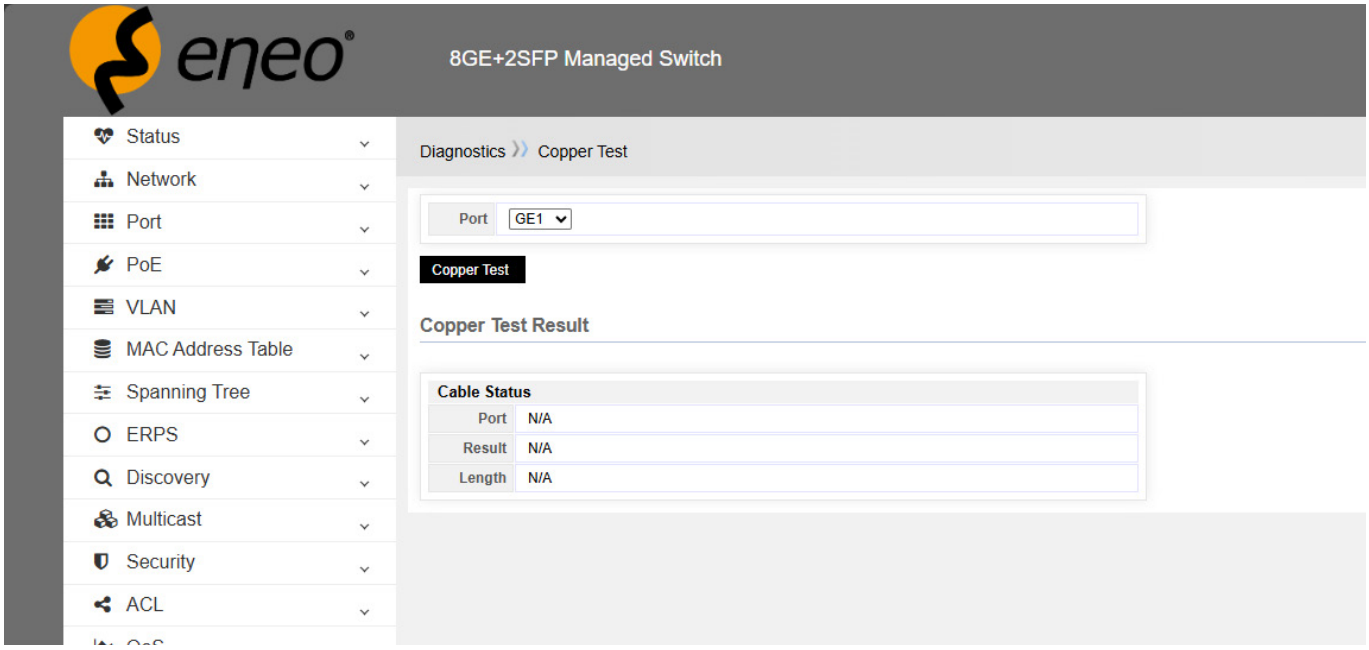
12.5 – Copper test

VCT is the abbreviation for Virtual Cable Test, a common feature in network communication devices.

VCT uses TDR (Time Domain Reflectometry) to detect the physical condition of network cables.

The principle of TDR detection is similar to that of radar. It works by sending a pulse signal through an active line and detecting the result of the reflection of the transmitted pulse signal to detect the cable fault. When the transmitted pulse signal passes through the end of the cable or the fault point of the cable, part or all of the pulse energy is reflected back to the original transmission source. VCT technology determines the time at which the signal arrives at or returns from the fault point, depending on its transmission status in the cable, and then converts the corresponding time into the distance value according to the formula. VCT can detect cable condition, fault distance, polarity reversal, insertion signal attenuation, return signal attenuation, etc

The user can use the VCT features to detect Ethernet connection cables and turn on the Ethernet cable detection system. Detection includes short circuits and interruptions in the receive and transmit directions of the cable, as well as the faulty position of the cable.



