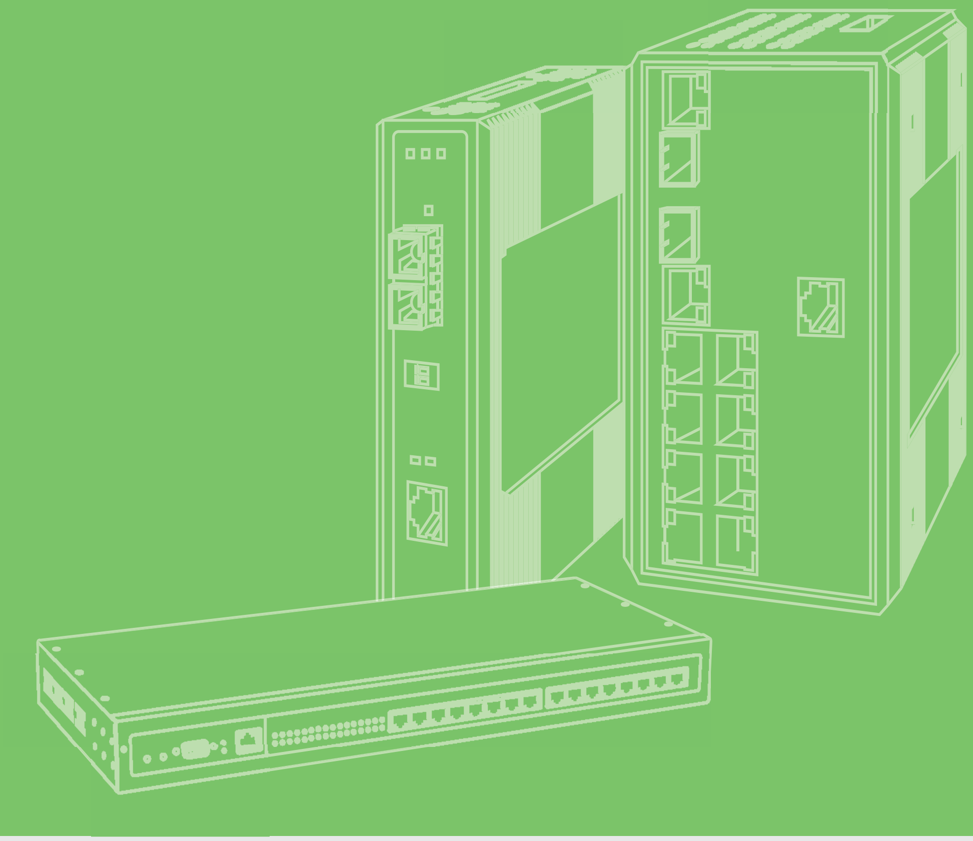
User Manual



EKI-9512 ETBN Series

Ethernet Train Backbone Node Management Guide

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Edition 1

Printed in Taiwan May 2022

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Contents

List of Figures

Chapter 1

Introduction to ETBN

1.1 IEC-61375-2-5 TTDP (Train Topology Discovery Protocol)

1.1.1 TTDP introduction

Train Topology Discovery Protocol (TTDP) is designed for train dispatch. When the train cars configuration is changed, the IP address of the Ethernet switches in the train cars is also re-configured. An ETBN (Ethernet Train Backbone Network) switch with TTDP function re-configures the IP address and Gateway IP if the train network topology changes due to the new train car configuration.

At the core of the communication technology geared towards highspeed trains is the IEC-61375-2-5 Ethernet based control system. The IEC-61375-2-5 standard is released by the International Electrotechnical Commission (IEC) and defines the ETB for Ethernet technology to proceed on train network applications.

TTDP only manages all nodes on ETB - ETBN and the local area networks in the train group, ECN (Ethernet Consist Network). According to the detected ETBNs and ECNs, TTDP can actively build the train topology.

The following diagram and corresponding abbreviations provide an overview of the TTDP introduction.

- CstUUID: Consist Universal Unique ID
- Dir1: consist reference direction
- Dir2: opposite direction
- Position: define its own position/identity in the consist.
- CNID: number of Subnet in the consist.
- ETBID: Backbone ID, ETB0 (for TCMS) or ETB1 (for Multimedia)

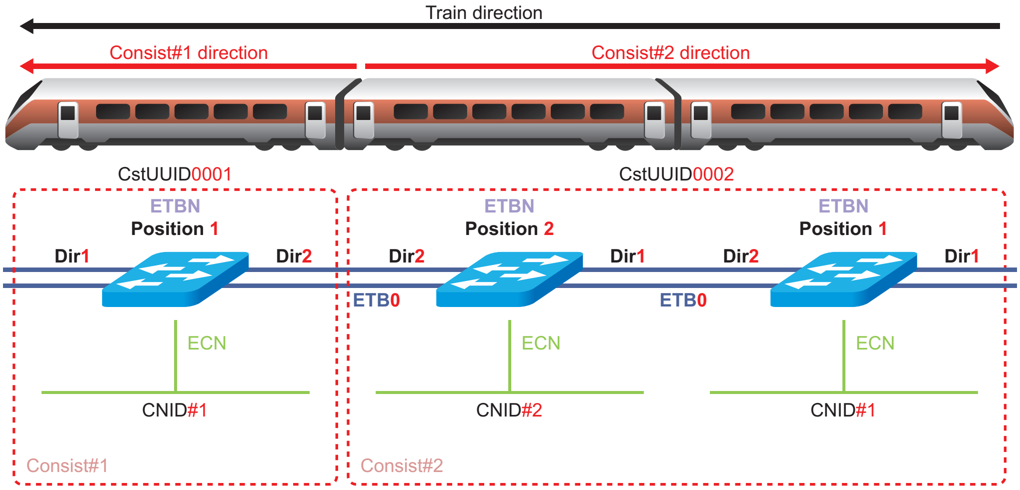


Figure 1.1 TTDP Introduction

TTDP provides the following application services on an ETBN router:

- Dynamic IP Addressing (R-NAT / Absolute)
- Routing (between different consist networks)
- ETBN Redundancy

1.1.2 Dynamic IP Addressing

TTDP configure the train car order (topology) after the ETB initiation (starting from the smallest CstUUID), and calculates the train network directory table, which contains the ETBN ID and CN subnet ID. The IP address is dynamically assigned to the ETBN router and each ED under ECN based on the ETBN ID and CN subnet ID.

The EKI-9512-ETB series is equipped with TTDP function supporting two IP assignment modes: Absolute / R-NAT (IEC-61375-3-4).

1.1.2.1 Absolute Mode

When Absolute mode is selected for IP allocation, the ETBN IP and CN subnet IP addressing is automatically configured if the train topology order changes.

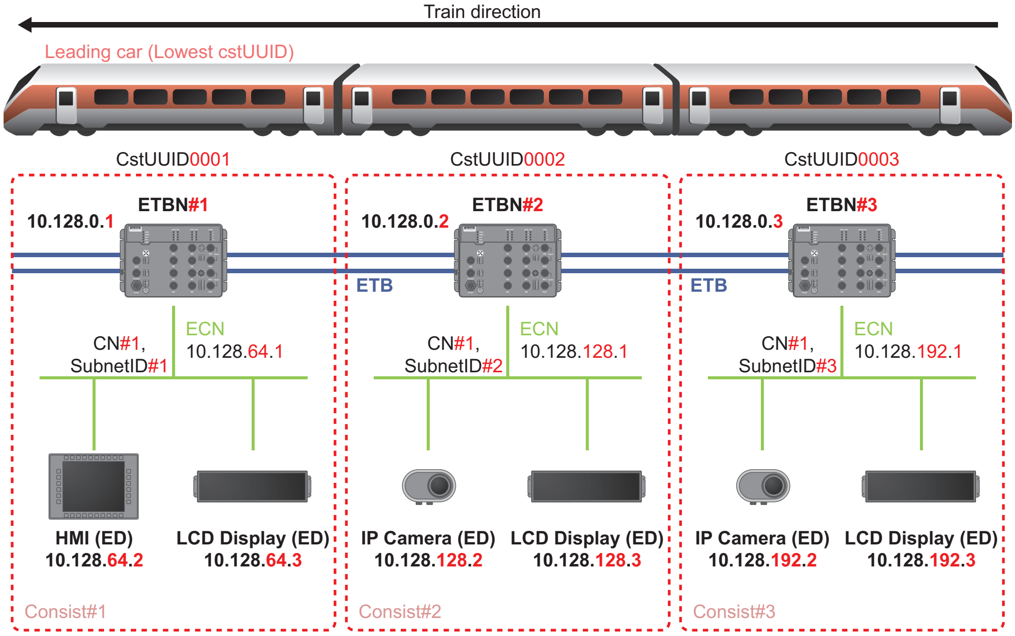


Figure 1.2 TTDP IP Addressing in Absolute Mode

1.1.2.2 R-NAT mode

TTDP supports R-NAT mode for train IP management. R-NAT is an algorithm for network address translation between ETB and ECN. R-NAT uses the rules for train and Consist network addresses, and in the process, simplifying address translation management.

As an example, R-NAT supports end devices (EDs) in different cars to use a duplicate IP address. For this reason, it is not necessary to reconfigure EDs when the order of train cars change. The address translation of CN subnet IPs in different

Consist addresses use the same range, for instance: 10.0.0.X/32 while communication takes place through NAT table (SIP and DIP replacement).

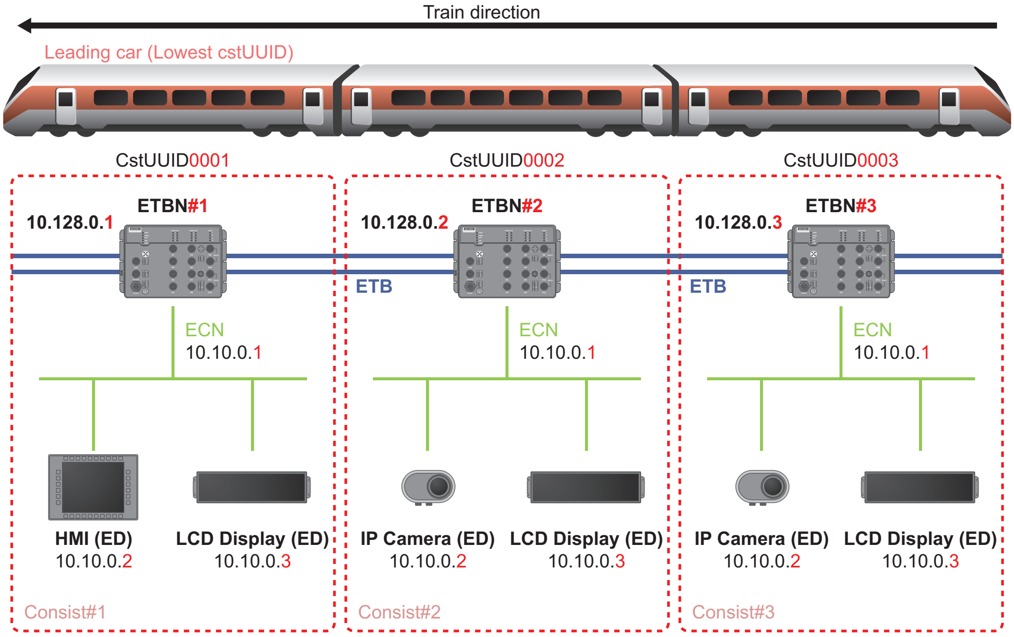
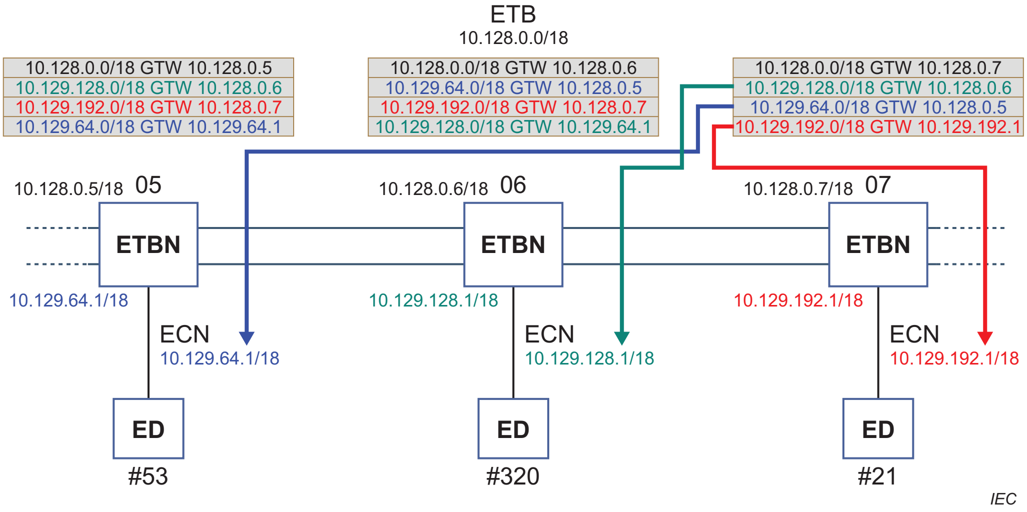


Figure 1.3 TTDP IP Addressing in R-NAT Mode

1.1.3 Routing

Once translation of ETBN IP and CN subnet IPs, an ETBN router defines a routing table to allow devices between to communicate. By establishing a communication route, traffic between ETBN and ECN can be managed effectively.



ETB
10.128.0.0/18
10.128.0.0/18 GTW 10.128.0.5
10.129.128.0/18 GTW 10.128.0.6
10.129.192.0/18 GTW 10.128.0.7
10.129.64.0/18 GTW 10.129.64.1
10.128.0.0/18 GTW 10.128.0.6
10.129.64.0/18 GTW 10.128.0.5
10.129.192.0/18 GTW 10.128.0.7
10.129.128.0/18 GTW 10.129.64.1
10.128.0.0/18 GTW 10.128.0.7
10.129.128.0/18 GTW 10.128.0.6
10.129.64.0/18 GTW 10.128.0.5
10.129.192.0/18 GTW 10.129.192.1
10.128.0.5/18 05
10.128.0.6/18 06
10.128.0.7/18 07
ETBN
ETBN
ETBN
10.129.64.1/18
10.129.128.1/18
10.129.192.1/18
ECN
10.129.64.1/18
ECN
10.129.128.1/18
ECN
10.129.192.1/18
ED
#53
ED
#320
ED
#21
IEC

Figure 1.4 TTDP ETBN and ECN Routing

In R-NAT mode, ETBN routers define synchronous 1-1 S-NAT and D-NAT tables for the assigned CN subnet IPs.

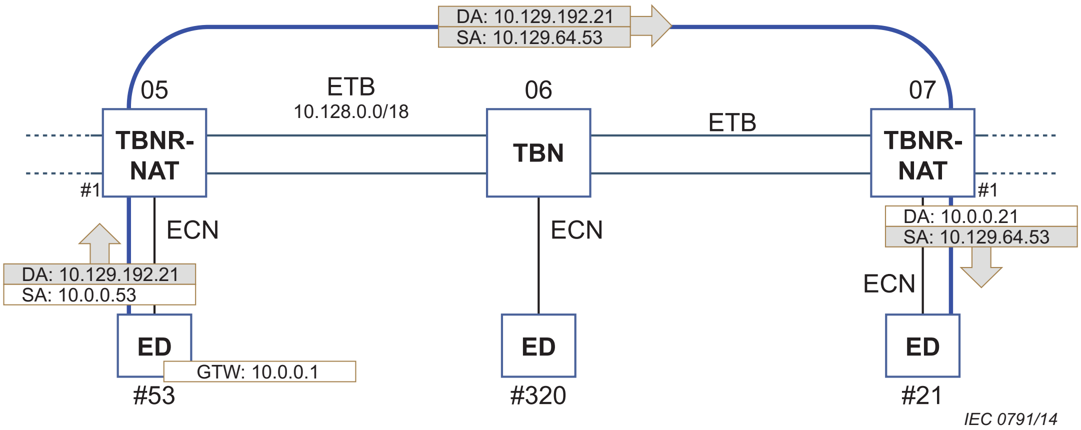


Figure 1.5 Defined 1-1 S-NAT and D-NAT Assignment

1.1.4 ETBN Redundancy

TTDP provides a virtual IP address backup mechanism for ETBNs within the same Consist. When ECNs are connected to more than two ETBNs, TTDP promotes the virtual IP address to activate (master) ETBN router, while ECN is uses the virtual IP address to transmit information between ETBN and ECN.

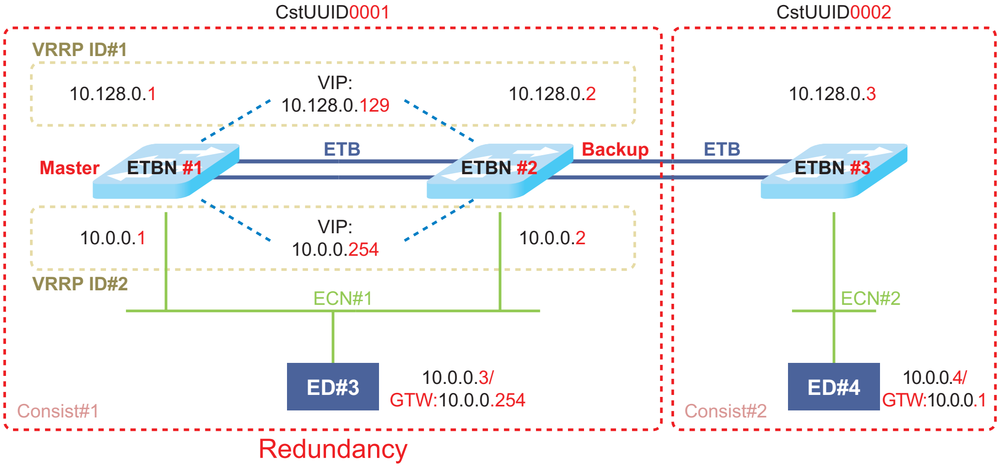


Figure 1.6 ETBN Redundancy

EKI-9512-ETB series supports virtual router redundancy protocol (VRRP) which provides automatic assignment of available IP routers. Given that the assignment mechanism for ETBN master/backup roles in redundancy is not clearly defined in the IEC-61375-2-5 standard, the EKI-9512-ETBN series achieves ETBN redundancy through the use of the VRRP networking protocol.

1.2 1.2IEC-61375-2-3 TRDP

1.2.1 TRDP Introduction

With the advent of high speed railway trains, control systems have been relegated to computer-based controllers. IEC-61375-2-3 standard defines the Ethernet Train Backbone (ETB) for Ethernet technology for use on train networking applications. It supports TRDP for such applications, improving operational efficiency, real-time transmission reliability, and mitigating configuration difficulties.

While TRDP mainly provides data exchange between EDs through the TCP/UDP transport layer, the exchange of data is accomplished based on stored configured information. The primary key for the configuration data is the communication identify, *ComID*. See the following TRDP Header for further information:

ComID	Description
100	TTDB—operational train directory status telegram
101	TTDB—operational train directory notification
102	TTDB—train directory information request
103	TTDB—train directory information reply
104	TTDB—consist information request
105	TTDB—consist information reply
106	TTDB—train network directory information request
107	TTDB—train network directory information reply
108	TTDB—operational train directory information request
109	TTDB—operational train directory information reply
110	TTDB—train information complete request
111	TTDB—train information complete reply

In the TRDP Header, the *MessageType* field includes the defined TRDP communication mode for the ED device, for example:

- PD = Process Data
- MD = Message Data

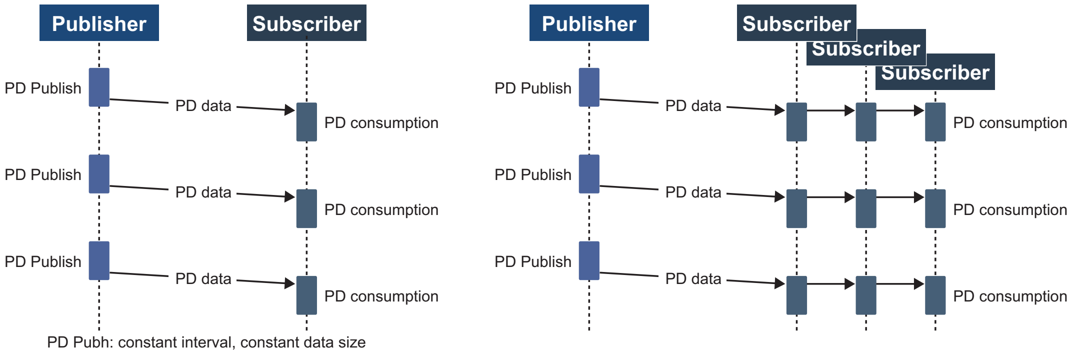


Figure 1.7 Communication Pattern (PD)

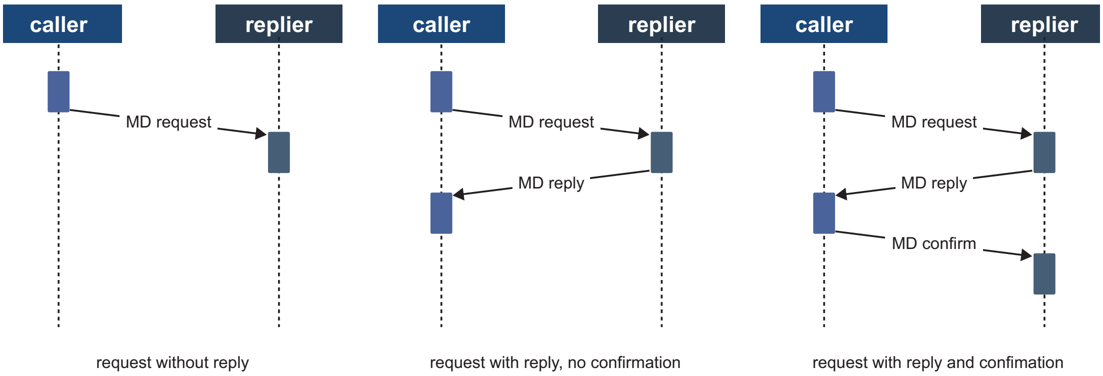


Figure 1.8 Communication Pattern (MD)

1.3 ETB Service interface diagram

The EKI-9512-ETB series supports the following Service Interfaces and ED-related topology information:

- TTDB: Train Topology Data Base
- TTDBM: TTDB Management Interface
- ECSP: ETB Control Server Provider
- ETBN: ETBN Service Interface

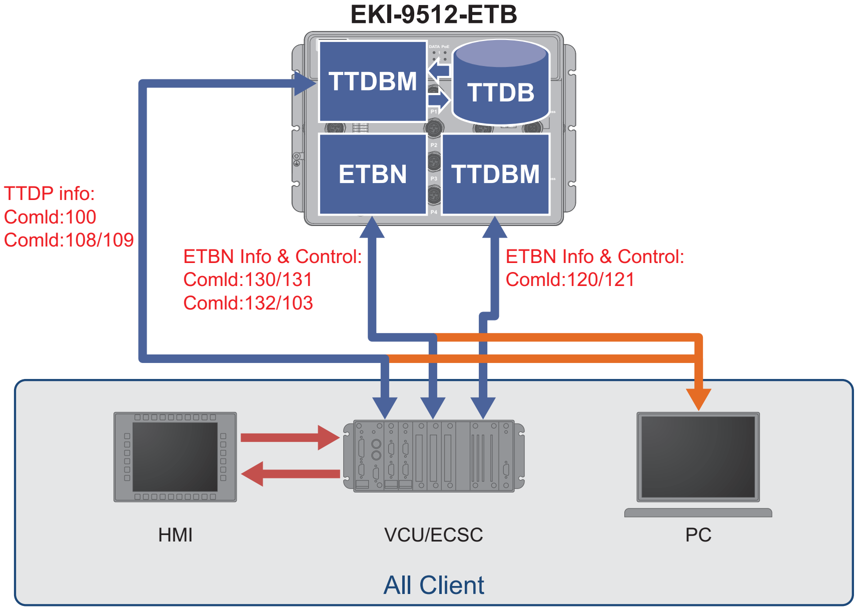


Figure 1.9 Communication Pattern (MD)

1.3.1 EKI-9512-ETB Service support list based on TRDP

Based on TRDP protocol, the EKI-9512-ETB series supports the following services:

1. ECSP control

ComID	MessageType	Role	Description
108	Mr	Listener	Operational train directory information
109	Mp	Replier	Operational train directory information
120	Pd	Subscriber	ECSP control telegram
121	Pd	Publisher	ECSP status telegram

Note! *Currently only inhibition and leading request are supported.*

2. ETBN control

ComID	MessageType	Role	Description
130	Mr	Listener	ETBN control and status data
131	Mp	Replier	ETBN control and status data

Note! *Currently only inhibition request control is supported.*

3. TTDB information provider

ComID	MessageType	Role	Description
100	Pd	Publisher	TTDB status information
102	Mr	Listener	TTDB information - train directory
103	Mp	Replier	TTDB information - train directory

4. ETBN information provider

ComID	MessageType	Role	Description
132	Mr	Listener	ETBN train network directory
133	Mp	Replier	ETBN train network directory

5. TCN-DNS resolution (optional)

ComID	MessageType	Role	Description
140	Mr	Listener	DNS resolving request message
141	Mp	Replier	DNS resolving request message

Note! *Currently only TCN-DNS request control is supported.*

1.4 How to Use this Document

This management guide is structured as follows:

1.5 Legal Information

Chapter 2

Configuration Guide

2.1 Topology Configuration for TTDP

2.1.1 Topology View

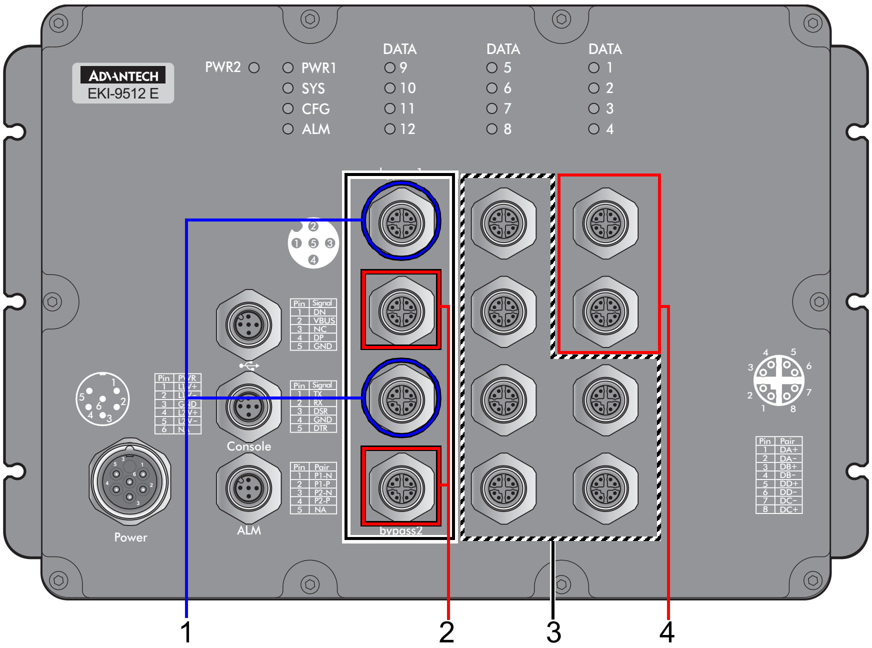


Figure 2.1 Default Topology View

No.	Description
1	LAG1 (P9, P11) for ETBN Direction 1
2	LAG2 (P10, P12) for ETBN Direction 2
3	P3-P8 for CN Subnet
4	P1-P2 (Default) VLAN Access to Device Via HTTP/Telnet

Note!

1). P9-10, P11-P12 support bypass relay function, when the device is powered off, ETBN can bypass the inactive device to ensure smooth network ETBN connection.

2). Once TTDP related settings are completed, launch begins.

3). After TTDP related settings are saved, operations is automatically initiated after system power up, see “TTDP Configuration Guide” on page 13.

5. After initial TTDP power up is completed, a TRDP ComID PD 100 packet is sent to the CN subnet, see “TTDP Configuration Guide” on page 13

(Refer to 2.2 TRDP Forwarding Introduction)

2.1.2 TTDP Configuration Guide

2.1.2.1 Overview of Management Methods

ETBN provides management and monitoring access through the following tools and interfaces:

Web: The ETBN Web interface provides management of all features. Through the use of the interface all common use cases can be easily managed.

CLI: The ETBN Line Interface is an industry standard CLI, providing at complete management support. Intended for advanced users, the CLI interface provides control for users requiring greater control.

Telnet: The ETBN application protocol is an industry standard bidirectional interactive virtual terminal connection intended for advanced users. The interface provides control for users requiring greater control.

2.1.2.2 Using the Web Interface

The ETBN Web interface is easily accessible for all users. The advantages of using the Web interface are as follows:

- Easy to use: The interface provides an easy to use method for managing all functionality.
- All common features: The interface provides access to all of the essential and available management features.
- Secure: The interface is a secure management method that can be easily accessed via regular HTTP and secure HTTP (HTTPS).

To access the Web interface, first enter the corresponding IP address in the IP address field of a browser. For further information about using the Web Interface see “Management & Configuration” on page 30.

2.1.2.3 Using Command Line Interface or Telnet

The ETBN CLI/Telnet are management methods aimed at advanced users looking for greater control. The following is a list of possible situation for the use of a CLI/Telnet interface:

- Comprehensive management feature set: The CLI interface provides all available management features in a switch device. Certain tasks not available with other management tools can be accessed through the use of the CLI interface.
- Secure management: Access to the CLI interface requires either a physical access to a switch device or the use of the Secure Shell (SSHv2) application for remote access to the CLI.
- Scripting: With a CLI/Telnet interface, automated configuration scripts can be developed.

2.1.2.4 TTDP Network Topology Configuration

The following is a TTDP network topology configuration example.

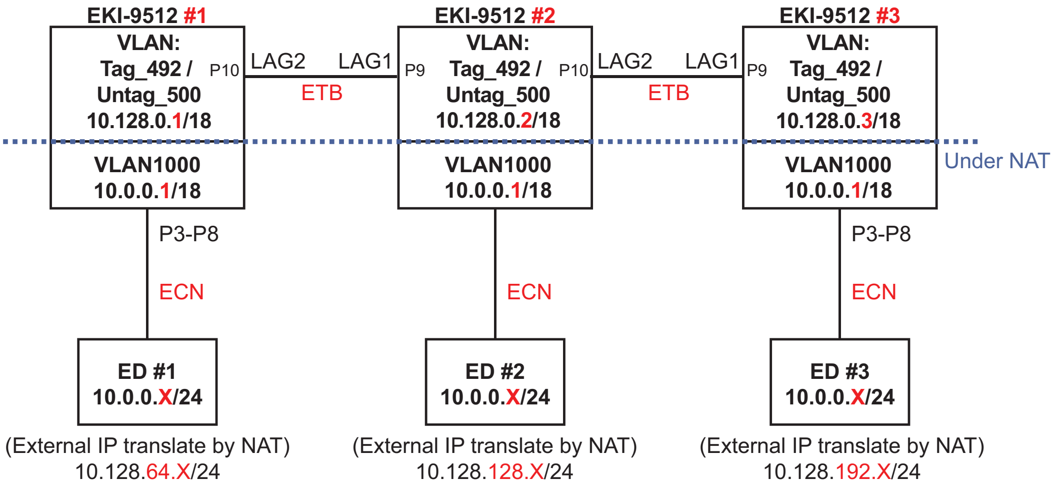


Figure 2.2 Default Topology View

No.	Description
1	LAG1 (P9, P11) for ETBN Direction 1
2	LAG2 (P10, P12) for ETBN Direction 2
3	P3-P8 for CN Subnet
4	P1-P2 (Default) VLAN Access to Device Via HTTP/Telnet

2.1.2.5 2.1.2.2TTDP CLI

The following section provides an example for configuring settings through a CLI interface.

1. Step1: Logging into CLI via Console / Telnet:

   I. Login via Telnet:

   – Telnet to IP: 192.168.1.1.

   – Enter the account and password: *admin/admin* to log in to the system.

   II. Console login:

   III. Login to console via terminal, baud rate: 115200.

   – Enter the account and password: *admin/admin* to log in to the system.

2. Step 2: Set Topology through CLI.
   See“Topology View” on page 13 for further details.
   EKI-9512 #1, 2, 3 are mirrored

```
configure
vlan 492
exit
vlan 500
exit

interface range GigabitEthernet 9-12
switchport hybrid allowed vlan remove 1
switchport hybrid allowed vlan add 492 tagged
switchport hybrid allowed vlan add 500 untagged
switchport hybrid pvid 500
exit
```

```
interface range LAG 1,2
switchport hybrid allowed vlan remove 1
switchport hybrid allowed vlan add 492 tagged
switchport hybrid allowed vlan add 500 untagged
switchport hybrid pvid 500
exit
vlan 1000
exit

interface range GigabitEthernet 3-8
switchport hybrid allowed vlan remove 1
switchport hybrid allowed vlan add 1000 untagged
switchport hybrid pvid 1000
exit

interface range GigabitEthernet 9,11
lag 1 mode static
exit

interface range GigabitEthernet 10,12
lag 2 mode static
exit

interface vlan 1000
ip address 10.0.0.254 mask 255.255.192.0
exit

lldp
end

interface range GigabitEthernet 1-2
lag 1 mode active
exit

interface range GigabitEthernet 3-4
lag 2 mode active
exit

interface vlan 1000
ip address 10.0.0.254 mask 255.255.192.0
exit

lldp
end
```

3. Step 3: Configure TTDP through a CLI interface.
   See“TTDP Network Topology Configuration” on page 15 for further details.

EKI-9512 #1

```
configure
ttdp
ttdp debug database
etb 0 cstuuid 30:26:ce:de:c9:e8:11:e3:9d:46:1a:51:49:32:ac:01
etb 0 cst-etbn-num 1
etb 0 position 1
etb 0 dir1 ports GigabitEthernet 9,11 vlan 500 lag 1
etb 0 dir2 ports GigabitEthernet 10,12 vlan 500 lag 2
etb 0 role not-redundant
etb 0 address-plan r-nat
etb 0 cst-cn-num 1
etb 0 cn cn-id 1 ports GigabitEthernet 3-8 vlan 1000
etb 0 state active
end
```

EKI-9512 #2

```
configure
ttdp
ttdp debug database
etb 0 cstuuid 30:26:ce:de:c9:e8:11:e3:9d:46:1a:51:49:32:ac:02
etb 0 cst-etbn-num 1
etb 0 position 1
etb 0 dir1 ports GigabitEthernet 9,11 vlan 500 lag 1
etb 0 dir2 ports GigabitEthernet 10,12 vlan 500 lag 2
etb 0 role not-redundant
etb 0 address-plan r-nat
etb 0 cst-cn-num 1
etb 0 cn cn-id 1 ports GigabitEthernet 3-8 vlan 1000
etb 0 state active
end
```

EKI-9512 #3

```
configure
ttdp
ttdp debug database
etb 0 cstuuid 30:26:ce:de:c9:e8:11:e3:9d:46:1a:51:49:32:ac:03
etb 0 cst-etbn-num 1
etb 0 position 1
etb 0 dir1 ports GigabitEthernet 9,11 vlan 500 lag 1
etb 0 dir2 ports GigabitEthernet 10,12 vlan 500 lag 2
etb 0 role not-redundant
etb 0 address-plan r-nat
etb 0 cst-cn-num 1
etb 0 cn cn-id 1 ports GigabitEthernet 3-8 vlan 1000
etb 0 state active
end
```

2.1.2.6 2.1.2.3TTDP WEB UI

1. Step1: Log in the Web Interface via a browser:

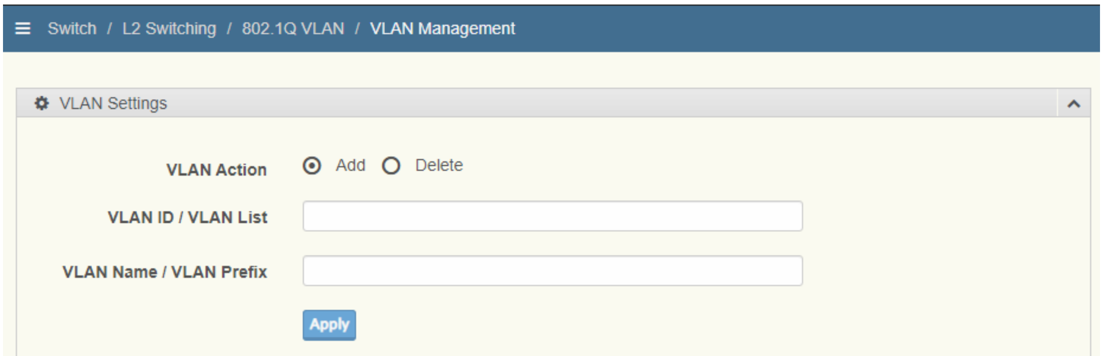
   I. In the IP address field, enter the IP address 192.168.1.1.

   II. Enter the account and password: *admin/admin* to log in to the system.

2. Step2: Configure network settings through the interface.
   See “Topology View” on page 13 for further details.
   To access this page, click **L2 Switching** > **802.1Q VLAN** > **VLAN Management** to create VLAN492, VLAN500, and VLAN1000.

   I. In the VLAN ID / VLAN field enter the VLAN to be created

   II. Click **Apply**.



☰ Switch / L2 Switching / 802.1Q VLAN / VLAN Management

VLAN Settings

VLAN Action ● Add ○ Delete

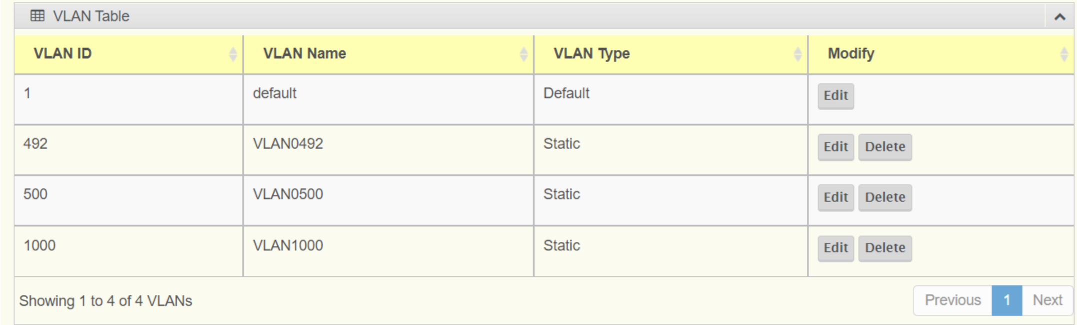
VLAN ID / VLAN List

VLAN Name / VLAN Prefix

Apply

Figure 2.3 L2 Switching > 802.1Q VLAN > VLAN Management

Available interfaces are displayed in the VLAN table as seen in the following figure.



VLAN Table

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit
492	VLAN0492	Static	Edit Delete
500	VLAN0500	Static	Edit Delete
1000	VLAN1000	Static	Edit Delete

Showing 1 to 4 of 4 VLANs

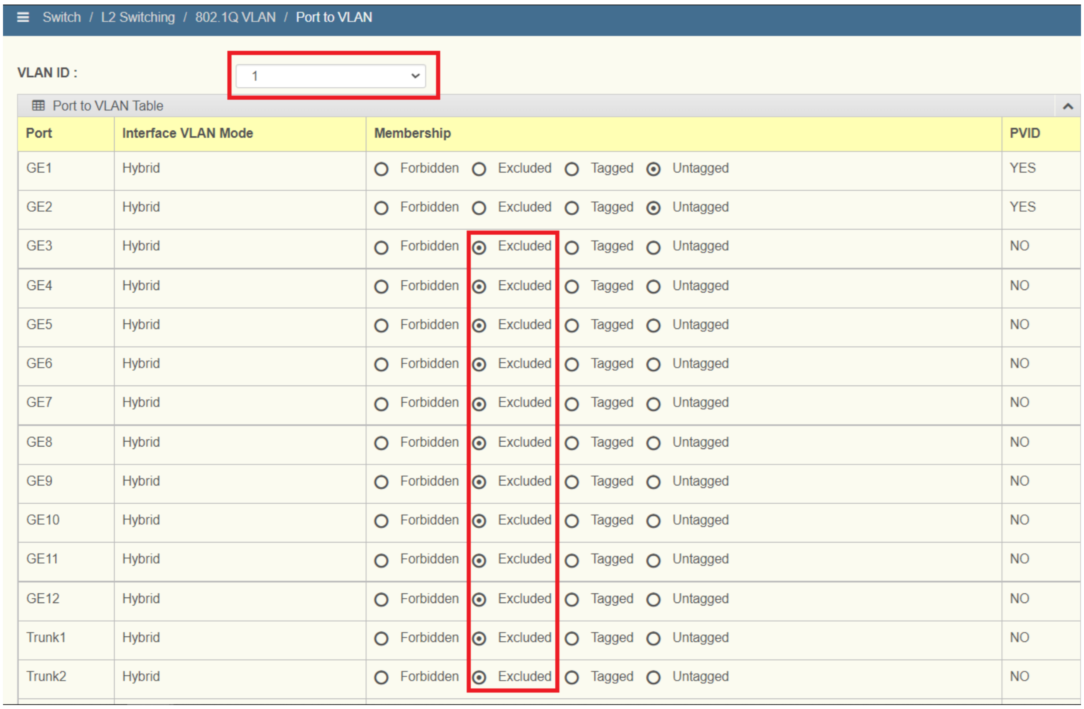
Previous 1 Next

Figure 2.4 VLAN Listing Pool

To remove a port from a VLAN see the following. For this example VLAN 1 is selected.

III. Click the VLAN ID drop-down menu to select a listing.

IV. Click the **Exclude** radio button to remove any ports from the listing. For this step GE3 to GE12, LAG1, and LAG2 are excluded.
Click **Apply** to save the updated setting.



VLAN ID : 1

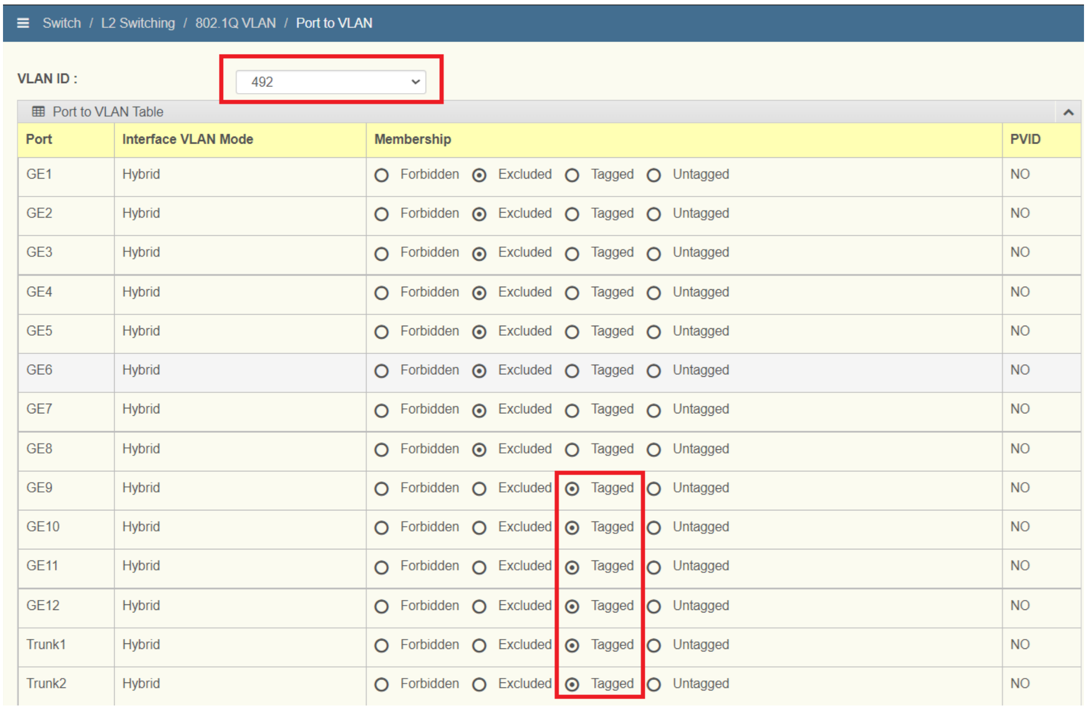
Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE3	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE4	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE5	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE6	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE7	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE8	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE9	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE10	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE11	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE12	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO

Figure 2.5 Excluding Ports from VLAN Membership

To add DIR1 and DIR2 interfaces to VLAN selection see the following. For this example, VLAN 492 is selected.

V. Click the VLAN ID drop-down menu to select a listing.

VI. Click the **Tagged** radio button to include any ports to the listing.
For this step GE3 to GE12, LAG1, and LAG2 are added.
Click **Apply** to save the updated setting.



VLAN ID : 492

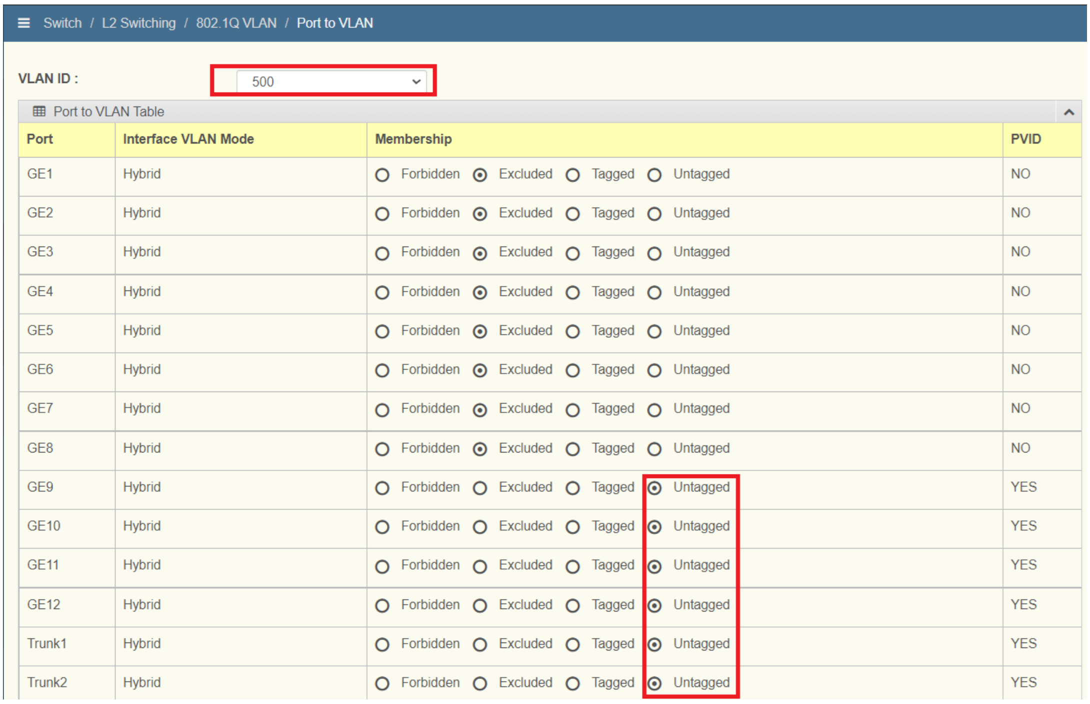
Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE3	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE4	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE5	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE6	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE7	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE8	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE9	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO
GE10	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO
GE11	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO
GE12	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO
Trunk1	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO
Trunk2	Hybrid	○ Forbidden ○ Excluded ● Tagged ○ Untagged	NO

Figure 2.6 Tagging Ports to VLAN Membership

To untag DIR1 and DIR2 interfaces from a VLAN see the following. For this example VLAN 500 is selected.

VII. Click the VLAN ID drop-down menu to select a listing.

VIII. Click the **Tagged** radio button to exclude any ports from the listing. For this step GE3 to GE12, LAG1, and LAG2 are untagged.
Click **Apply** to save the updated setting.



≡ Switch / L2 Switching / 802.1Q VLAN / Port to VLAN

VLAN ID : 500

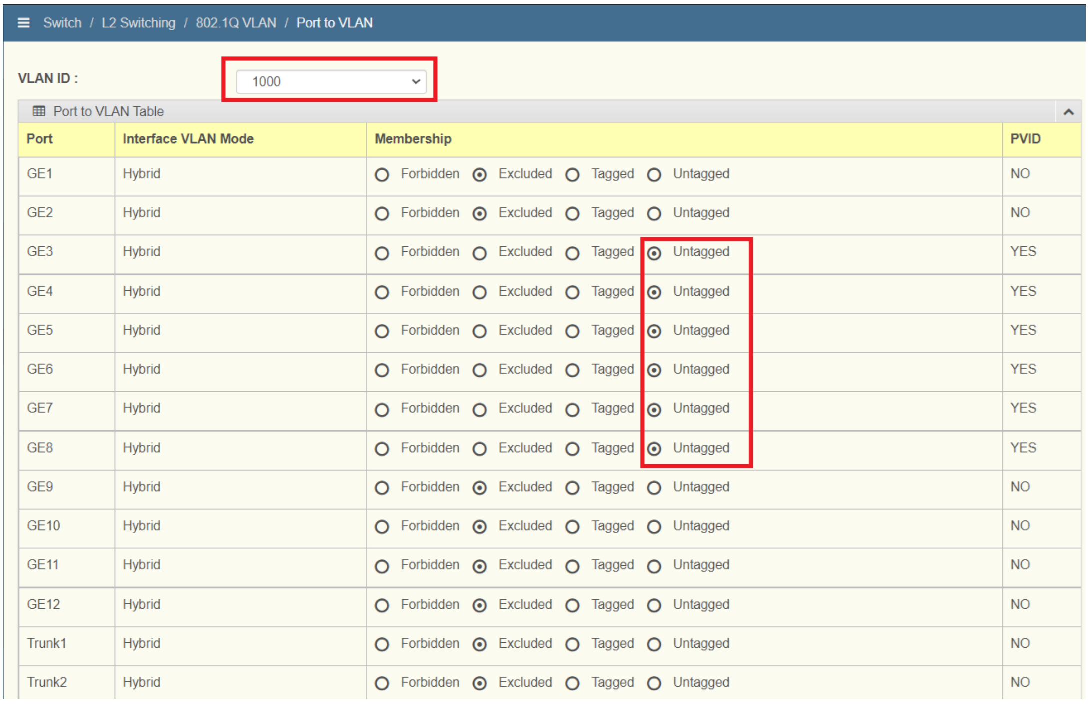
Port to VLAN Table

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE3	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE4	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE5	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE6	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE7	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE8	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE9	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE10	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE11	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE12	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
Trunk1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
Trunk2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES

Figure 2.7 Untagging Ports from VLAN Membership

IX. Click the VLAN ID drop-down menu to select a VLAN ID 1000, see the following figure.

X. Click the **Tagged** radio button to exclude the following ports: GE3 to GE8.
Click **Apply** to save the updated setting.



≡ Switch / L2 Switching / 802.1Q VLAN / Port to VLAN

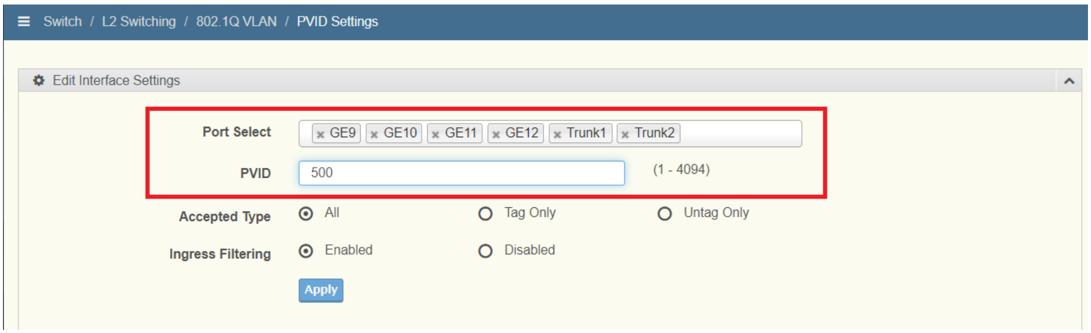
VLAN ID : 1000

Port to VLAN Table

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE3	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE5	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE6	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE7	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE8	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE9	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE10	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE11	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE12	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO

Figure 2.8 Untagging Ports from VLAN Membership

XI. Modify the PVID of the ports from GE3 to GE12, LAG1, and LAG2 to 500, see the following figure.
Click **Apply** to save the updated setting.



☰ Switch / L2 Switching / 802.1Q VLAN / PVID Settings

Edit Interface Settings

Port Select: × GE9 × GE10 × GE11 × GE12 × Trunk1 × Trunk2

PVID: 500 (1 - 4094)

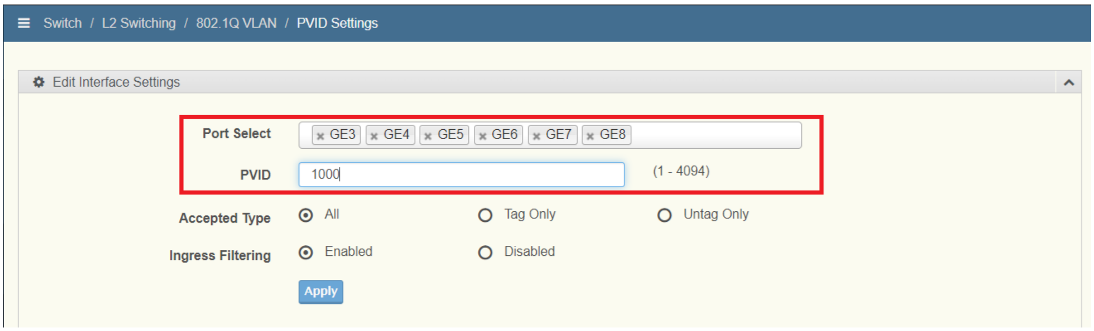
Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enabled ○ Disabled

Apply

Figure 2.9 Modifying Port PVID

XII. Modify the PVID of the GE3 to GE8 ports to 1000, see the following figure.
Click **Apply** to save the updated setting.



☰ Switch / L2 Switching / 802.1Q VLAN / PVID Settings

Edit Interface Settings

Port Select: × GE3 × GE4 × GE5 × GE6 × GE7 × GE8

PVID: 1000 (1 - 4094)

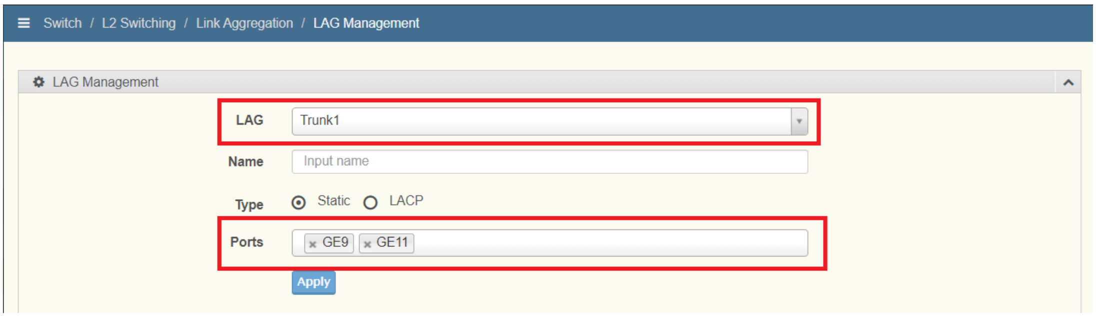
Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enabled ○ Disabled

Apply

Figure 2.10 Modifying Port PVID

XIII. Create aggregate port LAG 1, add GE9 and GE11 to LAG 1, see the following figure.
Click **Apply** to save the updated setting.



☰ Switch / L2 Switching / Link Aggregation / LAG Management

LAG Management

LAG: Trunk1

Name: Input name

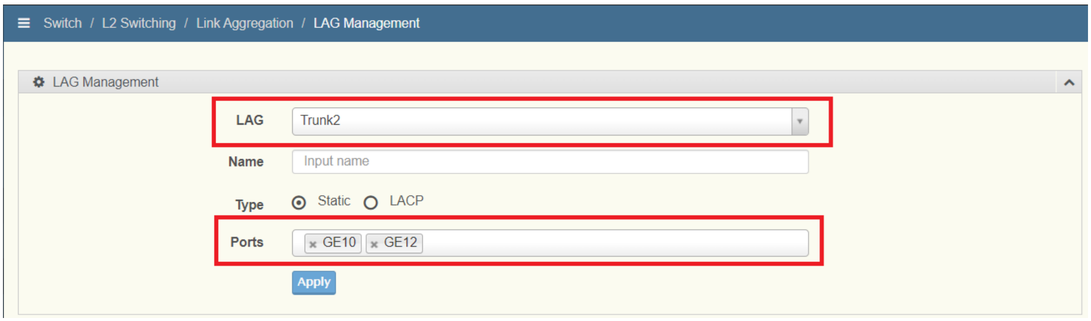
Type: ● Static ○ LACP

Ports: × GE9 × GE11

Apply

Figure 2.11 Creating Port Aggregates

XIV. Create aggregate port LAG 2, add GE10 and GE12 to LAG 2, see the following figure.
Click **Apply** to save the updated setting.



☰ Switch / L2 Switching / Link Aggregation / LAG Management

LAG Management

LAG: Trunk2

Name: Input name

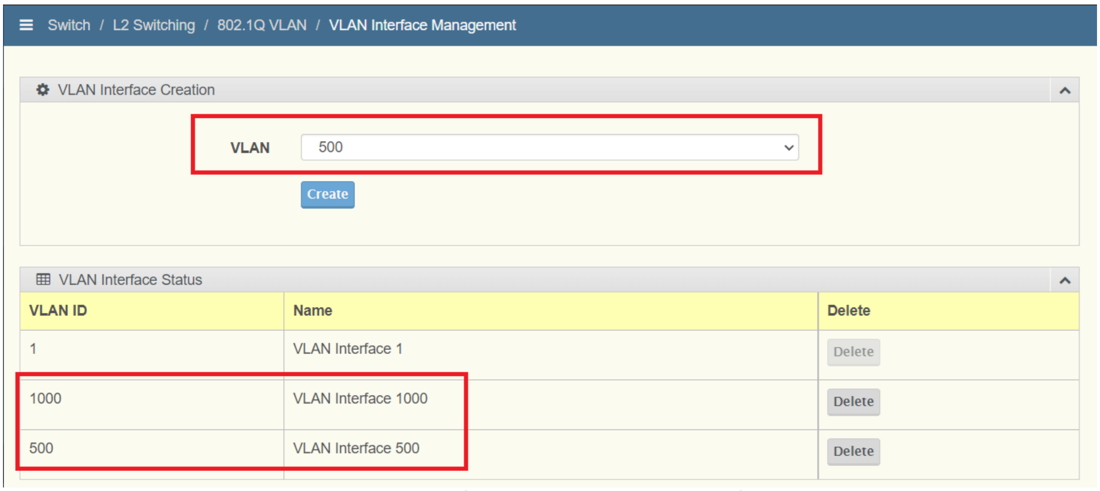
Type: ● Static ○ LACP

Ports: × GE10 × GE12

Apply

Figure 2.12 Creating Port Aggregates

XV. Create a VLAN interface, and create VLAN Interfaces from VLAN 500 and VLAN 1000 in sequence, see the following figure.
Click **Create** to define the updated selection.



Switch / L2 Switching / 802.1Q VLAN / VLAN Interface Management

VLAN Interface Creation

VLAN: 500

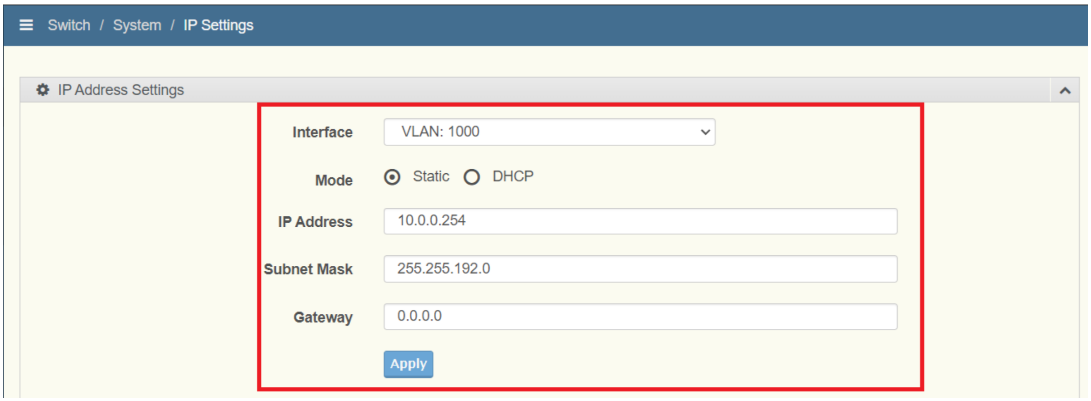
Create

VLAN Interface Status

VLAN ID	Name	Delete
1	VLAN Interface 1	Delete
1000	VLAN Interface 1000	Delete
500	VLAN Interface 500	Delete

Figure 2.13 Creating VLAN Interfaces

XVI. Create an IP address for VLAN 1000, see the following figure.
Click **Apply** to save the updated setting.



Switch / System / IP Settings

IP Address Settings

Interface: VLAN: 1000

Mode: ● Static ○ DHCP

IP Address: 10.0.0.254

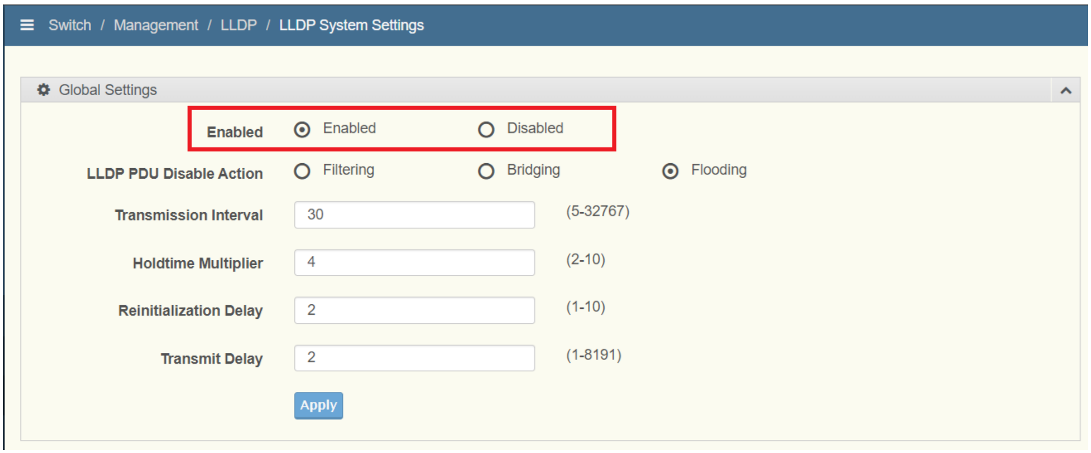
Subnet Mask: 255.255.192.0

Gateway: 0.0.0.0

Apply

Figure 2.14 Creating IP Addresses for VLAN

XVII. In the LLDP System Setting menu, click **Enabled** to update the setting. See the following figure.
Click **Apply** to save the updated setting.



Switch / Management / LLDP / LLDP System Settings

Global Settings

Enabled: ● Enabled ○ Disabled

LLDP PDU Disable Action: ○ Filtering ○ Bridging ● Flooding

Transmission Interval: 30 (5-32767)

Holdtime Multiplier: 4 (2-10)

Reinitialization Delay: 2 (1-10)

Transmit Delay: 2 (1-8191)

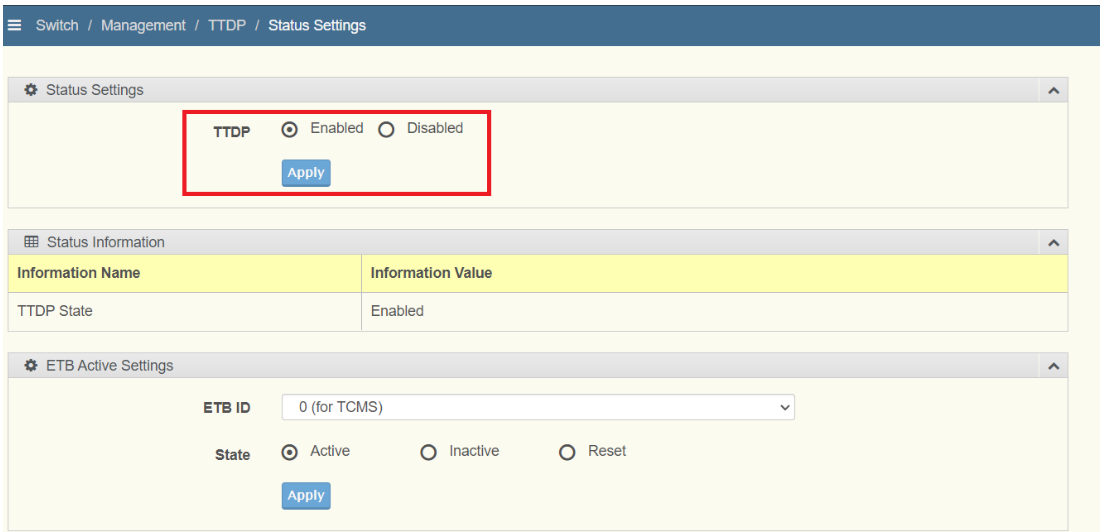
Apply

Figure 2.15 Enabling LLDP Settings

3. Step 3: Set TTDP through the Web interface.
See “TTDP Network Topology Configuration” on page 15 for further details.

I. From the LLDP System Settings menu, view TTDP and click Enabled.

II. Click **Apply** to save the settings.



☰ Switch / Management / TTDP / Status Settings

Status Settings

TTDP ● Enabled ○ Disabled

Apply

Status Information

Information Name	Information Value
TTDP State	Enabled

ETB Active Settings

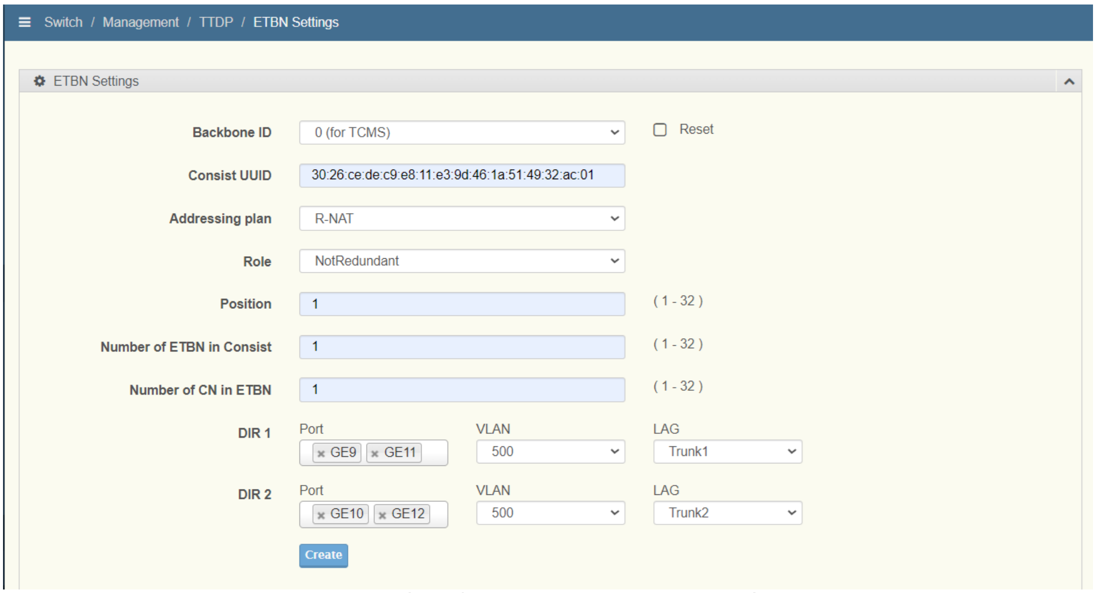
ETB ID: 0 (for TCMS)

State: ● Active ○ Inactive ○ Reset

Apply

Figure 2.16 Enabling TTDP Settings

III. To configure TTDP, modify ETBN Settings, see the following figure for further details.
Click **Create** to save the modified settings.



☰ Switch / Management / TTDP / ETBN Settings

ETBN Settings

Backbone ID: 0 (for TCMS) □ Reset

Consist UUID: 30:26:ce:de:c9:e8:11:e3:9d:46:1a:51:49:32:ac:01

Addressing plan: R-NAT

Role: NotRedundant

Position: 1 (1 - 32)

Number of ETBN in Consist: 1 (1 - 32)

Number of CN in ETBN: 1 (1 - 32)

DIR 1: Port: GE9, GE11 VLAN: 500 LAG: Trunk1

DIR 2: Port: GE10, GE12 VLAN: 500 LAG: Trunk2

Create

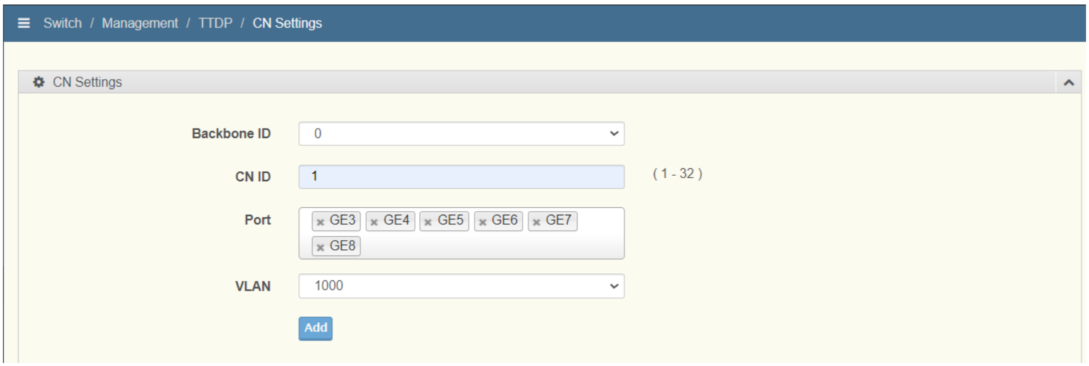
Figure 2.17 Configuring TTDP ETBN Settings

The following table describes the items in the previous figure.

Item	Description
Backbone ID	Click the drop-down menu to select the setting identifier from displayed options. Reset: Click the **Reset** radio button to initiate a reset of the selected setting.
Consist UUID	Enter the Universally Unique Identifier (UUID) to map the order/ position of the ETBN on the train backbone.
Addressing plan	Click the drop-down menu to select the type of IP assignment topology: ■ Absolute: ■ R-NAT (default): Railway-NAT translates IP addresses and populated dynamically based on the subnet allocation.

Item	Description
Role	Click the drop-down menu to select the role of the device: ■ Master: defines the device as the master router with the highest priority. ■ Backup: defines the device as the backup router in case the master fails. ■ NotRedundant: defines the device to operate on a non redundant scheme.
Position	Enter the string (1 - 32) to define the position of the
Number of CN in ETBN	Enter the string to identify the CN subset in each ETBN. The value is used to build train IP mapping, train routing definition, NAT rules.
Dir 1	Click the drop-down menu to define the following Dir1 and Dir2 settings: ■ Port: select from GE1 to GE12 ■ VLAN: select from 1, 492, 500, 1000 ■ LAG: select from Trunk1 to Trunk8
Dir 2	Click the drop-down menu to define the following Dir1 and Dir2 settings: ■ Port: select from GE1 to GE12 ■ VLAN: select from 1, 492, 500, 1000 ■ LAG: select from Trunk1 to Trunk8
Create	Click **Create** to set up the defined setting.

IV. To configure TTDP, modify CN Settings, see the following figure for further details.
Click **Add** to save the modified settings.



Backbone ID: 0

CN ID: 1 (1 - 32)

Port: GE3 GE4 GE5 GE6 GE7 GE8

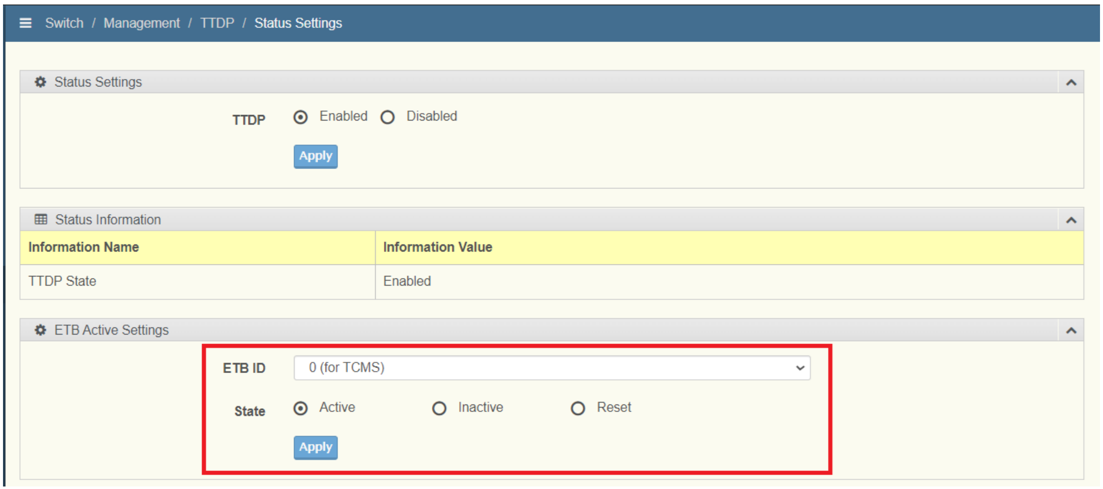
VLAN: 1000

Figure 2.18 Configuring TTDP CN Settings

The following table describes the items in the previous figure.

Item	Description
Backbone ID	Click the drop-down menu to select the setting identifier from displayed options. Reset: Click the **Reset** radio button to initiate a reset of the selected setting.
CN ID	Enter the variable to set the CN number corresponding to the related ETBN. **Note:** Under the same ETBN, each CN ID must be unique. If there are multiple CNs under the same ETBN, in R-NAT mode, the CN subnet IP will refer to the CN ID for addressing. (Ex. CN#1@ETBN#1: 10.1.0.X/16, CN#2@ETBN#1: 10.2.0.X/16)
Port	Select the corresponding CN.
VLAN	Click the drop-down menu to select corresponding VLAN.
Add	Click **Add** to save the values and update the screen.

V. To configure TTDP, modify ETB Active Settings, see the following figure for further details.
Click **Apply** to save the modified settings.



Switch / Management / TTDP / Status Settings

Status Settings

TTDP ● Enabled ○ Disabled

Apply

Status Information

Information Name	Information Value
TTDP State	Enabled

ETB Active Settings

ETB ID: 0 (for TCMS)

State ● Active ○ Inactive ○ Reset

Apply

Figure 2.19 Configuring TTDP Active Settings

The following table describes the items in the previous figure.

Item	Description
ETB ID	Click the drop-down menu to select the interface on the ETBN.
State	Click the radio button to apply the state on the selected interface: **Active**, Inactive, Reset.
Apply	Click **Apply** to save the values and update the screen.

2.2 TRDP Forwarding Introduction

The following illustrates a TRDP network topology example, see “TTDP Network Topology Configuration” on page 15 for further information.

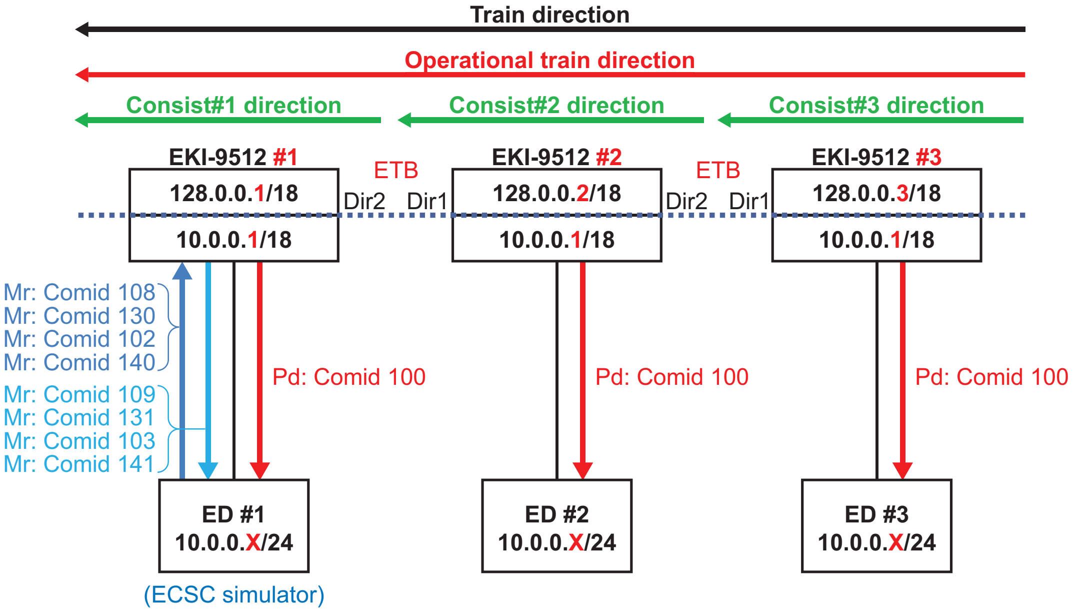


Figure 2.20 TRDP Forwarding Topology

Note!

1. Software version 6.00.005 currently supports the following TRDP ComID packets:

Send:

I. ComId 1 (Pd) - ETBCTRL telegram transmission
II. ComId 2 (Mn) - CSTINFO Notification Message
III. ComId 3 (Mn) - CSTINFO Request (CSTINFOCTRL)
IV. ComId 100 (Pd) - TTDB status information
V. ComId 109 (Pd) - Operational train directory information (Reply)
VI. ComId 131 (Mp) - ETBN control and status data (Reply)
VII. ComId 103 (Mp) - TTDB information for train directory (Reply)
VIII. ComId 141 (Mp) - DNS resolving request message (Reply)

Receive:

I. ComId 108 (Mr) - Operational train directory information (Request)
II. ComId 130 (Mr) - ETBN control and status data (Request)
III. ComId 102 (Mr) - TTDB information for train directory (Request)
IV. ComId 140 (Mr) - DNS resolving request message (Request)

Chapter 3

Firmware Upgrade Guide

EKI-9512 currently supports TFTP and HTTP for firmware updating. Updating can be managed by using the CLI and Web interface.

3.1 Firmware upgrade via CLI

The following section applies to TFTP only.

1. Step 1: Log in to CLI via a console / Telnet:

   I. Login via Telnet (only for P1-P2):
   - Telnet to IP: 192.168.1.1.
   - Enter the user name and password: *admin / admin* to log in to the system.

   II. Console login:
   - Console login through a terminal software, baud rate: 115200.
   - Enter the user name and password: *admin / admin* to log in to the system.

2. Step 2: Upgrading firmware through CLI:

   I. Connect to TFTP server via P1 or P2 network.

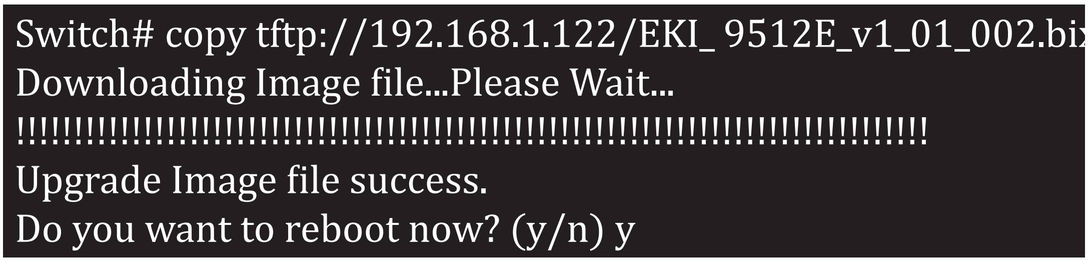
   II. Put EKI-9512E-6-00-04-Beta.bix in the specified TFTP server directory.

   III. Enter the CLI cmd:
   copy tftp://<TFTP Server IP>/EKI-9512E-6-00-04-Beta.bix flash://image0.

   IV. After the firmware upgrade is complete, the following displays
   Upgrade Image file success.

   V. The following message displays:
   Do you want to reboot now? (y/n)
   If a reboot is required after updating, press "y" to reboot.

   VI. Refer to the following figure for further information:



```
Switch# copy tftp://192.168.1.122/EKI_ 9512E_v1_01_002.bi
Downloading Image file...Please Wait...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Upgrade Image file success.
Do you want to reboot now? (y/n) y
```

Figure 3.1 Firmware Updating via CLI

3.2 Firmware upgrade via Web

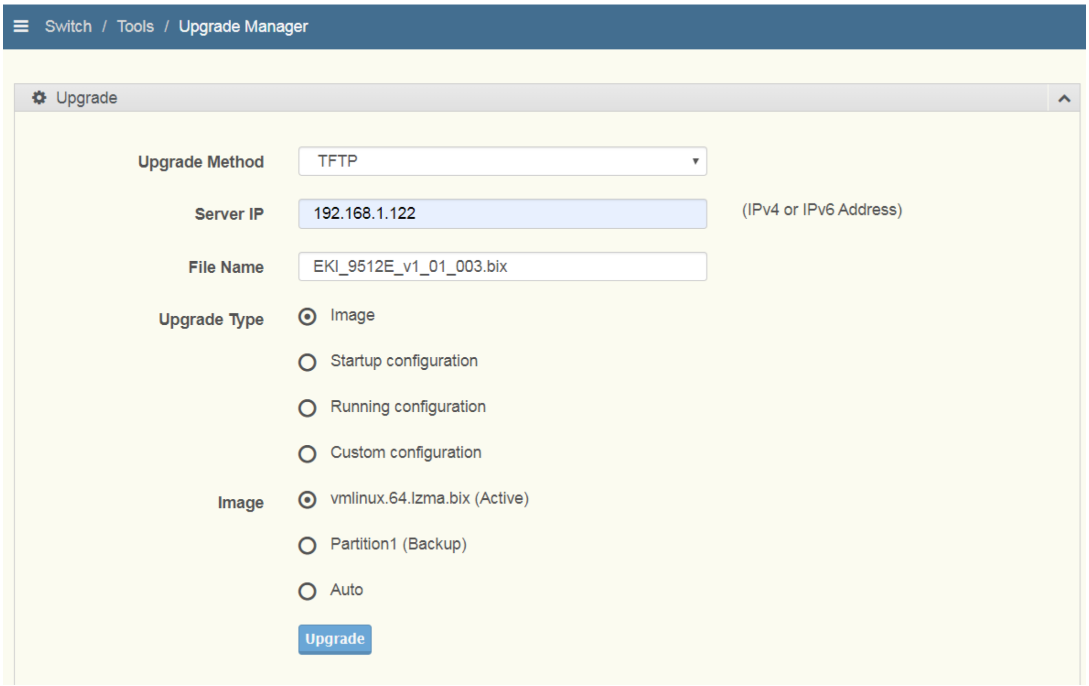
1. The following section applies to firmware upgrades through HTTP, applicable to P1 to P2), see “Topology Configuration for TTDP” on page 13.

   I. In the IP address, type in the following address: http://192.168.1.1.

   II. Enter the user name and password: *admin / admin* to log in to the system.

   III. From the root menu, click Tools > Upgrade Manager to view the firmware page.

IV. to update through TFTP see the following figure.



☰ Switch / Tools / Upgrade Manager

Upgrade

Upgrade Method: TFTP

Server IP: 192.168.1.122 (IPv4 or IPv6 Address)

File Name: EKI_9512E_v1_01_003.bix

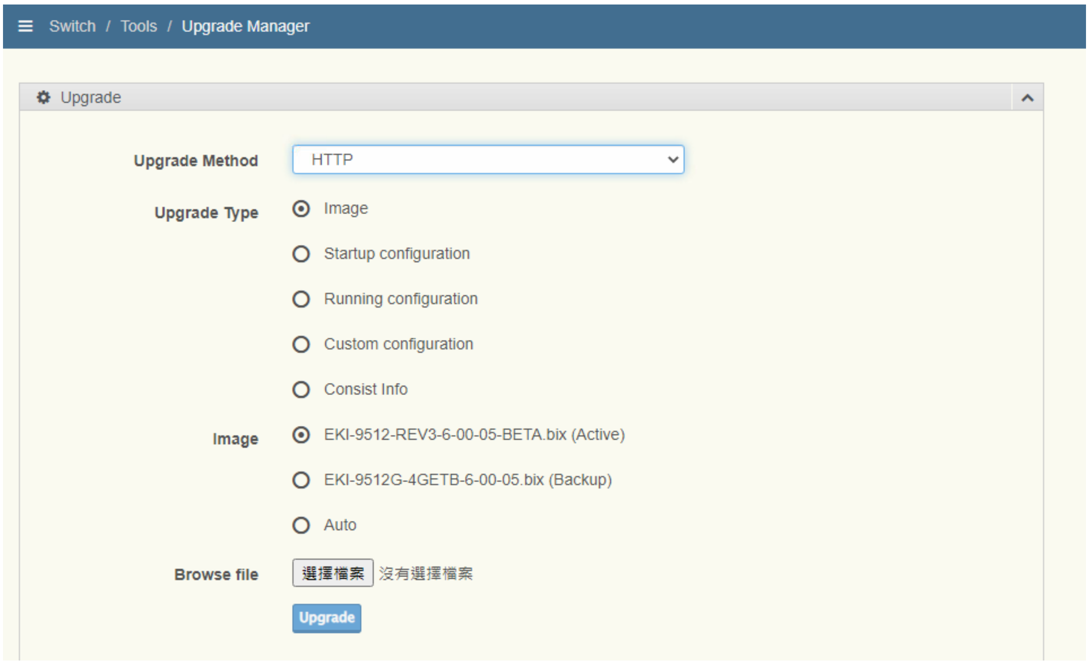
Upgrade Type:
- ● Image
- ○ Startup configuration
- ○ Running configuration
- ○ Custom configuration

Image:
- ● vmlinux.64.lzma.bix (Active)
- ○ Partition1 (Backup)
- ○ Auto

Upgrade

Figure 3.2 Upgrading via TFTP

V. To update through HTTP refer to the following figure.



☰ Switch / Tools / Upgrade Manager

Upgrade

Upgrade Method: HTTP

Upgrade Type:
- ● Image
- ○ Startup configuration
- ○ Running configuration
- ○ Custom configuration
- ○ Consist Info

Image:
- ● EKI-9512-REV3-6-00-05-BETA.bix (Active)
- ○ EKI-9512G-4GETB-6-00-05.bix (Backup)
- ○ Auto

Browse file: 選擇檔案 沒有選擇檔案

Upgrade

Figure 3.3 Upgrading via TFTP

Chapter 4

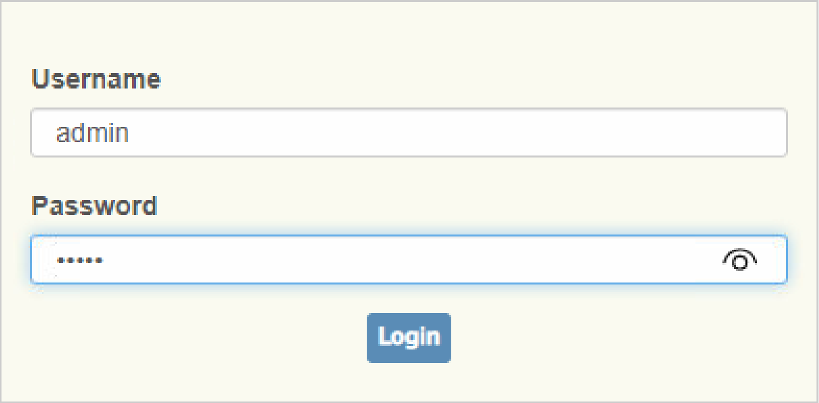
Management & Configuration

4.1 Log In

The switch can be configured through a networked computer. Ensure the computer is networked before attempting to access the interface. The management interface can be accessed via the default network configuration (DHCP).

Once the interface is accessed, the available management tools will be available, which will be described in the following sections.

1. On the networked computer, open up a web browser.
2. In the browser's address bar type in the switch's default IP address (192.168.1.1). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.



Username

admin

Password

•••••

Figure 4.1 Login Screen

4.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

4.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Tools** > **User Account**.
2. From the User drop-down menu, select the Admin (default) account.
3. In the **User Name** field, enter admin for this account. It is not necessary to change the user name, however, a change in the default settings increases the security settings.
4. In the **Password** field, type in the new password. Re-type the same password in the **Retype Password** field.
5. Click **Apply** to change the current account settings.

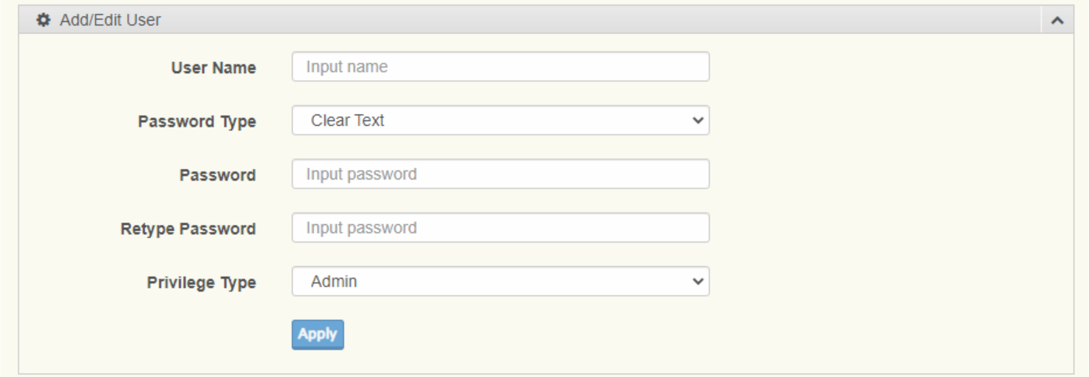


Figure 4.2 Changing a Default Password

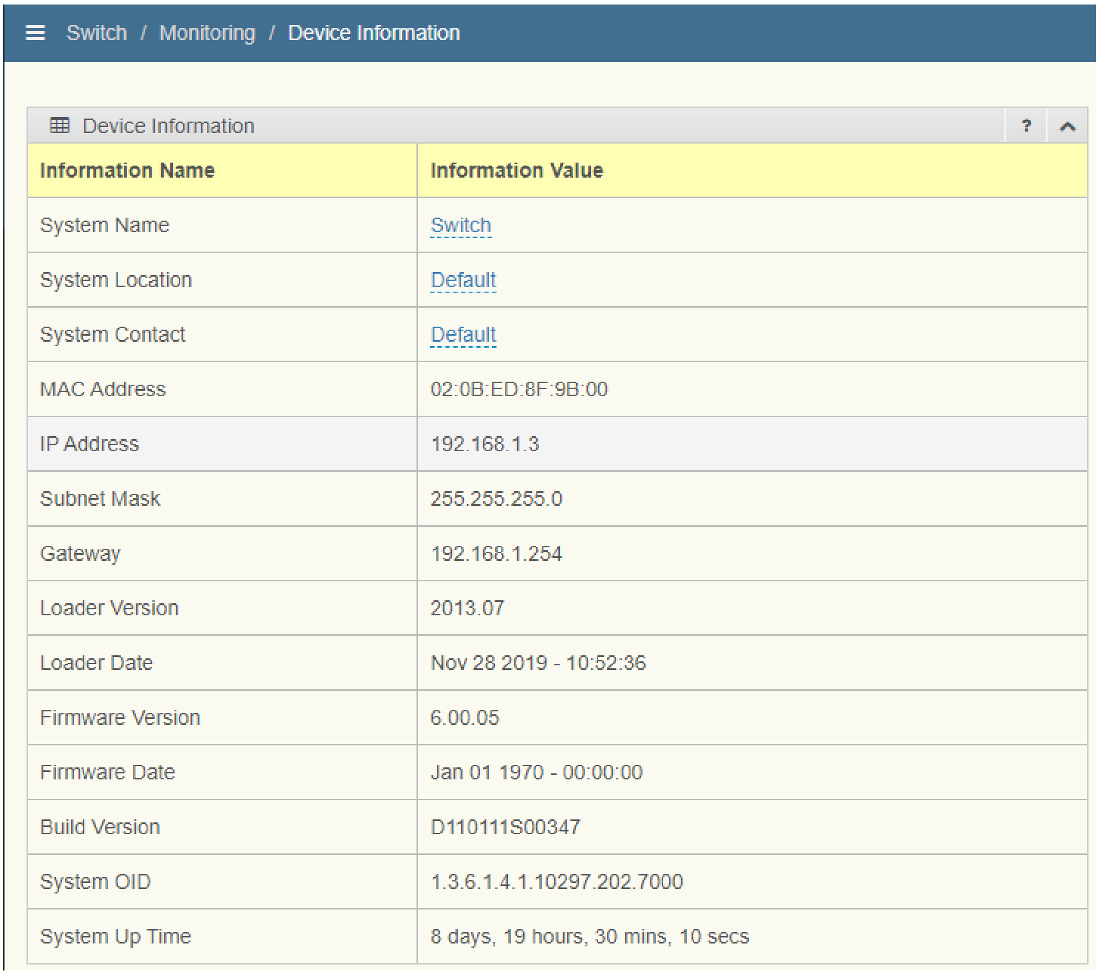
After saving all the desired settings, perform a system save (**Tools** > **Save Configuration**). The changes are saved.

4.3 Monitoring

4.3.1 Device Information

The Device Information menu lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. The information is for review only. To modify the device information, see the respective item within the user interface.

To access this page, click **Monitoring** > **Device Information**.



Information Name	Information Value
System Name	Switch
System Location	Default
System Contact	Default
MAC Address	02:0B:ED:8F:9B:00
IP Address	192.168.1.3
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
Loader Version	2013.07
Loader Date	Nov 28 2019 - 10:52:36
Firmware Version	6.00.05
Firmware Date	Jan 01 1970 - 00:00:00
Build Version	D110111S00347
System OID	1.3.6.1.4.1.10297.202.7000
System Up Time	8 days, 19 hours, 30 mins, 10 secs

Figure 4.3 Monitoring > Device Information

The following table describes the items in the previous figure.

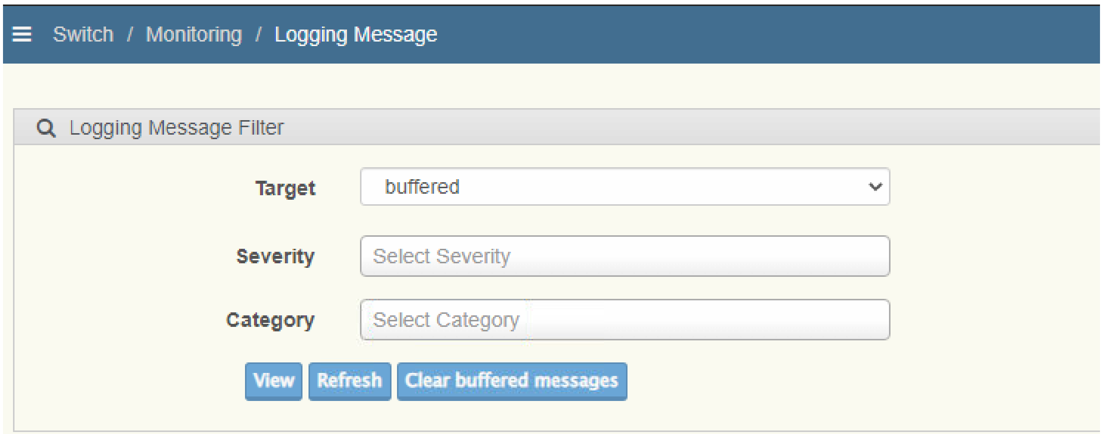
Item	Description
System Name	Click **Switch** to enter the system name: up to 128 alphanumeric characters (default is Switch).
System Location	Click **Default** to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click **Default** to enter the contact person: up to 128 alphanumeric characters (default is Default).
MAC Address	Displays the MAC address of the switch.
IP Address	Displays the assigned IP address of the switch.
Subnet Mask	Displays the assigned subnet mask of the switch.
Gateway	Displays the assigned gateway of the switch.
Loader Version	Displays the current loader version of the switch.
Loader Date	Displays the current loader build date of the switch.

Item	Description
Firmware Version	Displays the current firmware version of the switch.
Firmware Date	Displays the current firmware build date of the switch.
System Object ID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.

4.3.2 Logging Message

The Logging Message Filter page allows you to enable the display of logging message filter.

To access this page, click **Monitoring** > **Logging Message**.



Target: buffered

Severity: Select Severity

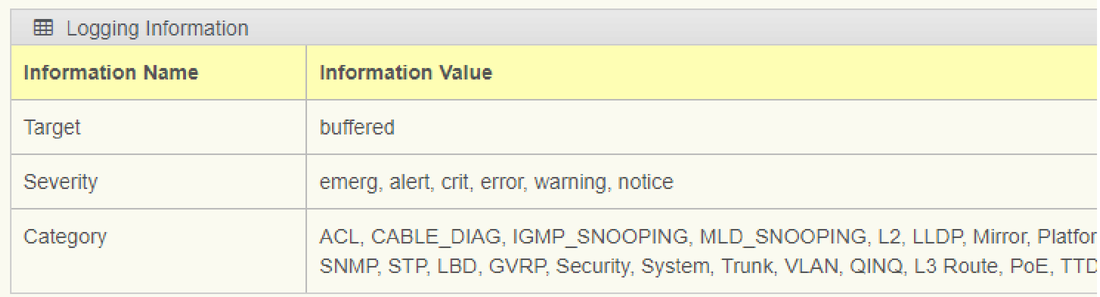
Category: Select Category

Figure 4.4 Monitoring > Logging Message

The following table describes the items in the previous figure.

Item	Description
Target	Click the drop-down menu to select a target to store the log messages. ■ Buffered: Store log messages in RAM. All log messages are cleared after system reboot. ■ File: Store log messages in a file.
Severity	The setting allows you to designate a severity level for the Logging Message Filter function. Click the drop-down menu to select the severity level target setting. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity. ■ alert: Indicates action must be taken immediately. ■ crit: Indicates critical conditions. ■ error: Indicates error conditions. ■ warning: Indicates warning conditions. ■ notice: Indicates normal but significant conditions. ■ info: Indicates informational messages. ■ debug: Indicates debug-level messages.
Category	Click the drop-down menu to select the category level target setting.
View	Click **View** to display all Logging Information and Logging Message information.
Refresh	Click **Refresh** to update the screen.
Clear buffered messages	Click **Clear buffered messages** to clear the logging buffer history list.

Logging Information settings are informational only as shown in the following:

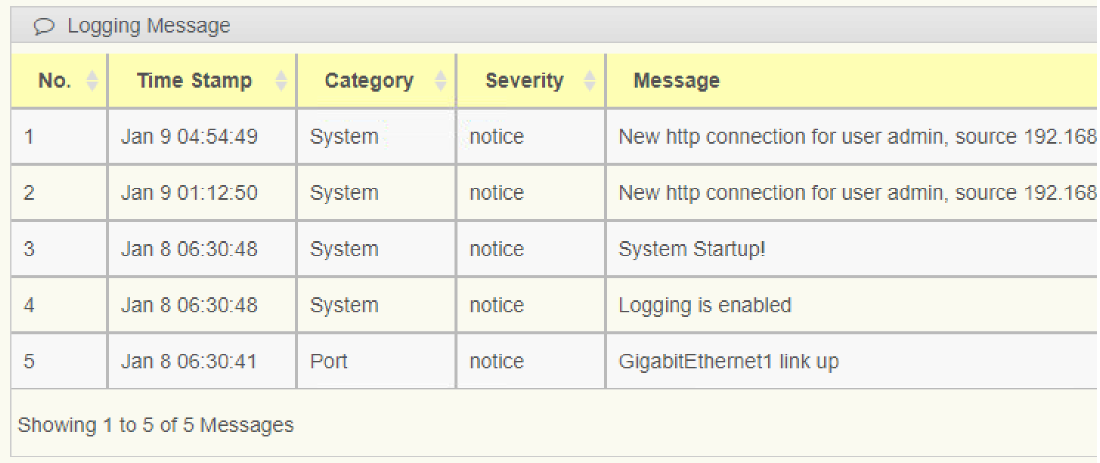


Logging Information

Information Name	Information Value
Target	buffered
Severity	emerg, alert, crit, error, warning, notice
Category	ACL, CABLE_DIAG, IGMP_SNOOPING, MLD_SNOOPING, L2, LLDP, Mirror, Platfor SNMP, STP, LBD, GVRP, Security, System, Trunk, VLAN, QINQ, L3 Route, PoE, TTD

Figure 4.5 Monitoring > Logging Message

Logging Message settings are informational only as shown in the following:



Logging Message

No.	Time Stamp	Category	Severity	Message
1	Jan 9 04:54:49	System	notice	New http connection for user admin, source 192.168
2	Jan 9 01:12:50	System	notice	New http connection for user admin, source 192.168
3	Jan 8 06:30:48	System	notice	System Startup!
4	Jan 8 06:30:48	System	notice	Logging is enabled
5	Jan 8 06:30:41	Port	notice	GigabitEthernet1 link up

Showing 1 to 5 of 5 Messages

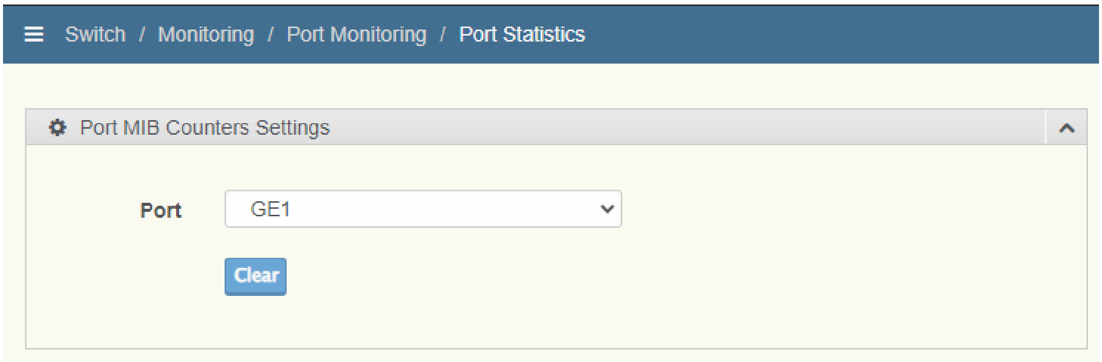
Figure 4.6 Monitoring > Logging Message

4.3.3 Port Monitoring

Port Network Monitor is a bandwidth and network monitoring tool for the purpose of capturing network traffic and measuring of network throughput. The monitoring functionality includes listing of port statistics as well as port utilization.

4.3.3.1 Port Statistics

To access this page, click **Monitoring** > **Port Monitoring** > **Port Statistics**.



Switch / Monitoring / Port Monitoring / Port Statistics

Port MIB Counters Settings

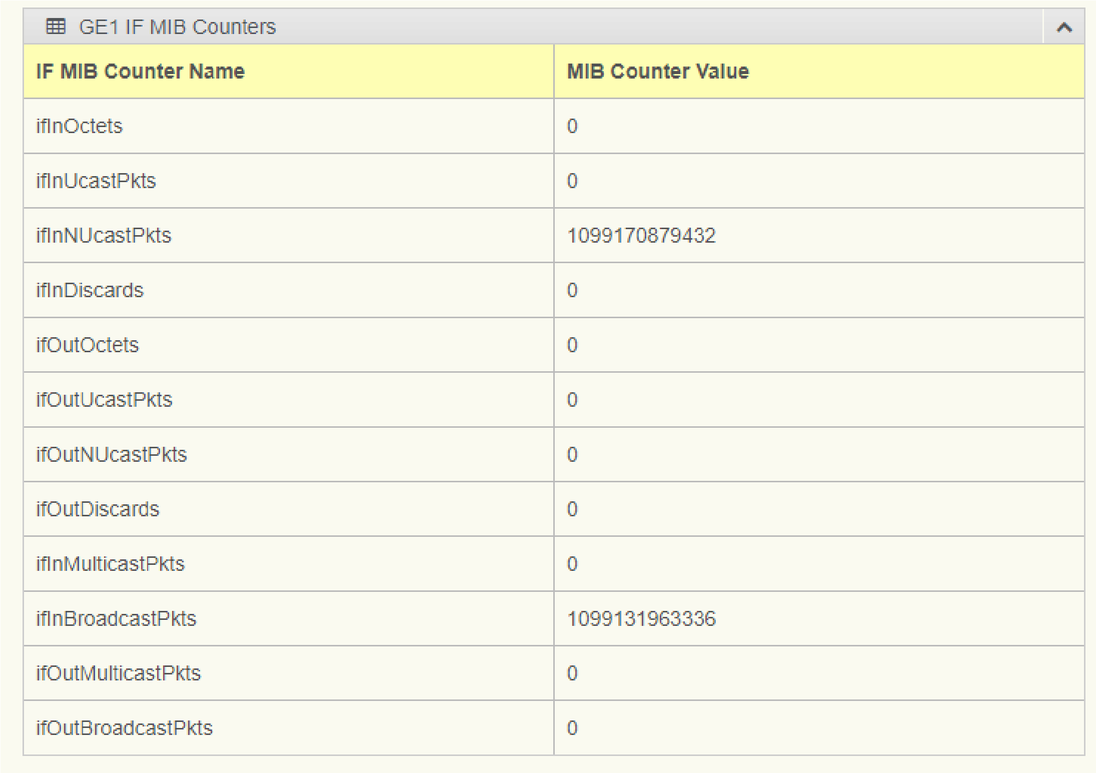
Port: GE1

Figure 4.7 Monitoring > Port Monitoring > Port Statistics

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click **Clear** to clear the counter selections.