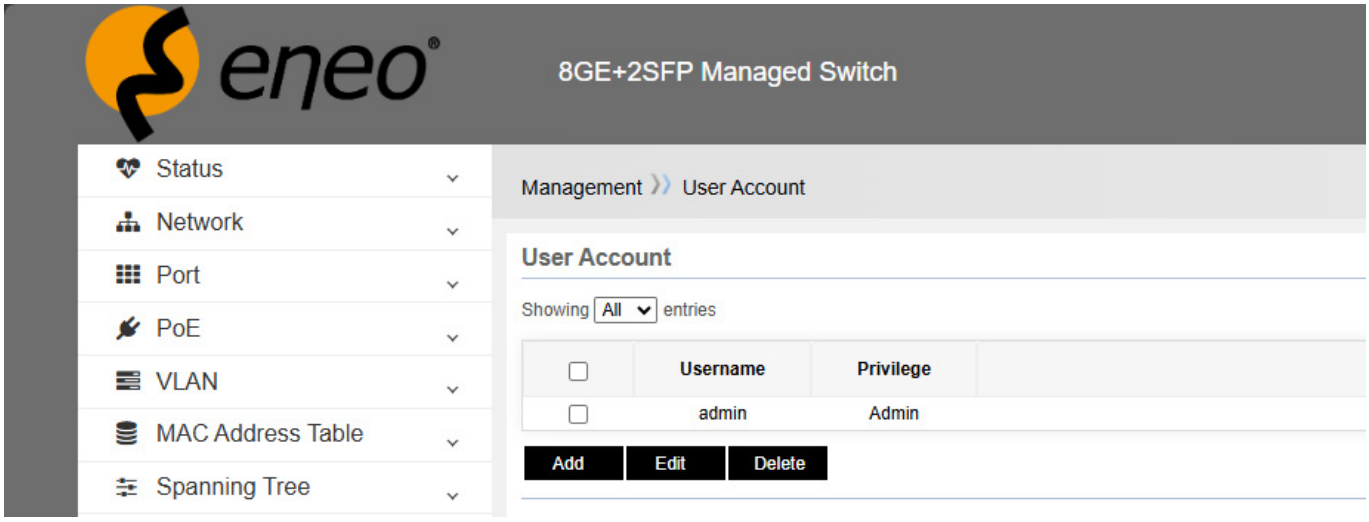
Select a port and click the 'Copper test' button.

If the network cable is disconnected, a test result will be displayed indicating the length, i.e. how many metres the cable is disconnected. The margin of error is approximately 1 metre, so this function can be used to check for network cable errors.

13 – MANAGEMENT

13.1 – User account

Click 'Add' to add a new user.



Enter the username and password and confirm the password.

There are two levels: Admin and User.

The administrator can manage all functions of the switch system.

The user can only manage some functions of the switch.