IF MIB Counters settings are informational only as shown in the following:

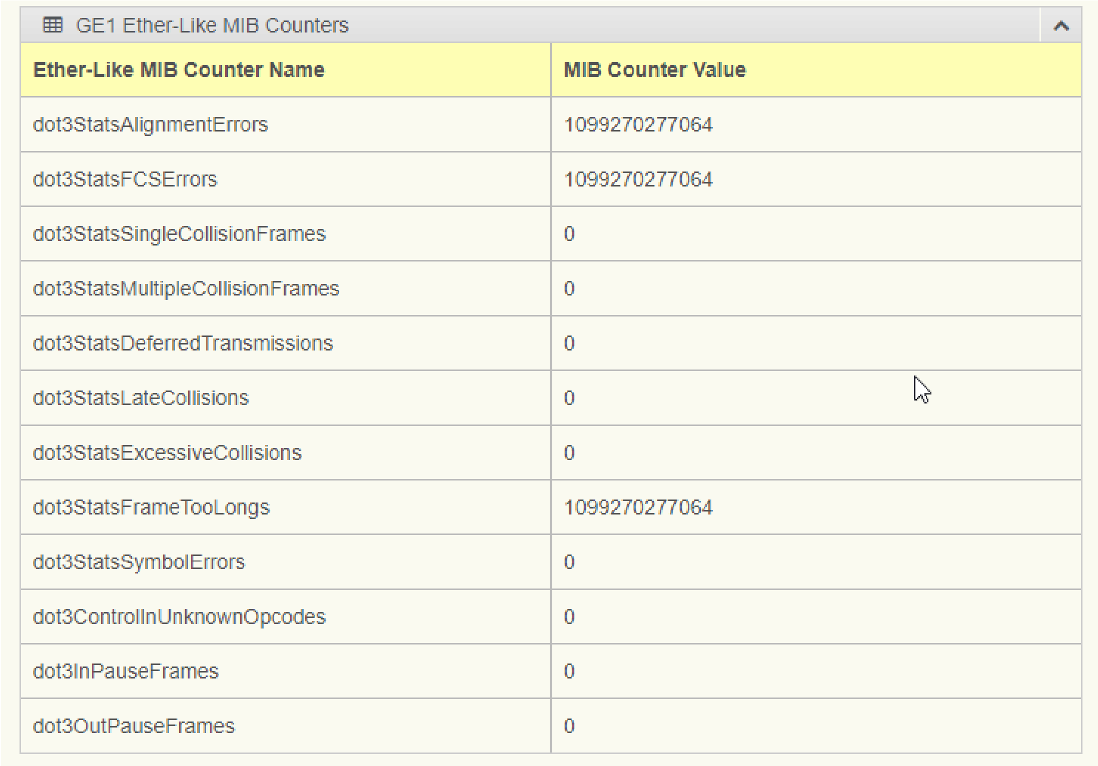


GE1 IF MIB Counters

IF MIB Counter Name	MIB Counter Value
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	1099170879432
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	1099131963336
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Figure 4.8 Monitoring > Port Monitoring > Port Statistics

Ether-Like MIB Counters settings are informational only as shown in the following:

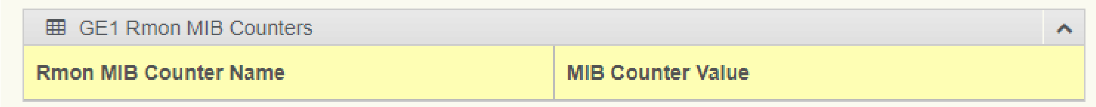


GE1 Ether-Like MIB Counters

Ether-Like MIB Counter Name	MIB Counter Value
dot3StatsAlignmentErrors	1099270277064
dot3StatsFCSErrors	1099270277064
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	1099270277064
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Figure 4.9 Monitoring > Port Monitoring > Port Statistics

Rmon MIB Counters settings are informational only as shown in the following:



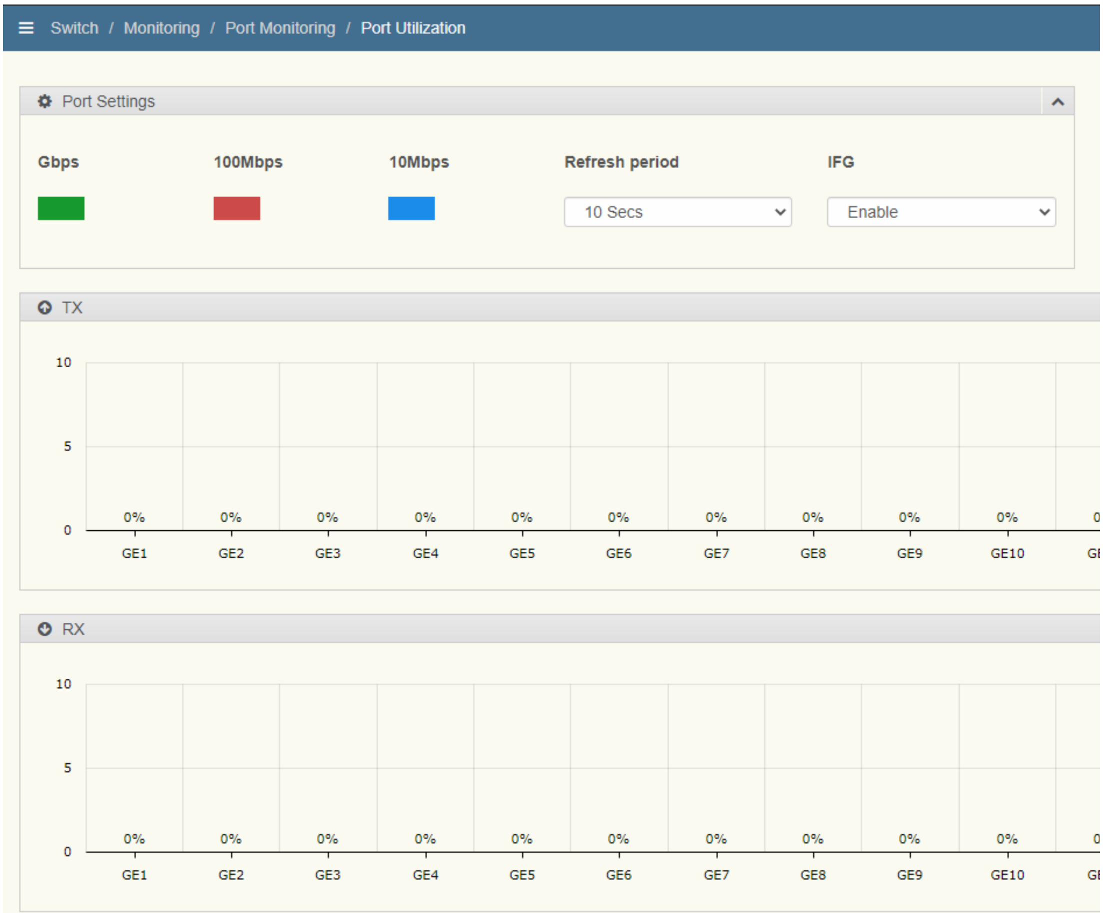
GE1 Rmon MIB Counters

Rmon MIB Counter Name	MIB Counter Value

Figure 4.10 Monitoring > Port Monitoring > Port Statistics

4.3.3.2 Port Utilization

To access this page, click **Monitoring** > **Port Monitoring** > **Port Utilization**.



≡ Switch / Monitoring / Port Monitoring / Port Utilization

Port Settings

Gbps	100Mbps	10Mbps	Refresh period	IFG
🟩	🟥	🟦	10 Secs	Enable

Figure 4.11 Monitoring > Port Monitoring > Port Utilization

The following table describes the items in the previous figure.

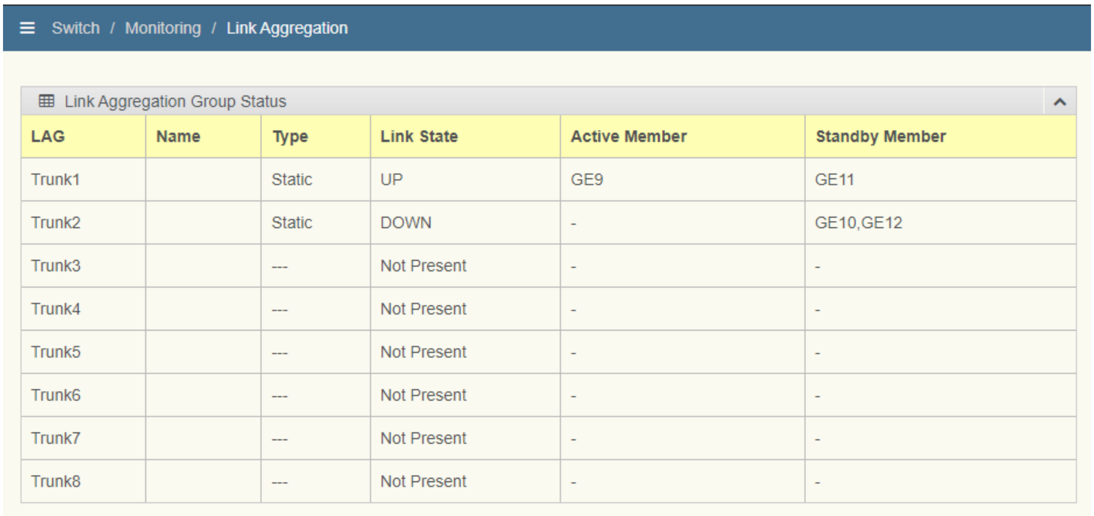
Item	Description
Refresh period	Click the drop-down menu to select and designate a period (second intervals) to refresh the information (TX and RX) listings.
IFG	Click the drop-down menu to enable or disable the Interframe Gap (IFG) statistic.

4.3.4 Link Aggregation

The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state and membership type for each port.

To access this page, click **Monitoring** > **Link Aggregation**.

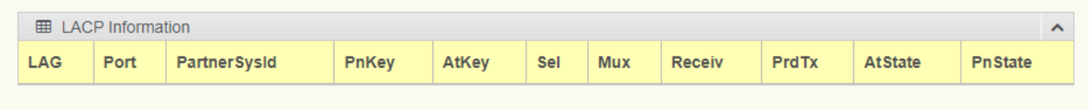
Link Aggregation Group Status settings are informational only as shown in the following:


Switch / Monitoring / Link Aggregation
Link Aggregation Group Status

LAG	Name	Type	Link State	Active Member	Standby Member
Trunk1		Static	UP	GE9	GE11
Trunk2		Static	DOWN	-	GE10,GE12
Trunk3		---	Not Present	-	-
Trunk4		---	Not Present	-	-
Trunk5		---	Not Present	-	-
Trunk6		---	Not Present	-	-
Trunk7		---	Not Present	-	-
Trunk8		---	Not Present	-	-

Figure 4.12 Monitoring > Link Aggregation

LACP Information settings are informational only as shown in the following:



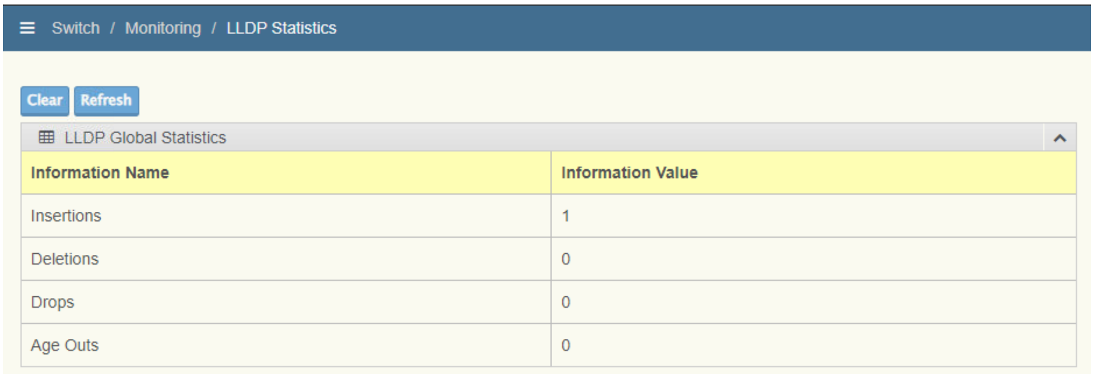
LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState

Figure 4.13 Monitoring > Link Aggregation

4.3.5 LLDP Statistics

The LLDP Statistics page displays both the global and port LLDP statistics.

To access this page, click **Monitoring** > **LLDP Statistics**.



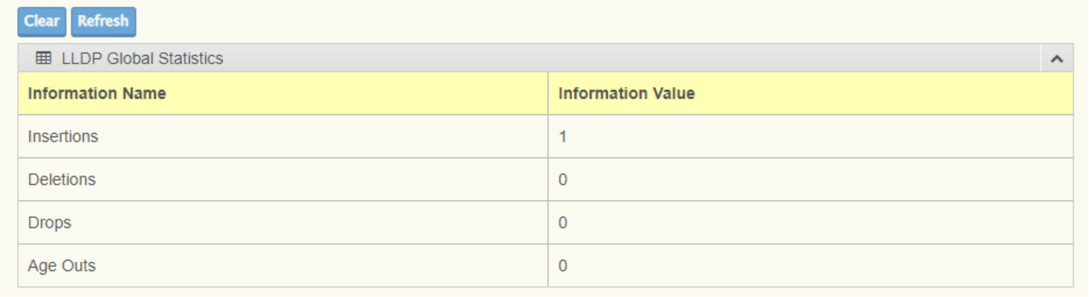
Information Name	Information Value
Insertions	1
Deletions	0
Drops	0
Age Outs	0

Figure 4.14 Monitoring > LLDP Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to reset the LLDP Statistics for all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

The ensuing table for **LLDP Global Statistics** settings are informational only and display the following: Insertions, Deletions, Drops and Age Outs.

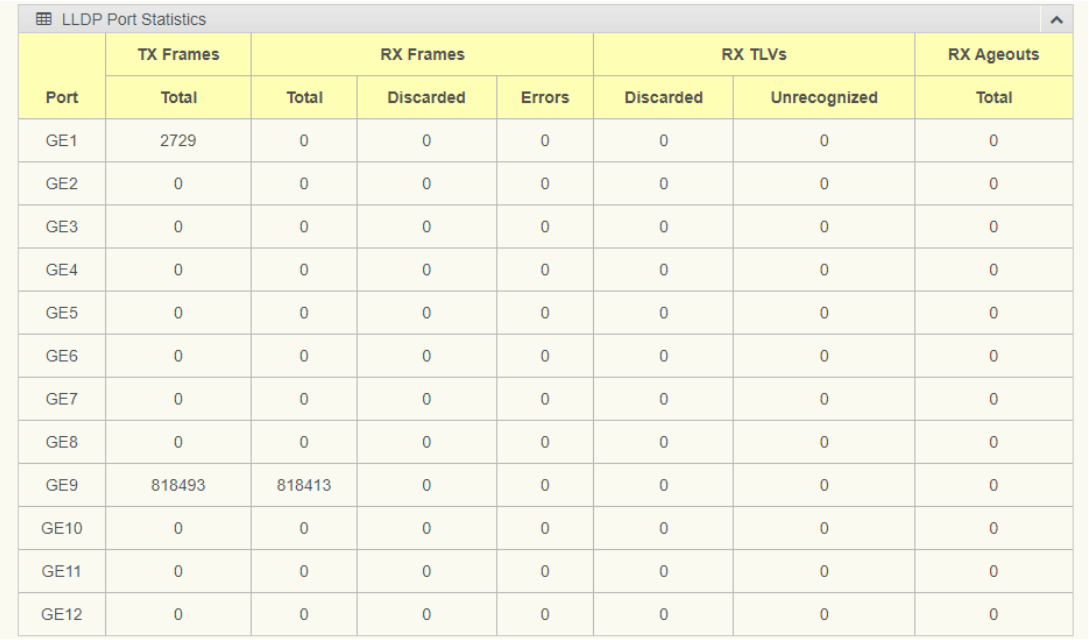


LLDP Global Statistics

Information Name	Information Value
Insertions	1
Deletions	0
Drops	0
Age Outs	0

Figure 4.15 Monitoring > LLDP Statistics

LLDP Port Statistics settings are informational only as shown in the following:



LLDP Port Statistics

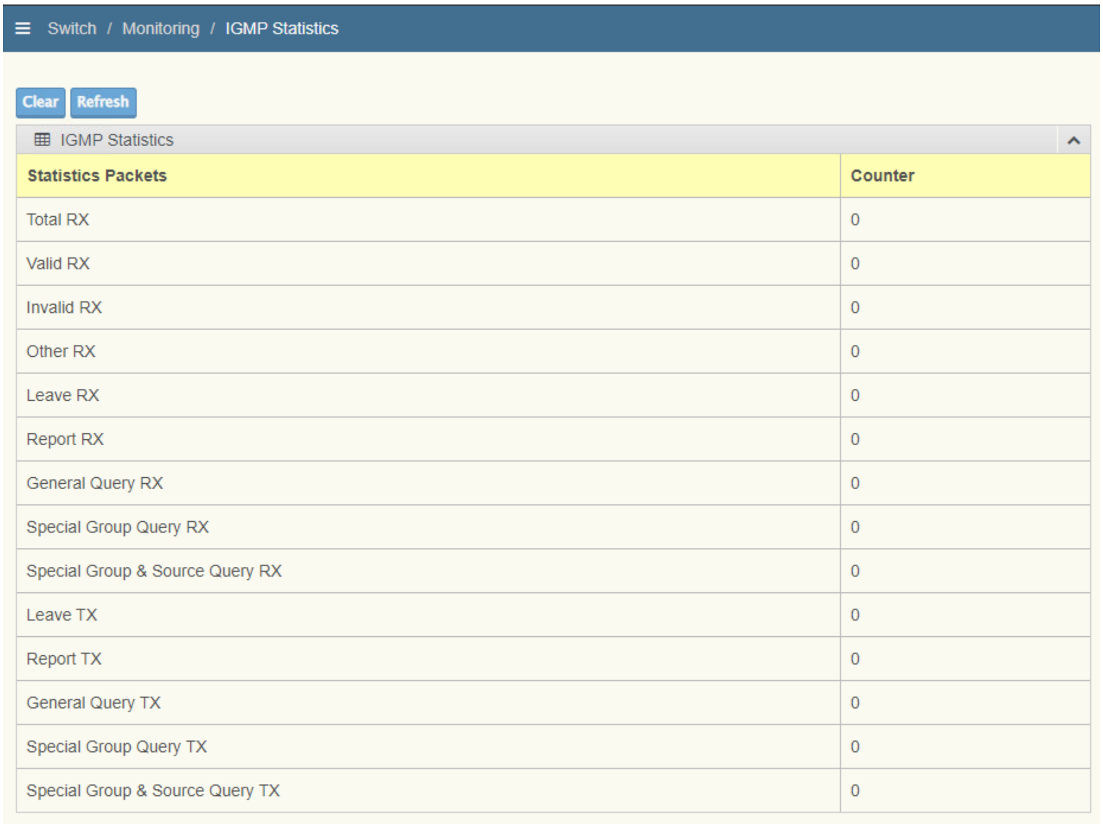
	TX Frames	RX Frames			RX TLVs		RX Ageouts
Port	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	2729	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	818493	818413	0	0	0	0	0
GE10	0	0	0	0	0	0	0
GE11	0	0	0	0	0	0	0
GE12	0	0	0	0	0	0	0

Figure 4.16 Monitoring > LLDP Statistics

4.3.6 IGMP Statistics

The IGMP Statistics function displays statistical package information for IP multicasting.

To access this page, click **Monitoring** > **IGMP Statistics**.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 4.17 Monitoring > IGMP Statistics

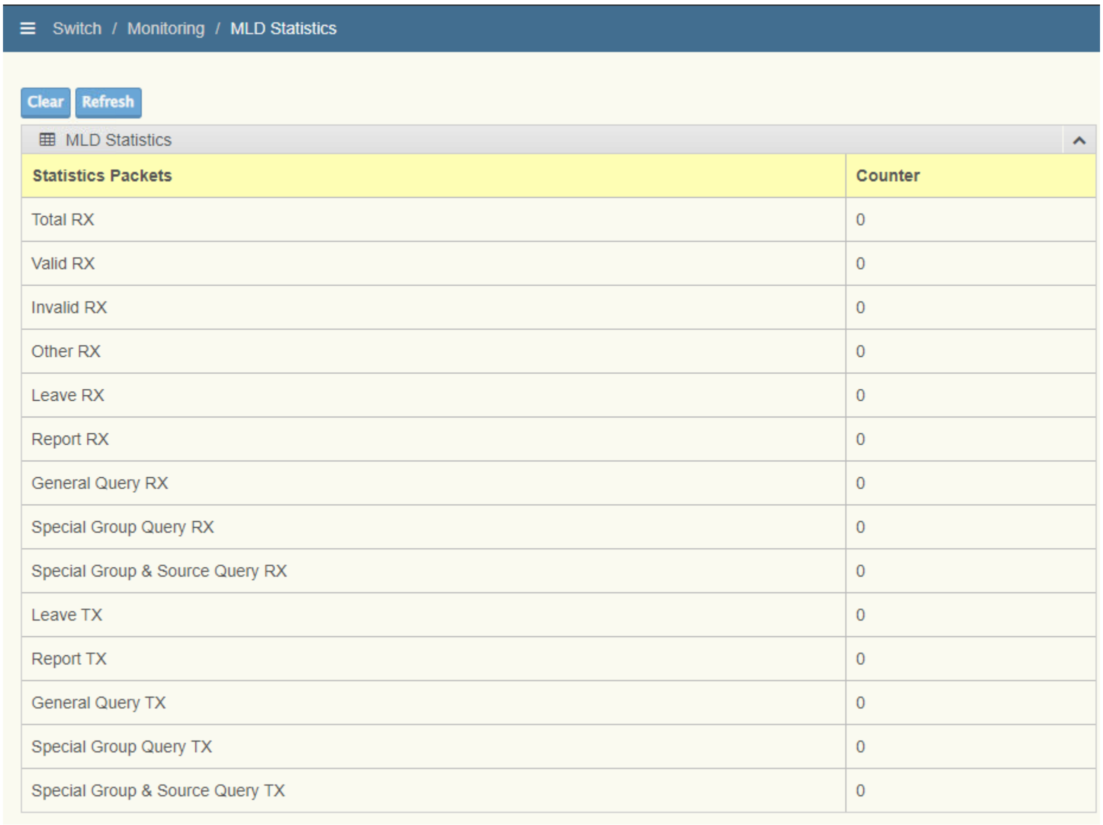
The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh IGMP Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

4.3.7 MLD Statistics

The IGMP Statistics function displays statistical package information for IP multicasting.

To access this page, click **Monitoring** > **MLD Statistics**.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 4.18 Monitoring > MLD Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh MLD Statistics of all the interfaces.
Refresh	Click **Refresh** to update the data on the screen with the present state of the data in the switch.

4.4 System

4.4.1 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option.

To access this page, click **System** > **IP Settings**.

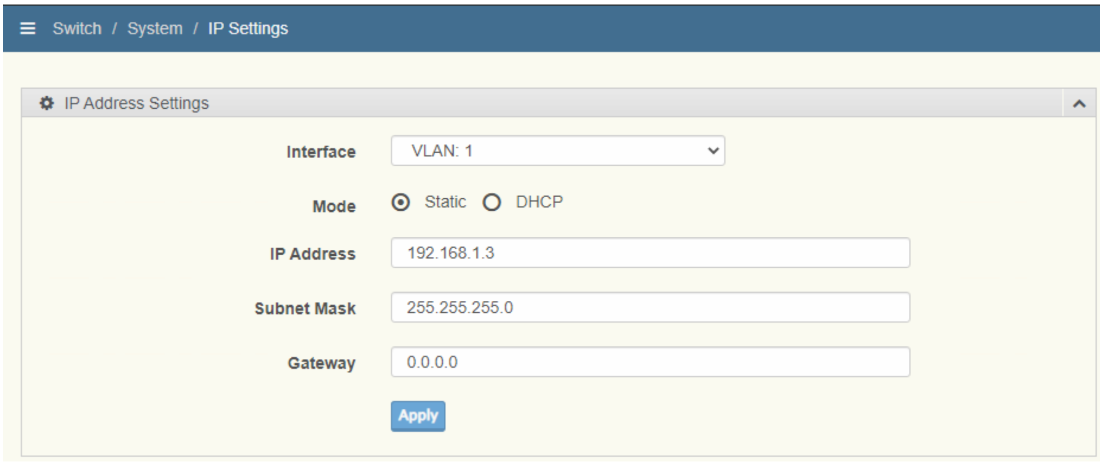
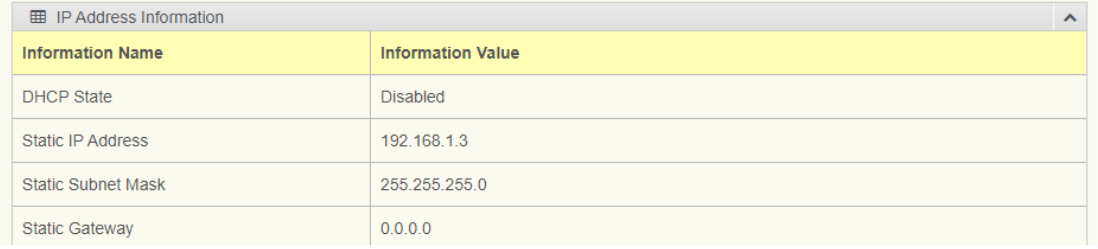


Figure 4.19 System > IP Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select an available interface option to configure its settings.
Mode	Click the radio button to select the IP Address Setting mode: Static or DHCP.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.1.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Gateway	Enter a value to specify the default gateway for the interface. The default is 192.168.1.254.
Apply	Click **Apply** to save the values and update the screen.

IP Address Information settings are informational only as shown in the following:



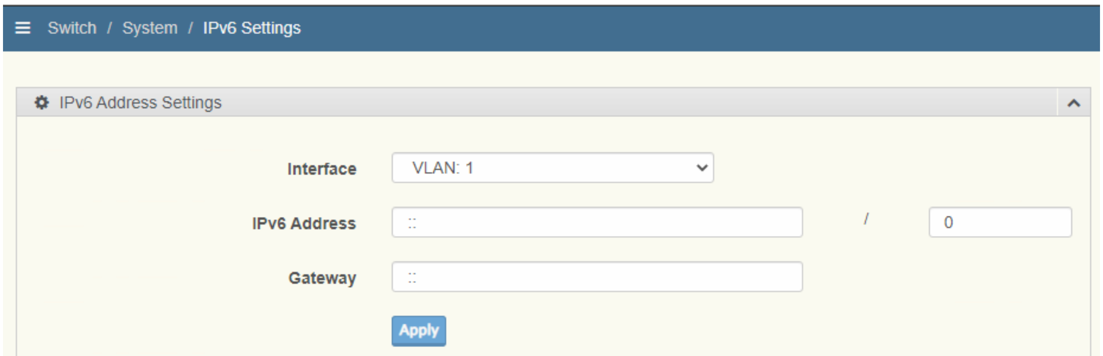
IP Address Information

Information Name	Information Value
DHCP State	Disabled
Static IP Address	192.168.1.3
Static Subnet Mask	255.255.255.0
Static Gateway	0.0.0.0

Figure 4.20 System > IP Settings

4.4.2 IPv6 Settings

To access this page, click **System** > **IPv6 Settings**.



Switch / System / IPv6 Settings

IPv6 Address Settings

Interface: VLAN: 1

IPv6 Address: :: / 0

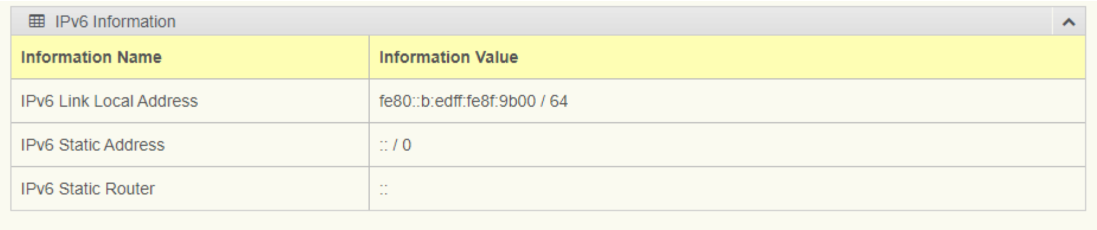
Gateway: ::

Figure 4.21 System > IPv6 Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select an available interface option to configure its settings.
IPv6 Address	Enter the IPv6 address for the system.
Gateway	Enter the gateway address for the system.
Apply	Click **Apply** to save the values and update the screen.

IPv6 Information settings are informational only as shown in the following:



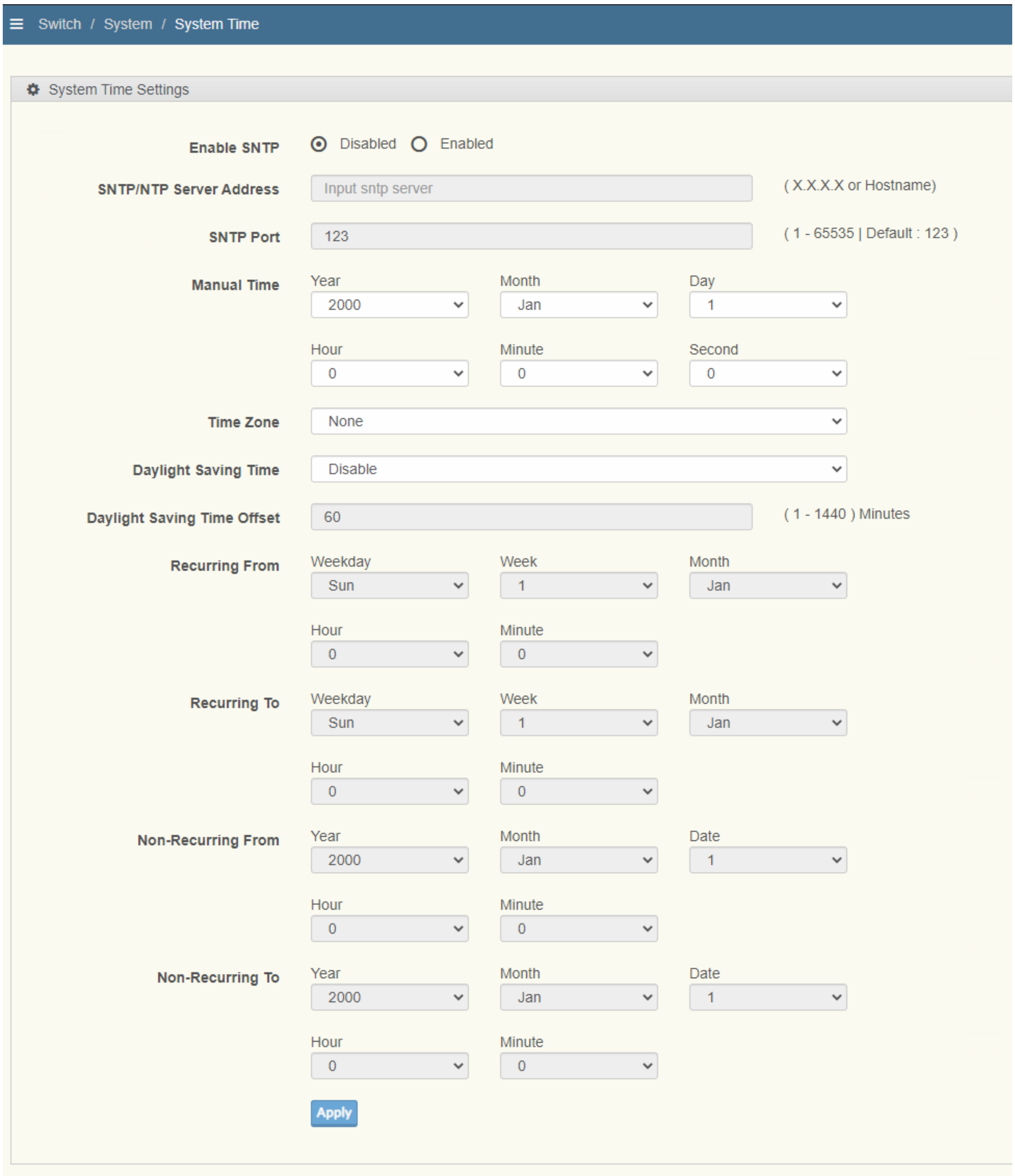
IPv6 Information

Information Name	Information Value
IPv6 Link Local Address	fe80::b:edff:fe8f:9b00 / 64
IPv6 Static Address	:: / 0
IPv6 Static Router	::

Figure 4.22 System > IPv6 Settings

4.4.3 System Time

To access this page, click **System** > **System Time**.



Enable SNTP: ● Disabled ○ Enabled

SNTP/NTP Server Address: Input sntp server (X.X.X.X or Hostname)

SNTP Port: 123 (1 - 65535 | Default : 123)

Manual Time: Year 2000, Month Jan, Day 1; Hour 0, Minute 0, Second 0

Time Zone: None

Daylight Saving Time: Disable

Daylight Saving Time Offset: 60 (1 - 1440) Minutes

Recurring From: Weekday Sun, Week 1, Month Jan; Hour 0, Minute 0

Recurring To: Weekday Sun, Week 1, Month Jan; Hour 0, Minute 0

Non-Recurring From: Year 2000, Month Jan, Date 1; Hour 0, Minute 0

Non-Recurring To: Year 2000, Month Jan, Date 1; Hour 0, Minute 0

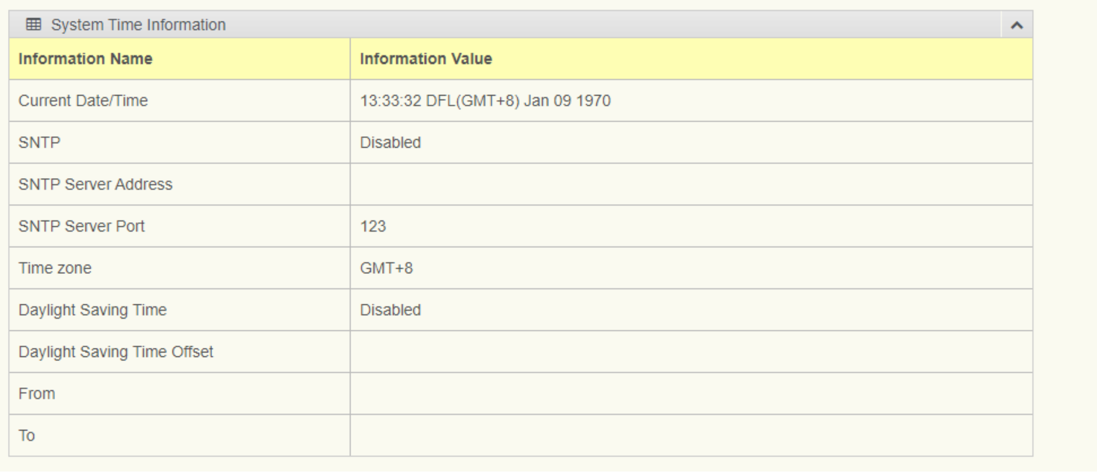
Figure 4.23 System > System Time

The following table describes the items in the previous figure.

Item	Description
Enable SNTP	Click the radio button to enable or disable the SNTP.
SNTP/NTP Server Address	Enter the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
SNTP Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 to 65535 (default: 123).
Manual Time	Click the drop-down menus to set local date and time of the system.
Time Zone	Click the drop-down menu to select a system time zone.

Item	Description
Daylight Saving Time	Click the drop-down menu to enable or disable the daylight saving time settings.
Daylight Saving Time Offset	Enter the offsetting variable in seconds to adjust for daylight saving time.
Recurring From	Click the drop-down menu to designate the start date and time for daylight saving time.
Recurring To	Click the drop-down menu to designate the end date and time for daylight saving time.
Non-Recurring From	Click the drop-down menu to designate a start date and time for a non-recurring daylight saving time event.
Non-Recurring To	Click the drop-down menu to designate the end date and time for a non-recurring daylight saving time event.
Apply	Click **Apply** to save the values and update the screen.

System Time Information settings are informational only as shown in the following:



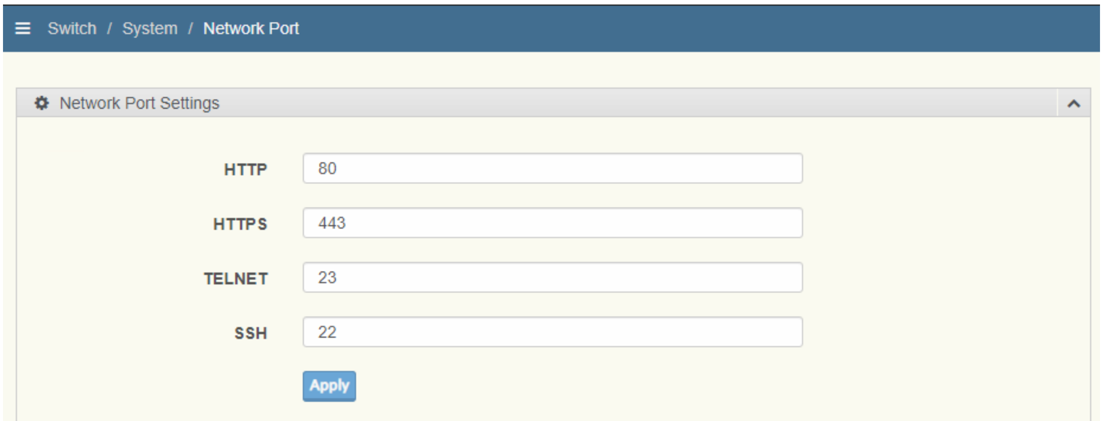
System Time Information

Information Name	Information Value
Current Date/Time	13:33:32 DFL(GMT+8) Jan 09 1970
SNTP	Disabled
SNTP Server Address	
SNTP Server Port	123
Time zone	GMT+8
Daylight Saving Time	Disabled
Daylight Saving Time Offset	
From	
To	

Figure 4.24 System > System Time

4.4.4 Network Port

To access this page, click **System** > **Network Port**.



HTTP 80

HTTPS 443

TELNET 23

SSH 22

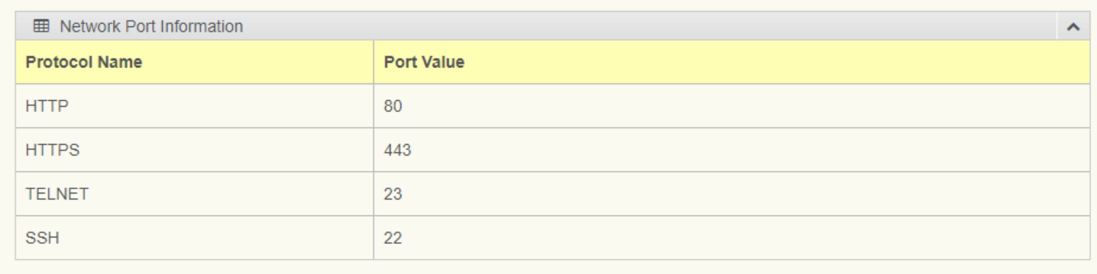
Figure 4.25 System > Network Port

The following table describes the items in the previous figure.

Item	Description
HTTP	Enter the value to designate the port number for the HTTP protocol (default: 80).

Item	Description
HTTPS	Enter the value to designate the port number for the HTTPS protocol (default: 443).
TELNET	Enter the value to designate the port number for the Telnet protocol (default: 23).
SSH	Enter the value to designate the port number for the Secure Shell protocol (default: 22).
Apply	Click **Apply** to save the values and update the screen.

Network Port Information settings are informational only as shown in the following:



Network Port Information

Protocol Name	Port Value
HTTP	80
HTTPS	443
TELNET	23
SSH	22

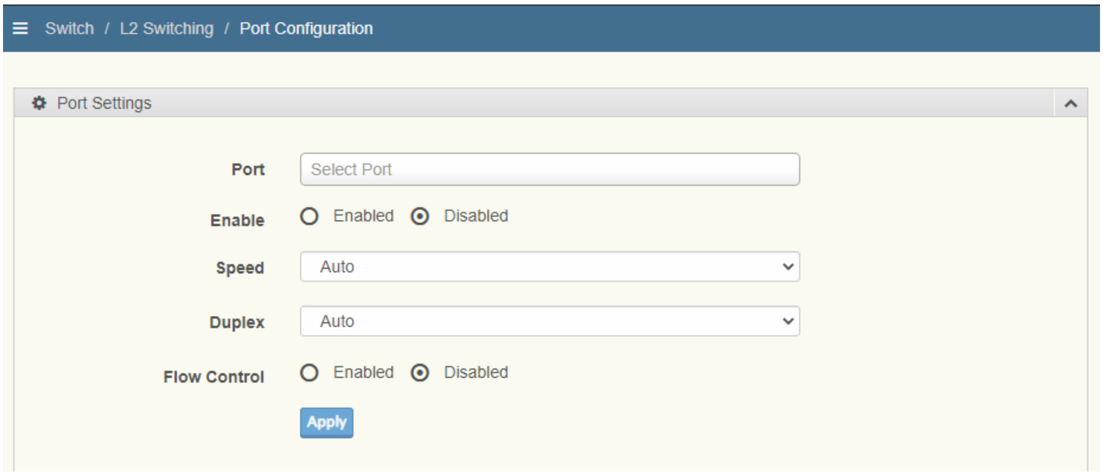
Figure 4.26 System > Network Port

4.5 L2 Switching

4.5.1 Port Configuration

Port Configuration describes how to use the user interface to configure LAN ports on the switch.

To access this page, click **L2 Switching** > **Port Configuration**.



Port: Select Port

Enable: ○ Enabled ● Disabled

Speed: Auto

Duplex: Auto

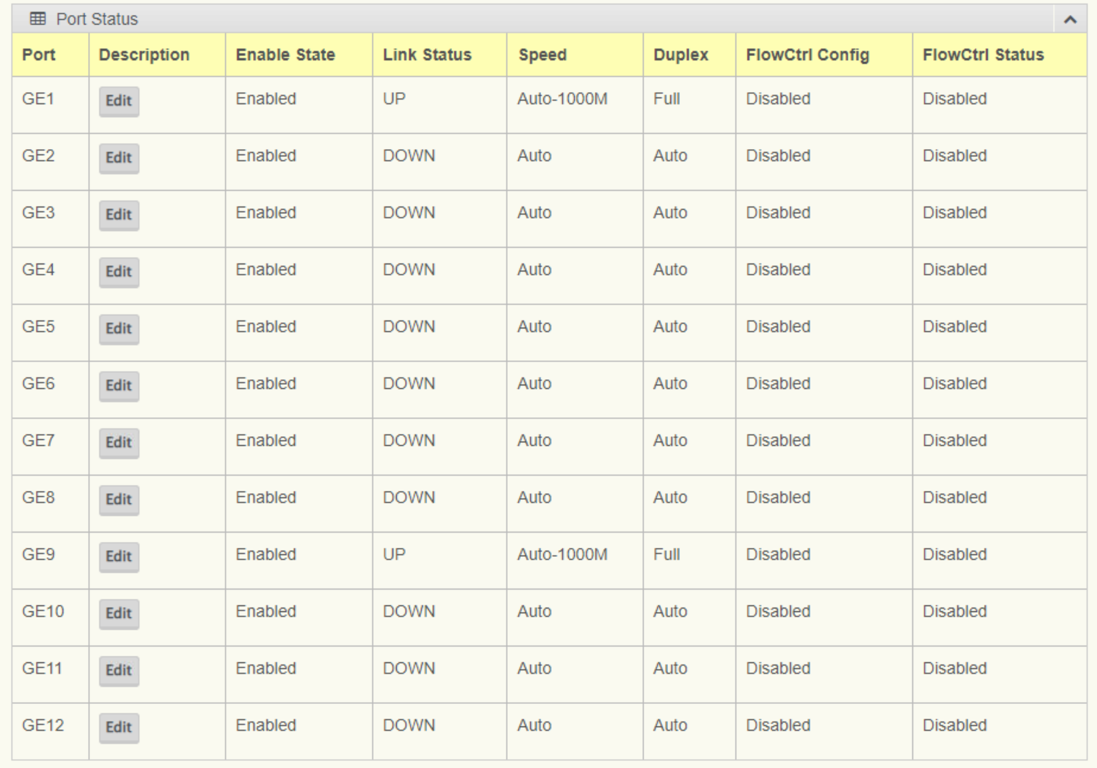
Flow Control: ○ Enabled ● Disabled

Figure 4.27 L2 Switching > Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port for the L2 Switch setting (GE1 to GE8).
Enabled	Click the radio-button to enable or disable the Port Setting function.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Duplex	Click the drop-down menu to select the duplex setting: Half or Full.
Flow Control	Click the radio button to enable or disable the flow control function.
Apply	Click **Apply** to save the values and update the screen.

Port Status settings are informational only as shown in the following:



Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	UP	Auto-1000M	Full	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE9	Edit	Enabled	UP	Auto-1000M	Full	Disabled	Disabled
GE10	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE11	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE12	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

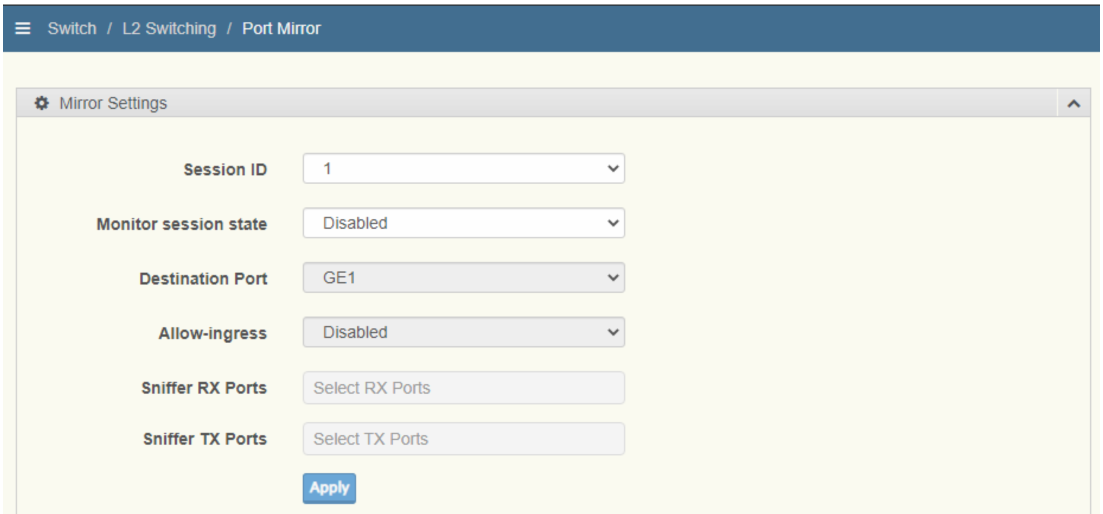
Figure 4.28 L2 Switching > Port Configuration

4.5.2 Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data or diagnose errors on a network or to mirror either inbound or outbound traffic (or both).

There are no preset values in the Port Mirror. The displayed values do not represent the actual setting values.

To access this page, click **L2 Switching** > **Port Mirror**.



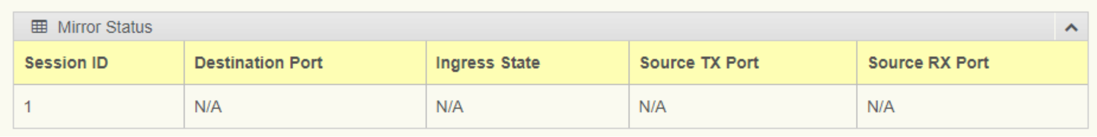
Session ID	1
Monitor session state	Disabled
Destination Port	GE1
Allow-ingress	Disabled
Sniffer RX Ports	Select RX Ports
Sniffer TX Ports	Select TX Ports

Figure 4.29 L2 Switching > Port Mirror

The following table describes the items in the previous figure.

Item	Description
Session ID	Click the drop-down menu to select a port mirroring session from the list. The number of sessions allowed is platform specific.
Monitor session state	Click the drop-down menu to enable or disable the session mode for a selected session ID.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s).
Allow-ingress	Click the drop-down menu to enable or disable the Allow-ingress function.
Sniffer RX Ports	Enter the variable to define the RX port.
Sniffer TX Ports	Enter the variable to define the TX port.
Apply	Click **Apply** to save the values and update the screen.

Mirror Status settings are informational only as shown in the following:


Mirror Status

Session ID	Destination Port	Ingress State	Source TX Port	Source RX Port
1	N/A	N/A	N/A	N/A

Figure 4.30 L2 Switching > Port Mirror

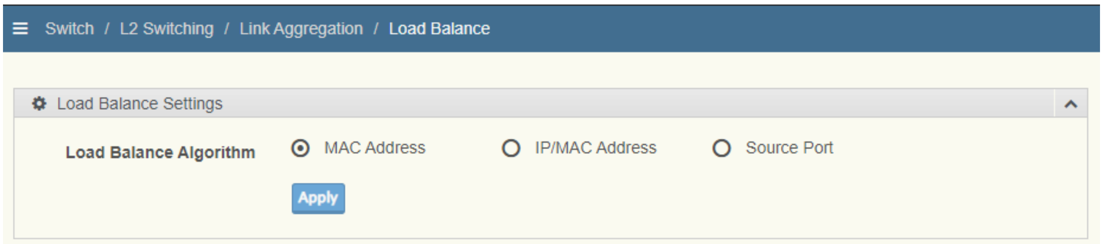
4.5.3 Link Aggregation

Link Aggregation is a method for combining multiple network connections in parallel in order to increase throughput beyond the capability of a single connection, and to provide redundancy in case one of the links should fail.

4.5.3.1 Load Balance

The Load Balancing page allows you to select between a MAC Address or IP/MAC Address algorithm for the even distribution of IP traffic across two or more links.

To access this page, click **L2 Switching** > **Link Aggregation** > **Load Balance**.


Switch / L2 Switching / Link Aggregation / Load Balance

Load Balance Settings

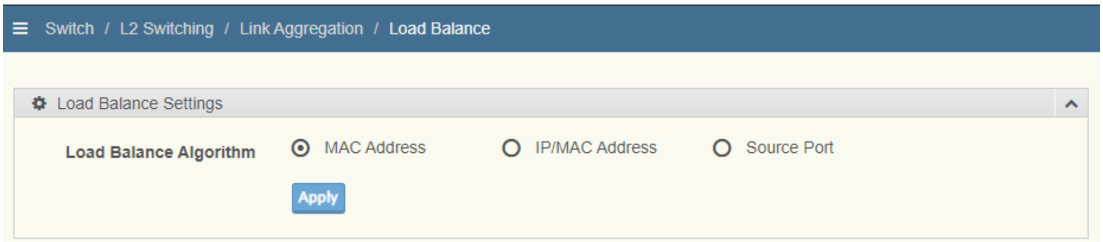
Load Balance Algorithm ● MAC Address ○ IP/MAC Address ○ Source Port

Figure 4.31 L2 Switching > Link Aggregation > Load Balance

The following table describes the items in the previous figure.

Item	Description
Load Balance Algorithm	Select the radio button to select the Load Balance Setting: MAC Address, IP/MAC Address, or Source Port.
Apply	Click **Apply** to save the values and update the screen.

Load Balance Information settings are informational only as shown in the following:



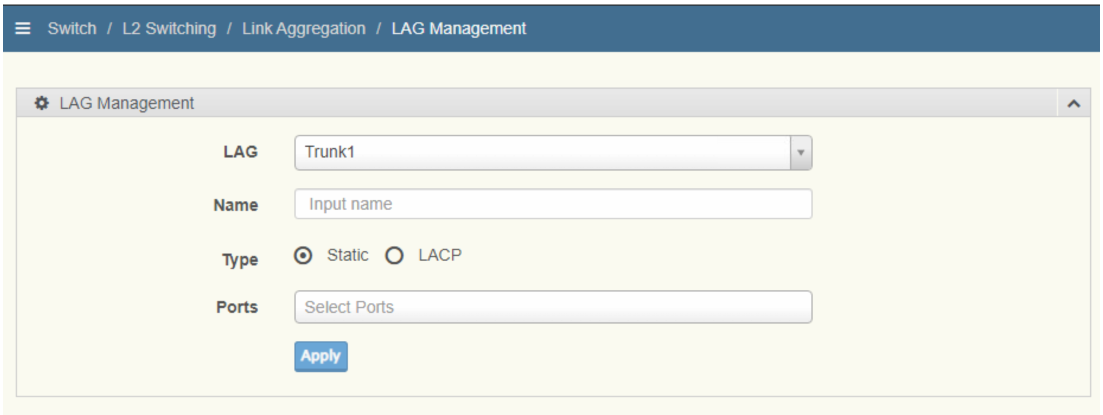
Load Balance Algorithm ● MAC Address ○ IP/MAC Address ○ Source Port

Figure 4.32 L2 Switching > Link Aggregation > Load Balance

4.5.3.2 LAG Management

Link aggregation is also known as trunking. It is a feature available on the Ethernet gateway and is used with Layer 2 Bridging. Link aggregation allows for the logical merging of multiple ports into a single link.

To access this page, click **L2 Switching** > **Link Aggregation** > **LAG Management**.



LAG: Trunk1

Name: Input name

Type: ● Static ○ LACP

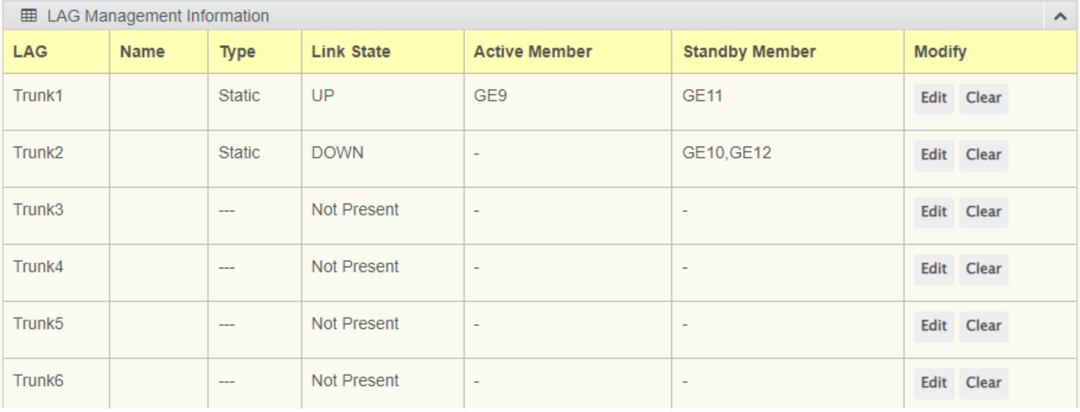
Ports: Select Ports

Figure 4.33 L2 Switching > Link Aggregation > LAG Management

The following table describes the items in the previous figure.

Item	Description
LAG	Click the drop-down menu to select the designated trunk group: Trunk 1 ~8.
Name	Enter an entry to specify the LAG name.
Type	Click the radio button to specify the type mode: Static or LACP.
Ports	Click the drop-down menu to select the designated ports: FE1-8 or GE1-2.
Apply	Click **Apply** to save the values and update the screen.

LAG Management Information settings are informational only as shown in the following:



LAG	Name	Type	Link State	Active Member	Standby Member	Modify
Trunk1		Static	UP	GE9	GE11	Edit Clear
Trunk2		Static	DOWN	-	GE10,GE12	Edit Clear
Trunk3		---	Not Present	-	-	Edit Clear
Trunk4		---	Not Present	-	-	Edit Clear
Trunk5		---	Not Present	-	-	Edit Clear
Trunk6		---	Not Present	-	-	Edit Clear

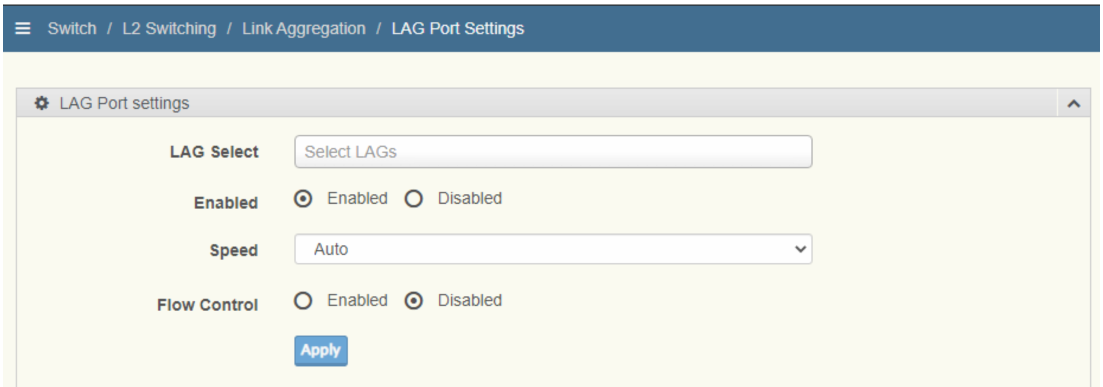
Figure 4.34 L2 Switching > Link Aggregation > LAG Management

4.5.3.3 LAG Port Settings

The LAG Port Settings page allows you to enable or disable, set LAG status, speed and flow control functions.

In this example we will configure a LAG between the following switches:

To access this page, click **L2 Switching** > **Link Aggregation** > **LAG Port Settings**.



≡ Switch / L2 Switching / Link Aggregation / LAG Port Settings

LAG Port settings

LAG Select: Select LAGs

Enabled: ● Enabled ○ Disabled

Speed: Auto

Flow Control: ○ Enabled ● Disabled

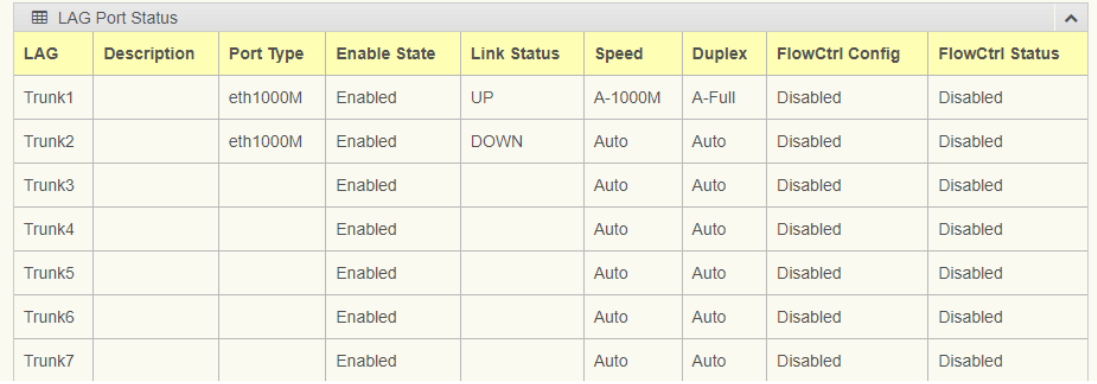
Apply

Figure 4.35 L2 Switching > Link Aggregation > LAG Port Settings

The following table describes the items in the previous figure.

Item	Description
LAG Select	Click the drop-down menu to select a predefined LAG trunk definition: LAG 1-8.
Enabled	Click the radio button to enable or disable the LAG Port.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Flow Control	Click the radio button to enable or disable the Flow Control for the LAG Port.
Apply	Click **Apply** to save the values and update the screen.

LAG Port Status settings are informational only as shown in the following:



LAG Port Status

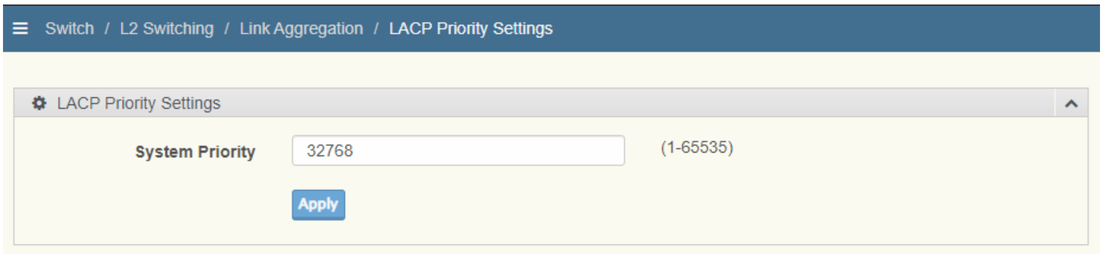
LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
Trunk1		eth1000M	Enabled	UP	A-1000M	A-Full	Disabled	Disabled
Trunk2		eth1000M	Enabled	DOWN	Auto	Auto	Disabled	Disabled
Trunk3			Enabled		Auto	Auto	Disabled	Disabled
Trunk4			Enabled		Auto	Auto	Disabled	Disabled
Trunk5			Enabled		Auto	Auto	Disabled	Disabled
Trunk6			Enabled		Auto	Auto	Disabled	Disabled
Trunk7			Enabled		Auto	Auto	Disabled	Disabled

Figure 4.36 L2 Switching > Link Aggregation > LAG Port Settings

4.5.3.4 LACP Priority Settings

The LACP Priority Settings page allows you to configure the system priority for LACP.

To access this page, click **L2 Switching** > **Link Aggregation** > **LACP Priority Settings**.



≡ Switch / L2 Switching / Link Aggregation / LACP Priority Settings

LACP Priority Settings

System Priority: 32768 (1-65535)

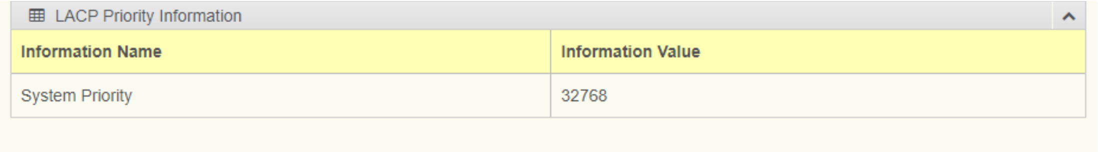
Apply

Figure 4.37 L2 Switching > Link Aggregation > LACP Priority Settings

The following table describes the items in the previous figure.

Item	Description
System Priority	Enter the value (1-65535) to designate the LACP system priority.
Apply	Click **Apply** to save the values and update the screen.

LACP Information settings are informational only as shown in the following:



LACP Priority Information

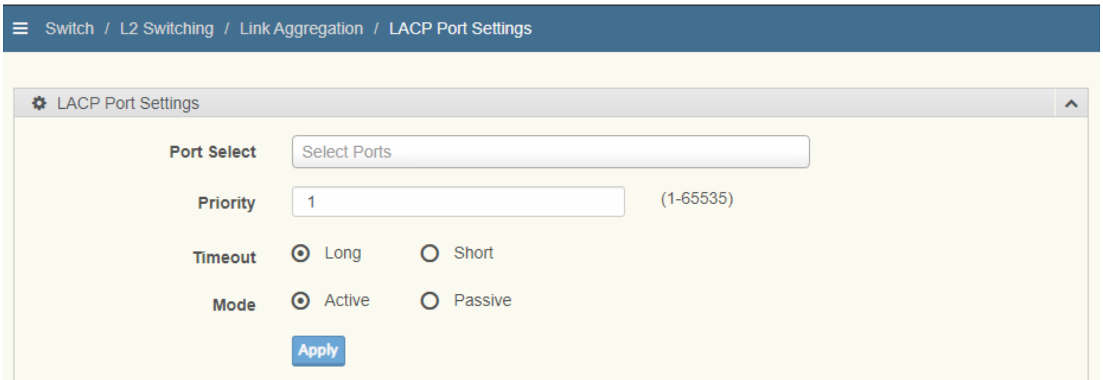
Information Name	Information Value
System Priority	32768

Figure 4.38 L2 Switching > Link Aggregation > LACP Priority Settings

4.5.3.5 LACP Port Settings

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. By configuring the LACP function, the switch can negotiate an automatic bundling of links by sending LACP packets to the peer device (also implementing LACP).

To access this page, click **L2 Switching** > **Link Aggregation** > **LACP Port Settings**.



≡ Switch / L2 Switching / Link Aggregation / LACP Port Settings

LACP Port Settings

Port Select: Select Ports

Priority: 1 (1-65535)

Timeout: ● Long ○ Short

Mode: ● Active ○ Passive

Apply

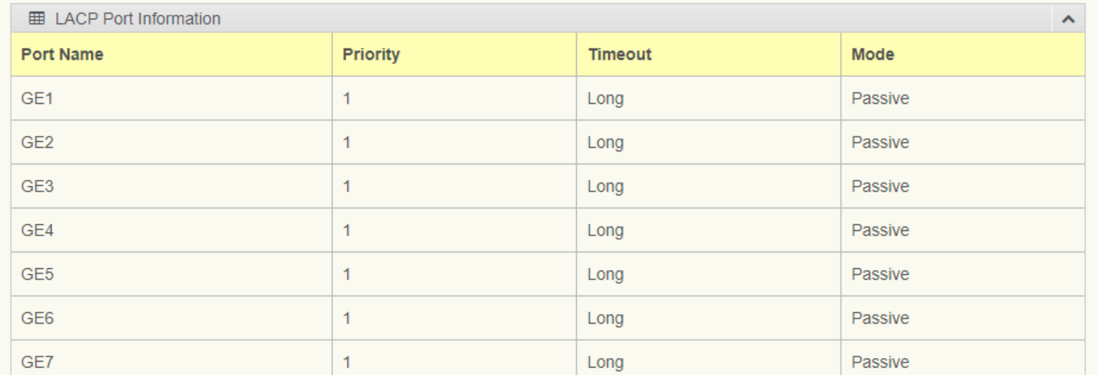
Figure 4.39 L2 Switching > Link Aggregation > LACP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select a port for the LACP Port Settings. The listed available settings are: FE1-FE8, GE1-GE2. However, the available settings are dependent on the connected LACP device and may not be listed as displayed in the current figure.
Priority	Enter a variable (1 to 65535) to assign a priority to the defined port selection.
Timeout	Click the radio button to select a long or short timeout period.

Item	Description
Mode	Click the radio button to select the setting mode: Active or Passive. ■ Active: Enables LACP unconditionally. ■ Passive: Enables LACP only when an LACP device is detected (default state).
Apply	Click **Apply** to save the values and update the screen.

LACP Port Information settings are informational only as shown in the following:



LACP Port Information

Port Name	Priority	Timeout	Mode
GE1	1	Long	Passive
GE2	1	Long	Passive
GE3	1	Long	Passive
GE4	1	Long	Passive
GE5	1	Long	Passive
GE6	1	Long	Passive
GE7	1	Long	Passive

Figure 4.40 L2 Switching > Link Aggregation > LACP Port Settings

4.5.4 802.1Q VLAN

The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

The 802.1Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned following the AP group, while the inner VLAN ID is assigned dynamically by the AAA server.

4.5.4.1 VLAN Management

The management of VLANs is available through the VLAN Settings page. Through this page you can add or delete VLAN listings and add a prefix name to an added entry.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **VLAN Management**.

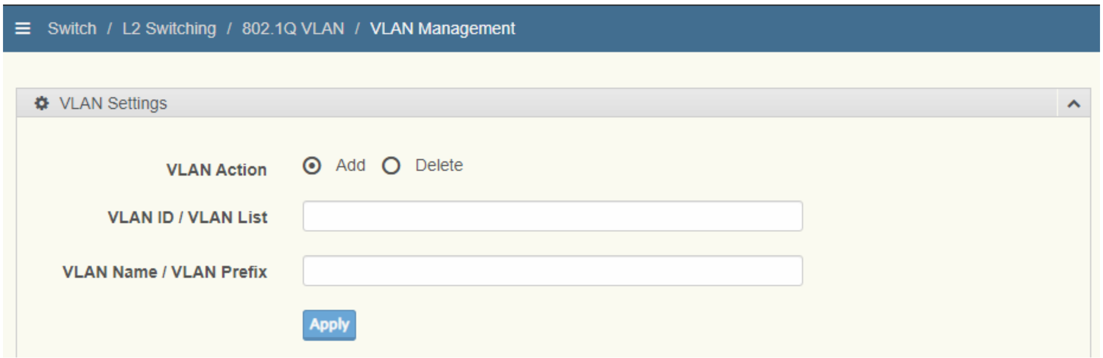
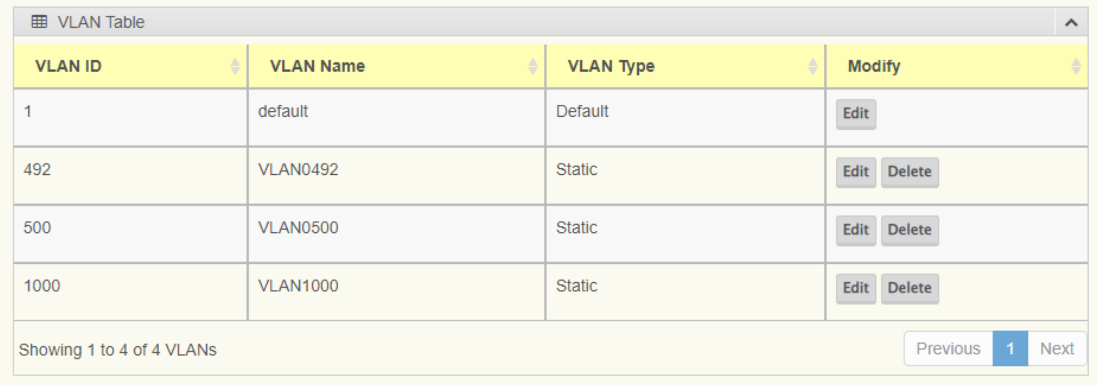


Figure 4.41 L2 Switching > 802.1Q VLAN > VLAN Management

The following table describes the items in the previous figure.

Item	Description
VLAN Action	Click the radio button to add or delete the VLAN entry (VLAN ID or VLAN list) designated in the following field.
VLAN ID / List	Enter the name of the VLAN entry to setup.
VLAN Name / Prefix	Enter the prefix to be used by the VLAN list entry in the previous field.
Apply	Click **Apply** to save the values and update the screen.

VLAN Table settings are described in the following:



VLAN Table

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit
492	VLAN0492	Static	Edit Delete
500	VLAN0500	Static	Edit Delete
1000	VLAN1000	Static	Edit Delete

Showing 1 to 4 of 4 VLANs

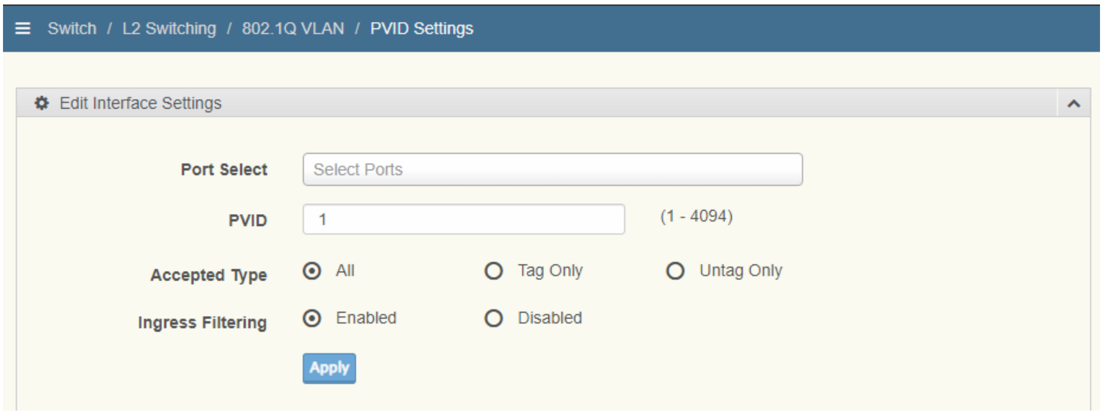
Figure 4.42 L2 Switching > 802.1Q VLAN > VLAN Management

Item	Description
Edit	Click **Edit** to modify the VLAN entry.
Delete	Click **Delete** to remove the VLAN entry.
Previous	Click **Previous** to scroll to the page occurring in the previous table.
Next	Click **Next** to scroll to the page occurring in the following table.

4.5.4.2 PVID Settings

The PVID Settings page allows you to designate a PVID for a selected port, define the accepted type and enable/disable the ingress filtering.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **PVID Settings**.



Port Select: Select Ports

PVID: 1 (1 - 4094)

Accepted Type: ● All ○ Tag Only ○ Untag Only

Ingress Filtering: ● Enabled ○ Disabled

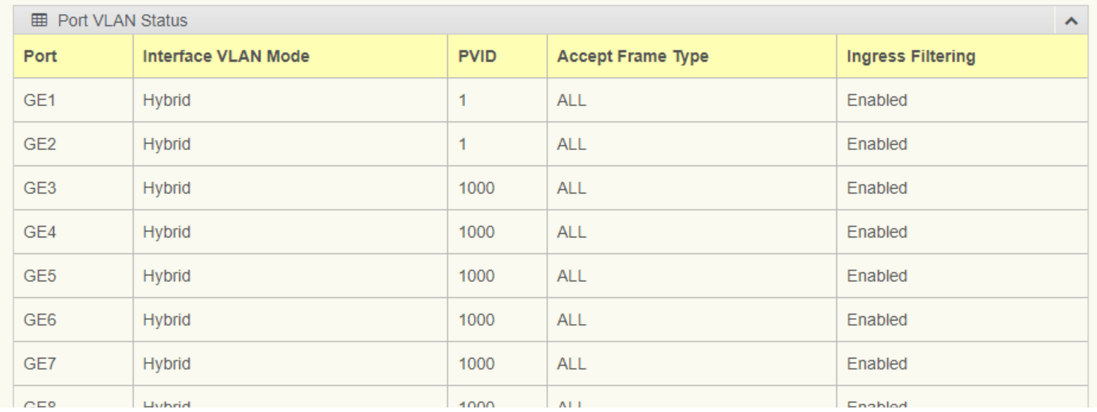
Figure 4.43 L2 Switching > 802.1Q VLAN > PVID Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a port and edit its settings: FE1-FE8, GE1-GE2, or Trunk1 - Trunk8.
PVID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. Range: 1 to 4094, default 1.
Accepted Type	Click the radio button to specify which frames to forward. Tag Only discards any untagged or priority tagged frames. Untag Only discards any tagged frames. All accepts all untagged and tagged frames. Whichever you select, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. Default: All.

Item	Description
Ingress Filtering	Click the radio button to specify how you want the port to handle tagged frames. If you enable Ingress Filtering, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select Disabled, all tagged frames will be accepted. Default: Disabled.
Apply	Click **Apply** to save the values and update the screen.

Port VLAN Status settings are informational only as shown in the following:



Port VLAN Status

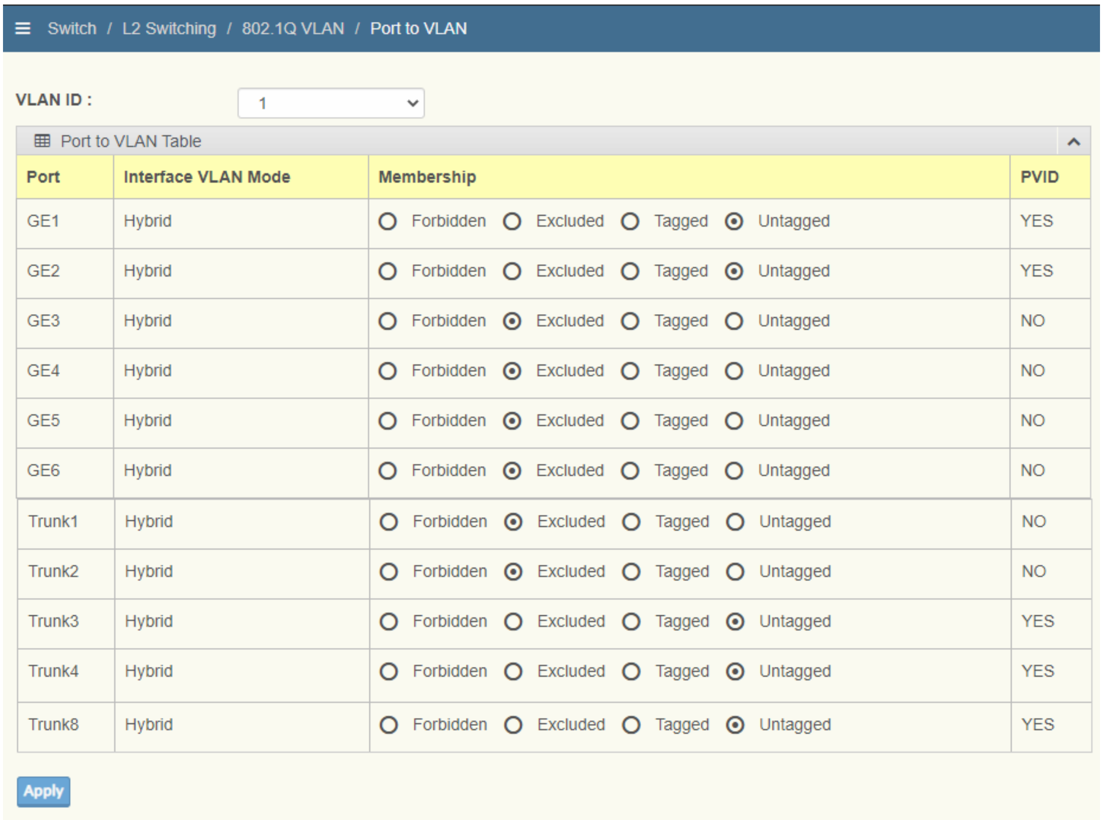
Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering
GE1	Hybrid	1	ALL	Enabled
GE2	Hybrid	1	ALL	Enabled
GE3	Hybrid	1000	ALL	Enabled
GE4	Hybrid	1000	ALL	Enabled
GE5	Hybrid	1000	ALL	Enabled
GE6	Hybrid	1000	ALL	Enabled
GE7	Hybrid	1000	ALL	Enabled
GE8	Hybrid	1000	ALL	Enabled

Figure 4.44 L2 Switching > 802.1Q VLAN > PVID Settings

4.5.4.3 Port to VLAN

The Port to VLAN page allows you to add a port to a VLAN and select the related parameters.

To access this page, click **L2 Switching** > **802.1Q VLAN** > **Port to VLAN**.



VLAN ID : 1

Port to VLAN Table

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE2	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
GE3	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE4	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE5	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
GE6	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk1	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk2	Hybrid	○ Forbidden ● Excluded ○ Tagged ○ Untagged	NO
Trunk3	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
Trunk4	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES
Trunk8	Hybrid	○ Forbidden ○ Excluded ○ Tagged ● Untagged	YES

Figure 4.45 L2 Switching > 802.1Q VLAN > Port to VLAN

The following table describes the items in the previous figure.

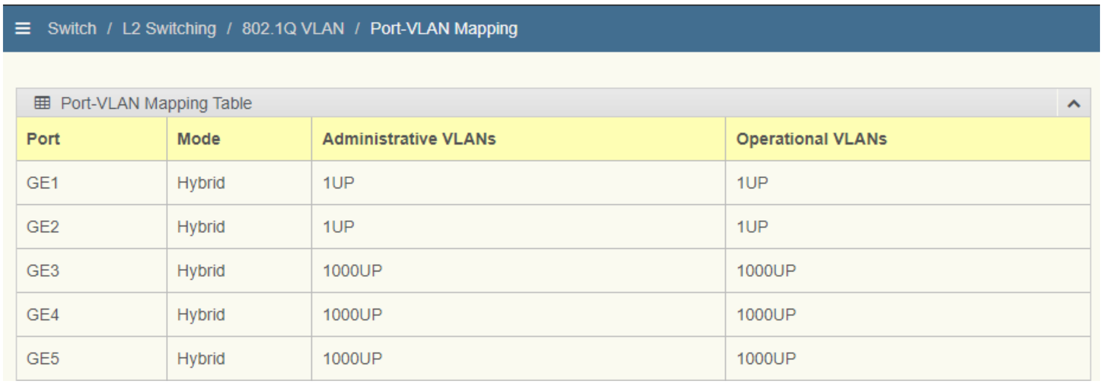
Item	Description
Port	Displays the assigned port to the entry.
Interface VLAN Mode	Displays the assigned mode to the listed VLAN port. ■ Hybrid: Port hybrid model. ■ Access: Port hybrid model. ■ Trunk: Port hybrid model. ■ Tunnel: Port hybrid model.
Membership	Displays the assigned membership status of the port entry, options include: Forbidden, Excluded Tagged or Untagged.
Apply	Click **Apply** to save the values and update the screen.

Note! *The previous figure was modified for instructional purposes.*

4.5.4.4 Port-VLAN Mapping

To access this page, click **L2 Switching** > **802.1Q VLAN** > **Port-VLAN Mapping**.

Port VLAN Status settings are informational only as shown in the following:

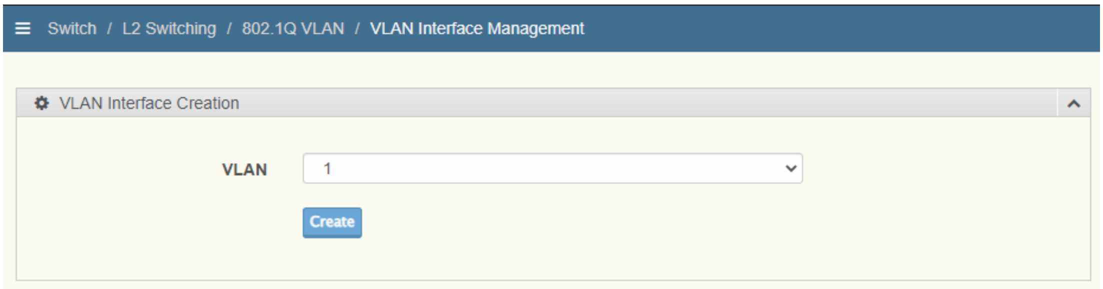


Port	Mode	Administrative VLANs	Operational VLANs
GE1	Hybrid	1UP	1UP
GE2	Hybrid	1UP	1UP
GE3	Hybrid	1000UP	1000UP
GE4	Hybrid	1000UP	1000UP
GE5	Hybrid	1000UP	1000UP

Figure 4.46 L2 Switching > 802.1Q VLAN > Port-VLAN Mapping

4.5.4.5 VLAN Interface Management

To access this page, click **L2 Switching** > **802.1Q VLAN** > **VLAN Interface Management**.


≡ Switch / L2 Switching / 802.1Q VLAN / VLAN Interface Management
VLAN Interface Creation
Create

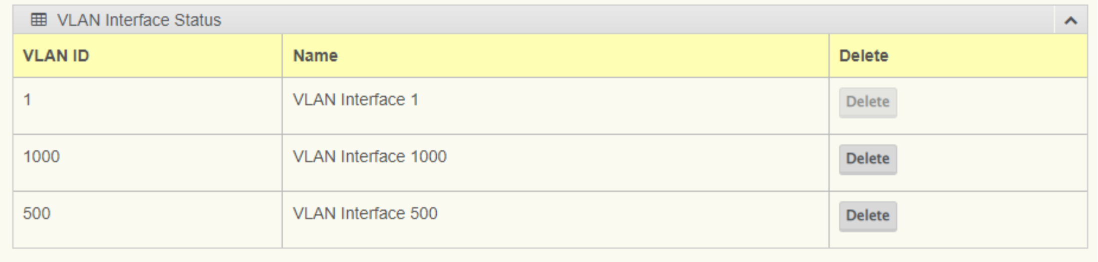
VLAN 1

Figure 4.47 L2 Switching > 802.1Q VLAN > VLAN Interface Management

The following table describes the items in the previous figure.

Item	Description
VLAN	Click the drop-down menu to select an existing VLAN to access the management capabilities of the device. Note: A VLAN interface must already exist to be available in the VLAN Interface Creation option.
Create	Click **Create** to create a new VLAN interface.

VLAN Interface Status settings are informational only as shown in the following:



VLAN Interface Status

VLAN ID	Name	Delete
1	VLAN Interface 1	Delete
1000	VLAN Interface 1000	Delete
500	VLAN Interface 500	Delete

Figure 4.48 L2 Switching > 802.1Q VLAN > VLAN Interface Management

4.5.5 Q-in-Q

Q-in-Q is commonly referred as VLAN stacking in which VLANs are nested by adding two tags to each frame instead of one. Network service provider and users both can use VLANs and makes it possible to have more than the 4094 separate VLANs allowed by 802.1Q.

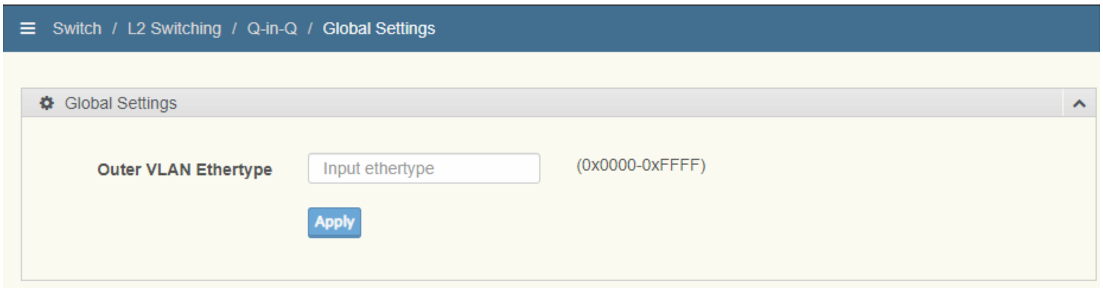
There are three ways in which a machine can be connected to a network carrying double-tagged 802.1ad traffic:

- via a untagged port, where both inner and outer VLANs are handled by the switch or switches (so the attached machine sees ordinary Ethernet frames);
- via a single-tagged (tunnel) port, where the outer VLAN only is handled by the switch (so the attached machine sees single-tagged 802.1Q VLAN frames); or
- via a double-tagged (trunk) port, where both inner and outer VLANs are handled by the attached machine (which sees double-tagged 802.1ad VLAN frames).

4.5.5.1 Global Settings

The Global Settings page allows you to set the outer VLAN Ethertype setting.

To access this page, click **L2 Switching** > **Q-in-Q** > **Global Settings**.



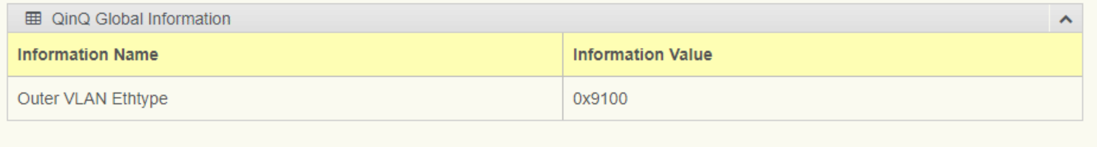
Outer VLAN Ethertype: Input ethertype (0x0000-0xFFFF)

Figure 4.49 L2 Switching > Q-in-Q > Global Settings

The following table describes the items in the previous figure.

Item	Description
Outer VLAN Ethertype	Enter the outer VLAN handled by the switch giving the attached machine a single-tagged 802.1Q VLAN frame.
Apply	Click **Apply** to save the values and update the screen.

QinQ Global Information settings are informational only as shown in the following:



QinQ Global Information

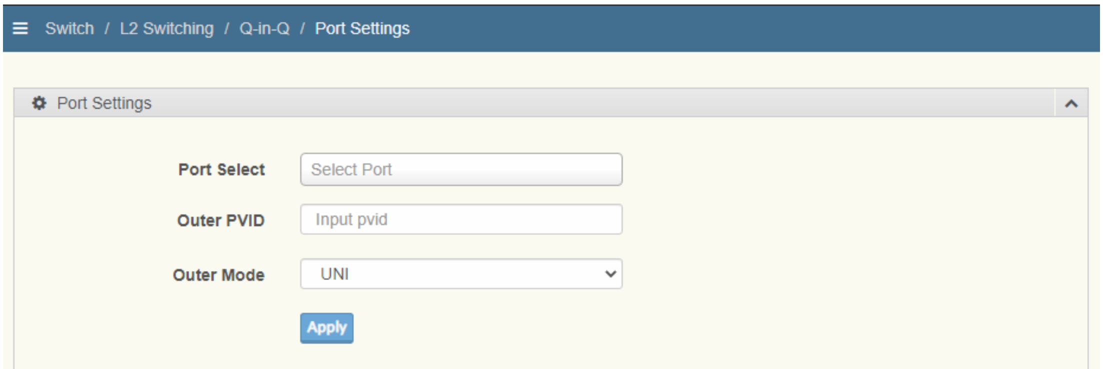
Information Name	Information Value
Outer VLAN Ethtype	0x9100

Figure 4.50 L2 Switching > Q-in-Q > Global Settings

4.5.5.2 Port Settings

The Port Settings page allows you to define the outer PVID and outer mode for a selected port.

To access this page, click **L2 Switching** > **Q-in-Q** > **Port Settings**.



Port Select: Select Port

Outer PVID: Input pvid

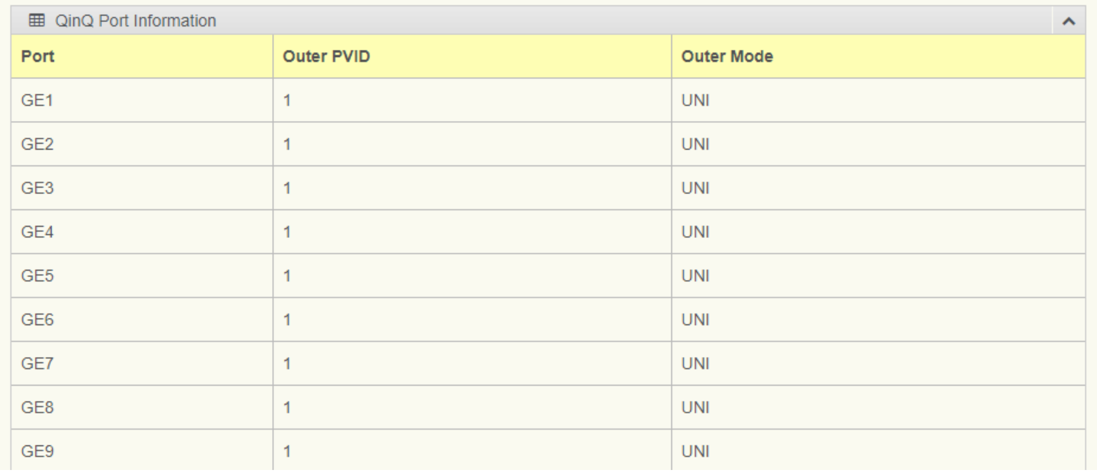
Outer Mode: UNI

Figure 4.51 L2 Switching > Q-in-Q > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the switch port (part of VLAN configuration) to configure the selection as a tunnel port.
Outer PVID	Enter the Port VLAN ID (PVID) to assigned the native VLAN ID. All untagged traffic coming in or out of the 802.1Q port is forwarded based on the PVID value
Outer Mode	Click the drop-down menu to select between UNI or NNI role. ■ UNI: Selects a user-network interface which specifies communication between the specified user and a specified network. ■ NNI: Selects a network-to-network interface which specifies communication between two specified networks.
Apply	Click **Apply** to save the values and update the screen.

QinQ Port Information settings are informational only as shown in the following:



QinQ Port Information

Port	Outer PVID	Outer Mode
GE1	1	UNI
GE2	1	UNI
GE3	1	UNI
GE4	1	UNI
GE5	1	UNI
GE6	1	UNI
GE7	1	UNI
GE8	1	UNI
GE9	1	UNI

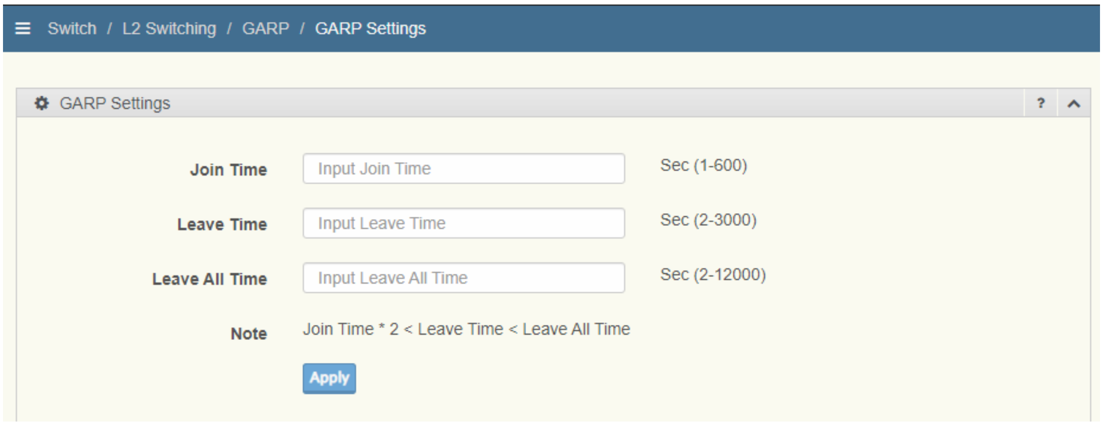
Figure 4.52 L2 Switching > Q-in-Q > Port Settings

4.5.6 GARP

The Generic Attribute Registration Protocol (GARP) is a local area network (LAN) protocol. The protocol defines procedures for the registration and de-registration of attributes (network identifiers or addresses) by end stations and switches with each other.

4.5.6.1 GARP Settings

To access this page, click **L2 Switching** > **GARP** > **GARP Settings**.



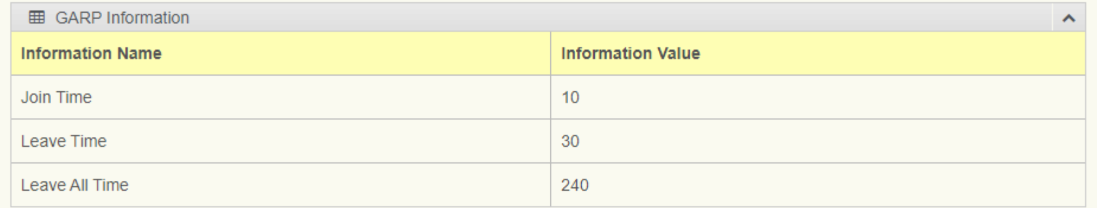
Join Time	Input Join Time	Sec (1-600)
Leave Time	Input Leave Time	Sec (2-3000)
Leave All Time	Input Leave All Time	Sec (2-12000)
Note	Join Time * 2 < Leave Time < Leave All Time	

Figure 4.53 L2 Switching > GARP > GARP Settings

The following table describes the items in the previous figure.

Item	Description
Join Time	Enter a value to specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 6 and 600. An instance of this timer exists for each GARP participant for each port.
Leave Time	Enter a value to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 12 and 3000. An instance of this timer exists for each GARP participant for each port.
Leave All Time	Enter a value to specify the Leave All Time controls how frequently Leave All PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 12 and 12000. An instance of this timer exists for each GARP participant for each port.
Apply	Click **Apply** to save the values and update the screen.

GARP Information settings are informational only as shown in the following:



GARP Information

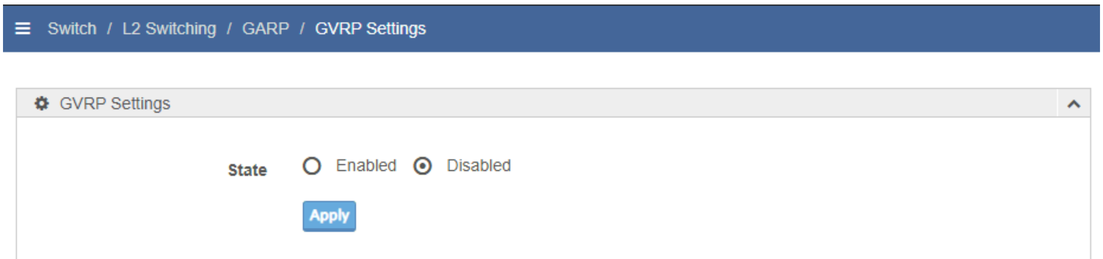
Information Name	Information Value
Join Time	10
Leave Time	30
Leave All Time	240

Figure 4.54 L2 Switching > GARP > GARP Settings

4.5.6.2 GVRP Settings

The GVRP Settings page allows you to enable or disable the GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) protocol which facilitates control of virtual local area networks (VLANs) within a larger network.

To access this page, click **L2 Switching** > **GARP** > **GVRP Settings**.



Switch / L2 Switching / GARP / GVRP Settings

GVRP Settings

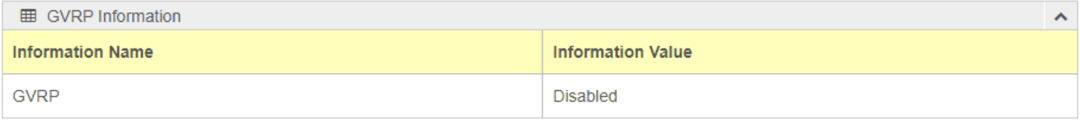
State ○ Enabled ● Disabled

Figure 4.55 L2 Switching > GARP > GVRP Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click to enable or disable the GARP VLAN Registration Protocol administrative mode for the switch. The factory default is Disable.
Apply	Click **Apply** to save the values and update the screen.

GVRP Information settings are informational only as shown in the following:



GVRP Information

Information Name	Information Value
GVRP	Disabled

Figure 4.56 L2 Switching > GARP > GVRP Settings

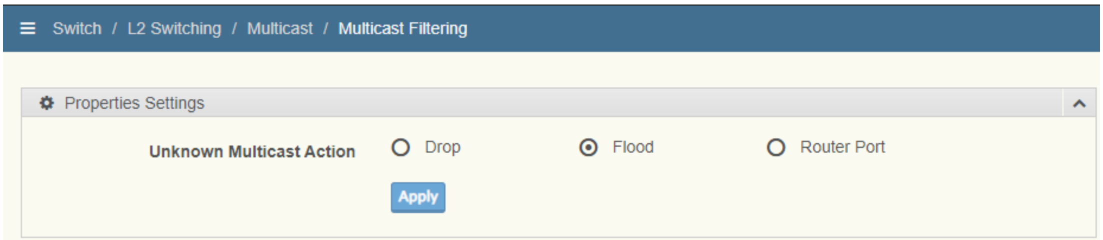
4.5.7 Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

4.5.7.1 Multicast Filtering

The Multicast Filtering page allows for the definition of action settings when an unknown multicast request is received. The options include: Drop, Flood, or Router Port.

To access this page, click **L2 Switching** > **Multicast** > **Multicast Filtering**.



Switch / L2 Switching / Multicast / Multicast Filtering

Properties Settings

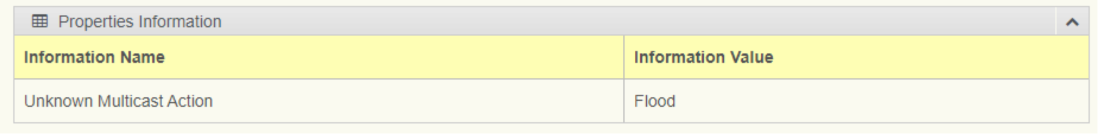
Unknown Multicast Action ○ Drop ● Flood ○ Router Port

Figure 4.57 L2 Switching > Multicast > Multicast Filtering

The following table describes the items in the previous figure.

Item	Description
Unknown Multicast Action	Select the configuration protocol: Drop, Flood, or Router Port, to apply for any unknown multicast event.
Apply	Click **Apply** to save the values and update the screen.

Properties Information settings are informational only as shown in the following:



Properties Information

Information Name	Information Value
Unknown Multicast Action	Flood

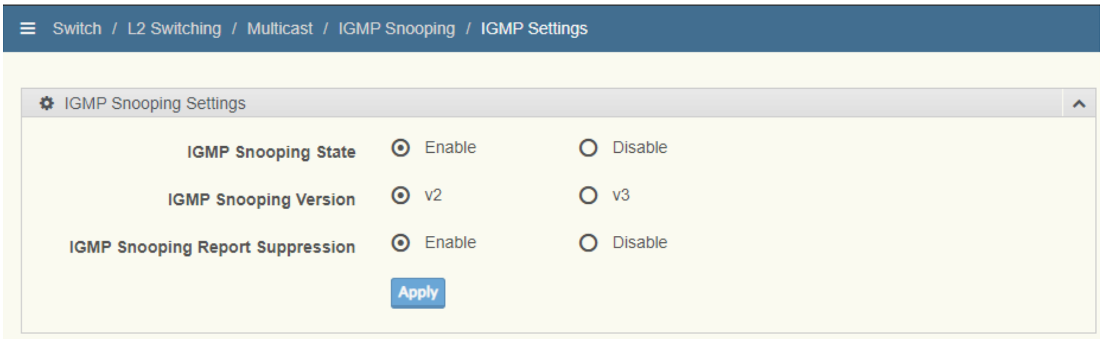
Figure 4.58 L2 Switching > Multicast > Multicast Filtering

4.5.7.2 IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast streams. Multicasts can be filtered from the links which do not need them in turn controlling which ports receive specific multicast traffic.

4.5.7.2.1 IGMP Settings

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Settings**.



Switch / L2 Switching / Multicast / IGMP Snooping / IGMP Settings

IGMP Snooping Settings

IGMP Snooping State ● Enable ○ Disable

IGMP Snooping Version ● v2 ○ v3

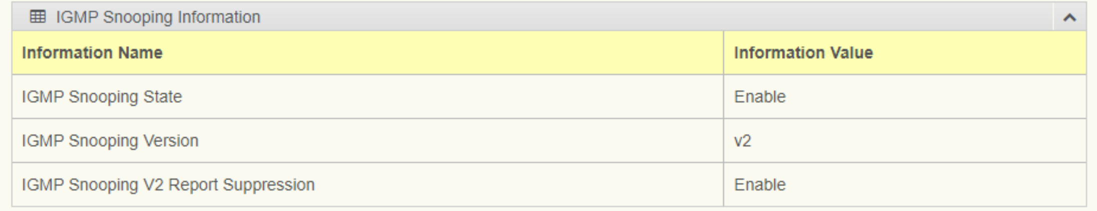
IGMP Snooping Report Suppression ● Enable ○ Disable

Figure 4.59 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The following table describes the items in the previous figure.

Item	Description
IGMP Snooping State	Select **Enable** or **Disable** to designate the IGMP Snooping State.
IGMP Snooping Version	Select designate the IGMP Snooping Version: V2 or V3.
IGMP Snooping Report Suppression	Select **Enable** or **Disable** to setup the report suppression for IGMP Snooping.
Apply	Click **Apply** to save the values and update the screen.

IGMP Snooping Information settings are informational only as shown in the following:

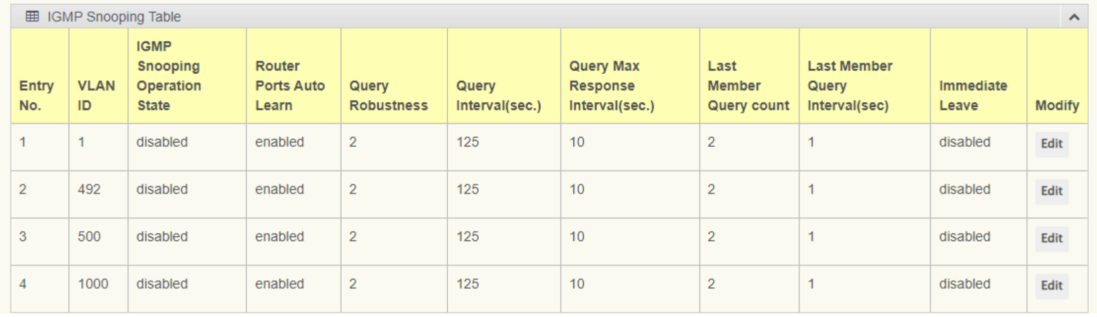


IGMP Snooping Information

Information Name	Information Value
IGMP Snooping State	Enable
IGMP Snooping Version	v2
IGMP Snooping V2 Report Suppression	Enable

Figure 4.60 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

IGMP Snooping Table settings are shown in the following:



IGMP Snooping Table

Entry No.	VLAN ID	IGMP Snooping Operation State	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	disabled	enabled	2	125	10	2	1	disabled	Edit
2	492	disabled	enabled	2	125	10	2	1	disabled	Edit
3	500	disabled	enabled	2	125	10	2	1	disabled	Edit
4	1000	disabled	enabled	2	125	10	2	1	disabled	Edit

Figure 4.61 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

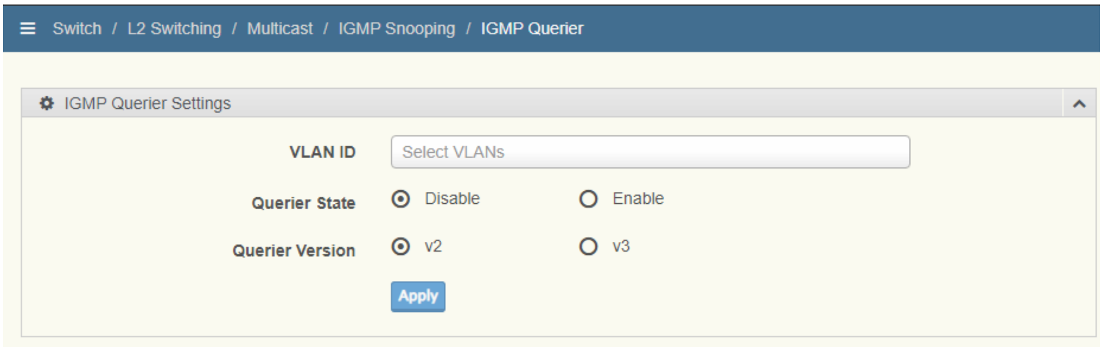
The following table describes the items in the previous figure.

Item	Description
Edit	Click Edit to modify the Snooping table entry.

4.5.7.2.2 *IGMP Querier*

IGMP Querier allows snooping to function by creating the tables for snooping. General queries must be unconditionally forwarded by all switches involved in IGMP snooping.

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Querier**.



☰ Switch / L2 Switching / Multicast / IGMP Snooping / IGMP Querier

IGMP Querier Settings

VLAN ID: Select VLANs

Querier State: ● Disable ○ Enable

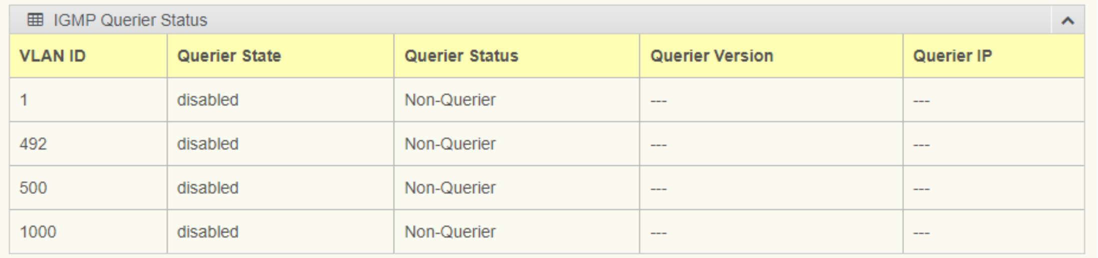
Querier Version: ● v2 ○ v3

Figure 4.62 L2 Switching > Multicast > IGMP Snooping > IGMP Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define the local IGMP querier.
Querier State	Select **Disable** or **Enable** to configure the VLAN ID (IGMP Querier).
Querier Version	Select the querier version (V2 or V3) designated to the selected VLAN ID.
Apply	Click **Apply** to save the values and update the screen.

IGMP Querier Status settings are shown in the following:

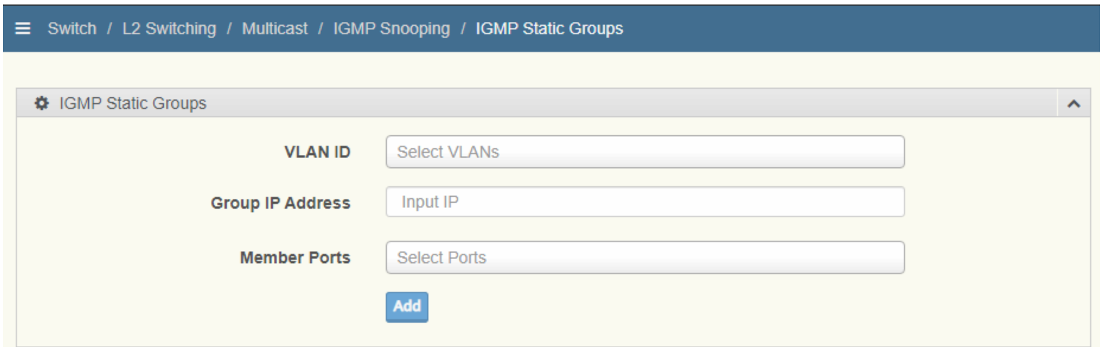


IGMP Querier Status

VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	disabled	Non-Querier	---	---
492	disabled	Non-Querier	---	---
500	disabled	Non-Querier	---	---
1000	disabled	Non-Querier	---	---

4.5.7.2.3 IGMP Static Groups

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **IGMP Static** Groups.



Switch / L2 Switching / Multicast / IGMP Snooping / IGMP Static Groups

IGMP Static Groups

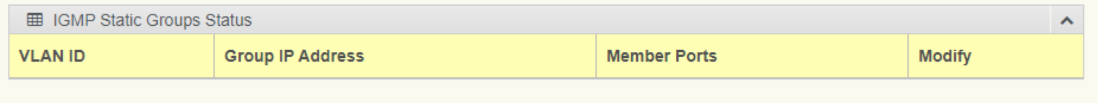
VLAN ID	Select VLANs
Group IP Address	Input IP
Member Ports	Select Ports

Figure 4.63 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define IGMP static group.
Group IP Address	Enter the IP address assigned to the VLAN ID.
Member Ports	Enter the port numbers to associate with the static group.
Add	Click **Add** to add an IGMP group.

IGMP Static Groups Status settings are informational only as shown in the following:



IGMP Static Groups Status

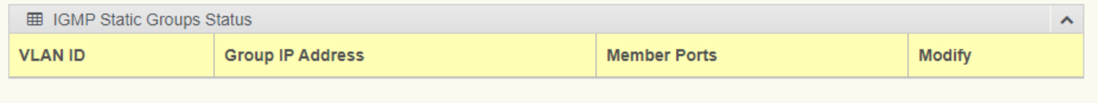
VLAN ID	Group IP Address	Member Ports	Modify

Figure 4.64 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

4.5.7.2.4 Multicast Groups

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **Multicast Groups**.

Multicast Groups settings are informational only.



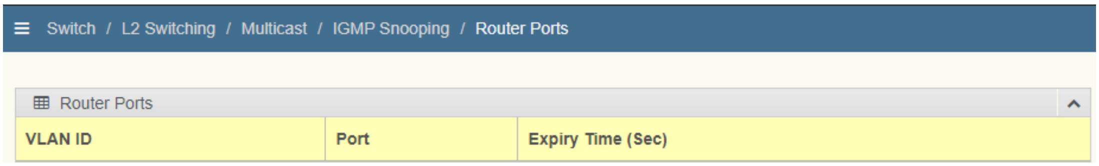
IGMP Static Groups Status

VLAN ID	Group IP Address	Member Ports	Modify

Figure 4.65 L2 Switching > Multicast > IGMP Snooping > Multicast Groups

4.5.7.2.5 Router Ports

To access this page, click **L2 Switching** > **Multicast** > **IGMP Snooping** > **Router Ports**.