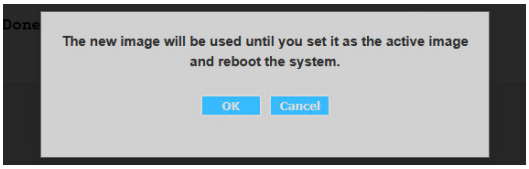
13.2 – Firmware

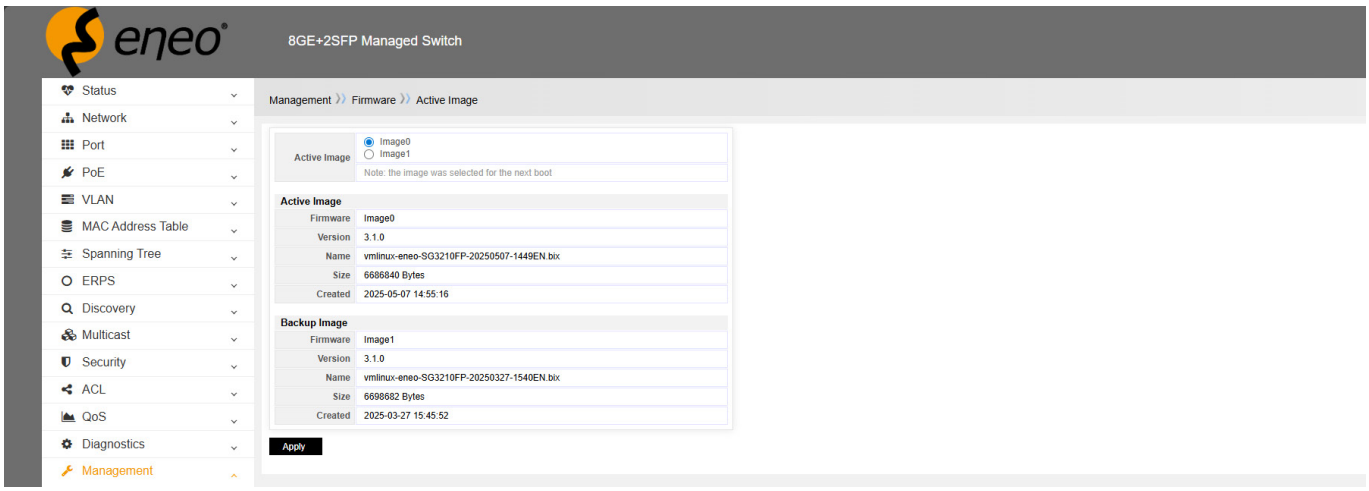
13.2.1 – Upgrade / Backup

The software system can be updated and backed up via TFTP or HTTP.

If you want to perform an update, select 'Upgrade' or "HTTP", then select the system update file and finally click on 'Apply'.

After the upgrade, the following information will be displayed. Click OK.





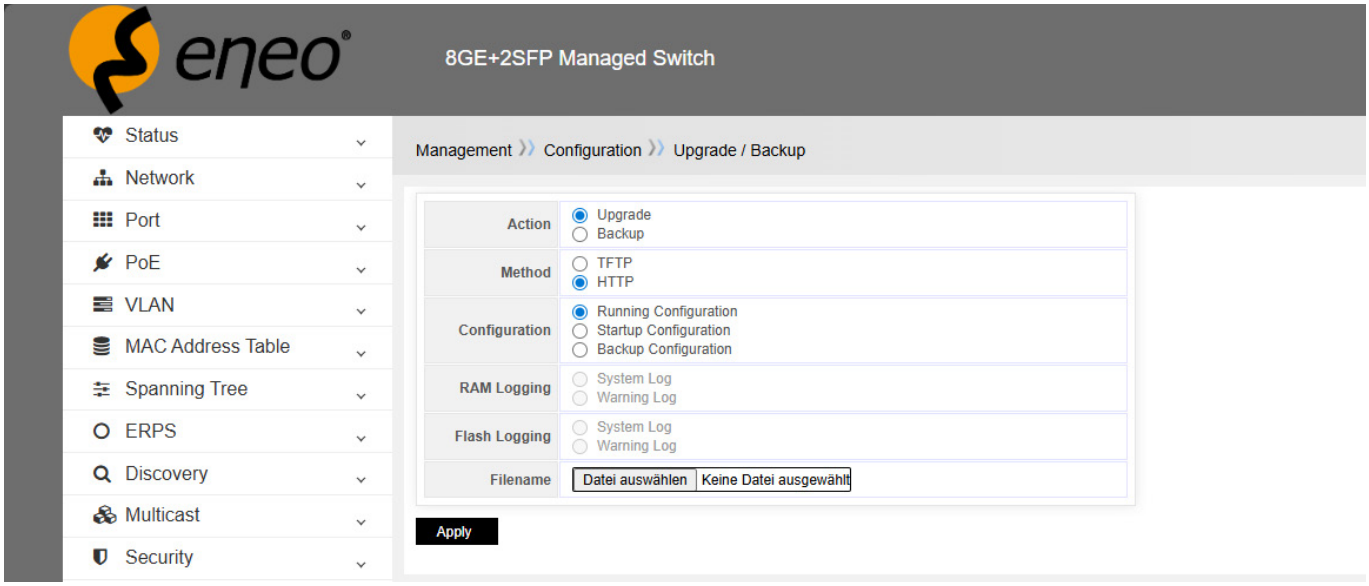
After the upgrade, you will notice that the upgrade file you just used corresponds to the updated Image1. Now select Image1 in the 'Active Image' option, click "Apply" to complete the upgrade, and finally click the 'Restart' button.

Note!

The switch is a dual IMG system. If Image1 is currently running, Image0 is updated. If Image0 is running, Image1 is updated.

13.3 – Configuration

13.3.1 – Upgrade / Backup / Factory settings



Action: Update/Backup

Update: Update parameters

Backup: Backup parameters

Method: TFTP/HTTP

Configuration

Current configuration: Parameters that the system executes

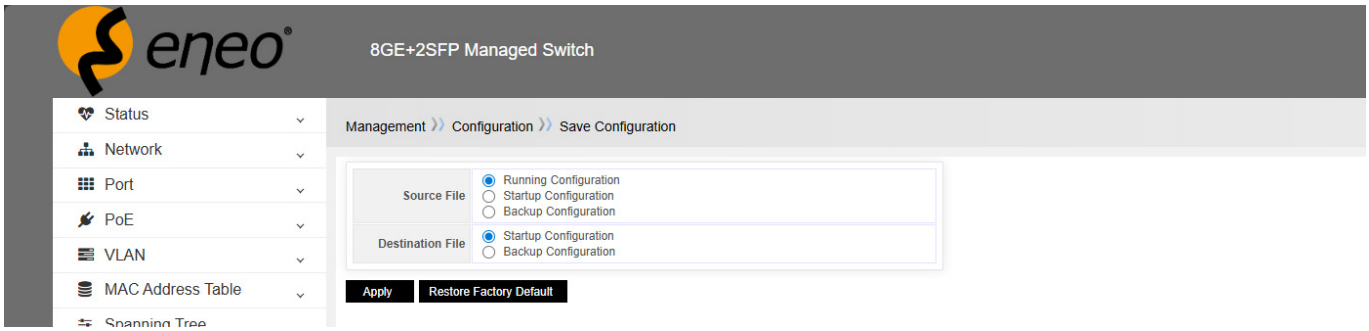
Start configuration: Parameters that are loaded when the system starts

Backup configuration: Parameters that have been backed up

Note!

When importing parameters, select the 'Start configuration' option.
Then click "Restart" to complete the import of the parameters.
When exporting parameters, select the 'Current configuration' option.