☰ Switch / L2 Switching / Multicast / IGMP Snooping / Router Ports
Router Ports

VLAN ID	Port	Expiry Time (Sec)

Figure 4.66 L2 Switching > Multicast > IGMP Snooping > Multicast Groups

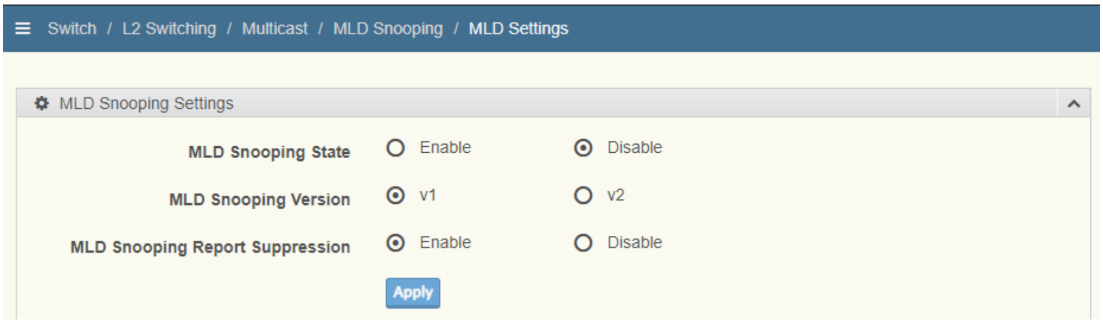
The ensuing table for **Router Ports** settings are informational only and display the following: VLAN ID, Port and Expiry Time (Sec).

4.5.7.3 MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (v1 or v2) and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

4.5.7.3.1 MLD Settings

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Settings**.


☰ Switch / L2 Switching / Multicast / MLD Snooping / MLD Settings
MLD Snooping Settings
Apply

MLD Snooping State ○ Enable ● Disable

MLD Snooping Version ● v1 ○ v2

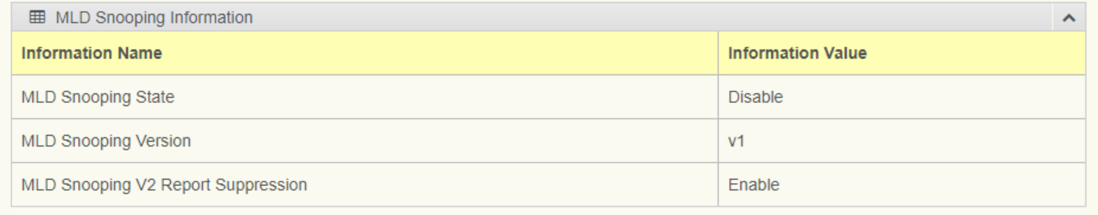
MLD Snooping Report Suppression ● Enable ○ Disable

Figure 4.67 L2 Switching > Multicast > MLD Snooping > MLD Settings

The following table describes the items in the previous figure.

Item	Description
MLD Snooping State	Select **Enable** or **Disable** to setup the MLD Snooping State.
MLD Snooping Version	Select the querier version (V1 or V2) designated to the MLD Snooping Version.
MLD Snooping Report Suppression	Select **Enable** or **Disable** to designate the status of the report suppression.
Apply	Click **Apply** to save the values and update the screen.

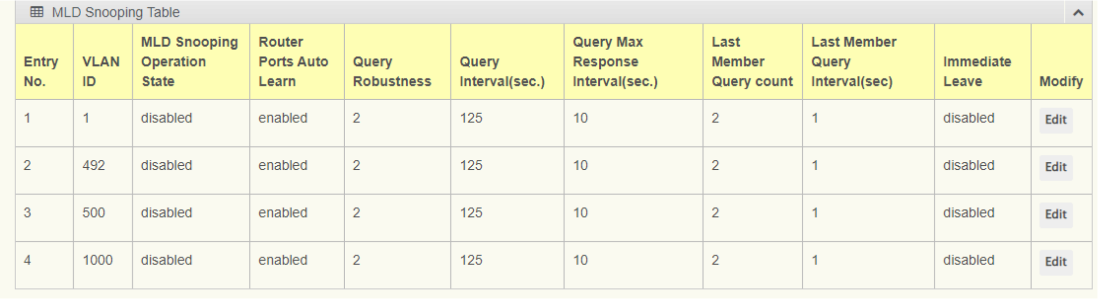
MLD Snooping Information settings are informational only.



Information Name	Information Value
MLD Snooping State	Disable
MLD Snooping Version	v1
MLD Snooping V2 Report Suppression	Enable

Figure 4.68 L2 Switching > Multicast > MLD Snooping > MLD Settings

MLD Snooping Table settings are informational only.



MLD Snooping Table

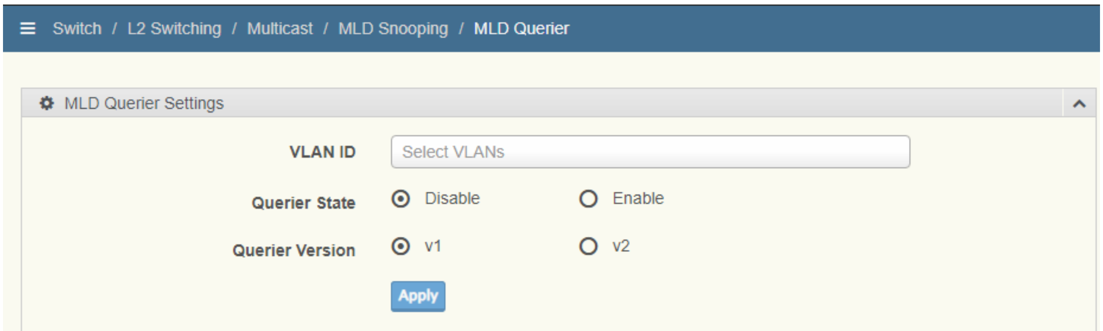
Entry No.	VLAN ID	MLD Snooping Operation State	Router Ports Auto Learn	Query Robustness	Query Interval(sec.)	Query Max Response Interval(sec.)	Last Member Query count	Last Member Query Interval(sec)	Immediate Leave	Modify
1	1	disabled	enabled	2	125	10	2	1	disabled	Edit
2	492	disabled	enabled	2	125	10	2	1	disabled	Edit
3	500	disabled	enabled	2	125	10	2	1	disabled	Edit
4	1000	disabled	enabled	2	125	10	2	1	disabled	Edit

Figure 4.69 L2 Switching > Multicast > MLD Snooping > MLD Settings

4.5.7.3.2 MLD Querier

The MLD Querier page allows you to select and enable/disable the MLD querier and define the version (IGMPv1 or IGMPv2) when enabled.

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Querier**.



≡ Switch / L2 Switching / Multicast / MLD Snooping / MLD Querier

MLD Querier Settings

VLAN ID: Select VLANs

Querier State: ● Disable ○ Enable

Querier Version: ● v1 ○ v2

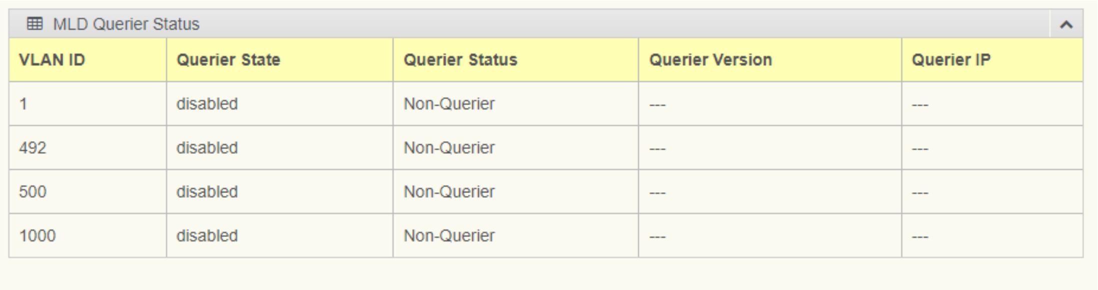
Apply

Figure 4.70 L2 Switching > Multicast > MLD Snooping > MLD Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to configure.
Querier State	Select **Enable** or **Disable** status on the selected VLAN. ■ Enable: Enable IGMP Querier Election. ■ Disable: Disable IGMP Querier Election.
Querier Version	Select the querier version (IGMPV1 or IGMPV2) designated to the MLD Querier function.
Apply	Click **Apply** to save the values and update the screen.

MLD Querier Status settings are informational only.



MLD Querier Status

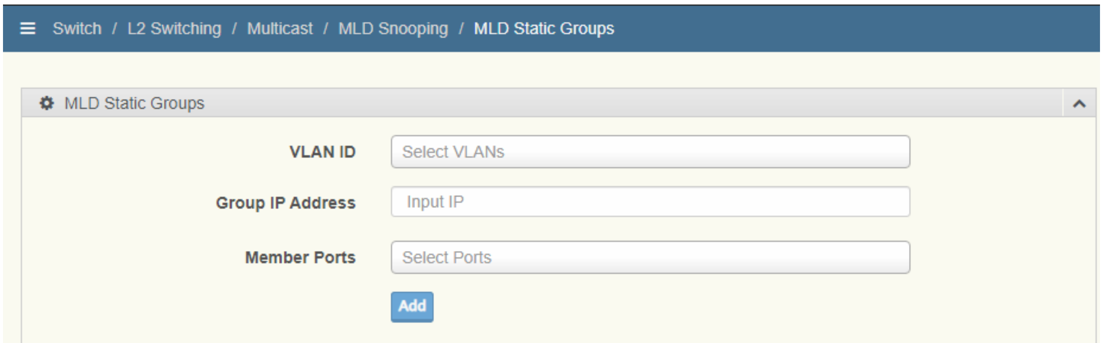
VLAN ID	Querier State	Querier Status	Querier Version	Querier IP
1	disabled	Non-Querier	---	---
492	disabled	Non-Querier	---	---
500	disabled	Non-Querier	---	---
1000	disabled	Non-Querier	---	---

Figure 4.71 L2 Switching > Multicast > MLD Snooping > MLD Querier

4.5.7.3.3 MLD Static Group

The MLD Static Group page allows you to configure specified ports as static member ports.

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **MLD Static Group**.



Switch / L2 Switching / Multicast / MLD Snooping / MLD Static Groups

MLD Static Groups

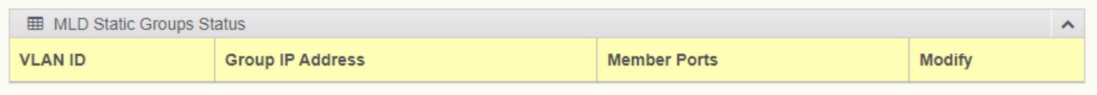
VLAN ID	Select VLANs
Group IP Address	Input IP
Member Ports	Select Ports

Figure 4.72 L2 Switching > Multicast > MLD Snooping > MLD Static Group

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to define the local MLD Static Group.
Group IP Address	Enter the IP address associated with the static group.
Member Ports	Enter the ports designated with the static group.
Add	Click **Add** to add a MLD static group.

MLD Static Groups Status settings are informational only.



MLD Static Groups Status

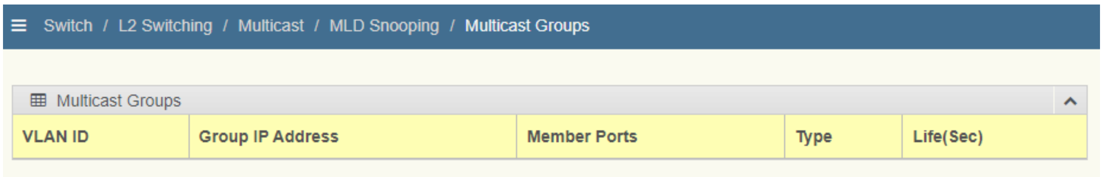
VLAN ID	Group IP Address	Member Ports	Modify

Figure 4.73 L2 Switching > Multicast > MLD Snooping > MLD Static Group

4.5.7.3.4 Multicast Groups

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Multicast Groups**.

Multicast Groups settings are informational only.



Switch / L2 Switching / Multicast / MLD Snooping / Multicast Groups

Multicast Groups

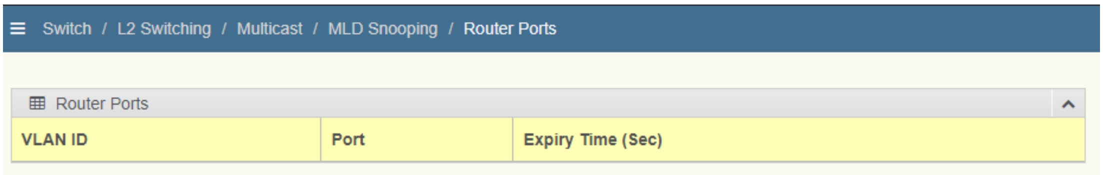
VLAN ID	Group IP Address	Member Ports	Type	Life(Sec)

Figure 4.74 L2 Switching > Multicast > MLD Snooping > MLD Groups

4.5.7.3.5 Router Ports

To access this page, click **L2 Switching** > **Multicast** > **MLD Snooping** > **Router Ports**.

Router Ports settings are informational only.



Switch / L2 Switching / Multicast / MLD Snooping / Router Ports

Router Ports

VLAN ID	Port	Expiry Time (Sec)

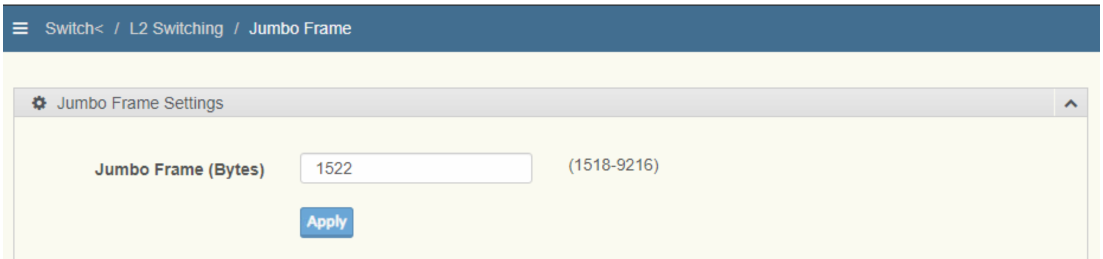
Figure 4.75 L2 Switching > Multicast > MLD Snooping > Router Ports

The following table describes the items in the previous figure.

4.5.7.4 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

To access this page, click **L2 Switching** > **Jumbo Frame**.



Jumbo Frame (Bytes) 1522 (1518-9216)

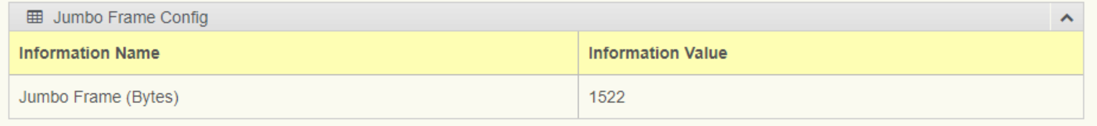
Apply

Figure 4.76 L2 Switching > Jumbo Frame

The following table describes the items in the previous figure.

Item	Description
Jumbo Frame (Bytes)	Enter the variable in bytes (1518 to 9216) to define the jumbo frame size.
Apply	Click **Apply** to save the values and update the screen.

Jumbo Frame Config settings are informational only.



Information Name	Information Value
Jumbo Frame (Bytes)	1522

Figure 4.77 L2 Switching > Jumbo Frame

4.5.7.5 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol to ensure loop-free topology for any bridged Ethernet local area network.

4.5.7.5.1 Rapid Spanning Tree Protocol (RSTP)

The network protocol Rapid Spanning Tree Protocol (RSTP: IEEE 802.1w) is an advancement over Spanning Tree Protocol (STP: IEEE802.1D) which promotes loop-free topology and high availability within Ethernet networks.

When compared to traditional daisy chain topology, RSTP networks offer high availability. In the event of network failure, devices can continue communicating as data is rerouted around the failure.

By using multiple switches, RSTP prevents network loops by blocking redundant paths on a network.

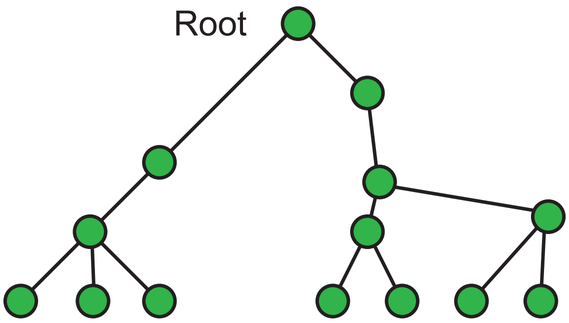


Figure 4.78 Spanning Tree Without Loops

4.5.7.5.2 Multiple RSTP (MSTP)

Another form of redundancy in topologies that include redundancy is the use of Multiple Spanning Tree Protocol (MSTP). As an extension of RSTP, MSTP enables VLANs to be grouped into a spanning-tree instance. This provides multiple forwarding paths for data traffic, enabling load balancing.

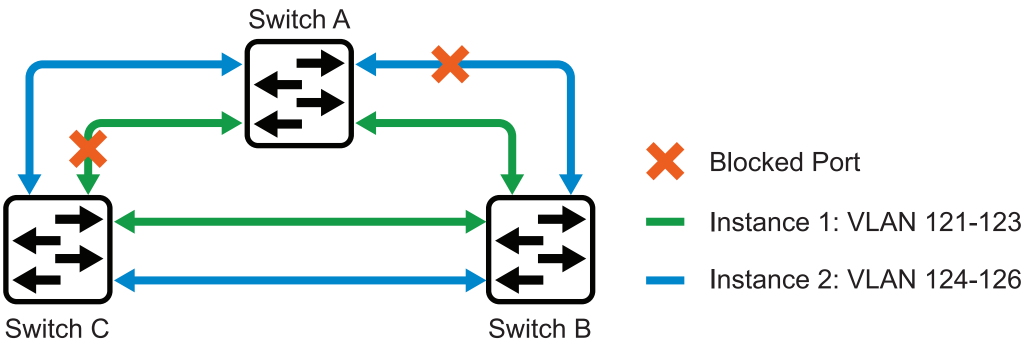
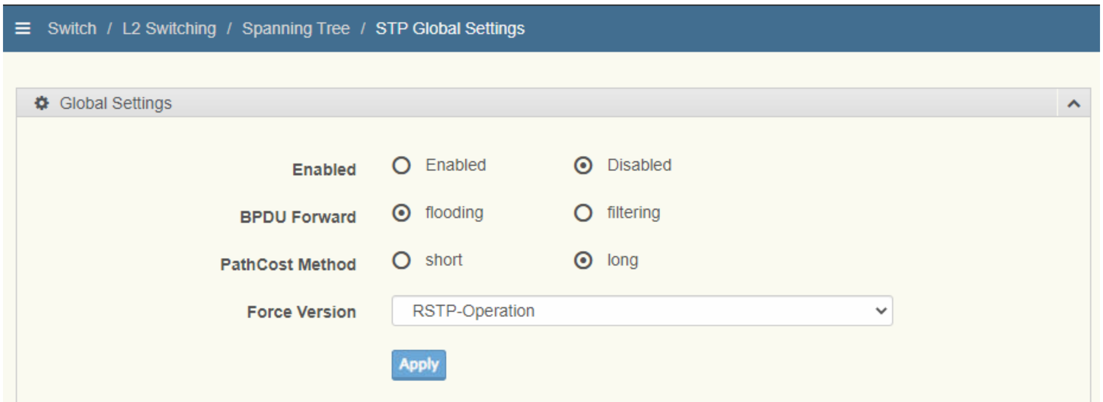


Figure 4.79 Multiple Spanning Tree Protocol Redundancy

4.5.7.5.3 STP Global Settings

The STP Global Settings page allows you to set the STP status, select the configuration for a BPDU packet, choose the path overhead, force version and set the configuration revision range.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Global Settings**.



≡ Switch / L2 Switching / Spanning Tree / STP Global Settings

Global Settings

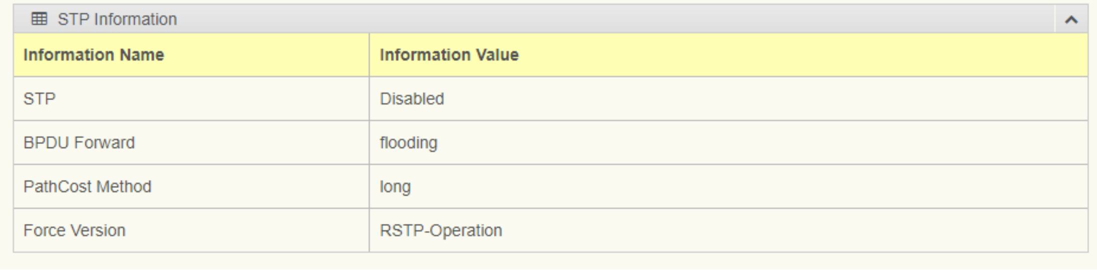
Enabled	○ Enabled	● Disabled
BPDU Forward	● flooding	○ filtering
PathCost Method	○ short	● long
Force Version	RSTP-Operation	

Figure 4.80 L2 Switching > Spanning Tree > STP Global Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click the radio-button to enable or disable the STP status.
BPDU Forward	Select **flooding** or **filtering** to designate the type of BPDU packet.
PathCost Method	Select short or long to define the method of used for path cost calculations.
Force Version	Click the drop-down menu to select the operating mode for STP. ■ STP-Compatible: 802.1D STP operation. ■ RSTP-Operation: 802.1w operation. ■ MSTP-Operation: 802.1s operation.
Apply	Click **Apply** to save the values and update the screen.

STP Information settings are informational only.



STP Information

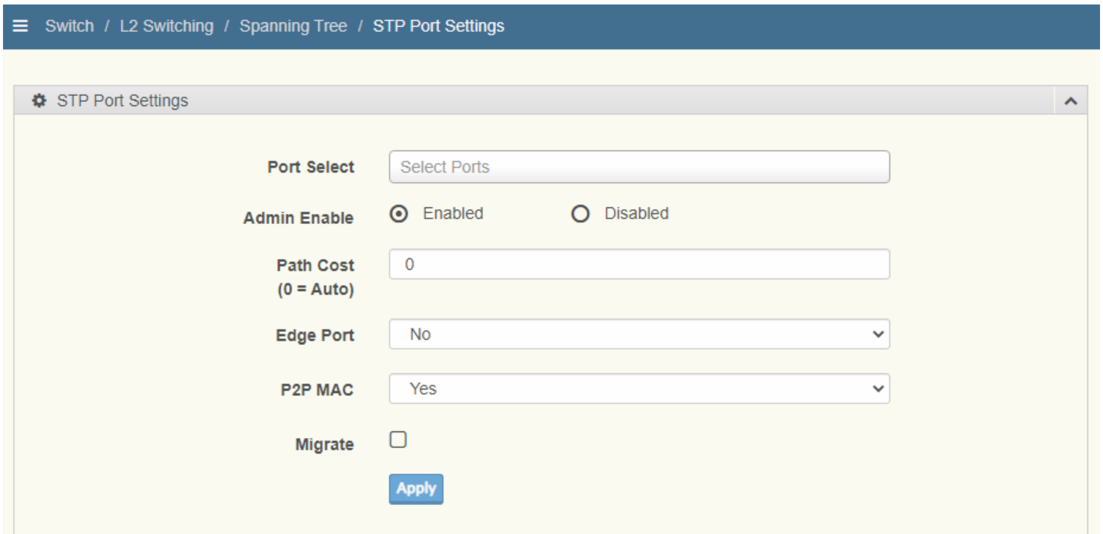
Information Name	Information Value
STP	Disabled
BPDU Forward	flooding
PathCost Method	long
Force Version	RSTP-Operation

Figure 4.81 L2 Switching > Spanning Tree > STP Global Settings

4.5.7.5.4 STP Port Settings

The STP Port Settings page allows you to configure the ports for the setting, port's contribution, configure edge port, and set the status of the BPDU filter.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Port Settings**.



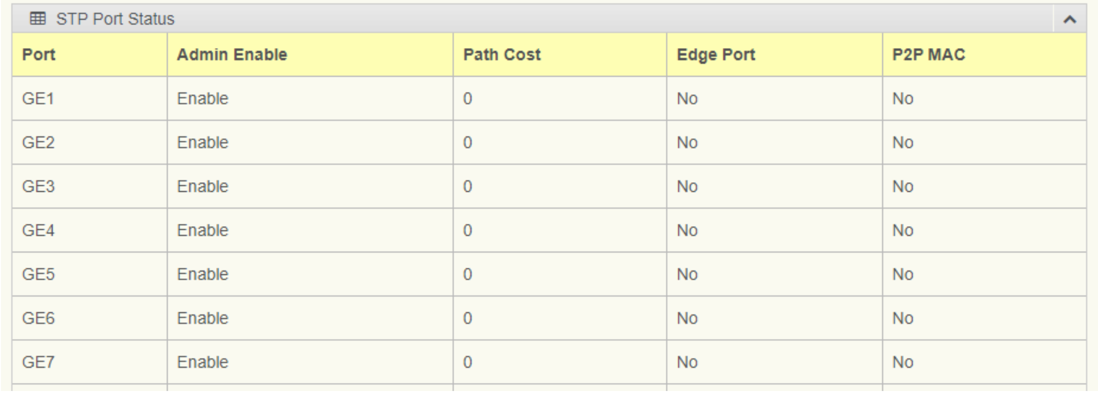
Port Select	Select Ports
Admin Enable	● Enabled ○ Disabled
Path Cost (0 = Auto)	0
Edge Port	No
P2P MAC	Yes
Migrate	□

Figure 4.82 L2 Switching > Spanning Tree > STP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.
Admin Enable	Select **Enabled** or **Disabled** to setup the admin profile for the STP port.
Path Cost (0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).
Edge Port	Click the drop-down menu to set the edge port configuration. ■ No: Force to false state (as link to a bridge). ■ Yes: Force to true state (as link to a host).
P2P MAC	Click the drop-down menu to set the Point-to-Point port configuration. ■ No: Force to false state. ■ Yes: Force to true state.
Migrate	Click the check box to enable the migrate function. Forces the port to use the new MST/RST BPDUs, requiring the switch to test on the LAN segment. for the presence of legacy devices, which are not able to understand the new BPDU formats.
Apply	Click **Apply** to save the values and update the screen.

STP Port Status settings are informational only.



STP Port Status

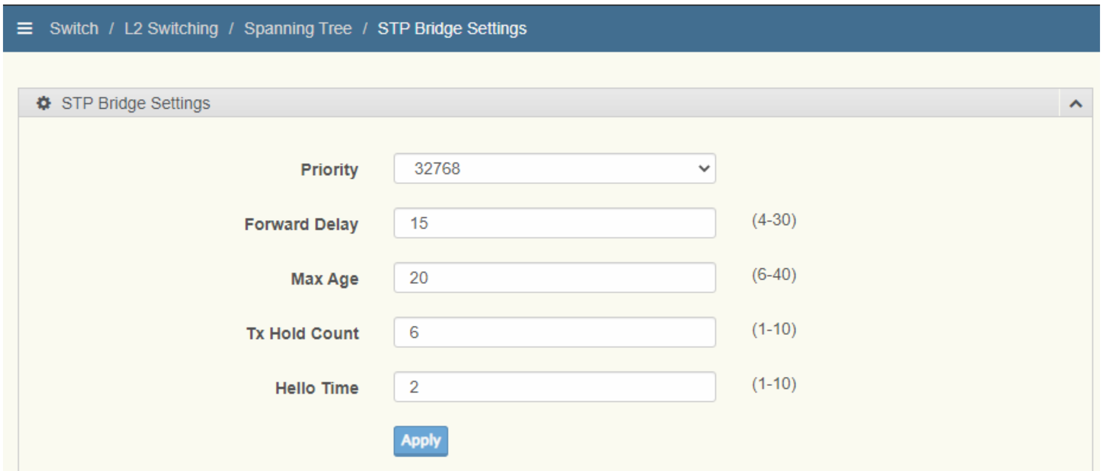
Port	Admin Enable	Path Cost	Edge Port	P2P MAC
GE1	Enable	0	No	No
GE2	Enable	0	No	No
GE3	Enable	0	No	No
GE4	Enable	0	No	No
GE5	Enable	0	No	No
GE6	Enable	0	No	No
GE7	Enable	0	No	No

Figure 4.83 L2 Switching > Spanning Tree > STP Port Settings

4.5.7.5.5 STP Bridge Settings

The STP Bridge Settings page allows you to configure the priority, forward delay, maximum age, Tx hold count, and the hello time for the bridge.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Bridge Settings**.



Switch / L2 Switching / Spanning Tree / STP Bridge Settings

STP Bridge Settings

Priority: 32768

Forward Delay: 15 (4-30)

Max Age: 20 (6-40)

Tx Hold Count: 6 (1-10)

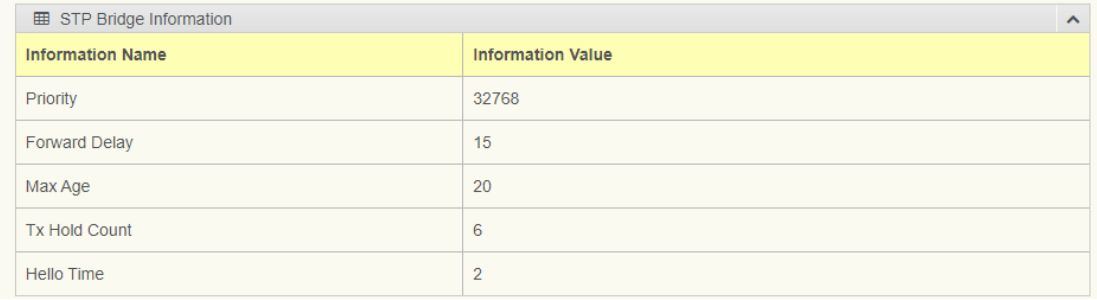
Hello Time: 2 (1-10)

Figure 4.84 L2 Switching > Spanning Tree > STP Bridge Settings

The following table describes the items in the previous figure.

Item	Description
Priority	Click the drop-down menu to select the STP bridge priority.
Forward Delay	Enter the variable (4 to 30) to set the forward delay for STP bridge settings.
Max Age	Enter the variable (6 to 40) to set the Max age for STP bridge settings.
Tx Hold Count	Enter the variable (1 to 10) to designate the TX hold count for STP bridge settings.
Hello Time	Enter the variable (1 to 10) to designate the Hello Time for STP bridge settings.
Apply	Click **Apply** to save the values and update the screen.

STP Bridge Information settings are informational only.

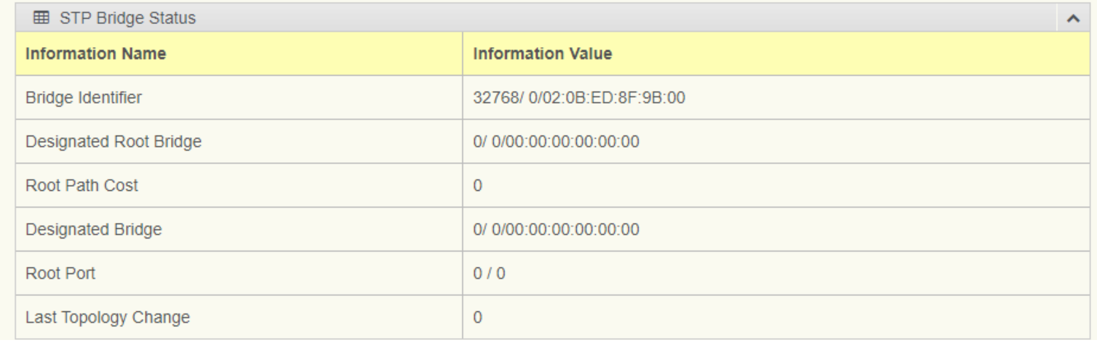


STP Bridge Information

Information Name	Information Value
Priority	32768
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 4.85 L2 Switching > Spanning Tree > STP Bridge Settings

STP Bridge Status settings are informational only.



STP Bridge Status

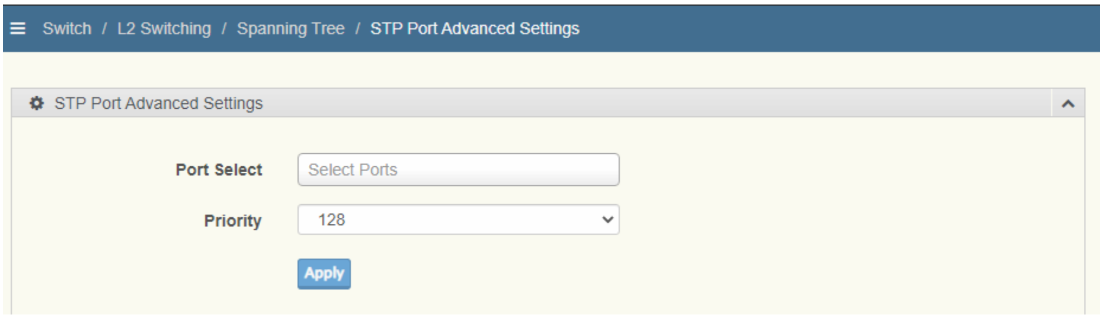
Information Name	Information Value
Bridge Identifier	32768/ 0/02:0B:ED:8F:9B:00
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Last Topology Change	0

Figure 4.86 L2 Switching > Spanning Tree > STP Bridge Settings

4.5.7.5.6 *STP Port Advanced Settings*

The STP Port Advanced Settings page allows you to select the port list to apply this setting.

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Port Advanced Settings**.



Switch / L2 Switching / Spanning Tree / STP Port Advanced Settings
STP Port Advanced Settings
Apply

Port Select: Select Ports

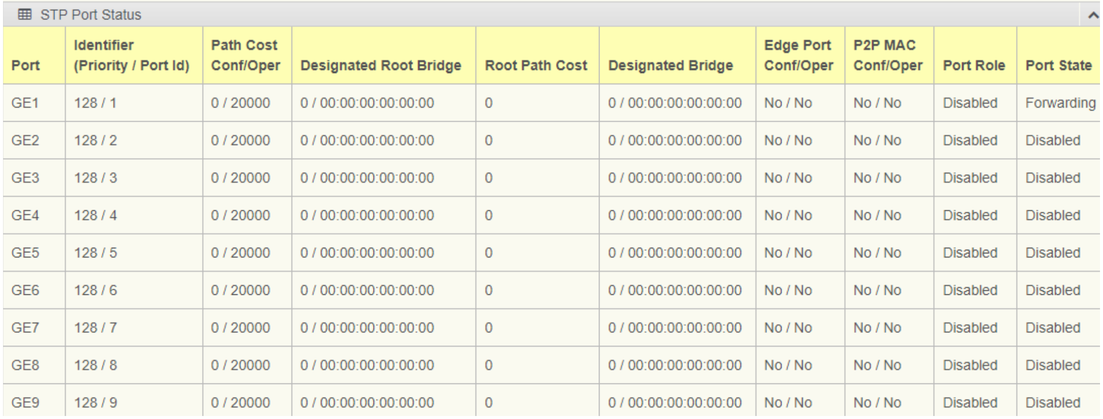
Priority: 128

Figure 4.87 L2 Switching > Spanning Tree > STP Port Advanced Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port to designate the STP settings.
Priority	Click the drop-down menu to designate a priority.
Apply	Click **Apply** to save the values and update the screen.

STP Port Status settings are informational only:



STP Port Status

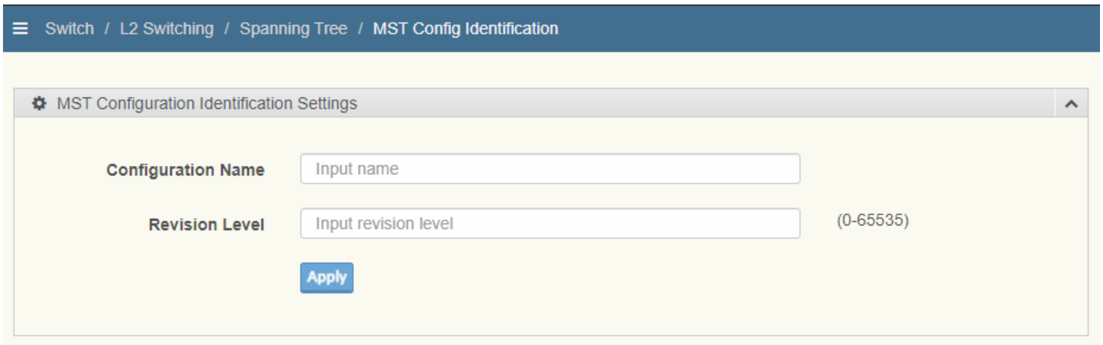
Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Forwarding
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE4	128 / 4	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE5	128 / 5	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE6	128 / 6	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE7	128 / 7	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE8	128 / 8	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled
GE9	128 / 9	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No	Disabled	Disabled

Figure 4.88 L2 Switching > Spanning Tree > STP Port Advanced Settings

4.5.7.5.7 MST Config Identification

The MST Config Identification page allows you to configure the identification setting name and the identification range.

To access this page, click **L2 Switching** > **Spanning Tree** > **MST Config Identification**.



Switch / L2 Switching / Spanning Tree / MST Config Identification

MST Configuration Identification Settings

Configuration Name: Input name

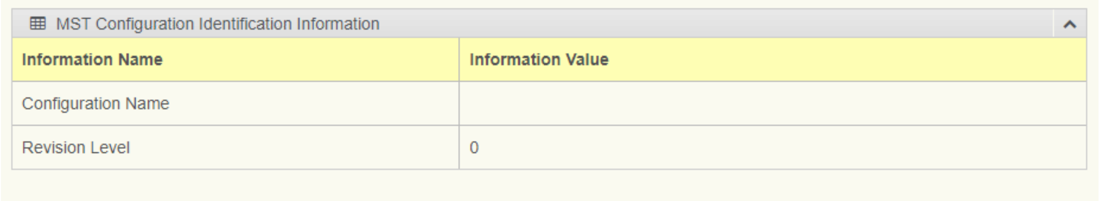
Revision Level: Input revision level (0-65535)

Figure 4.89 L2 Switching > Spanning Tree > MST Config Identification

The following table describes the items in the previous figure.

Item	Description
Configuration Name	Enter the identifier used to identify the configuration currently being used. It may be up to 32 characters.
Revision Level	Enter the identifier for the Revision Configuration, range: 0 to 65535 (default: 0).
Apply	Click **Apply** to save the values and update the screen.

MST Configuration Identification Information settings are informational only:



MST Configuration Identification Information

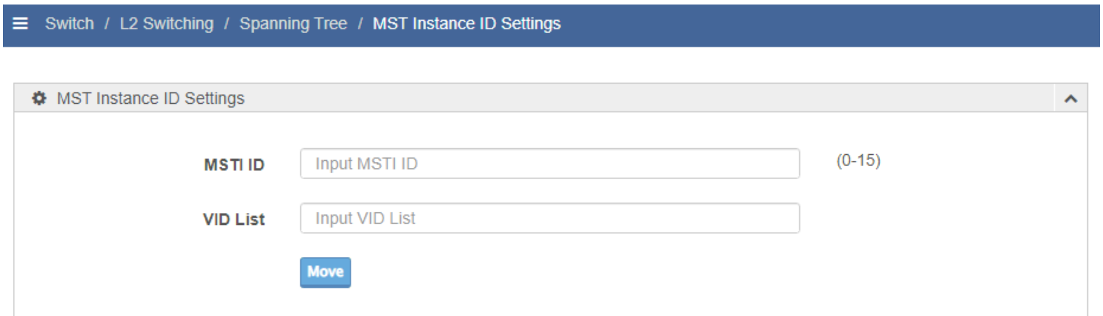
Information Name	Information Value
Configuration Name	
Revision Level	0

Figure 4.90 L2 Switching > Spanning Tree > MST Config Identification

4.5.7.5.8 MST Instance ID Settings

The MST Instance ID Settings page allows you to edit the MSTI ID and VID List settings.

To access this page, click **L2 Switching** > **Spanning Tree** > **MST Instance ID Settings**.



Switch / L2 Switching / Spanning Tree / MST Instance ID Settings

MST Instance ID Settings

MSTI ID: Input MSTI ID (0-15)

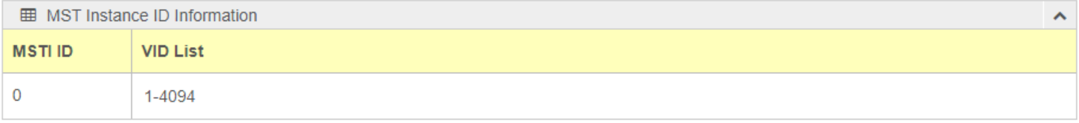
VID List: Input VID List

Figure 4.91 L2 Switching > Spanning Tree > MST Instance ID Settings

The following table describes the items in the previous figure.

Item	Description
MSTI ID	Enter the MST instance ID (0-15).
VID List	Enter the pre-configured VID list.
Move	Click **Move** to save the values and update the screen.

MST Instance ID Information settings are informational only:



MST Instance ID Information

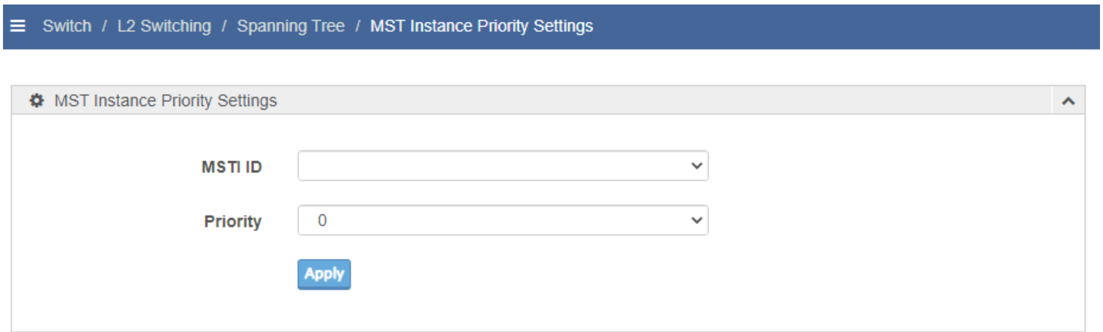
MSTI ID	VID List
0	1-4094

Figure 4.92 L2 Switching > Spanning Tree > MST Instance ID Settings

4.5.7.6 MST Instance Priority Settings

The MST Instance Priority Settings allows you to specify the MST instance and the bridge priority in that instance.

To access this page, click **L2 Switching** > **Spanning Tree** > **MST Instance Priority Settings**.



Switch / L2 Switching / Spanning Tree / MST Instance Priority Settings

MST Instance Priority Settings

MSTI ID:

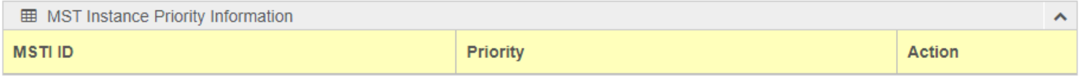
Priority: 0

Figure 4.93 L2 Switching > Spanning Tree > MST Instance Priority Settings

The following table describes the items in the previous figure.

Item	Description
MSTI ID	Click the drop-down menu to specify the MST instance.
Priority	Click the drop-down menu set the bridge priority in the specified MST instance
Apply	Click **Apply** to save the values and update the screen.

MST Instance Priority Information settings are informational only:



MST Instance Priority Information

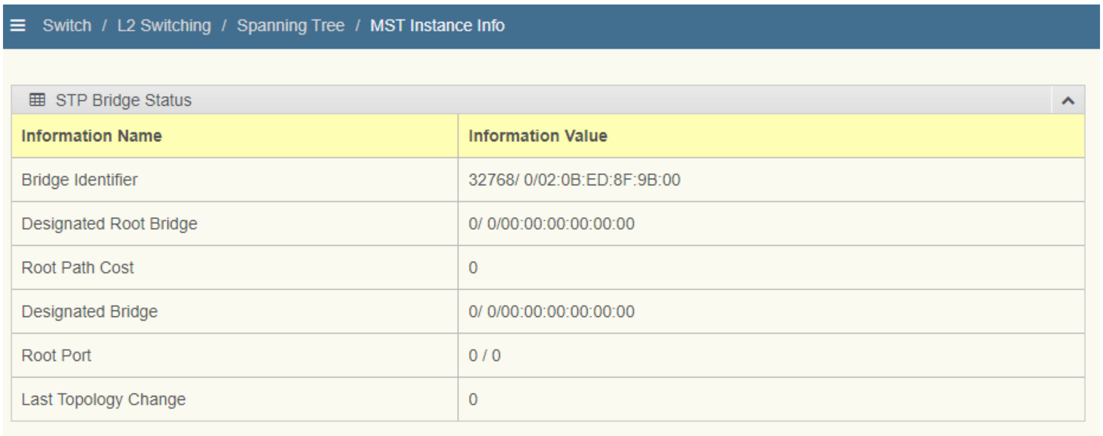
MSTI ID	Priority	Action

Figure 4.94 L2 Switching > Spanning Tree > MST Instance Priority Settings

4.5.7.7 MST Instance Info

To access this page, click **L2 Switching** > **Spanning Tree** > **MST Instance Info**.

The ensuing table for **STP Bridge Status** settings is as follows:



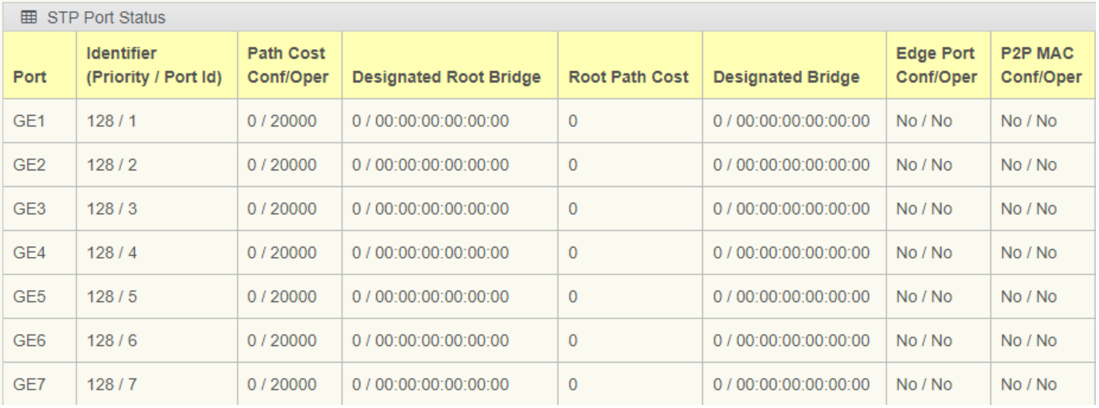
≡ Switch / L2 Switching / Spanning Tree / MST Instance Info

STP Bridge Status

Information Name	Information Value
Bridge Identifier	32768/ 0/02:0B:ED:8F:9B:00
Designated Root Bridge	0/ 0/00:00:00:00:00:00
Root Path Cost	0
Designated Bridge	0/ 0/00:00:00:00:00:00
Root Port	0 / 0
Last Topology Change	0

Figure 4.95 L2 Switching > Spanning Tree > MST Instance Info

STP Port Status settings are informational only:



STP Port Status

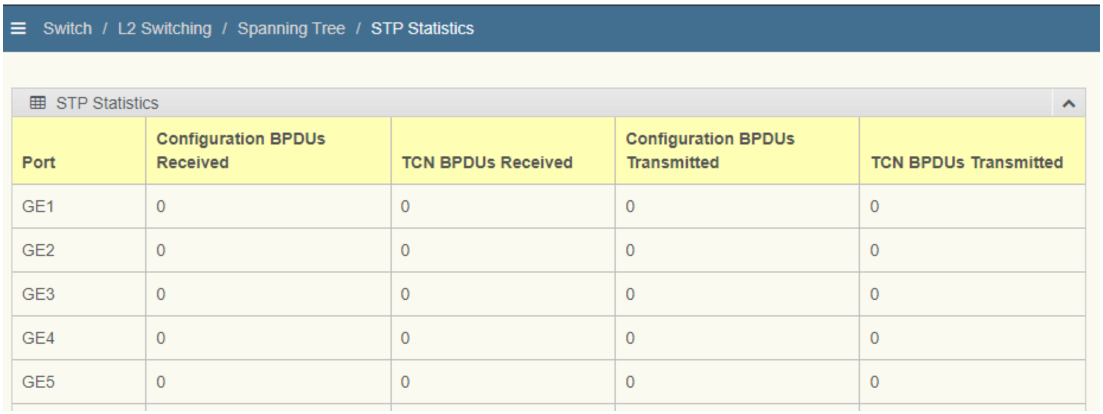
Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE4	128 / 4	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE5	128 / 5	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE6	128 / 6	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No
GE7	128 / 7	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	No / No

Figure 4.96 L2 Switching > Spanning Tree > MST Instance Info

4.5.7.7.1 STP Statistics

To access this page, click **L2 Switching** > **Spanning Tree** > **STP Statistics**.

STP Statistics are informational only as shown in the following:



≡ Switch / L2 Switching / Spanning Tree / STP Statistics

STP Statistics

Port	Configuration BPDUs Received	TCN BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted
GE1	0	0	0	0
GE2	0	0	0	0
GE3	0	0	0	0
GE4	0	0	0	0
GE5	0	0	0	0

Figure 4.97 L2 Switching > Spanning Tree > STP Statistics

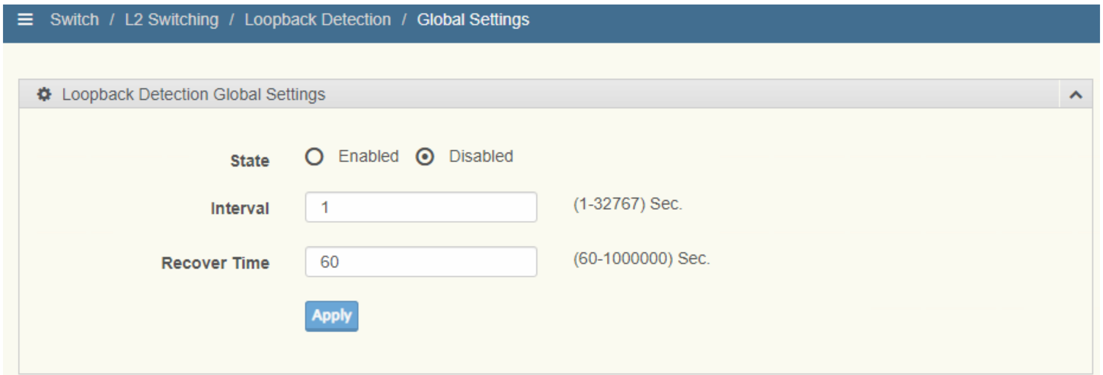
4.5.8 Loopback Detection

The Loopback Detection function is used to detect looped links. By sending detection frames and then checking to see if the frames returned to any port on the device, the function is used to detect loops.

4.5.8.1 Global Settings

The Global Settings page allows you to configure the state (enabled or disabled) of the function, select the interval at which frames are transmitted and the delay before recovery.

To access this page, click **L2 Switching** > **Loopback Detection** > **Global Settings**.



Switch / L2 Switching / Loopback Detection / Global Settings
Loopback Detection Global Settings
Apply

State ○ Enabled ● Disabled

Interval 1 (1-32767) Sec.

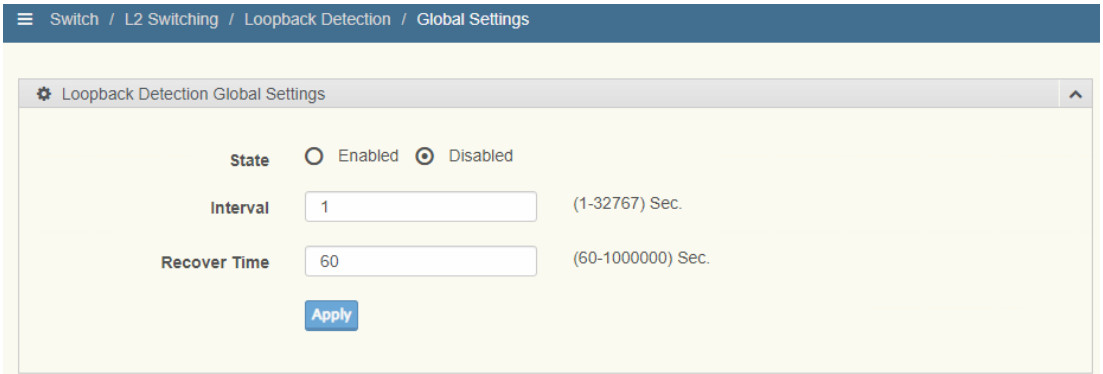
Recover Time 60 (60-1000000) Sec.

Figure 4.98 L2 Switching > Loopback Detection > Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the loopback mode.
Interval	Enter the variable in seconds (1 to 32767) to set the interval at which frames are transmitted.
Recover Time	Enter the variable in seconds (60 to 1000000) to define the delay before recovery.
Apply	Click **Apply** to save the values and update the screen.

Loopback Detection Global Information settings are informational only:



Switch / L2 Switching / Loopback Detection / Global Settings
Loopback Detection Global Settings
Apply

State ○ Enabled ● Disabled

Interval 1 (1-32767) Sec.

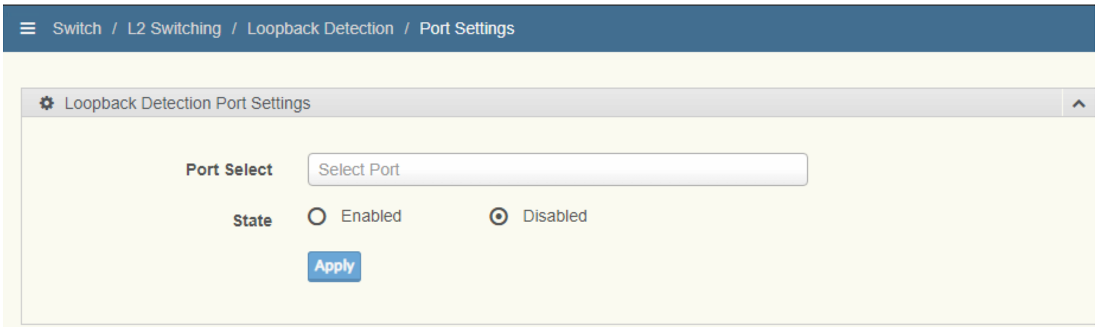
Recover Time 60 (60-1000000) Sec.