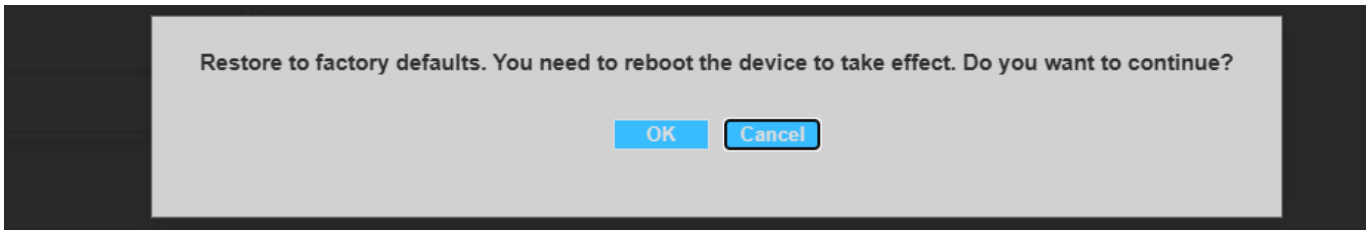
13.3.2 – Save configuration

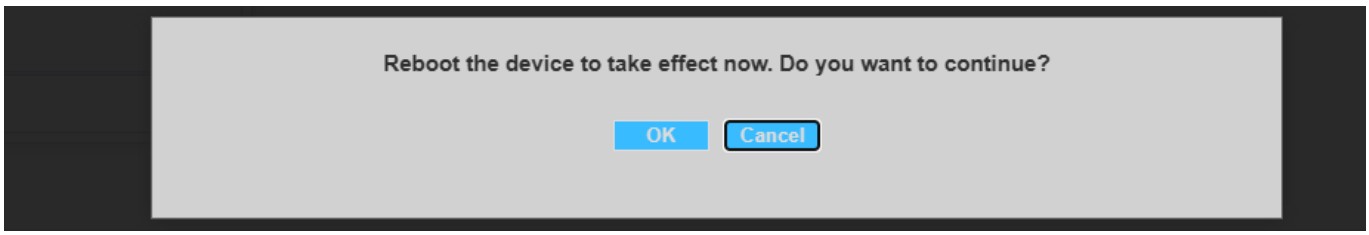


Copy the source file to the destination file to save the parameters.
The easiest way to do this is to click on the 'Save' button in the top right-hand corner.

Reset to factory settings

If you want to reset the device to the factory settings, click on 'Restore Factory Default' and follow the instructions.





To prevent this setting from being made accidentally, it must be confirmed twice.

To do this, click on 'OK' each time.

14 – FAQ

14.1 – Connection status display malfunction (connection error)

Check whether the connection end is connected to the PC network card or another Ethernet interface.

Check whether the connection access point is rusty or damaged.

Check the configuration of this port (duplex and speed) via the WEB and ensure that the configuration matches that of the other end of the connection.

Note!

If duplex and speed are fixed for this port, the configuration of one connection must match that of the other, otherwise no connection can be established.

14.2 – Normal connection status display, but no communication

Check the web page to see if the port is stopped (enter 'Port Configuration'). If the port is stopped, please activate it.

Check the web page to see if the port is isolated by VLAN. For comparison with other ports: Only if the port is set to 'Access' in the same VLAN can they communicate with each other.

14.3 – Login to the switch not possible

Check whether the switch is switched on.

If the connection fails, check the switch's response with 'Ping'. If there is no response, check the IP address configuration of the PC and the switch. Determine the cause of the problem based on the HTTP connection feedback.

Check the IP address settings

1. Check that the IP address and subnet mask of the PC are set correctly. Enter 'ipconfig' in the command line window and press the Enter key to check the IP address configuration of the PC.
2. Check that the IP address, subnet mask and default gateway of the switch are set correctly.
3. Check that the IP address of the switch is not already in use by other devices.

Check the login account

If the switch continuously prompts the user to enter their account and password when logging into WEB, this may mean that this account does not exist or that this password is invalid.

14.4 – Switch does not start

1. Check whether the serial interface number is incorrect; this is usually COM1 or COM2.
2. Ensure that the software is configured as follows: 115200 bps, 8 data bits, 1 stop bit, no parity check and no flow control.
3. Check whether the PC's serial interface is working properly: You can use the mouse to check whether the serial interface is working.
4. Make sure that no other program is using this serial port: In Windows, a serial port cannot be used by multiple programs at the same time.

14.5 – Power failure

Check the power indicator. If the indicator is not lit, the power connection may be damaged. Make sure that the power supply is normal and check that the connection between the switch and its power supply is stable and reliable.

Version: 07 / 2025

VIDEOR E. Hartig GmbH | Carl-Zeiss-Straße 8 | 63322 Rödermark | Germany | Tel. +49.6074.888-0 | Fax +49.6074.888-100 |
Amtsgericht Offenbach am Main | HRB 32047 | UIN DE 113592980 |
Geschäftsführer / Managing Directors: Lars Hagenlocher, Dominik Mizdrak

www.eneo-security.com | info@eneo-security.com