Figure 4.99 L2 Switching > Loopback Detection > Global Settings

4.5.8.2 Port Settings

The Port Settings page allows you to select ports that are detected by the loopback detection function and configure their status (enabled or disabled).

To access this page, click **L2 Switching** > **Loopback Detection** > **Port Settings**.



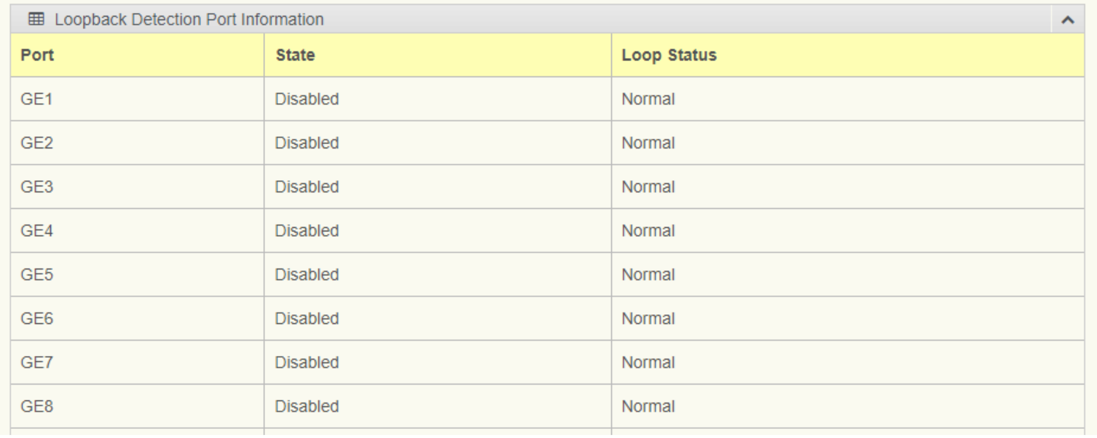
☰ Switch / L2 Switching / Loopback Detection / Port Settings
Loopback Detection Port Settings
Port Select
Select Port
State
○ Enabled
● Disabled
Apply

Figure 4.100 L2 Switching > Loopback Detection > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to define the local loopback detection setting.
Enabled	Select **Enabled** or **Disabled** to setup the Loopback Detection function.
Apply	Click **Apply** to save the values and update the screen.

Loopback Detection Port Information settings are informational only:



Loopback Detection Port Information

Port	State	Loop Status
GE1	Disabled	Normal
GE2	Disabled	Normal
GE3	Disabled	Normal
GE4	Disabled	Normal
GE5	Disabled	Normal
GE6	Disabled	Normal
GE7	Disabled	Normal
GE8	Disabled	Normal

Figure 4.101 L2 Switching > Loopback Detection > Port Settings

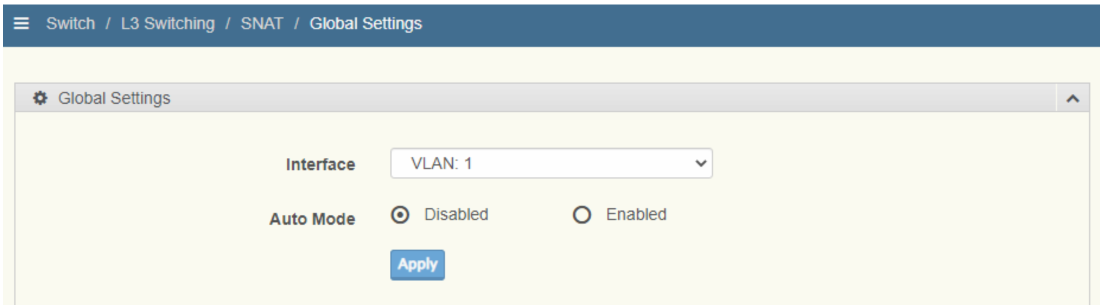
4.6 L3 Switching

4.6.1 SNAT (Source NAT)

Source NAT (SNAT) is the most common form of NAT. SNAT changes the source address of the packets passing through the switch. SNAT is typically used when an internal (private) host needs to initiate a session to an external (public) host. The device acting as an agent between the Internet (public) network and the local (private) network translates in real time the source destination IP address of a client on the network. For this reason, a source IP translation enables a single public address to represent a significantly larger number of private addresses.

4.6.1.1 Global Settings

To access this page, click **L3 Switching > SNAT > Global Settings**.



Interface: VLAN: 1

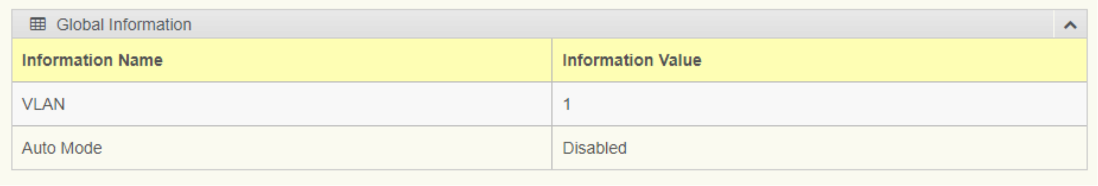
Auto Mode: ● Disabled ○ Enabled

Figure 4.102 L3 Switching > SNAT > Global Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Auto Mode	Select **Enabled** or **Disabled** to setup the auto mode.
Apply	Click **Apply** to save the values and update the screen.

Global Information settings are informational only:



Information Name	Information Value
VLAN	1
Auto Mode	Disabled

Figure 4.103 L3 Switching > SNAT > Global Settings

4.6.1.2 Entry Settings

To access this page, click **L3 Switching > SNAT > Entry Settings**.

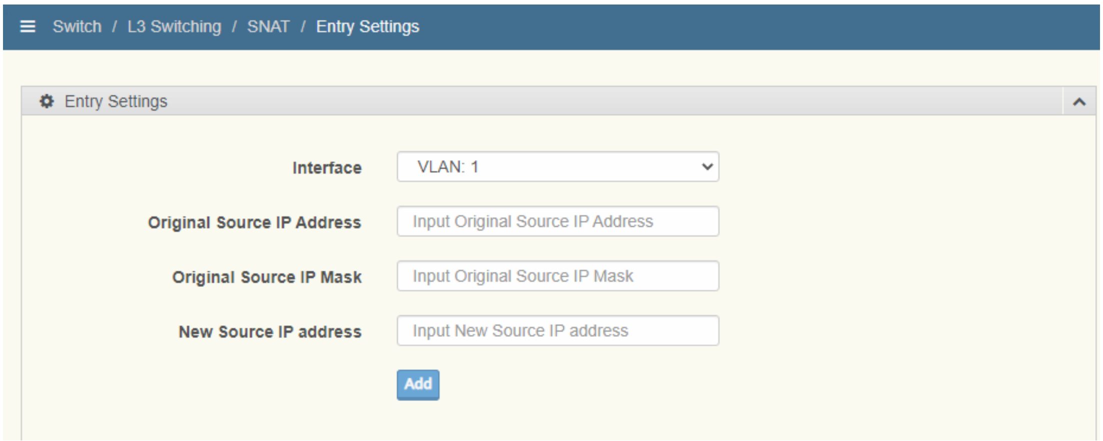

Switch / L3 Switching / SNAT / Entry Settings
Entry Settings
Interface
VLAN: 1
Original Source IP Address
Input Original Source IP Address
Original Source IP Mask
Input Original Source IP Mask
New Source IP address
Input New Source IP address
Add

Figure 4.104 L3 Switching > SNAT > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface.
Original Source IP Address	Enter the original IP address to apply this rule. The address is the IP address to allow traffic to an external network.
Original Source IP Mask	Enter the IP netmask to specify the IP address to allow traffic to an external network.
New Source IP address	Enter the public IP address to configure the SNAT rule and specifies the external IP address for which outbound packets are translated.
Add	Click **Add** to save the values and update the screen.

Entry Information settings are informational only:

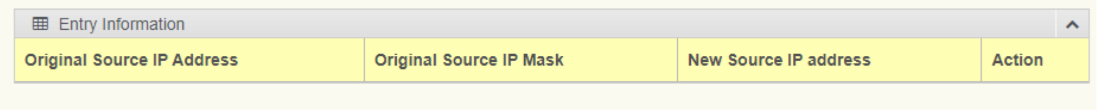


Figure 4.105 L3 Switching > SNAT > Entry Settings

4.6.2 DNAT (Destination NAT)

4.6.2.1 Entry Settings

Destination NAT (DNAT) changes the destination address of packets passing through the switch. DNAT is typically used when an external (public) host needs to initiate a session with an internal (private) host.

To access this page, click **L3 Switching > DNAT > Entry Settings**.

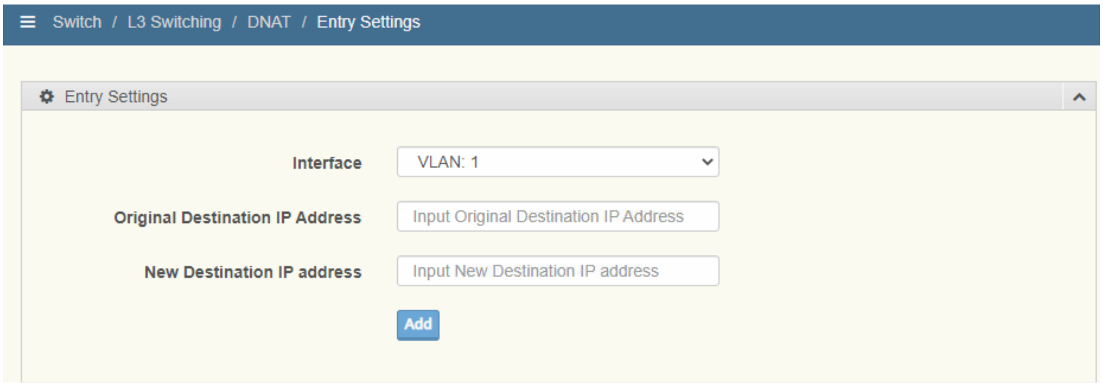
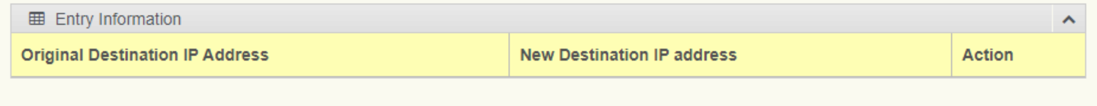

Switch / L3 Switching / DNAT / Entry Settings
Entry Settings
Interface
VLAN: 1
Original Destination IP Address
Input Original Destination IP Address
New Destination IP address
Input New Destination IP address
Add

Figure 4.106 L3 Switching > DNAT > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface on which to apply the rule.
Original Destination IP Address	Enter the IP address to specify the public address to be translated. In the packet being inspected, this IP address is the one that appears as the destination IP address of the packet. The packet destination address is the one translated by this DNAT rule.
New Destination IP address	Enter the IP address to specify the destination address on inbound packets to be translated.
Add	Click **Add** to save the values and update the screen.

Entry Information are informational only as shown in the following:



Entry Information

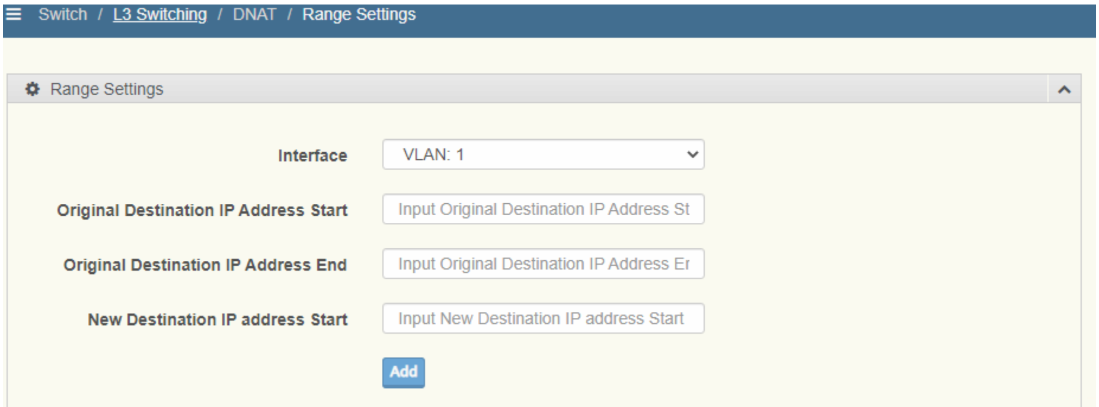
Original Destination IP Address	New Destination IP address	Action

Figure 4.107 L3 Switching > DNAT > Entry Settings

4.6.2.2 Range Settings

Destination NAT (DNAT) allows you to create a rule to change the source IP address range from a public to private IP address range. When creating DNAT rules, you can specify the original and translated IP addresses by using the following formats:

To access this page, click **L3 Switching > DNAT > Range Settings**.



Switch / L3 Switching / DNAT / Range Settings

Range Settings

Interface: VLAN: 1

Original Destination IP Address Start: Input Original Destination IP Address St

Original Destination IP Address End: Input Original Destination IP Address Er

New Destination IP address Start: Input New Destination IP address Start

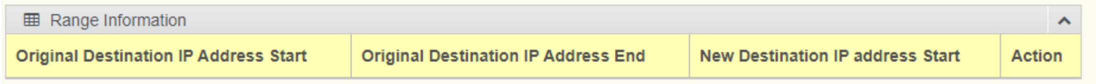
Figure 4.108 L3 Switching > DNAT > Range Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface on which to apply the rule.
Original Destination IP Address Start	Enter the starting range of IP addresses to specify the public address to be translated. In the packet being inspected, the range is the one that appears as the destination IP address of the packet. The packet destination address is the one translated by this DNAT rule.
Original Destination IP Address End	Enter the ending range of IP addresses to specify the public address to be translated. In the packet being inspected, this IP address is the one that appears as the destination IP address of the packet. The packet destination addresses are the ones translated by this DNAT rule.

Item	Description
New Destination IP Address Start	Enter the IP address to specify the starting IP address to which the destination addresses on packets (inbound) are translated.
Add	Click **Add** to save the values and update the screen.

Range Settings are informational only as shown in the following:



Range Information

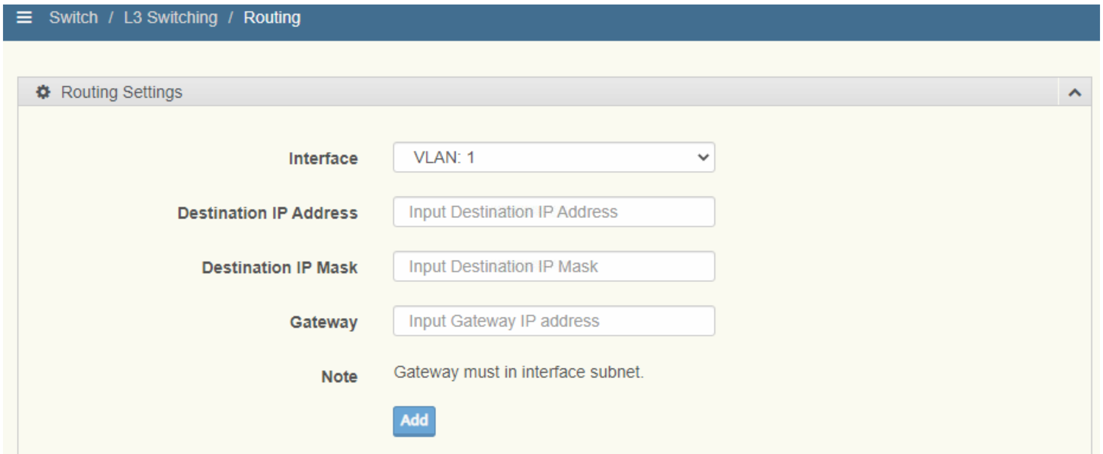
Original Destination IP Address Start	Original Destination IP Address End	New Destination IP address Start	Action

Figure 4.109 L3 Switching > DNAT > Range Settings

4.6.3 Routing

The device provides static routing capabilities. The routing capabilities provide the necessary forwarding information between broadcast domains, allowing for a decrease in broadcast domains and improved network efficiency.

To access this page, click **L3 Switching** > **Routing**.



Switch / L3 Switching / Routing

Routing Settings

Interface: VLAN: 1

Destination IP Address: Input Destination IP Address

Destination IP Mask: Input Destination IP Mask

Gateway: Input Gateway IP address

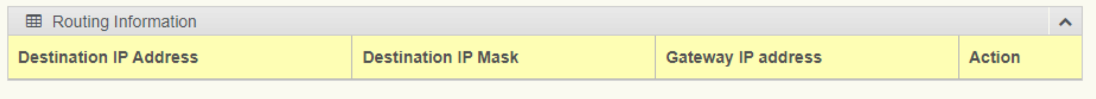
Note: Gateway must in interface subnet.

Figure 4.110 L3 Switching > Routing

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface on which to apply the rule.
Destination IP Address	Enter the IP address of the output interface on which all packets are sent.
Destination IP Mask	Enter the IP netmask of the output interface on which all packets are sent.
Gateway	Enter the gateway address (last resort) to which all unroutable packets are sent.
Add	Click **Add** to save the values and update the screen.

Routing Information are informational only as shown in the following:



Routing Information

Destination IP Address	Destination IP Mask	Gateway IP address	Action

Figure 4.111 L3 Switching > Routing

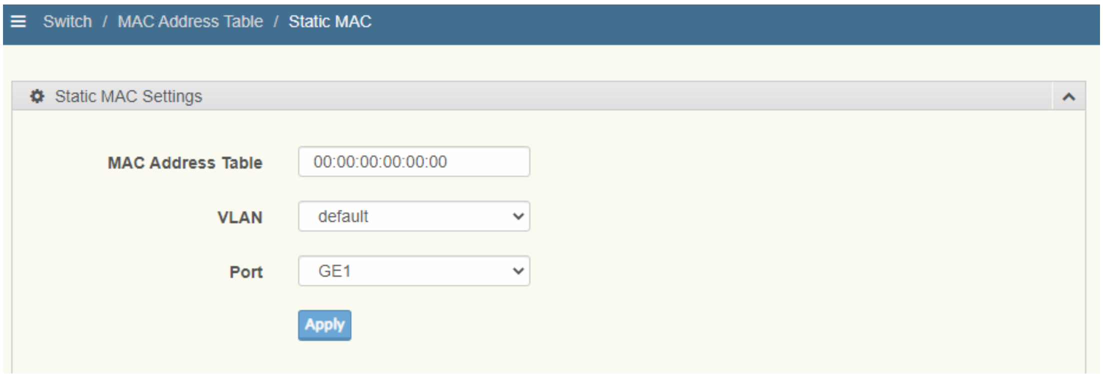
4.7 MAC Address Table

The MAC Address Table provides access to the Static MAC Settings, MAC Aging Time, and Dynamic Forwarding.

4.7.1 Static MAC

The Static MAC page allows you to configure the address for forwarding of packets, the VLAN ID of the listed MAC address and the designated Port.

To access this page, click **MAC Address Table** > **Static MAC**.



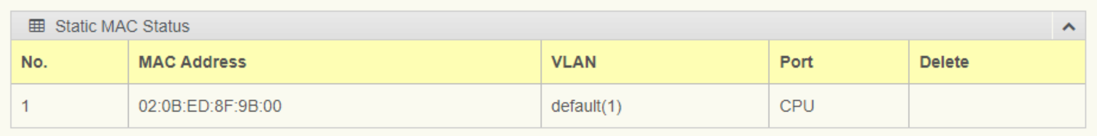
MAC Address Table: 00:00:00:00:00:00
VLAN: default
Port: GE1

Figure 4.112 MAC Address Table > Static MAC

The following table describes the items in the previous figure.

Item	Description
MAC Address	Enter the MAC address to which packets are statically forwarded.
VLAN	Click the drop-down menu to select the VLAN ID number of the VLAN for which the MAC address is residing.
Port	Click the drop-down menu to select the port number.
Apply	Click **Apply** to save the values and update the screen.

Static MAC Status are informational only as shown in the following:



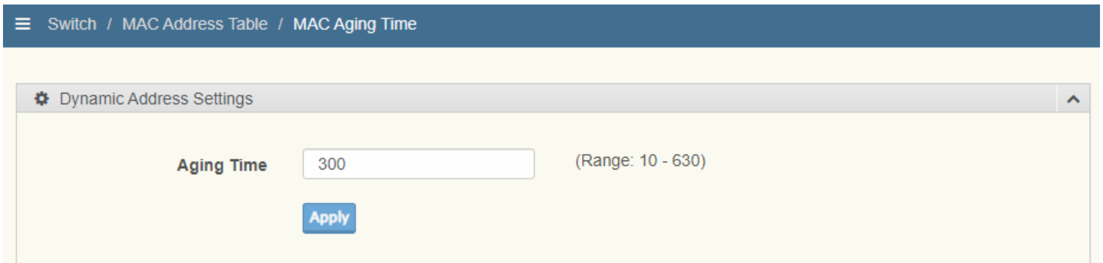
No.	MAC Address	VLAN	Port	Delete
1	02:0B:ED:8F:9B:00	default(1)	CPU	

Figure 4.113 MAC Address Table > Static MAC

4.7.2 MAC Aging Time

The MAC Aging Time page allows you to set the MAC address of the aging time to study. If the aging time for a MAC address expires, the address in the table is removed.

To access this page, click **MAC Address Table** > **MAC Aging Time**.



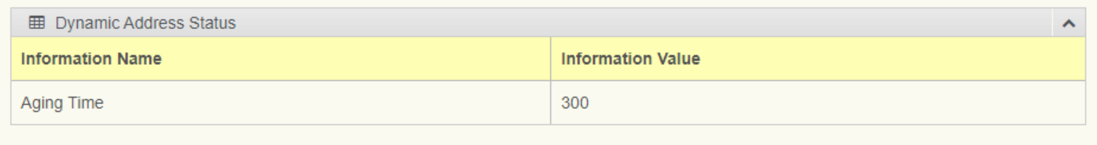
Aging Time: 300 (Range: 10 - 630)

Figure 4.114 MAC Address Table > MAC Aging Time

The following table describes the items in the previous figure.

Item	Description
Aging Time	Enter the variable (10 to 630) to define the counter time required for aging.
Apply	Click **Apply** to save the values and update the screen.

Dynamic Address Status are informational only as shown in the following:



Dynamic Address Status

Information Name	Information Value
Aging Time	300

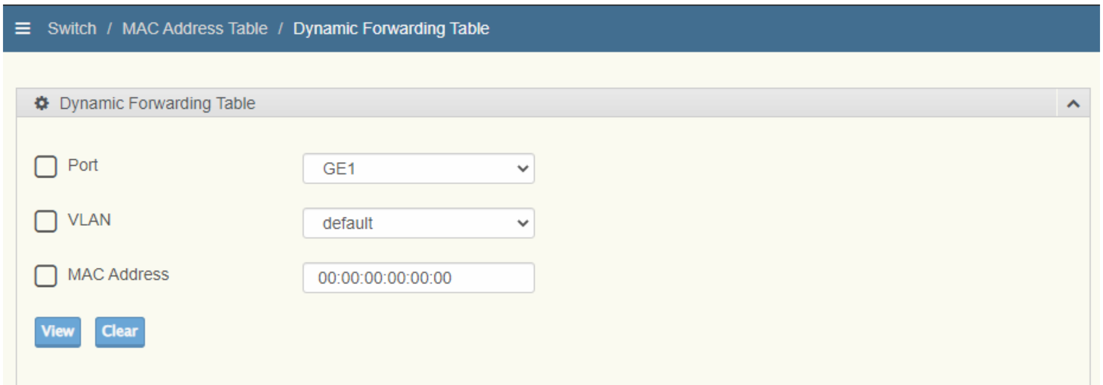
Figure 4.115 MAC Address Table > MAC Aging Time

4.7.3 Dynamic Forwarding Table

The Dynamic Forwarding function allows you to configure an address tables, which contain the following:

- The port each hardware address is associated with
- The VLAN to show or clear dynamic MAC entries
- The MAC address selection

To access this page, click **MAC Address Table** > **Dynamic Forwarding Table**.



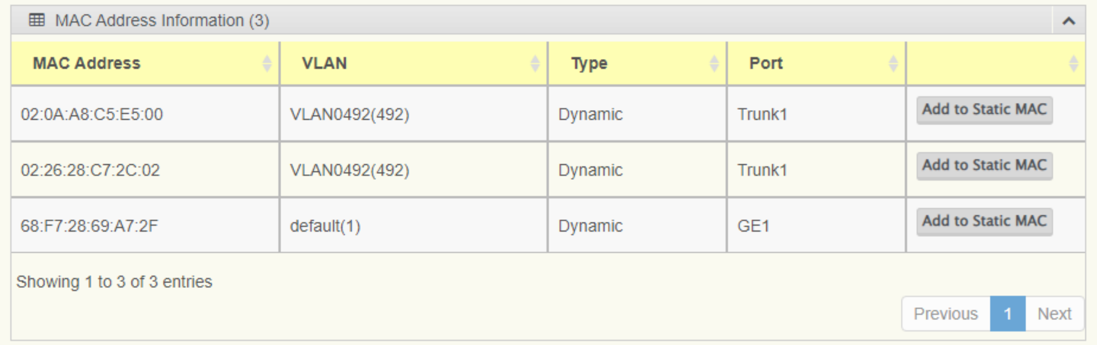
□ Port	GE1
□ VLAN	default
□ MAC Address	00:00:00:00:00:00

Figure 4.116 MAC Address Table > Dynamic Forwarding Table

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port number to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
VLAN	Click the drop-down menu to select the VLAN to show or clear dynamic MAC entries.
MAC Address	Enter the MAC address to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
View	Click **View** to display the MAC address information.
Clear	Click **Clear** to clear the MAC Address Information table.

MAC Address Information are informational only as shown in the following:



MAC Address Information (3)

MAC Address	VLAN	Type	Port	
02:0A:A8:C5:E5:00	VLAN0492(492)	Dynamic	Trunk1	Add to Static MAC
02:26:28:C7:2C:02	VLAN0492(492)	Dynamic	Trunk1	Add to Static MAC
68:F7:28:69:A7:2F	default(1)	Dynamic	GE1	Add to Static MAC

Showing 1 to 3 of 3 entries

Figure 4.117 MAC Address Table > Dynamic Forwarding Table

4.8 Security

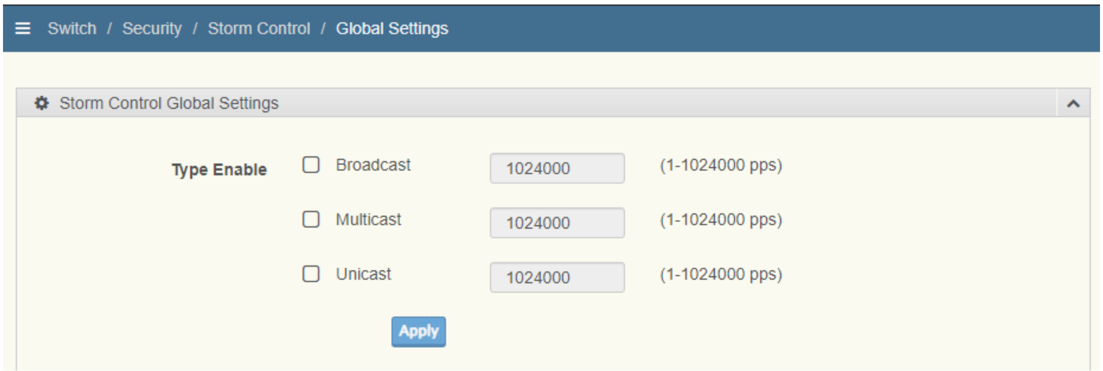
The Security function allows for the configuration of Storm Control, Port Security, Protected Ports, DoS Prevention, Applications, 802.1x, and IP Security.

4.8.1 Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

4.8.1.1 Global Settings

To access this page, click **Security** > **Storm Control** > **Global Settings**.



≡ Switch / Security / Storm Control / Global Settings

Storm Control Global Settings

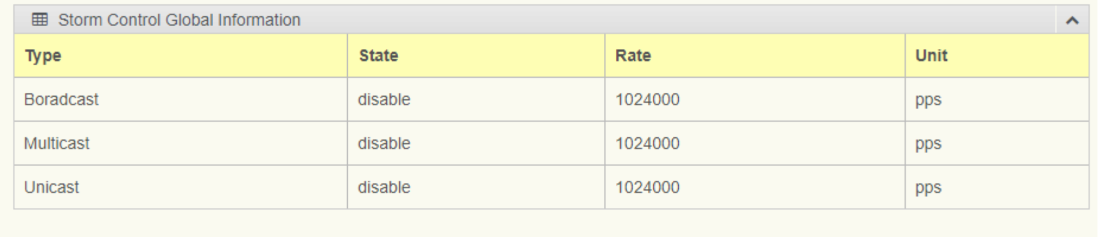
Type Enable	□ Broadcast	1024000	(1-1024000 pps)
	□ Multicast	1024000	(1-1024000 pps)
	□ Unicast	1024000	(1-1024000 pps)

Figure 4.118 Security > Storm Control > Global Settings

The following table describes the items in the previous figure.

Item	Description
Type enable	Select or deselect a storm control setting for either broadcast streams, multicast streams, or unicast streams. ■ Broadcast: sets the storm control on broadcast traffic as suppression level in packets per second (1 to 1024000 PPS). Default: 1024000 pps. ■ Multicast: sets the storm control on multicast traffic as suppression level in packets per second (1 to 1024000 PPS). Default: 1024000 pps. ■ Unicast: sets the storm control on unknown unicast traffic as suppression level in packets per second (1 to 1024000 PPS). Default: 1024000 pps.
Apply	Click **Apply** to save the values and update the screen.

Storm Control Global Information are informational only as shown in the following:



Storm Control Global Information

Type	State	Rate	Unit
Boradcast	disable	1024000	pps
Multicast	disable	1024000	pps
Unicast	disable	1024000	pps

Figure 4.119 Security > Storm Control > Global Settings

4.8.2 Port Security

The Port Security page allows you to configure port isolation behavior.

To access this page, click **Security** > **Port Security**.

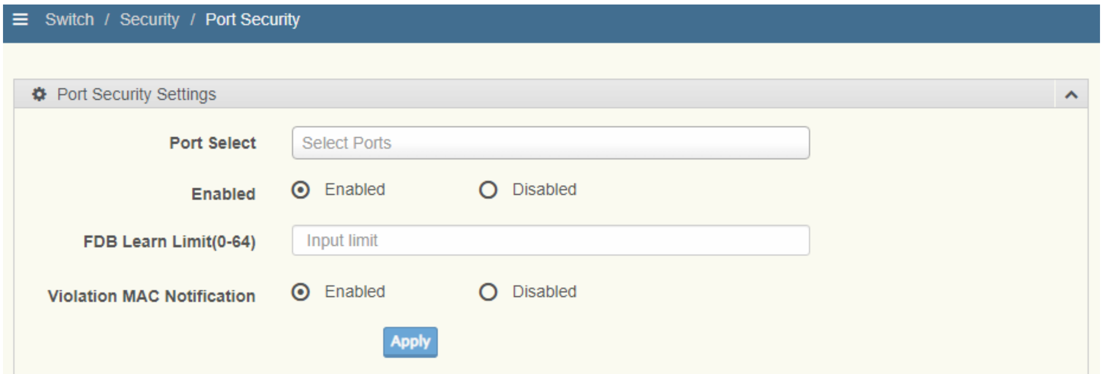
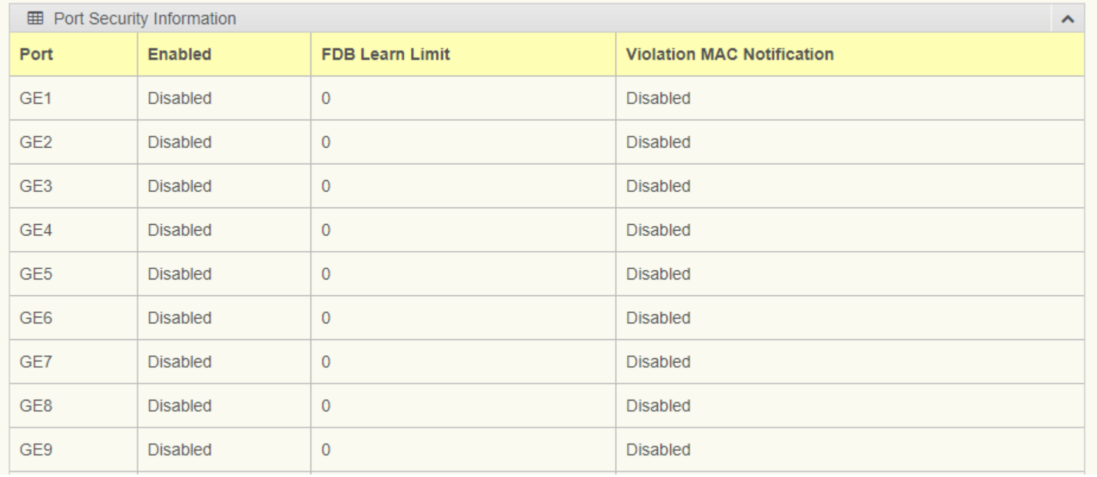


Figure 4.120 Security > Port Security

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter a single or multiple port numbers to configure.
Enabled	Select **Enabled** or **Disabled** to define the selected Port.
FDB Learn Limit (0-64)	Enter the variable (0 to 64) to set the learn limit for the FDB setting.
Violation MAC Notification	Select **Enabled** or **Disabled** to define the selected Port.
Apply	Click **Apply** to save the values and update the screen.

Port Security Information are informational only as shown in the following:



Port Security Information

Port	Enabled	FDB Learn Limit	Violation MAC Notification
GE1	Disabled	0	Disabled
GE2	Disabled	0	Disabled
GE3	Disabled	0	Disabled
GE4	Disabled	0	Disabled
GE5	Disabled	0	Disabled
GE6	Disabled	0	Disabled
GE7	Disabled	0	Disabled
GE8	Disabled	0	Disabled
GE9	Disabled	0	Disabled

Figure 4.121 Security > Port Security

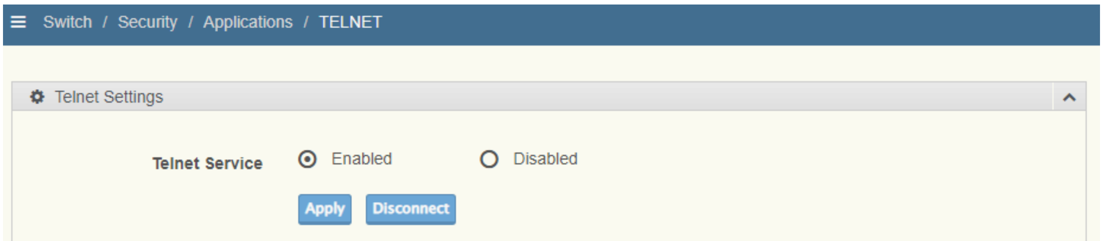
4.8.3 Applications

The Applications function allows you to configure various types of AAA lists.

4.8.3.1 TELNET

The TELNET page allows you to combine all kinds of AAA lists with the Telnet line.

To access this page, click **Security** > **Applications** > **TELNET**.



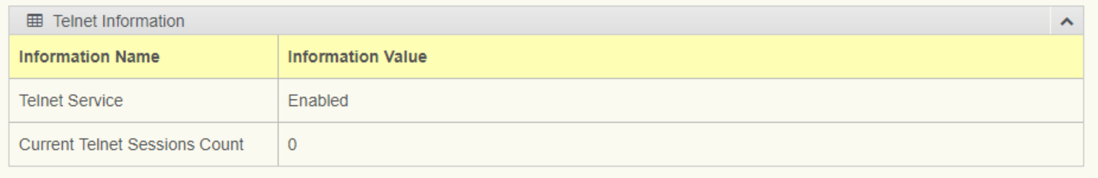
Telnet Service ● Enabled ○ Disabled

Figure 4.122 Security > Applications > TELNET

The following table describes the items in the previous figure.

Item	Description
Telnet Service	Click **Enabled** or **Disabled** to set remote access through the Telnet Service function.
Apply	Click **Apply** to save the values and update the screen.
Disconnect	Click **Disconnect** to disable the current Telnet service.

Telnet Information are informational only as shown in the following:



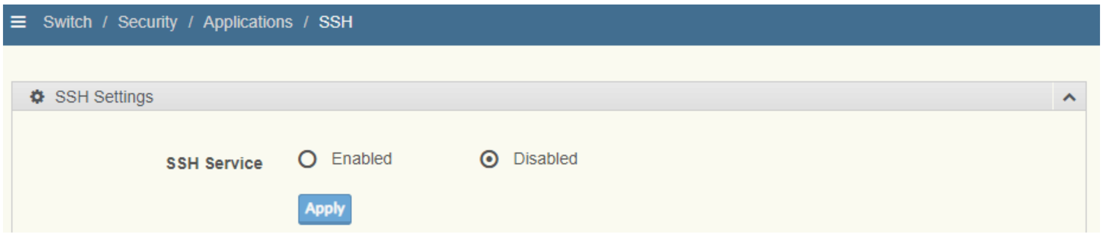
Information Name	Information Value
Telnet Service	Enabled
Current Telnet Sessions Count	0

Figure 4.123 Security > Applications > TELNET

4.8.3.2 SSH

Secure Shell (SSH) is a protocol providing secure (encrypted) management connection to a remote device.

To access this page, click **Security** > **Applications** > **SSH**.



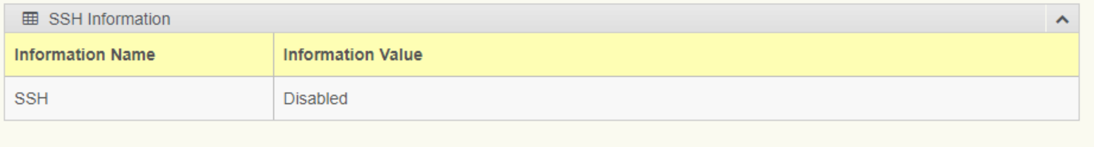
SSH Service ○ Enabled ● Disabled

Figure 4.124 Security > Applications > SSH

The following table describes the items in the previous figure.

Item	Description
SSH Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through the Secure Shell (SSH) function.
Apply	Click **Apply** to save the values and update the screen.

SSH Information are informational only as shown in the following:



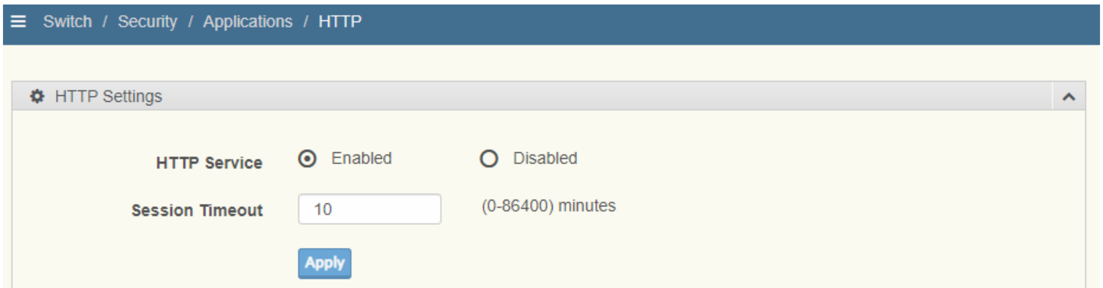
Information Name	Information Value
SSH	Disabled

Figure 4.125 Security > Applications > SSH

4.8.3.3 HTTP

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

To access this page, click **Security** > **Applications** > **HTTP**.



Switch / Security / Applications / HTTP

HTTP Settings

HTTP Service ● Enabled ○ Disabled

Session Timeout 10 (0-86400) minutes

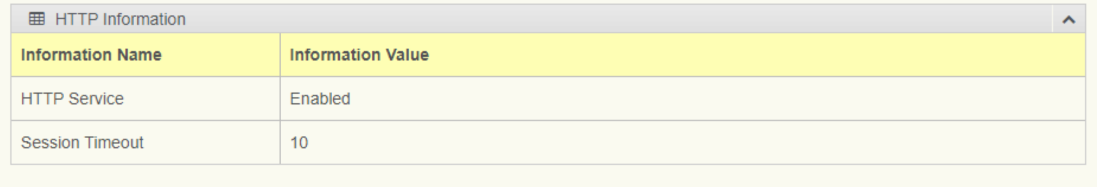
Apply

Figure 4.126 Security > Applications > HTTP

The following table describes the items in the previous figure.

Item	Description
HTTP Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through HTTP function.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the screen.

HTTP Information are informational only as shown in the following:



HTTP Information

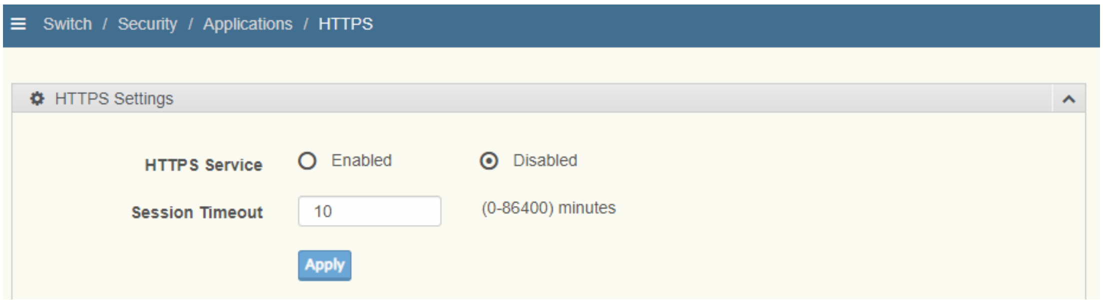
Information Name	Information Value
HTTP Service	Enabled
Session Timeout	10

Figure 4.127 Security > Applications > HTTP

4.8.3.4 HTTPS

The HTTPS page allows you to combine all kinds of AAA lists on the HTTPS line. Attempts to access the switch's Web UI from HTTPS are first authenticated.

To access this page, click **Security** > **Applications** > **HTTPS**.



Switch / Security / Applications / HTTPS

HTTPS Settings

HTTPS Service ○ Enabled ● Disabled

Session Timeout 10 (0-86400) minutes

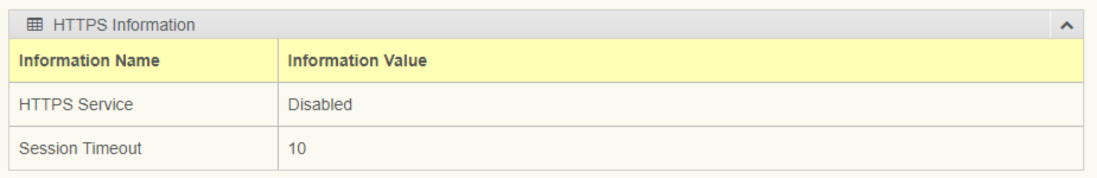
Apply

Figure 4.128 Security > Applications > HTTPS

The following table describes the items in the previous figure.

Item	Description
HTTPS Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation over HTTPS.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the screen.

HTTPS Information are informational only as shown in the following:



HTTPS Information

Information Name	Information Value
HTTPS Service	Disabled
Session Timeout	10

Figure 4.129 Security > Applications > HTTPS

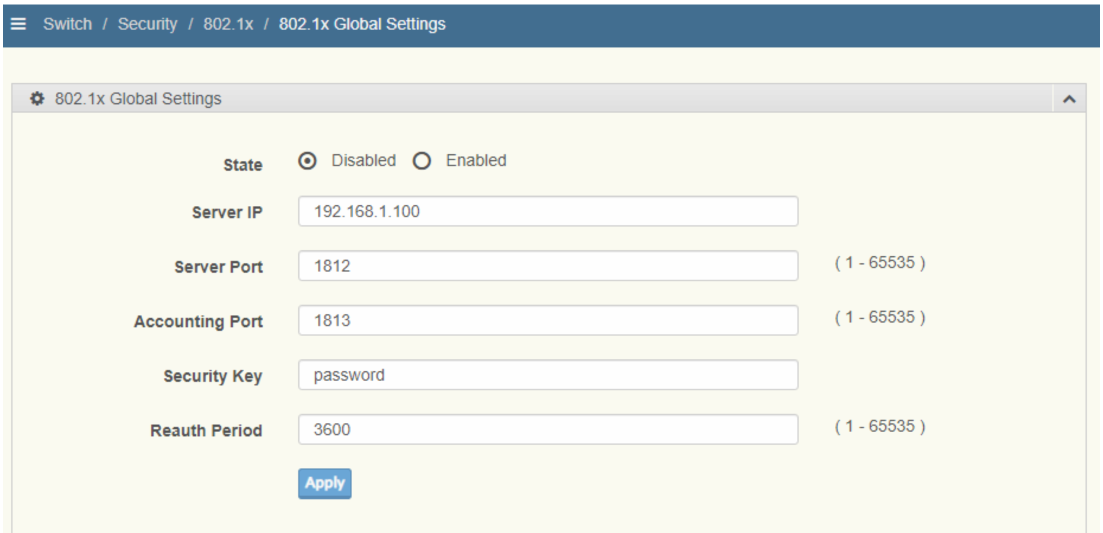
4.8.4 802.1x

The 802.1x function provides port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

4.8.4.1 802.1x Settings

The 802.1x Settings page allows you to set the state (enabled or disabled) for the selected IP server address, port, accounting port and associated password, including a re-authentication period.

To access this page, click **Security** > **802.1x** > **802.1x Settings**.



Switch / Security / 802.1x / 802.1x Global Settings

802.1x Global Settings

State ● Disabled ○ Enabled

Server IP 192.168.1.100

Server Port 1812 (1 - 65535)

Accounting Port 1813 (1 - 65535)

Security Key password

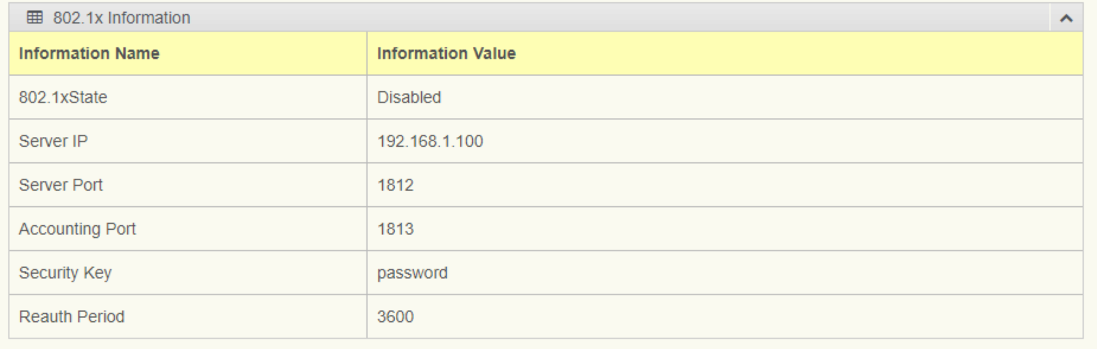
Reauth Period 3600 (1 - 65535)

Figure 4.130 Security > 802.1x > 802.1x Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to set up 802.1x Setting function.
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Accounting Port	Enter the port number (1 to 65535) assigned to the listed server IP configured to provide authorization and authentication for network access.
Security Key	Enter the variable to define the network security key used in authentication.
Reauth Period	Enter the variable in seconds to define the period of time between authentication attempts.
Apply	Click **Apply** to save the values and update the screen.

802.1x Information are informational only as shown in the following:



802.1x Information

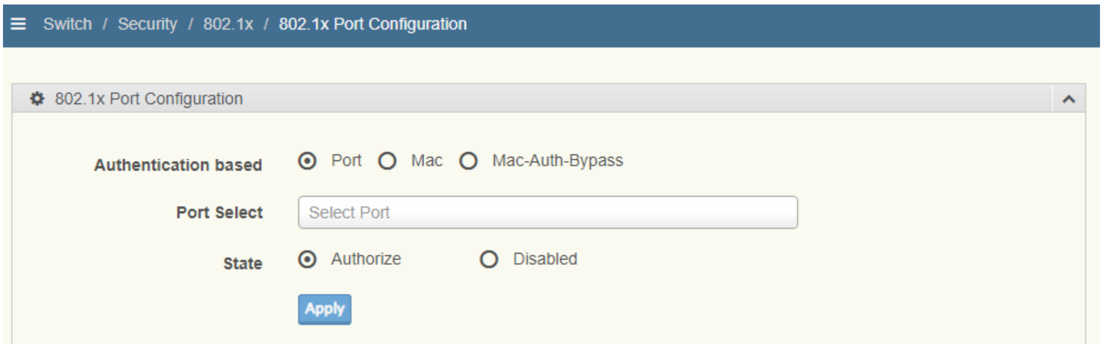
Information Name	Information Value
802.1xState	Disabled
Server IP	192.168.1.100
Server Port	1812
Accounting Port	1813
Security Key	password
Reauth Period	3600

Figure 4.131 Security > 802.1x > 802.1x Settings

4.8.4.2 802.1x Port Configuration

The 802.1x Port Configuration page allows you to identify the authorization state for a port by using a MAC or Port authentication base.

To access this page, click **Security** > **802.1x** > **802.1x Port Configuration**.



Switch / Security / 802.1x / 802.1x Port Configuration

802.1x Port Configuration

Authentication based ◉ Port ○ Mac ○ Mac-Auth-Bypass

Port Select: Select Port

State ◉ Authorize ○ Disabled

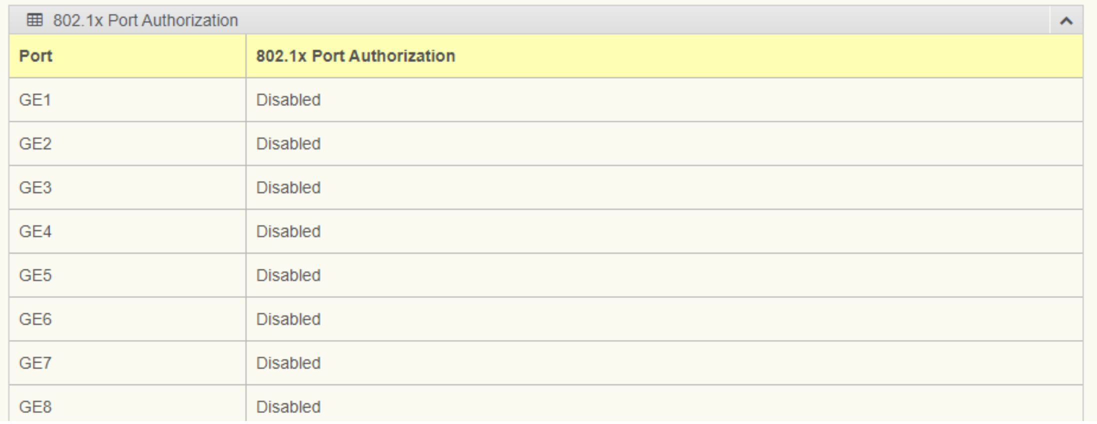
Apply

Figure 4.132 Security > 802.1x > 802.1x Port Configuration

The following table describes the items in the previous figure.

Item	Description
Authentication based	Click **Port** or **Mac** to designate the type of configuration for the 802.1x Port setting.
Port Select	Enter the port number associated with the configuration setting.
State	Click **Authorize** or **Disabled** to define the listed port's state mode.
Apply	Click **Apply** to save the values and update the screen.

802.1x Port Authorization are informational only as shown in the following:



802.1x Port Authorization

Port	802.1x Port Authorization
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled

Figure 4.133 Security > 802.1x > 802.1x Port Configuration

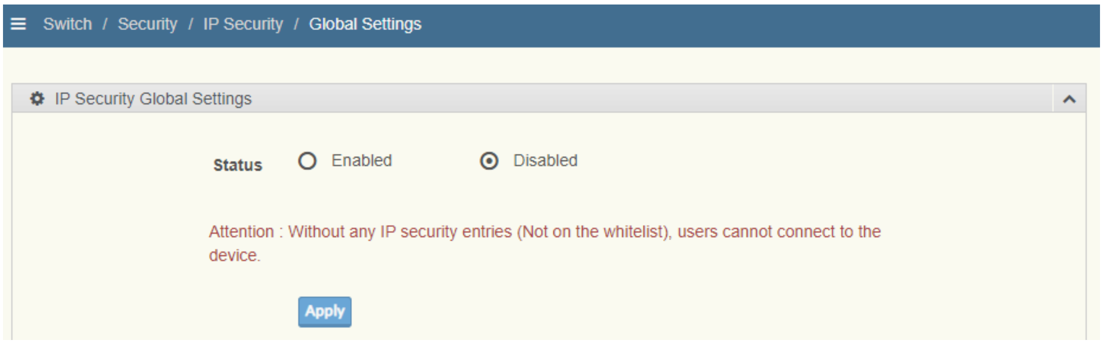
4.8.5 IP Security

This section provides you a means to configure the IP Security features available on the device.

4.8.5.1 Global Settings

The Global Settings page allows you to set the IP Security status (enabled or disabled).

To access this page, click **Security** > **IP Security** > **Global Settings**.



☰ Switch / Security / IP Security / Global Settings

IP Security Global Settings

Status ○ Enabled ● Disabled

Attention : Without any IP security entries (Not on the whitelist), users cannot connect to the device.

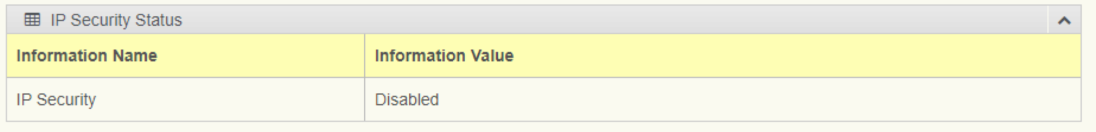
Figure 4.134 Security > IP Security > Global Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click **Enabled** or **Disabled** to define the global setting for the IP security function.
Apply	Click **Apply** to save the values and update the screen.

Note! *Without IP security entries (not on Whitelist), users can not connect to the device.*

IP Security Status are informational only as shown in the following:



IP Security Status

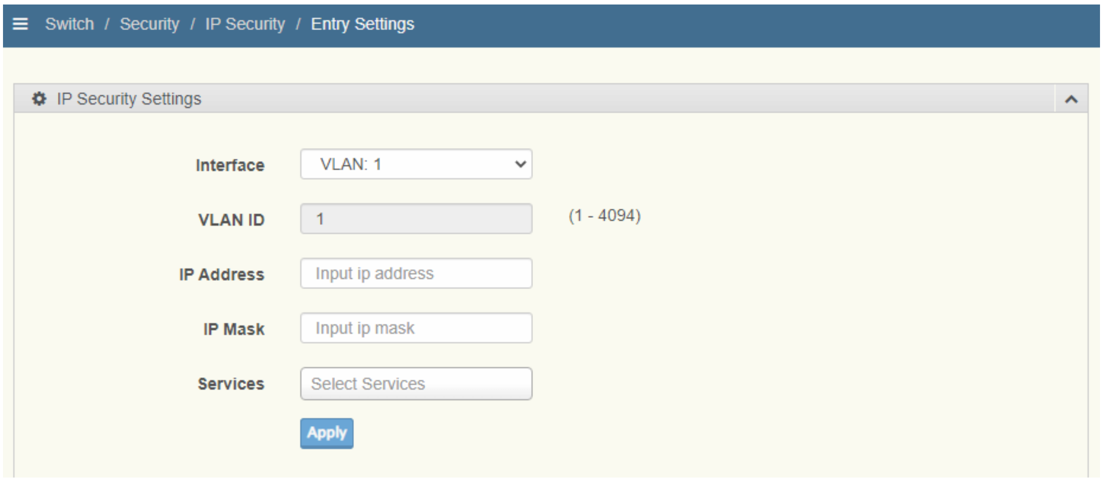
Information Name	Information Value
IP Security	Disabled

Figure 4.135 Security > IP Security > Global Settings

4.8.5.2 Entry Settings

Once the Global Setting is enabled, use the Entry Settings to define an IP Security entry.

To access this page, click **Security** > **IP Security** > **Entry Settings**.



Switch / Security / IP Security / Entry Settings

IP Security Settings

Interface: VLAN: 1

VLAN ID: 1 (1 - 4094)

IP Address: Input ip address

IP Mask: Input ip mask

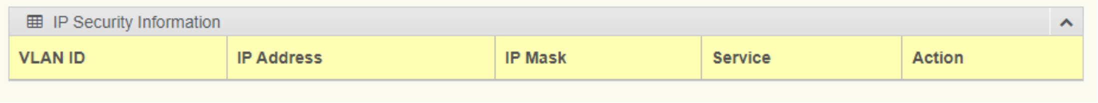
Services: Select Services

Figure 4.136 Security > IP Security > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the interface to the requested setting.
VLAN ID	
IP Address	Enter the source IP address to apply the IP Security function.
IP Mask	Enter the IP address for use in masking the previous IP Address.
Services	Enter the type of services to associate with the entry setting.
Apply	Click **Apply** to save the values and update the screen.

IP Security Information are informational only as shown in the following:



IP Security Information

VLAN ID	IP Address	IP Mask	Service	Action

Figure 4.137 Security > IP Security > Entry Settings

4.9 QoS

The QoS function allows you to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

4.9.1 General

Traditionally, networks operate on a best-effort delivery basis, all traffic has equal priority and an equal chance of being delivered in a timely manner. When there is congestion, all traffic has an equal chance of being dropped.

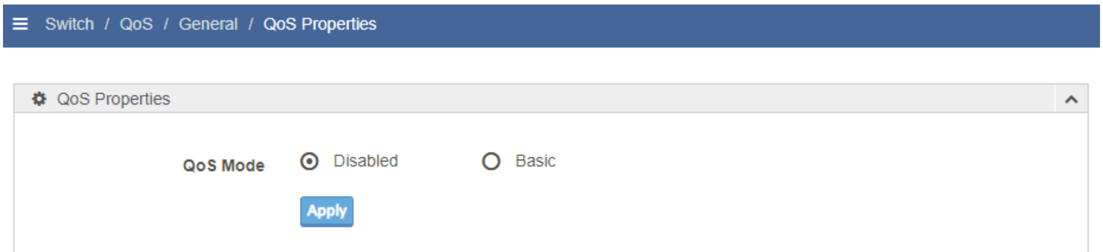
The QoS feature can be configured for congestion-management and congestion-avoidance to specifically manage the priority of the traffic delivery. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

The QoS implementation is based on the prioritization values in Layer 2 frames.

4.9.1.1 QoS Properties

The QoS Properties allows you to set the QoS mode.

To access this page, click **QoS** > **General** > **QoS Properties**.



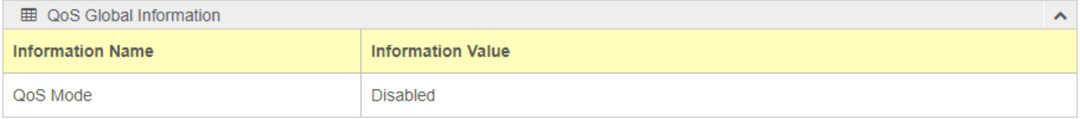
QoS Mode ● Disabled ○ Basic

Figure 4.138 QoS > General > QoS Properties

The following table describes the items in the previous figure.

Item	Description
QoS Mode	Select **Disabled** or **Basic** to setup the QoS function.
Apply	Click **Apply** to save the values and update the screen.

QoS Global Information are informational only as shown in the following:



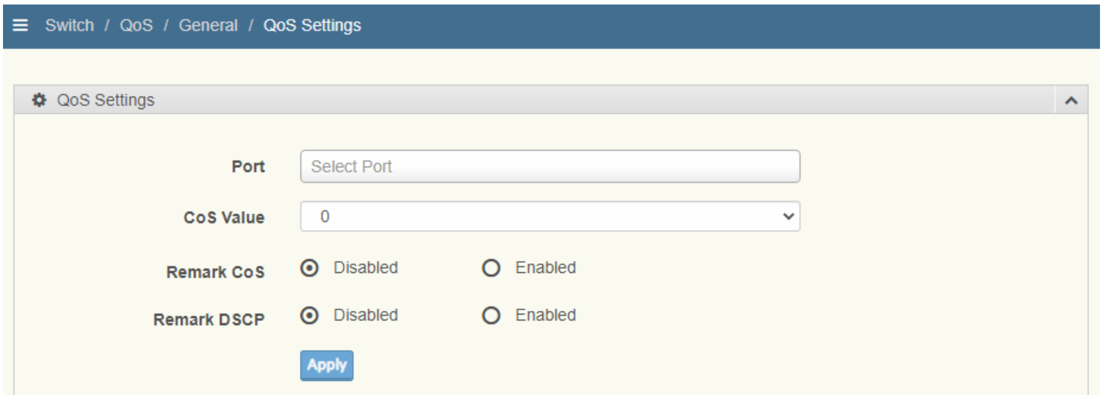
Information Name	Information Value
QoS Mode	Disabled

Figure 4.139 QoS > General > QoS Properties

4.9.1.2 QoS Settings

Once the QoS function is enabled, you can configure the available settings.

To access this page, click **QoS** > **General** > **QoS Settings**.



Port: Select Port

CoS Value: 0

Remark CoS: ● Disabled ○ Enabled

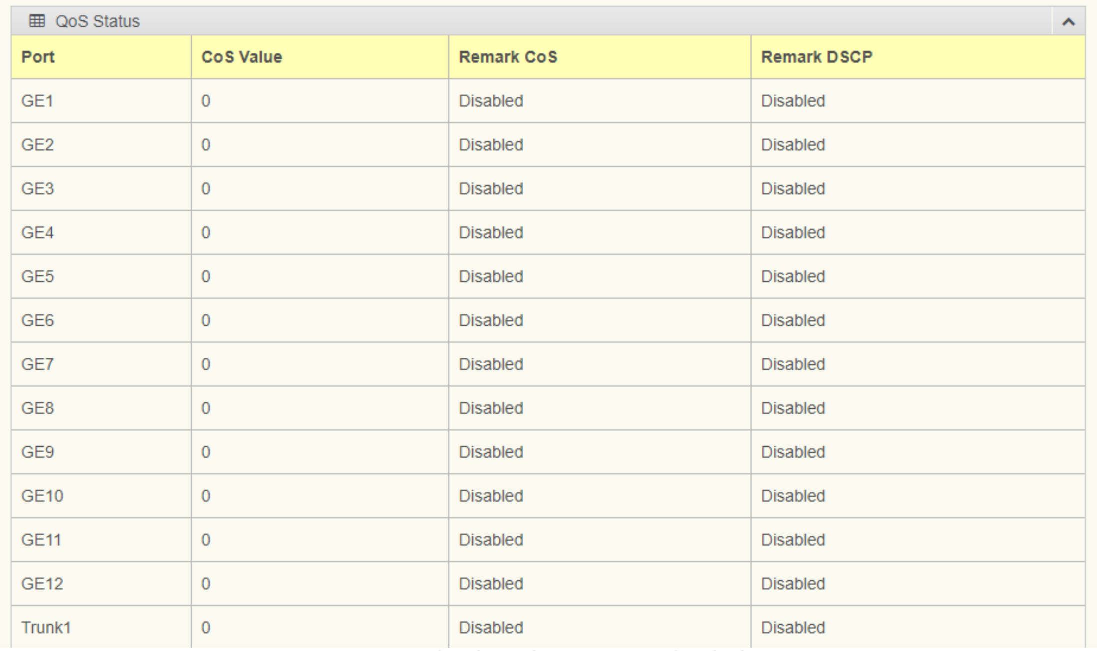
Remark DSCP: ● Disabled ○ Enabled

Figure 4.140 QoS > General > QoS Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to associate with the QoS setting.
CoS Value	Click the drop-down menu to designate the Class of Service (CoS) value (0 to 7) for the Port entry.
Remark CoS	Click **Disabled** or **Enabled** to setup the Remark CoS function. When enabled the LAN (preassigned priority values) is marked at Layer 2 boundary to CoS values.
Remark DSCP	Click **Disabled** or **Enabled** to setup the DSCP remark option for the QoS function.
Apply	Click **Apply** to save the values and update the screen.

QoS Status are informational only as shown in the following:



Port	CoS Value	Remark CoS	Remark DSCP
GE1	0	Disabled	Disabled
GE2	0	Disabled	Disabled
GE3	0	Disabled	Disabled
GE4	0	Disabled	Disabled
GE5	0	Disabled	Disabled
GE6	0	Disabled	Disabled
GE7	0	Disabled	Disabled
GE8	0	Disabled	Disabled
GE9	0	Disabled	Disabled
GE10	0	Disabled	Disabled
GE11	0	Disabled	Disabled
GE12	0	Disabled	Disabled
Trunk1	0	Disabled	Disabled

Figure 4.141 QoS > General > QoS Settings

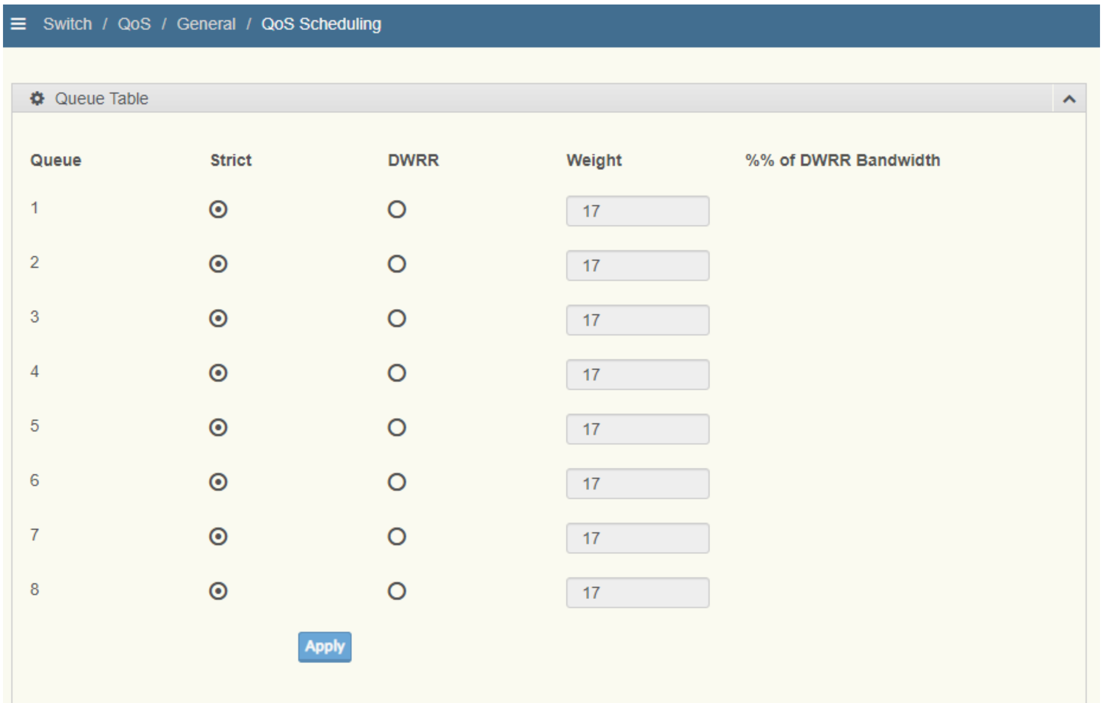
4.9.1.3 Queue Scheduling

The switch support eight CoS queues for each egress port. For each of the eight queues, two types of scheduling can be configured: Strict Priority and Weighted Round Robin (WRR).

Strict Priority scheduling is based on the priority of queues. Packets in a high-priority queue are always sent first and packets in a low-priority queue are only sent after all the high priority queues are empty.

Weighted RoundRobin (WRR) scheduling is based on the user priority specification to indicate the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents low-priority queues from being completely ignored during periods of high priority traffic. The WRR scheduler sends some packets from each queue in turn.

To access this page, click **QoS** > **General** > **QoS Scheduling**.



Switch / QoS / General / QoS Scheduling

Queue Table

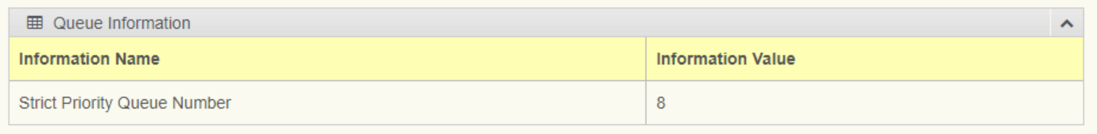
Queue	Strict	DWRR	Weight	%% of DWRR Bandwidth
1	●	○	17	
2	●	○	17	
3	●	○	17	
4	●	○	17	
5	●	○	17	
6	●	○	17	
7	●	○	17	
8	●	○	17	

Figure 4.142 QoS > General > QoS Scheduling

The following table describes the items in the previous figure.

Item	Description
Queue	Queue entry for egress port.
Strict	Select Strict to assign the scheduling designation to the selected queue.
WRR	Select WRR to assign the scheduling designation to the selected queue.
Weight	Enter a queue priority (weight) relative to the defined entries (WRR only).
% of WRR Bandwidth	Displays the allotted bandwidth for the queue entry in percentage values.
Apply	Click **Apply** to save the values and update the screen.

Queue Information are informational only as shown in the following:



Queue Information

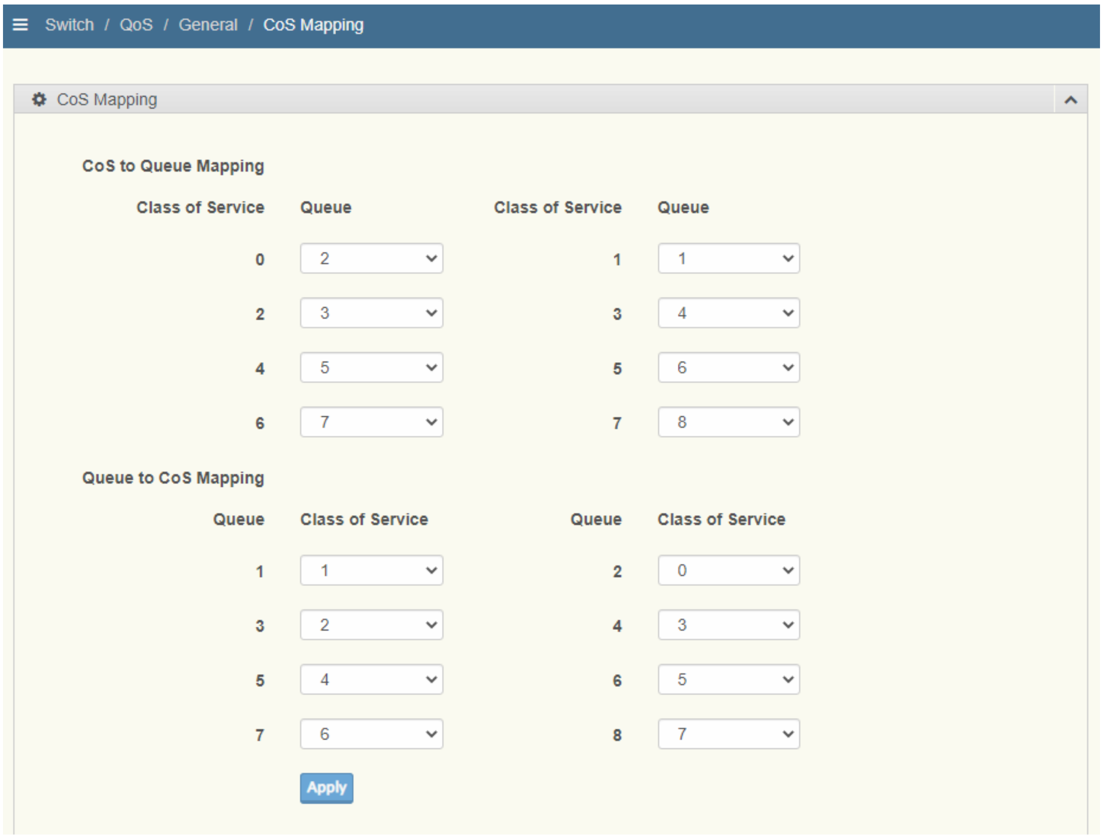
Information Name	Information Value
Strict Priority Queue Number	8

Figure 4.143 QoS > General > QoS Scheduling

4.9.1.4 CoS Mapping

The CoS Mapping allows you to apply CoS mapping.

To access this page, click **QoS** > **General** > **CoS Mapping**.



CoS to Queue Mapping

Class of Service	Queue	Class of Service	Queue
0	2	1	1
2	3	3	4
4	5	5	6
6	7	7	8

Queue to CoS Mapping

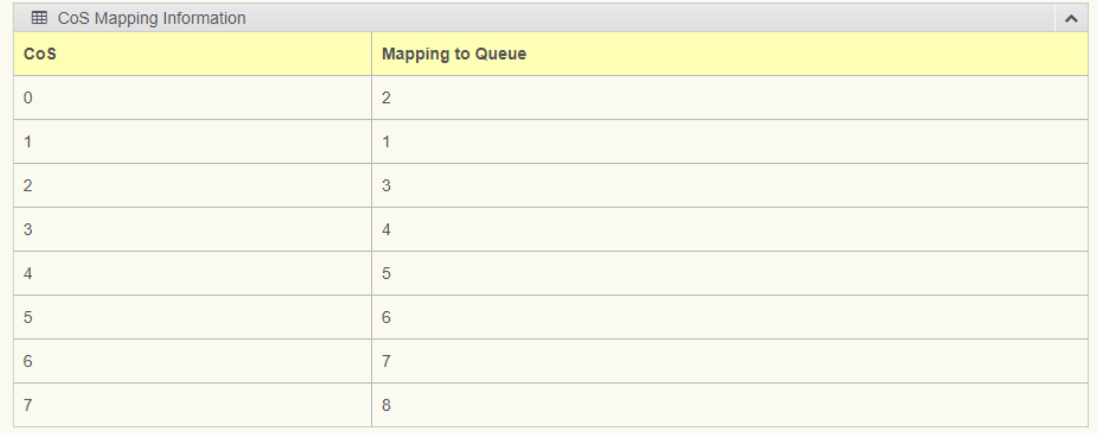
Queue	Class of Service	Queue	Class of Service
1	1	2	0
3	2	4	3
5	4	6	5
7	6	8	7

Figure 4.144 QoS > General > CoS Mapping

The following table describes the items in the previous figure.

Item	Description
CoS to Queue Mapping	
Class of Service	Displays the CoS for the queue entry.
Queue	Click the drop-down menu to select the queue priority for selected CoS.
Queue to CoS Mapping	
Queue	Displays the queue entry for CoS mapping.
Class of Service	Click the drop-down menu to select the CoS type.
Apply	Click **Apply** to save the values and update the screen.

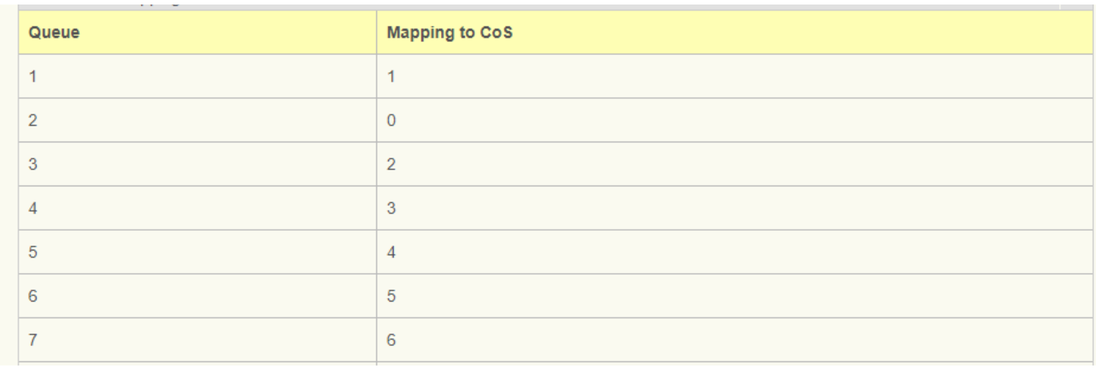
CoS Mapping Information are informational only as shown in the following:



CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Figure 4.145 QoS > General > CoS Mapping

Queue Mapping Information are informational only as shown in the following:



Queue	Mapping to CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6

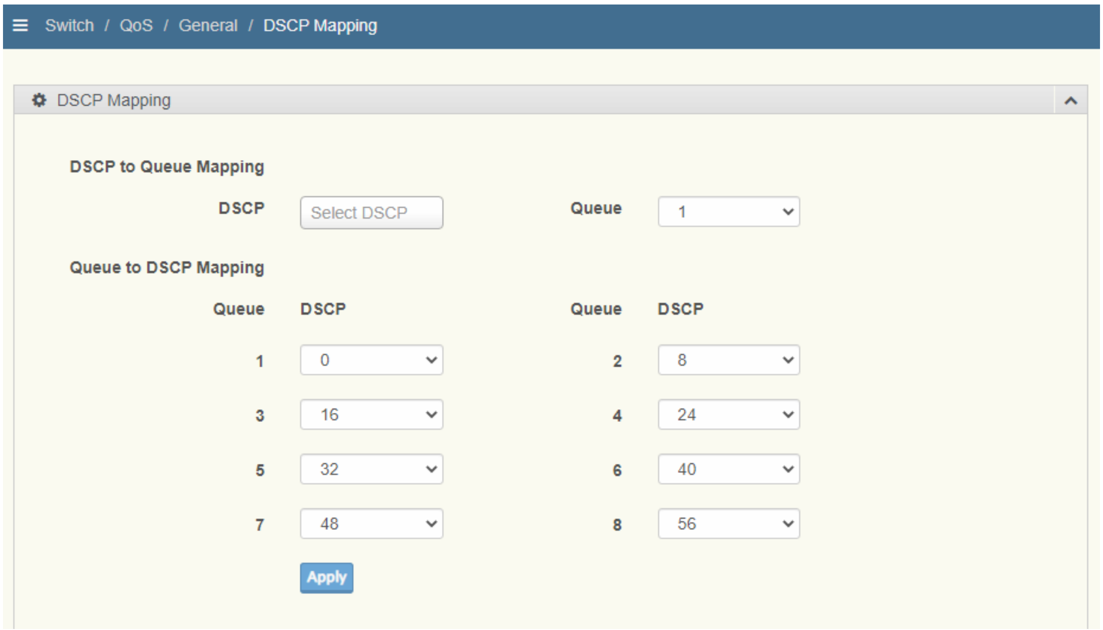
Figure 4.146 QoS > General > CoS Mapping

4.9.1.5 DSCP Mapping

The DSCP to Queue mapping function maps queue values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the DSCP to Queue map.

If these values are not appropriate for your network, you need to modify them.

To access this page, click **QoS** > **General** > **DSCP Mapping**.



DSCP to Queue Mapping

DSCP: Select DSCP   Queue: 1

Queue to DSCP Mapping

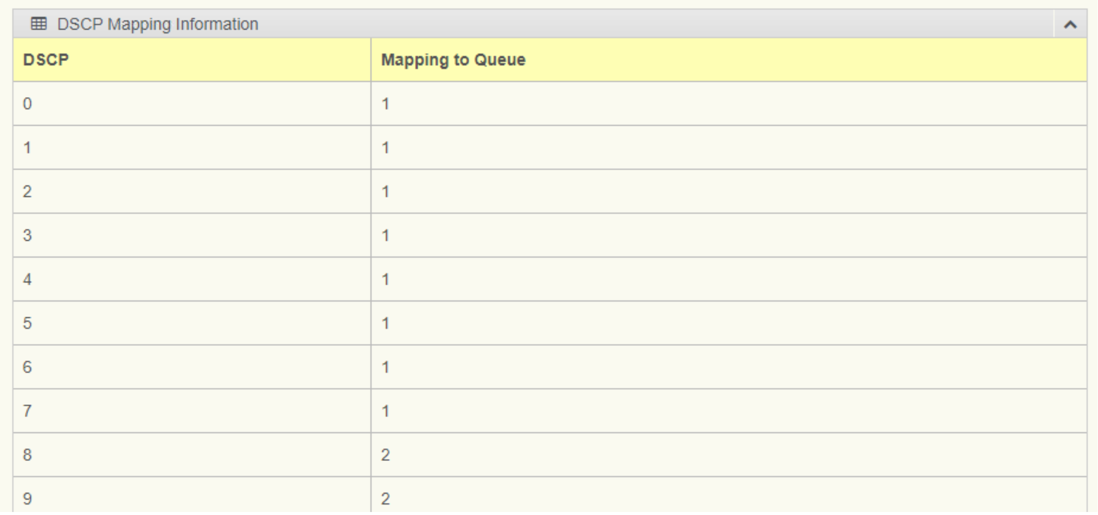
Queue	DSCP	Queue	DSCP
1	0	2	8
3	16	4	24
5	32	6	40
7	48	8	56

Figure 4.147 QoS > General > DSCP Mapping

The following table describes the items in the previous figure.

Item	Description
DSCP to Queue Mapping	
DSCP	Enter the DSCP entry to define the precedence values.
Queue	Click the drop-down menu to select the queue designation for the DSCP value.
Queue to DSCP Mapping	
Queue	Displays the queue value for the DSCP map.
DSCP	Click the drop-down menu to select the DSCP entry to define the precedence values.
Apply	Click **Apply** to save the values and update the screen.

DSCP Mapping Information are informational only as shown in the following:

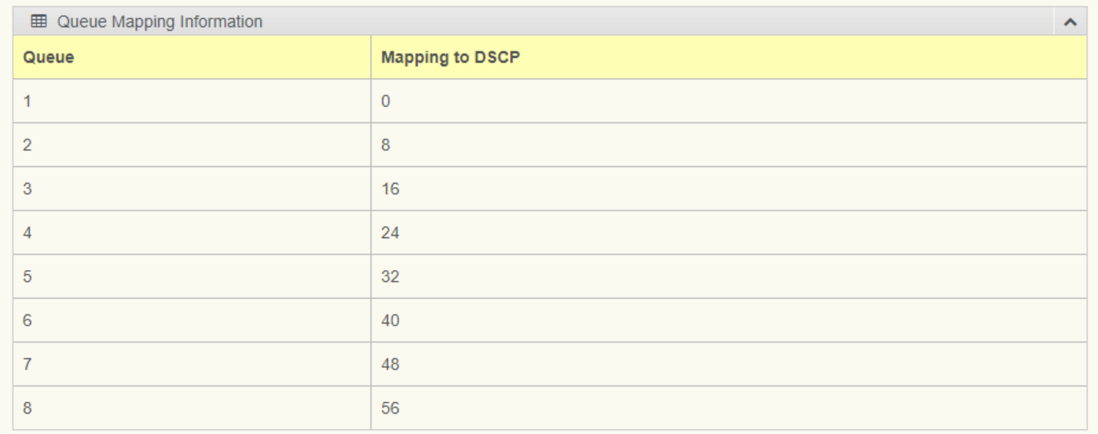


DSCP Mapping Information

DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2

Figure 4.148 QoS > General > DSCP Mapping

Queue Mapping Information are informational only as shown in the following:



Queue Mapping Information

Queue	Mapping to DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

Figure 4.149 QoS > General > DSCP Mapping

4.9.2 QoS Basic Mode

Quality of Service (QoS) allows to give preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size sending the packets without any assurance of reliability, delay bounds, or throughput.

QoS mode supports two modes: 802.1p and DSCP.

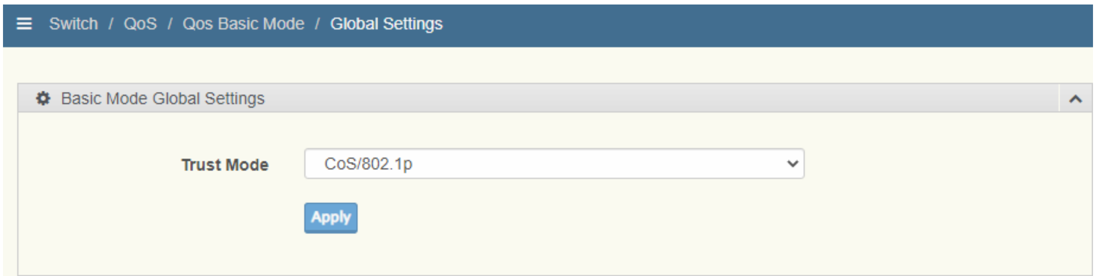
4.9.2.1 Global Settings

The Global Settings page allows you to configure the trust behavior for QoS Basic Mode. The configuration is enabled when **QoS Properties** is set to **Basic**.

When enabled, the packets entering the QoS domain are then classified at the edge of the domain.

To access this page, click **QoS** > **QoS Basic Mode** > **Global Settings**.

The function is only available when **QoS Properties** is set to **Basic**.



≡ Switch / QoS / Qos Basic Mode / Global Settings
Basic Mode Global Settings

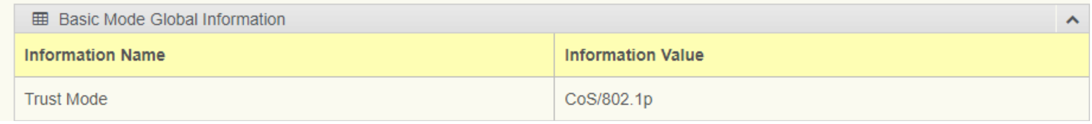
Trust Mode: CoS/802.1p

Figure 4.150 QoS > QoS Basic Mode > Global Settings

The following table describes the items in the previous figure.

Item	Description
Trust Mode	Click **Trust Mode** to select trust behavior: ■ CoS/802.1p: Map traffic to queues based on the VPT field (VLAN tag) or on the per-port default CoS/802.1p value when no VLAN tag on the incoming packet is available. ■ DSCP: All IP traffic is mapped to queues based on the DSCP field in IP header. The best effort queue is used for mapping when traffic is not IP traffic. ■ CoS/802.1p-DSCP: For IP traffic the trust CoS mode for non-IP traffic and trust DSCP mode is used.

QoS Information are informational only as shown in the following:



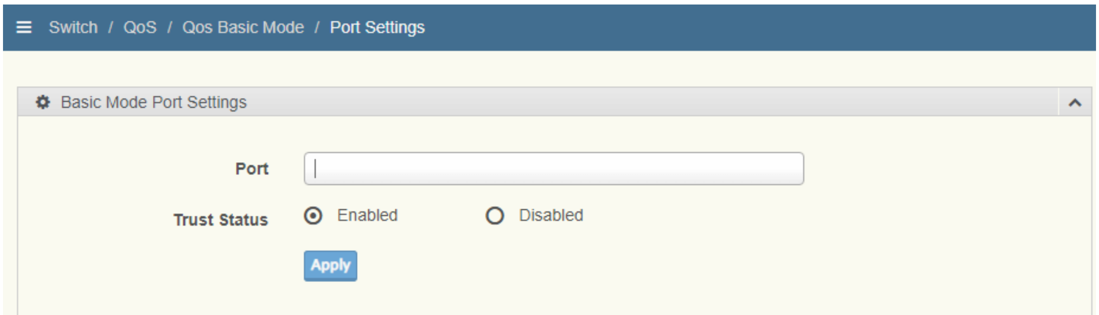
Information Name	Information Value
Trust Mode	CoS/802.1p

Figure 4.151 QoS > QoS Basic Mode > Global Settings

4.9.2.2 Port Settings

The Port Settings page allows you to define a trust state (enabled or disabled) to a listed port.

To access this page, click **QoS** > **QoS Basic Mode** > **Port Settings**.



Port:

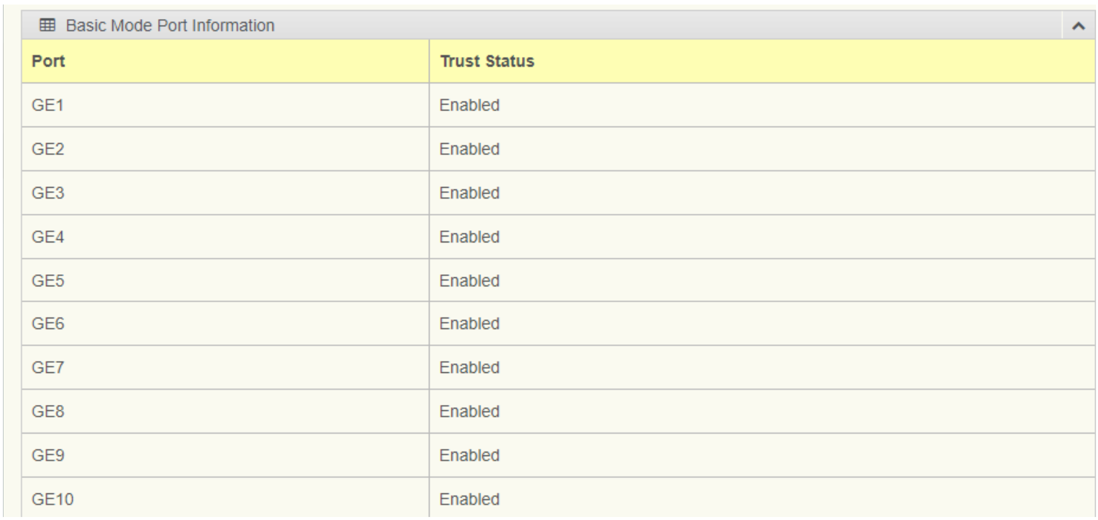
Trust Status: ● Enabled ○ Disabled

Figure 4.152 QoS > QoS Basic Mode > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the QoS basic mode setting: GE1 ~ 12, Trunk1 ~ 8.
Trust State	Select **Enabled** or **Disabled** to set the port's trust state status.
Apply	Click **Apply** to save the values and update the screen.

QoS Port Status are informational only as shown in the following:



Basic Mode Port Information

Port	Trust Status
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
GE9	Enabled
GE10	Enabled

Figure 4.153 QoS > QoS Basic Mode > Port Settings

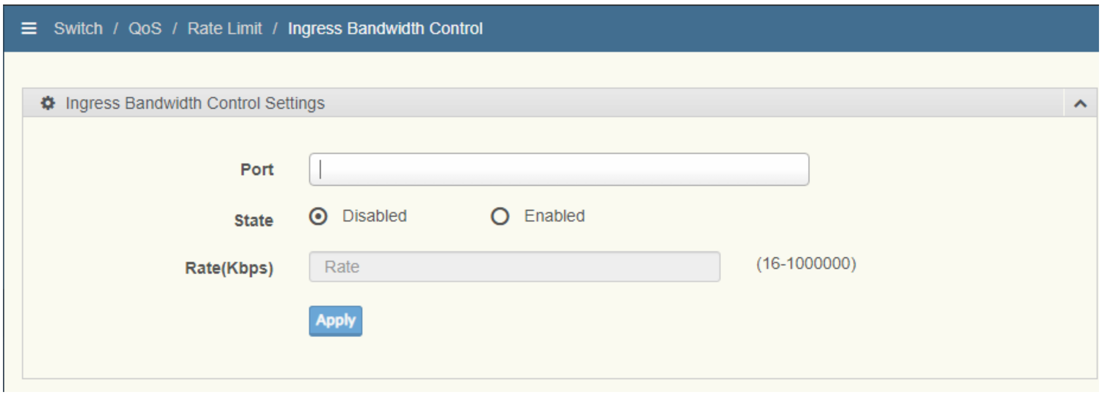
4.9.3 Rate Limit

Rate Limits features control on a per port basis. Bandwidth control is supported for the following: Ingress Bandwidth Control, Egress Bandwidth Control and Egress Queue.

4.9.3.1 Ingress Bandwidth Control

The Ingress Bandwidth Control page allows you to configure the bandwidth control for a listed port.

To access this page, click **QoS** > **Rate Limit** > **Ingress Bandwidth Control**.



Switch / QoS / Rate Limit / Ingress Bandwidth Control
Ingress Bandwidth Control Settings

Port

State ● Disabled ○ Enabled

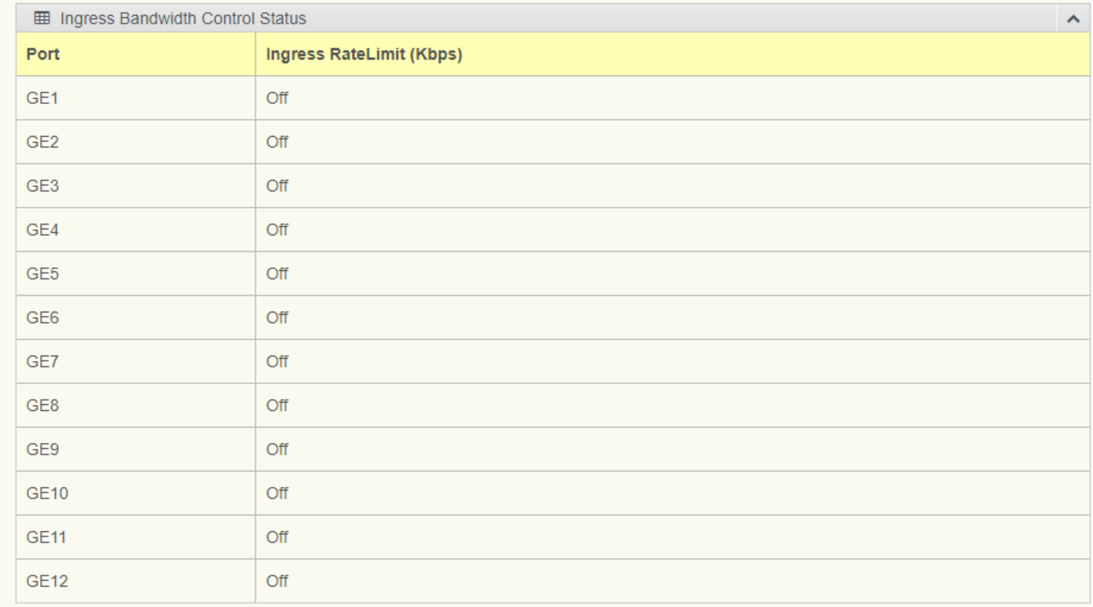
Rate(Kbps) Rate (16-1000000)

Figure 4.154 QoS > Rate Limit > Ingress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to assign the rule: GE1 ~ 12, Trunk1 ~ 8.
State	Select **Disabled** or **Enabled** to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port. The setting is enabled when **State** is enabled.
Apply	Click **Apply** to save the values and update the screen.

Ingress Bandwidth Control Status are informational only as shown in the following:



Ingress Bandwidth Control Status

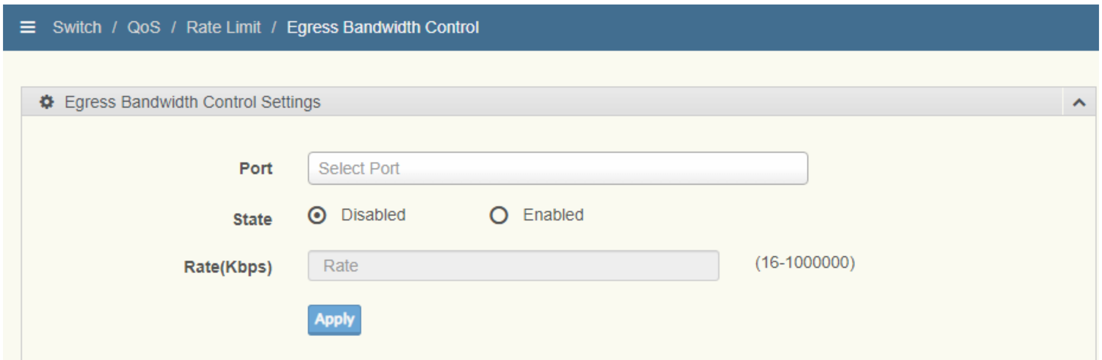
Port	Ingress RateLimit (Kbps)
GE1	Off
GE2	Off
GE3	Off
GE4	Off
GE5	Off
GE6	Off
GE7	Off
GE8	Off
GE9	Off
GE10	Off
GE11	Off
GE12	Off

Figure 4.155 QoS > Rate Limit > Ingress Bandwidth Control

4.9.3.2 Egress Bandwidth Control

The Egress Bandwidth Control page allows you to set the egress bandwidth control for a listed port.

To access this page, click **QoS** > **Rate Limit** > **Egress Bandwidth Control**.



☰ Switch / QoS / Rate Limit / Egress Bandwidth Control
Egress Bandwidth Control Settings

Port: Select Port

State: ● Disabled ○ Enabled

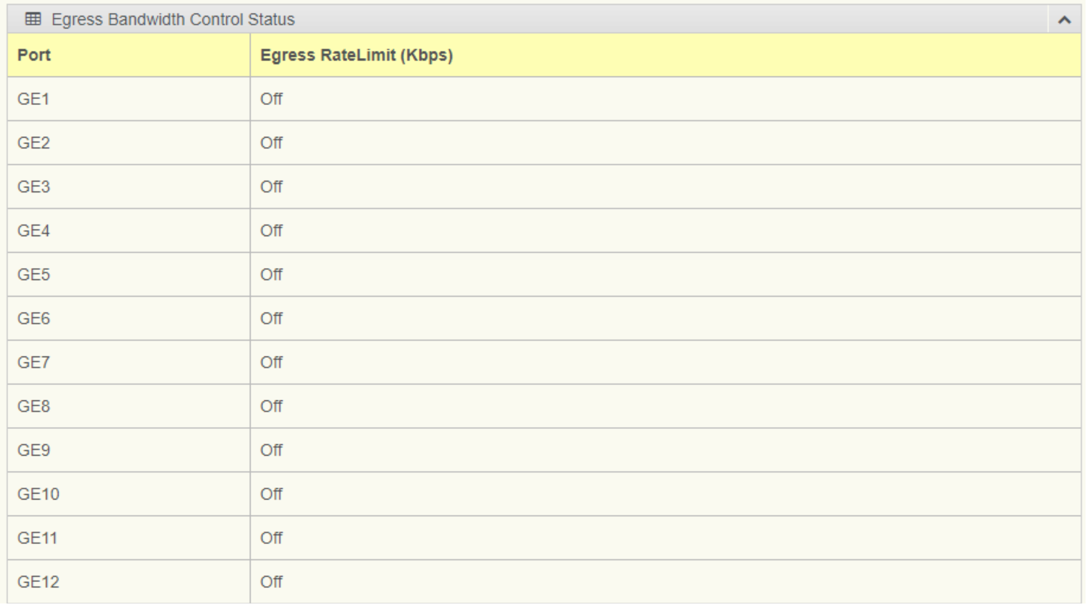
Rate(Kbps): Rate (16-1000000)

Figure 4.156 QoS > Rate Limit > Egress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to set the Egress Bandwidth Control: GE1 ~ 12, Trunk1 ~ 8.
State	Select **Disabled** or **Enabled** to set the Egress Bandwidth Control state.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate. The setting is enabled when **State** is enabled.
Apply	Click **Apply** to save the values and update the screen.

Egress Bandwidth Control Status are informational only as shown in the following:



Egress Bandwidth Control Status

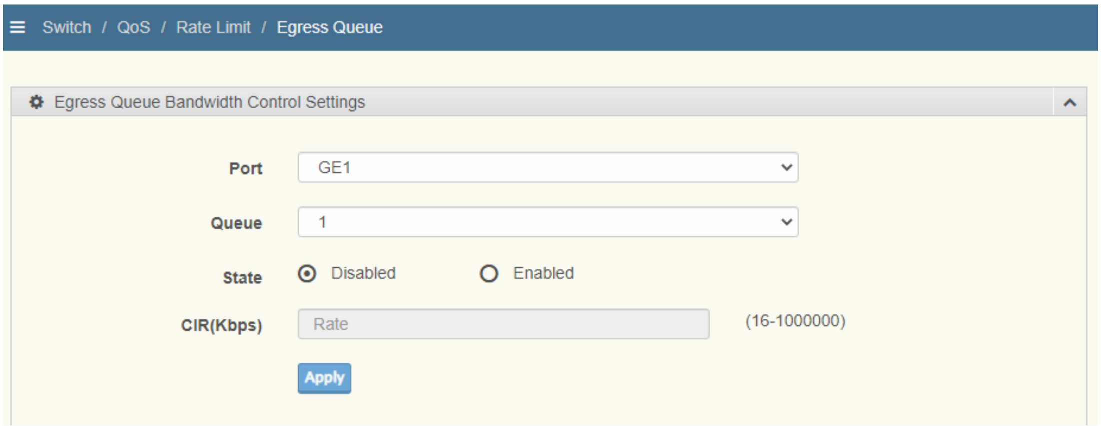
Port	Egress RateLimit (Kbps)
GE1	Off
GE2	Off
GE3	Off
GE4	Off
GE5	Off
GE6	Off
GE7	Off
GE8	Off
GE9	Off
GE10	Off
GE11	Off
GE12	Off

Figure 4.157 QoS > Rate Limit > Egress Bandwidth Control

4.9.3.3 Egress Queue

The Egress Queue page allows you to set the egress bandwidth parameters.

To access this page, click **QoS** > **Rate Limit** > **Egress Queue**.



Switch / QoS / Rate Limit / Egress Queue

Egress Queue Bandwidth Control Settings

Port: GE1

Queue: 1

State: ● Disabled ○ Enabled

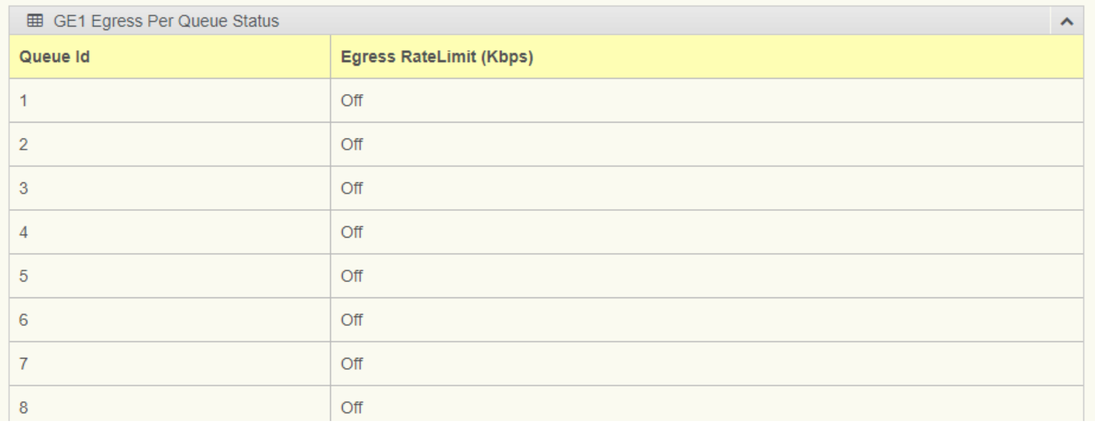
CIR(Kbps): Rate (16-1000000)

Figure 4.158 QoS > Rate Limit > Egress Queue

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port to define the Egress queue: GE1 ~ 12.
Queue	Click the drop-down menu to set the queue order for the Egress setting: 1 ~ 8.
State	Click **Disabled** or **Enabled** to set the Egress queue state.
CIR (Kbps)	Enter the value in Kbps (16 to 1000000) to set the CIR rate for the Egress queue. The setting is enabled when **State** is enabled.
Apply	Click **Apply** to save the values and update the screen.

GE1 Egress Per Queue Status are informational only as shown in the following:



GE1 Egress Per Queue Status

Queue Id	Egress RateLimit (Kbps)
1	Off
2	Off
3	Off
4	Off
5	Off
6	Off
7	Off
8	Off

Figure 4.159 QoS > Rate Limit > Egress Queue

4.10 Management

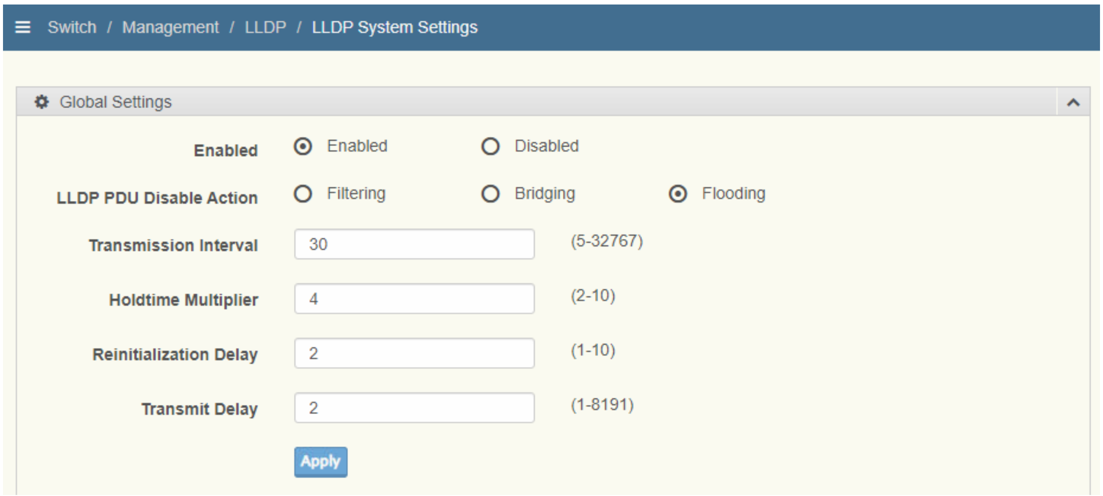
4.10.1 LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

4.10.1.1 LLDP System Settings

The LLDP System Settings allows you to configure the status (enabled or disabled) for the protocol, set the interval for frame transmission, set the hold time multiplier and the re-initialization delay.

To access this page, click **Management** > **LLDP** > **LLDP System Settings**.



≡ Switch / Management / LLDP / LLDP System Settings

Global Settings

Enabled: ● Enabled ○ Disabled

LLDP PDU Disable Action: ○ Filtering ○ Bridging ● Flooding

Transmission Interval: 30 (5-32767)

Holdtime Multiplier: 4 (2-10)

Reinitialization Delay: 2 (1-10)

Transmit Delay: 2 (1-8191)

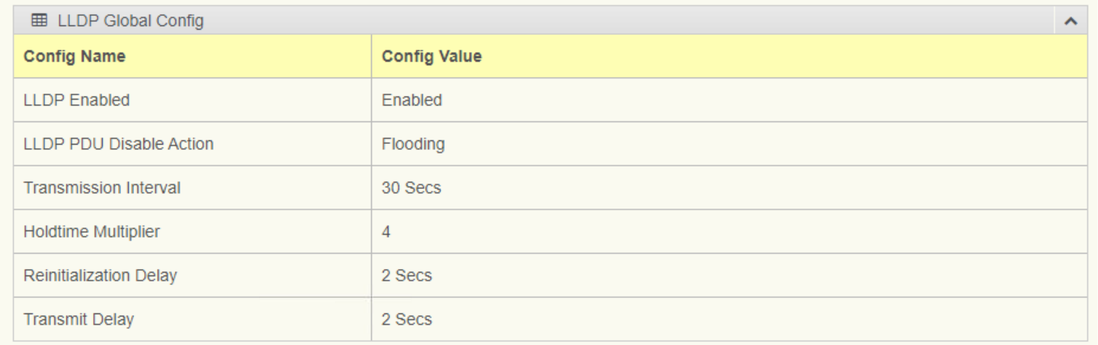
Apply

Figure 4.160 Management > LLDP > LLDP System Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click **Enabled** or **Disabled** to set the Global Settings state.
LLDP PDU Disable Action	Click to select the LLDP PDU handling action when LLDP is globally disabled. Options include: Filtered, Bridged, or Flooded.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5 to 32768 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay length before re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Apply	Click **Apply** to save the values and update the screen.

LLDP Global Config are informational only as shown in the following:



LLDP Global Config

Config Name	Config Value
LLDP Enabled	Enabled
LLDP PDU Disable Action	Flooding
Transmission Interval	30 Secs
Holdtime Multiplier	4
Reinitialization Delay	2 Secs
Transmit Delay	2 Secs

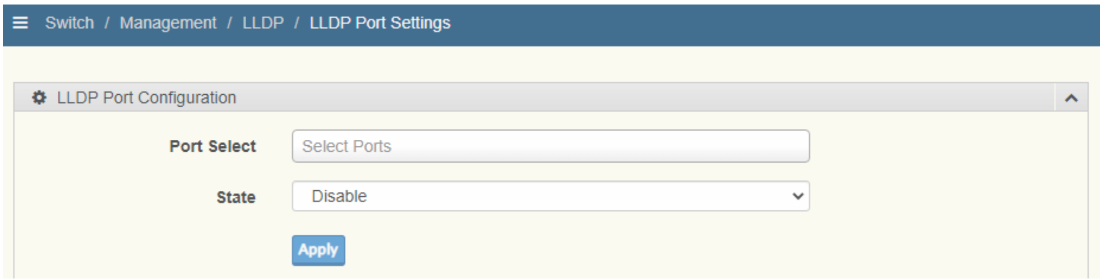
Figure 4.161 Management > LLDP > LLDP System Settings

4.10.1.2 LLDP Port Settings

The LLDP Port Settings page allows you to configure the state (enabled or disabled) of the selected port.

To access this page, click **Management** > **LLDP** > **LLDP Port Settings**.

The **LLDP Port Configuration** menu displays.



Port Select: Select Ports

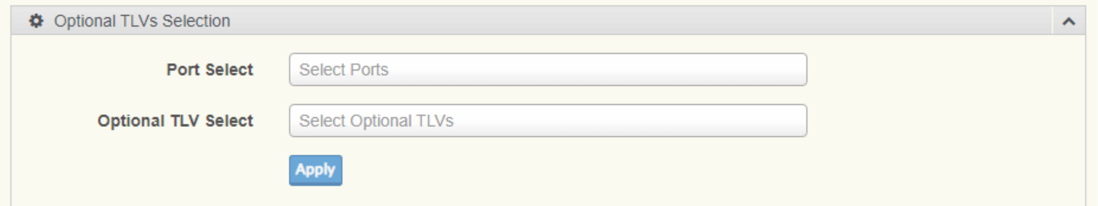
State: Disable

Figure 4.162 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the LLDP setting.
State	Click the drop-down menu to select the LLDP port state.
Apply	Click **Apply** to save the values and update the screen.

Optional TLVs Selection is described in the following figure and tables.



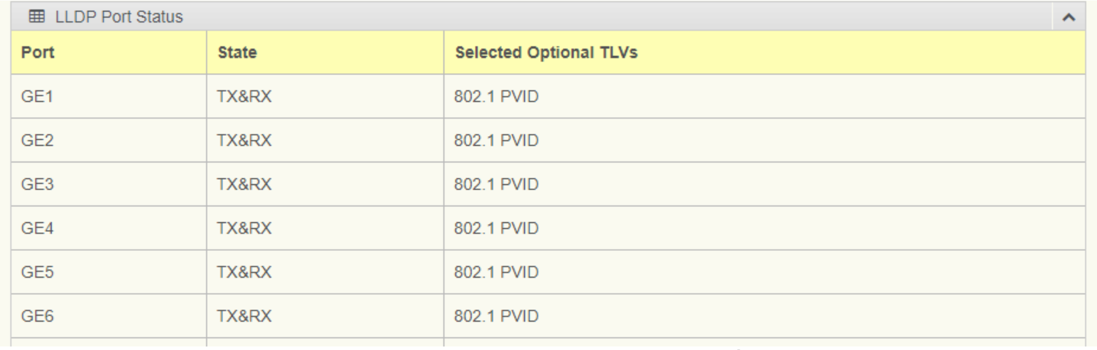
Port Select: Select Ports

Optional TLV Select: Select Optional TLVs

Figure 4.163 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

Item	Description
Port Select	Enter the port number associated with the TLV (optional) selection.
Optional TLV Select	Click the drop-down menu to select the LLDP optional TLVs to be carried (multiple selections are allowed). ■ System Name: To include system name TLV in LLDP frames. ■ Port Description: To include port description TLV in LLDP frames. ■ System Description: To include system description TLV in LLDP frames. ■ System Capability: To include system capability TLV in LLDP frames. ■ 802.3 MAC-PHY: ■ 802.3 Link Aggregation: ■ 802.3 Maximum Frame Size: ■ Management Address: ■ 802.1 PVID:
Apply	Click **Apply** to save the values and update the screen.

LLDP Port Status are informational only as shown in the following:

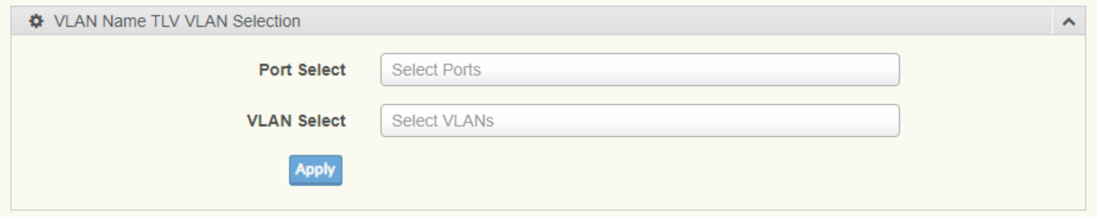


LLDP Port Status

Port	State	Selected Optional TLVs
GE1	TX&RX	802.1 PVID
GE2	TX&RX	802.1 PVID
GE3	TX&RX	802.1 PVID
GE4	TX&RX	802.1 PVID
GE5	TX&RX	802.1 PVID
GE6	TX&RX	802.1 PVID

Figure 4.164 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

VLAN Name TLV VLAN Selection is described in the following figure and tables.



VLAN Name TLV VLAN Selection

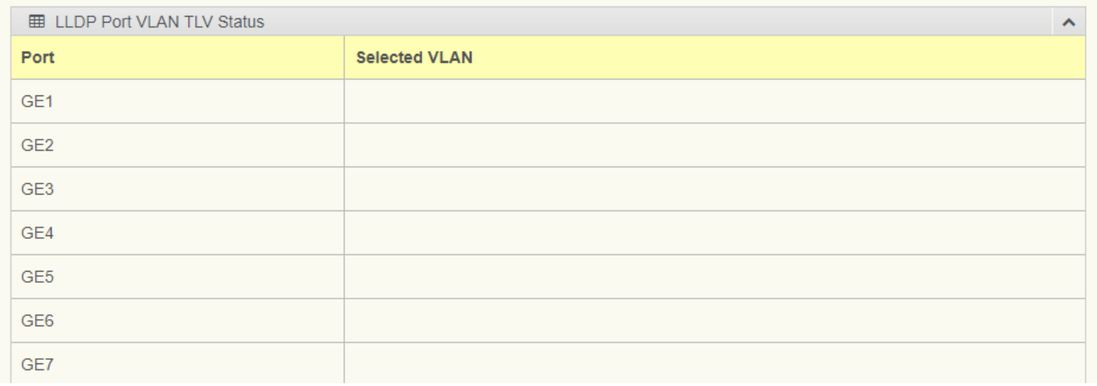
Port Select: Select Ports

VLAN Select: Select VLANs

Figure 4.165 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

Item	Description
Port Select	Enter the port number to associated with the TLV selection.
VLAN Select	Select the VLAN Name ID to be carried out (multiple selection is allowed).
Apply	Click **Apply** to save the values and update the screen.

LLDP Port VLAN TLV Status are informational only as shown in the following:



LLDP Port VLAN TLV Status

Port	Selected VLAN
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	

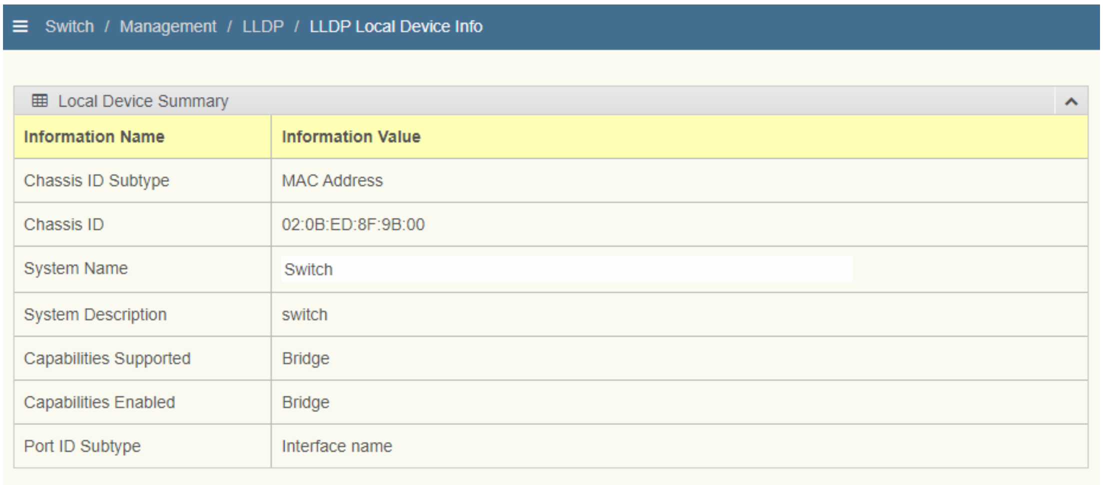
Figure 4.166 Management > LLDP > LLDP Port Settings > LLDP Port Configuration

4.10.1.3 LLDP Local Device Info

The LLDP Local Device Info page allows you to view information regarding network devices, providing that the switch has already obtained LLDP information on the devices.

To access this page, click **Management** > **LLDP** > **LLDP Local Device Info**.

Local Device Summary are informational only as shown in the following:



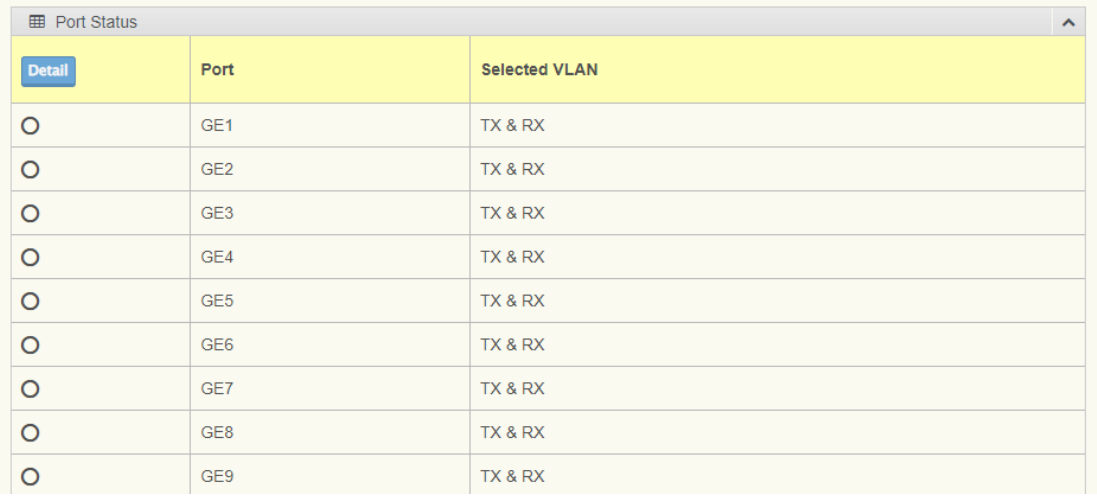
Switch / Management / LLDP / LLDP Local Device Info

Local Device Summary

Information Name	Information Value
Chassis ID Subtype	MAC Address
Chassis ID	02:0B:ED:8F:9B:00
System Name	Switch
System Description	switch
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Figure 4.167 Management > LLDP > LLDP Local Device Info

Port Status are informational only as shown in the following:



Port Status

Detail	Port	Selected VLAN
○	GE1	TX & RX
○	GE2	TX & RX
○	GE3	TX & RX
○	GE4	TX & RX
○	GE5	TX & RX
○	GE6	TX & RX
○	GE7	TX & RX
○	GE8	TX & RX
○	GE9	TX & RX

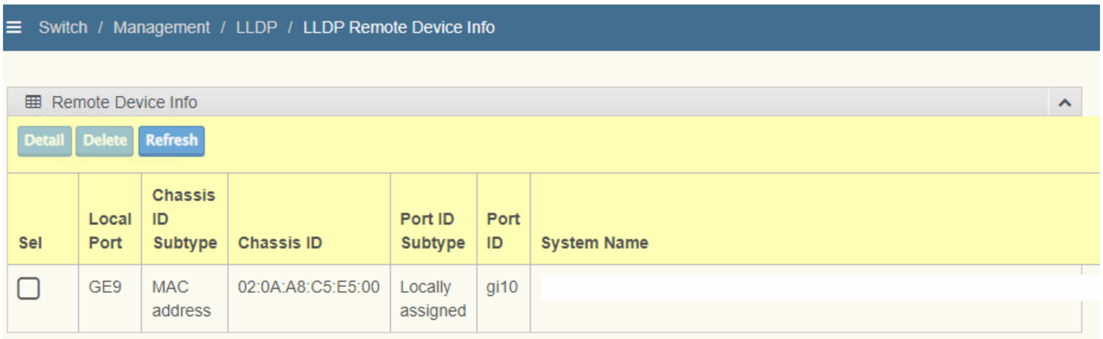
Figure 4.168 Management > LLDP > LLDP Local Device Info

Item	Description
Detail	Click **Detail** to view additional information for the selected entry.

4.10.1.4 LLDP Remote Device Info

The LLDP Remote Device Info page allows you to view information about remote devices, LLDP information must be available on the switch.

To access this page, click **Management** > **LLDP** > **LLDP Remote Device Info**.



Switch / Management / LLDP / LLDP Remote Device Info

Remote Device Info

Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name
□	GE9	MAC address	02:0A:A8:C5:E5:00	Locally assigned	gi10	

Figure 4.169 Management > LLDP > LLDP Remote Device Info

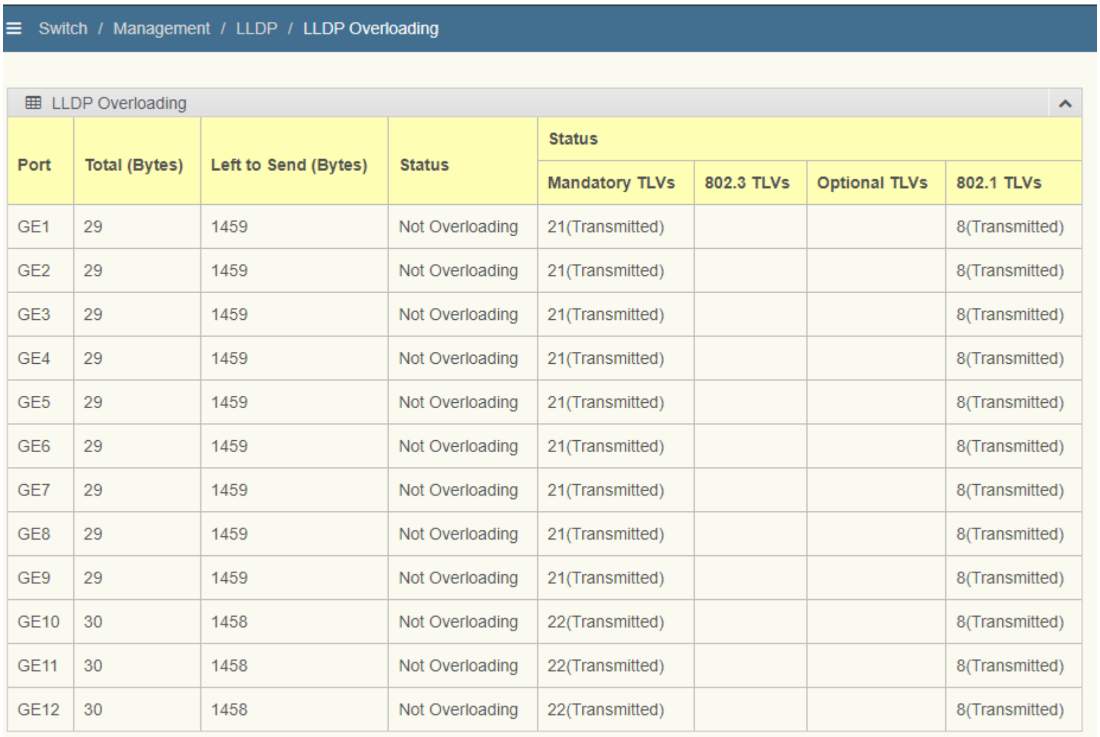
The following table describes the items in the previous figure.

Item	Description
Detail	Click to display the device details.
Delete	Click to delete the selected devices.
Refresh	Click to refresh the remote device information list.

4.10.1.5 LLDP Overloading

To access this page, click **Management** > **LLDP** > **LLDP Overloading**.

LLDP Overloading are informational only as shown in the following:



Port	Total (Bytes)	Left to Send (Bytes)	Status	Status			
				Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
GE1	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE2	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE3	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE4	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE5	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE6	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE7	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE8	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE9	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE10	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)
GE11	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)
GE12	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)

Figure 4.170 Management > LLDP > LLDP Remote Device Info

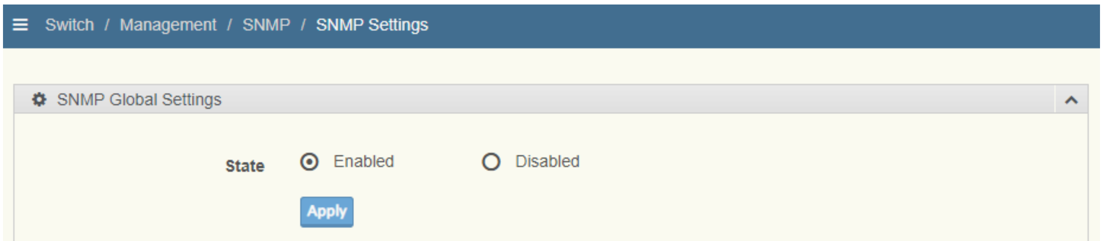
4.10.2 SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

4.10.2.1 SNMP Settings

The SNMP Settings page allows you to set the SNMP daemon state (enabled or disabled).

To access this page, click **Management** > **SNMP** > **SNMP Settings**.



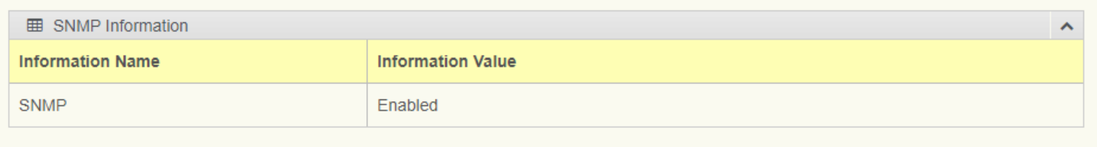
State ● Enabled ○ Disabled

Figure 4.171 Management > SNMP > SNMP Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to define the SNMP daemon.
Apply	Click **Apply** to save the values and update the screen.

SNMP Information are informational only as shown in the following:



SNMP Information

Information Name	Information Value
SNMP	Enabled

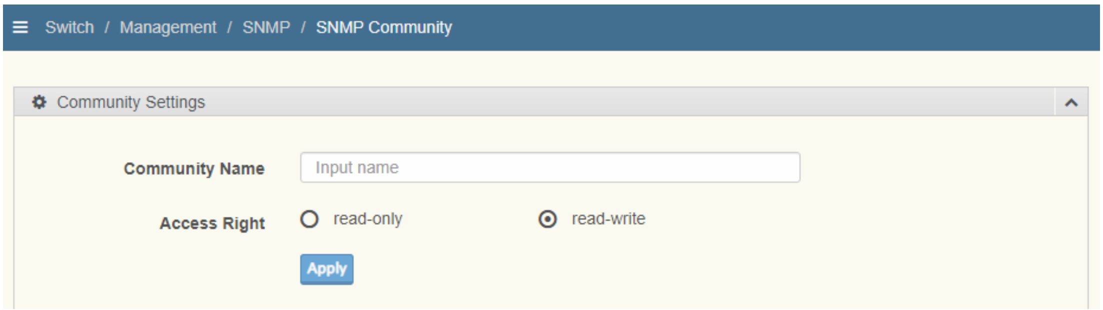
Figure 4.172 Management > SNMP > SNMP Settings

4.10.2.2 SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. It's role is similar to the password function. If SNMP v1 and SNMP v2c are used, you can go directly from the configuration settings to this page to configure the SNMP community.

To access this page, click **Management** > **SNMP** > **SNMP Community**.



Switch / Management / SNMP / SNMP Community

Community Settings

Community Name: Input name

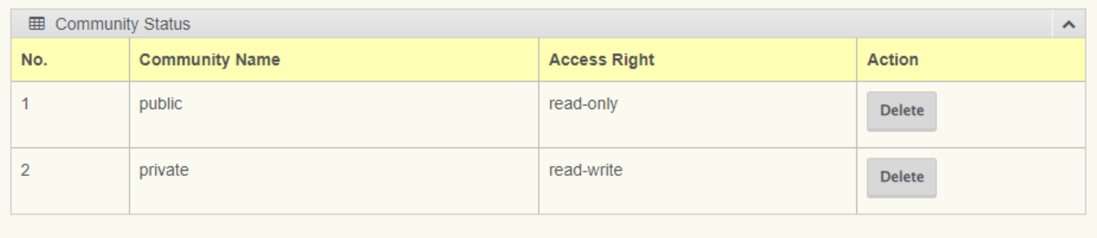
Access Right: ○ read-only ● read-write

Figure 4.173 Management > SNMP > SNMP Community

The following table describes the items in the previous figure.

Item	Description
Community Name	Enter a string to identify the community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or **read-write**).
Apply	Click **Apply** to save the values and update the screen.

Community Status are informational only as shown in the following:



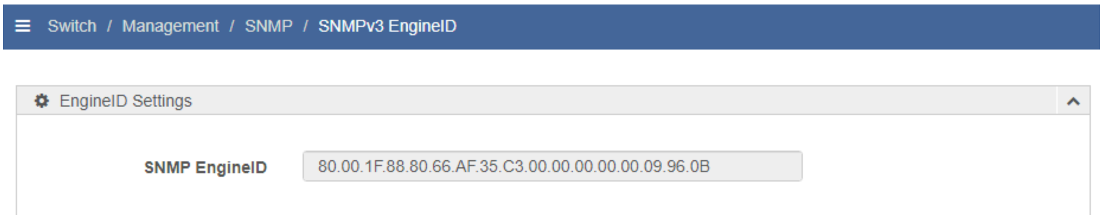
Community Status

No.	Community Name	Access Right	Action
1	public	read-only	Delete
2	private	read-write	Delete

Figure 4.174 Management > SNMP > SNMP Community

4.10.2.3 SNMPv3 EngineID

The SNMPv3 engine ID is available for display to identify the SNMP entity in the management domain.



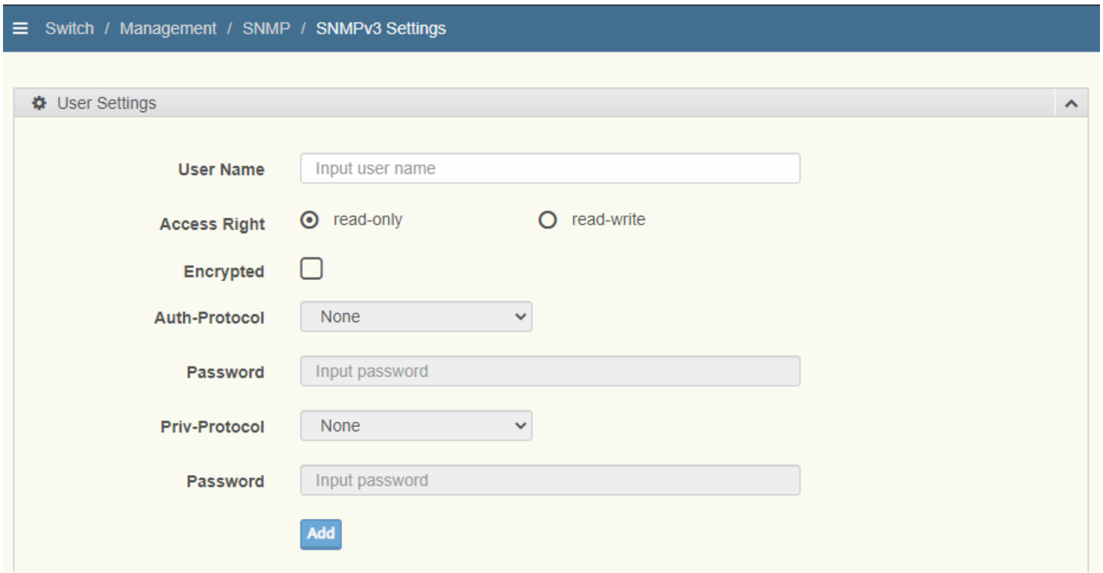
SNMP EngineID: 80.00.1F.88.80.66.AF.35.C3.00.00.00.00.00.09.96.0B

Figure 4.175 Management > SNMP > SNMPv3 EngineID

4.10.2.4 SNMPv3 Settings

The SNMP User Settings page allows you to create SNMP groups. The users have the same level of security and access control permissions as defined by the group settings.

To access this page, click **Management** > **SNMP** > **SNMPv3 Settings**.



User Name: Input user name

Access Right: ● read-only ○ read-write

Encrypted: □

Auth-Protocol: None

Password: Input password

Priv-Protocol: None

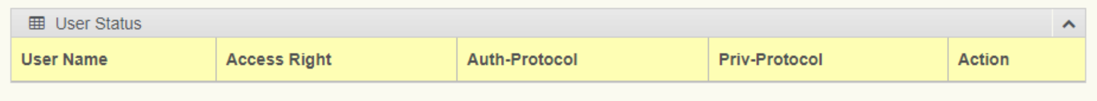
Password: Input password

Figure 4.176 Management > SNMP > SNMPv3 Settings

The following table describes the items in the previous figure.

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click **read-only** or **read-write** to define the access right for the profile.
Encrypted	Click the option to set the encrypted option for the user setting.
Auth-Protocol	Click the drop-down menu to select the authentication level: MD5 or SHA. The field requires a user password. ■ MD5: specify HMAC-MD5-96 authentication level ■ SHA: specify HMAC-SHA authentication protocol
Password	Enter the characters to define the password associated with the authentication protocol.
Priv-Protocol	Click the drop-down menu to select an authorization protocol: none or DES.The field requires a user password. ■ None: no authorization protocol in use ■ DES: specify 56-bit encryption in use
Password	Enter the characters to define the password associated with the authorization protocol.
Add	Click **Add** to save the values and update the screen.

User Status are informational only as shown in the following:



User Status

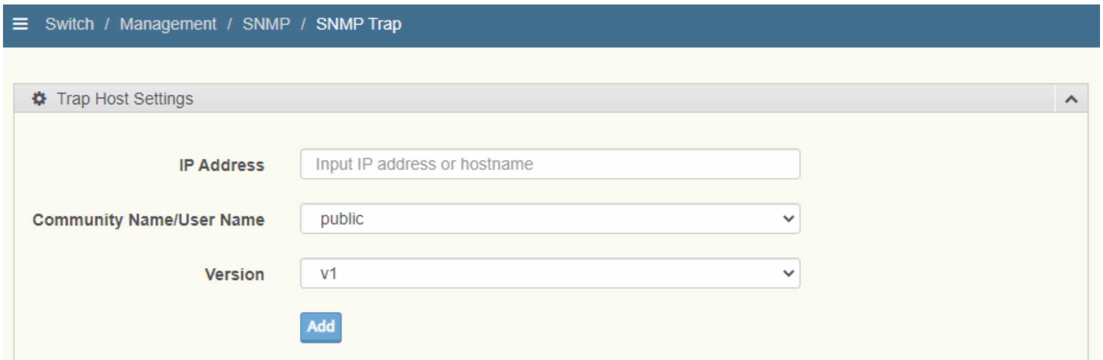
User Name	Access Right	Auth-Protocol	Priv-Protocol	Action

Figure 4.177 Management > SNMP > SNMPv3 Settings

4.10.2.5 SNMP Trap

The SNMP Trap page allows you to set the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message.

To access this page, click **Management** > **SNMP** > **SNMP Trap**.



☰ Switch / Management / SNMP / SNMP Trap

Trap Host Settings

IP Address: Input IP address or hostname

Community Name/User Name: public

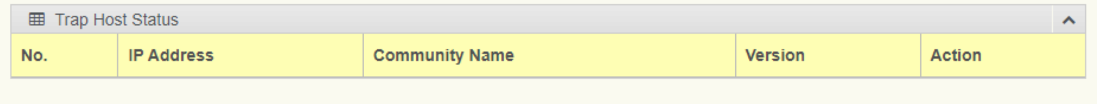
Version: v1

Figure 4.178 Management > SNMP > SNMP Trap

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address to designate the SNMP trap host.
Community Name / User Name	Click the drop-down menu to select a community string (public / private).
Version	Click the drop-down menu to designate the SNMP version credentials: **v1**, v2c - trap, v2c - inform, v3 - trap, v3 - inform.
Add	Click **Add** to save the values and update the screen.

Trap Host Status are informational only as shown in the following:



Trap Host Status

No.	IP Address	Community Name	Version	Action

Figure 4.179 Management > SNMP > SNMP Trap

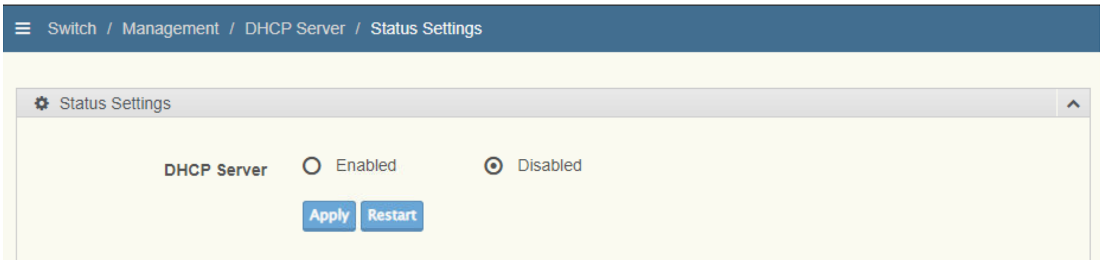
4.10.3 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network protocol enabling a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

4.10.3.1 Status Settings

The Status Settings page allows you to configure the DHCP server mode (enabled or disabled).

To access this page, click **Management** > **DHCP Server** > **Status Settings**.



≡ Switch / Management / DHCP Server / Status Settings

Status Settings

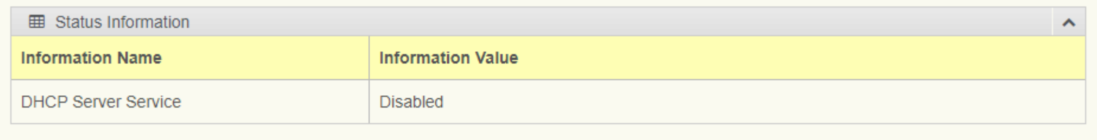
DHCP Server ○ Enabled ● Disabled

Figure 4.180 Management > DHCP Server > Status Settings

The following table describes the items in the previous figure.

Item	Description
DHCP Server	Select **Enable** or **Disable** to designate the DHCP server function type. When a new DHCP server mode is selected, the switch requires a system restart for the new mode to take effect.
Apply	Click **Apply** to save the values and update the screen.
Restart	Click **Restart** to have the switch perform a system restart function. In the event that the IP settings are changed, the DHCP server must be restarted for the IP settings to take effect.

Status Information are informational only as shown in the following:



Status Information

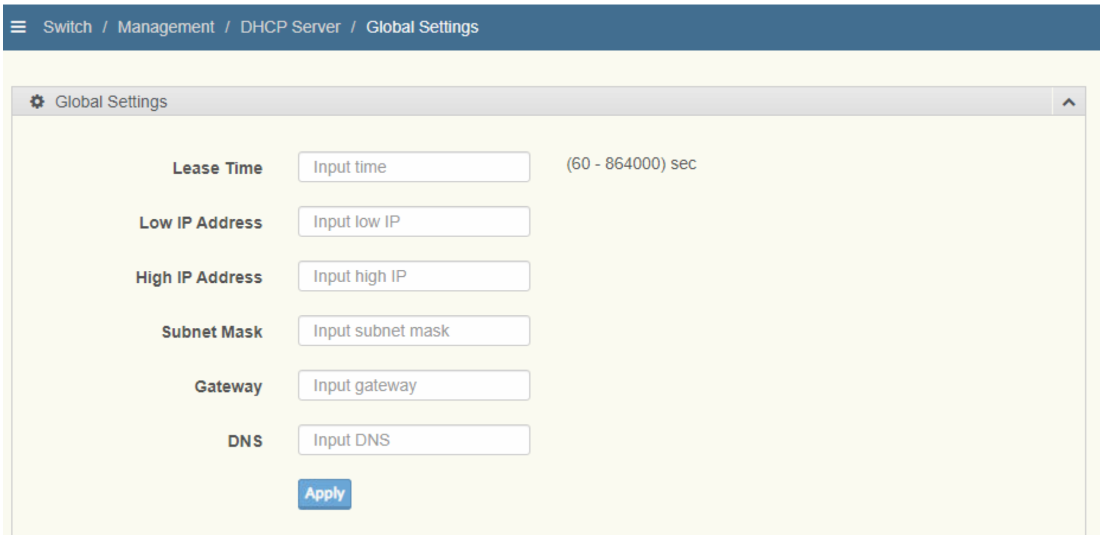
Information Name	Information Value
DHCP Server Service	Disabled

Figure 4.181 Management > DHCP Server > Status Settings

4.10.3.2 Global Settings

The Global Settings page allows you to configure the global settings for the DHCP function.

To access this page, click **Management** > **DHCP Server** > **Global Settings**.



≡ Switch / Management / DHCP Server / Global Settings

Global Settings

Lease Time: Input time (60 - 864000) sec

Low IP Address: Input low IP

High IP Address: Input high IP

Subnet Mask: Input subnet mask

Gateway: Input gateway

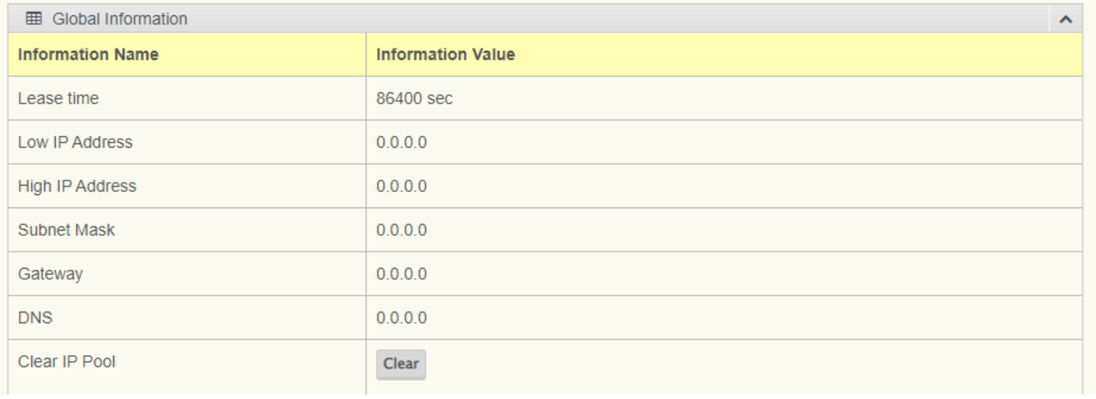
DNS: Input DNS

Figure 4.182 Management > DHCP Server > Global Settings

The following table describes the items in the previous figure.

Item	Description
Lease Time	Type in the value designating the lease time (60 - 864000) in seconds for each setting lease.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Enter the value designating the highest range in the IP address pool.
Subnet Mask	Enter the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

Global Information are informational only as shown in the following:



Global Information

Information Name	Information Value
Lease time	86400 sec
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Clear IP Pool	Clear

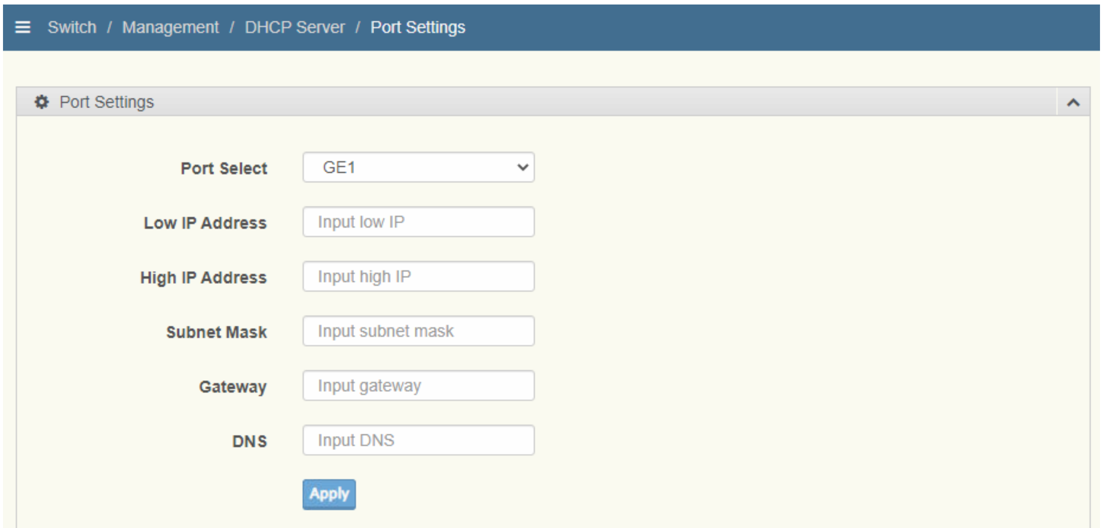
Figure 4.183 Management > DHCP Server > Global Settings

Item	Description
Clear	Click **Clear** to remove the entries from the IP pool.

4.10.3.3 Port Settings

The Port Settings page allows you to configure selected ports for the DHCP function.

To access this page, click **Management** > **DHCP Server** > **Port Settings**.



Port Select: GE1

Low IP Address: Input low IP

High IP Address: Input high IP

Subnet Mask: Input subnet mask

Gateway: Input gateway

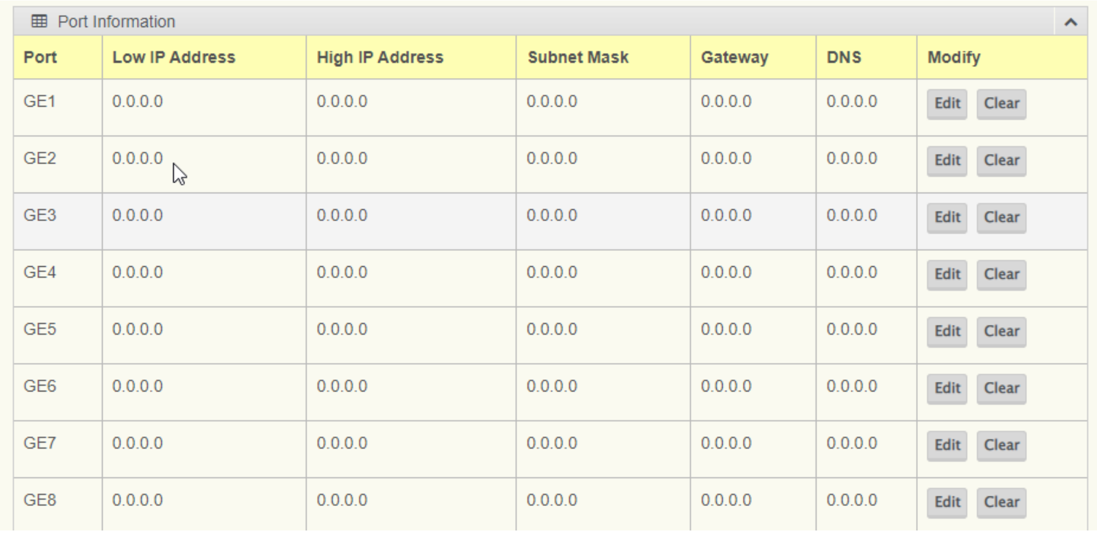
DNS: Input DNS

Figure 4.184 Management > DHCP Server > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The suboptions are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

Port Information are informational only as shown in the following:



Port Information

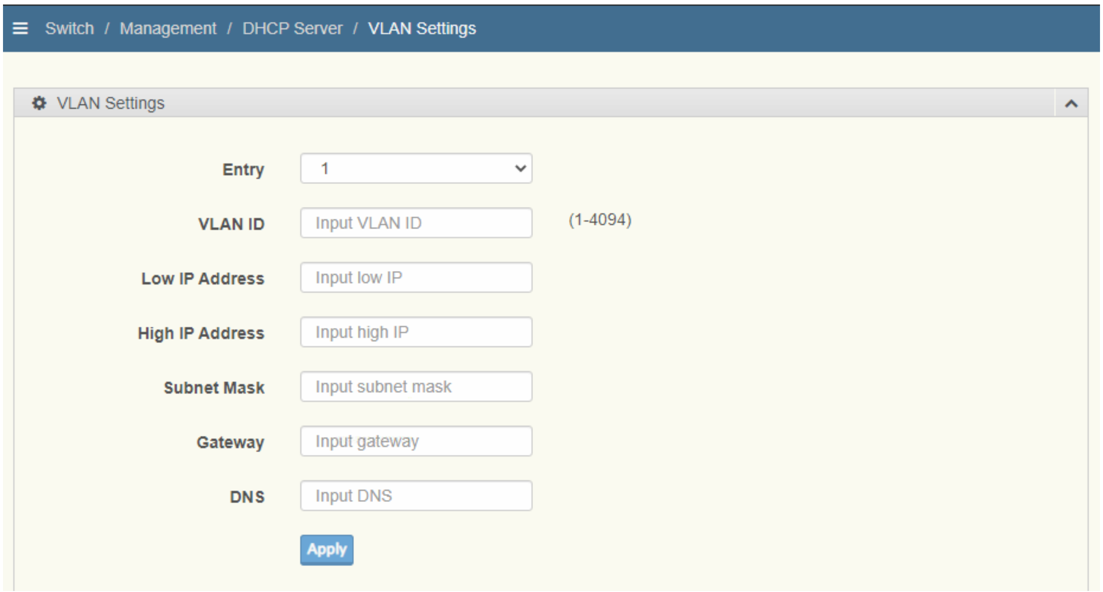
Port	Low IP Address	High IP Address	Subnet Mask	Gateway	DNS	Modify
GE1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE3	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE4	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE5	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE6	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE7	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE8	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear

Figure 4.185 Management > DHCP Server > Port Settings

Item	Description
Edit	Click **Edit** to modify the information for the selected port entry.
Clear	Click **Clear** to remove the information for the selected port entry.

4.10.3.4 VLAN Settings

To access this page, click **Management** > **DHCP Server** > **VLAN Settings**.



≡ Switch / Management / DHCP Server / VLAN Settings

VLAN Settings

Entry: 1

VLAN ID: Input VLAN ID (1-4094)

Low IP Address: Input low IP

High IP Address: Input high IP

Subnet Mask: Input subnet mask

Gateway: Input gateway

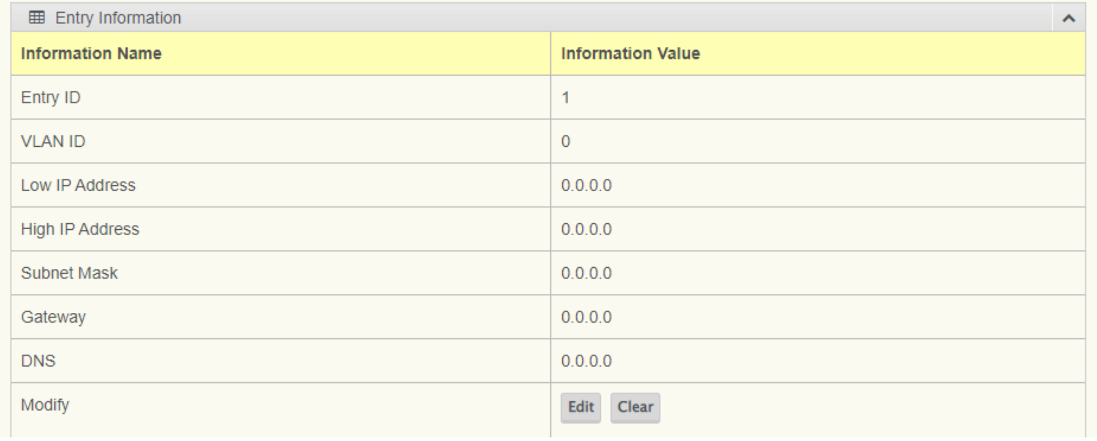
DNS: Input DNS

Figure 4.186 Management > DHCP Server > VLAN Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select the entry number for the VLAN setting.
VLAN ID	Type in the value designating the VLAN ID.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

Entry Information are informational only as shown in the following:



Entry Information

Information Name	Information Value
Entry ID	1
VLAN ID	0
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Modify	Edit Clear

Figure 4.187 Management > DHCP Server > VLAN Settings

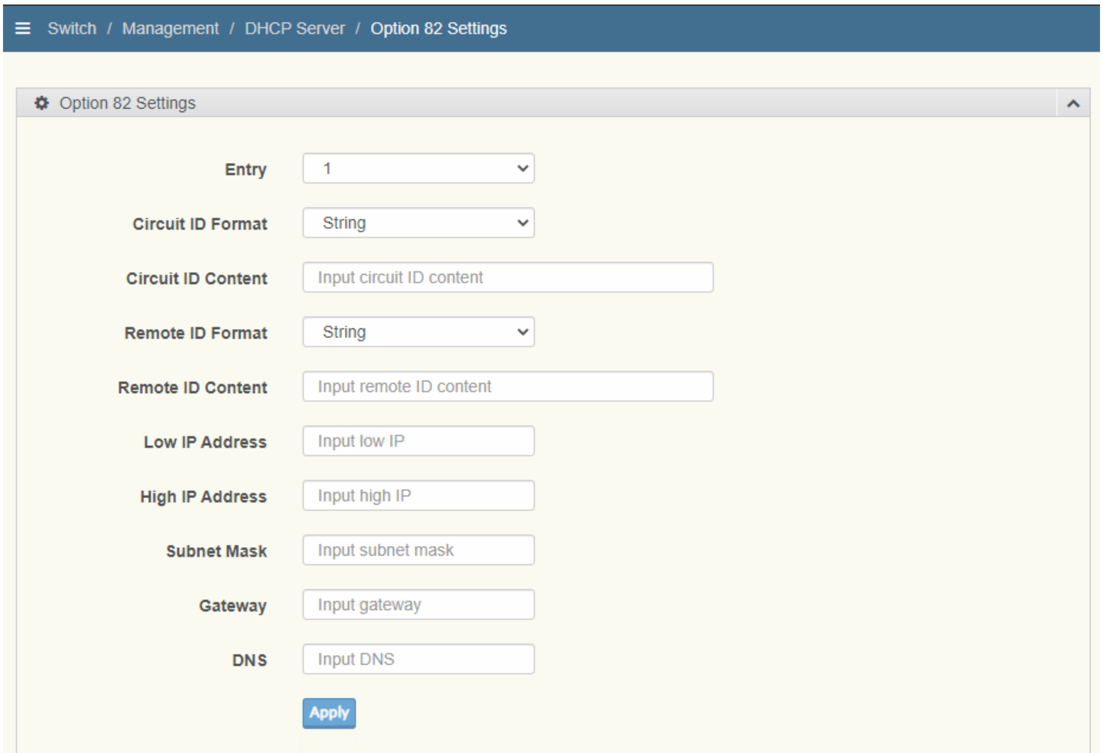
The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select a VLAN entry to display the corresponding information.
Edit	Click **Edit** to modify the information for the selected port entry.
Clear	Click **Clear** to remove the information for the selected port entry.

4.10.3.5 Option 82 Settings

The Option 82 Settings, also known as the DHCP relay agent information option, provide information about the network location of a DHCP client. In turn, the DHCP server uses the information to implement IP addresses or other parameters for the client.

To access this page, click **Management** > **DHCP Server** > **Option 82 Settings**.



Entry: 1
Circuit ID Format: String
Circuit ID Content: Input circuit ID content
Remote ID Format: String
Remote ID Content: Input remote ID content
Low IP Address: Input low IP
High IP Address: Input high IP
Subnet Mask: Input subnet mask
Gateway: Input gateway
DNS: Input DNS

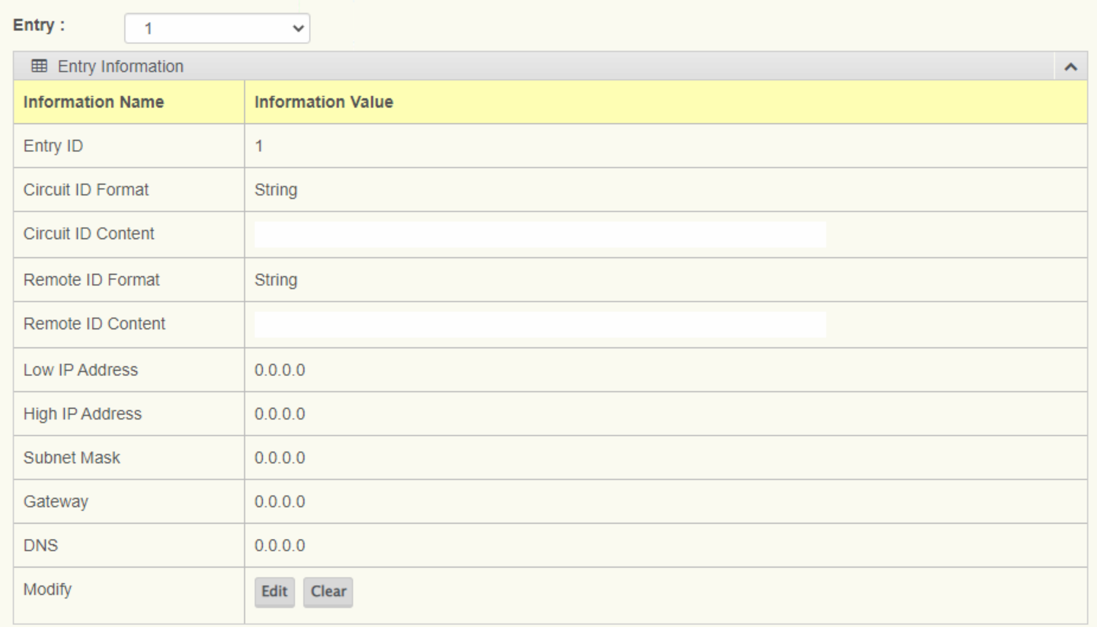
Figure 4.188 Management > DHCP Server > Option 82 Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select an entry for the Option 82 setting.
Circuit ID Format	Click the drop-down menu to select the format of the circuit ID: string or hex.
Circuit ID Content	Enter the circuit ID string on the switch on which the request was received.
Remote ID Format	Click the drop-down menu to select the format of the remote ID: string or hex.
Remote ID Content	Enter the remote ID string of the host.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.

Item	Description
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

Entry Information are informational only as shown in the following:



Entry : 1

Entry Information

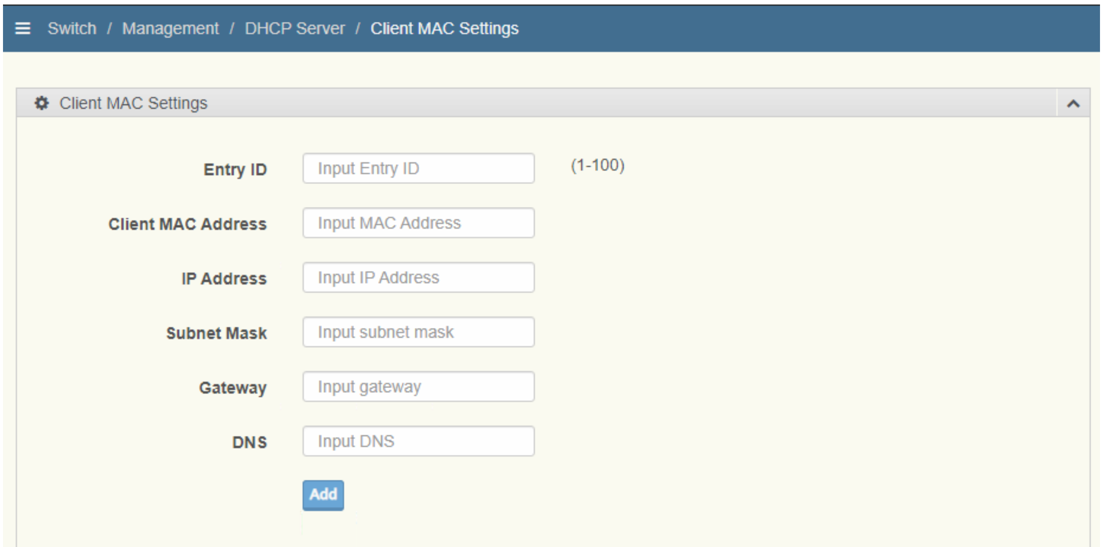
Information Name	Information Value
Entry ID	1
Circuit ID Format	String
Circuit ID Content	
Remote ID Format	String
Remote ID Content	
Low IP Address	0.0.0.0
High IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Modify	Edit Clear

Figure 4.189 Management > DHCP Server > Option 82 Settings

Item	Description
Entry	Click the drop-down menu to select an entry to display the corresponding information.
Edit	Click **Edit** to modify the information for the selected port entry.
Clear	Click **Clear** to remove the information for the selected port entry.

4.10.3.6 Client MAC Settings

To access this page, click **Management** > **DHCP Server** > **Client MAC Settings**.



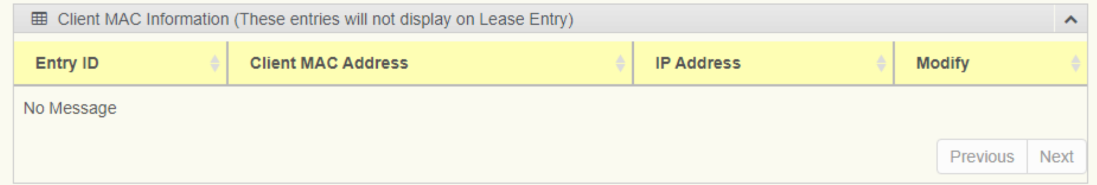
Entry ID	Input Entry ID (1-100)
Client MAC Address	Input MAC Address
IP Address	Input IP Address
Subnet Mask	Input subnet mask
Gateway	Input gateway
DNS	Input DNS

Figure 4.190 Management > DHCP Server > Client MAC Settings

The following table describes the items in the previous figure.

Item	Description
Entry ID	Enter a value to identify the setting entry.
Client MAC Address	Enter the MAC address corresponding to the entry.
IP Address	Enter the IP address corresponding to the client device for the entry.
Subnet Mask	Type in the value designating the subnet mask for the client MAC entry
Gateway	Type in the value designating the gateway for the client MAC entry.
DNS	Type in the value designating the DNS for the client MAC entry.
Apply	Click **Apply** to save the values and update the screen.

Client MAC Information are informational only as shown in the following:


Client MAC Information (These entries will not display on Lease Entry)

Entry ID	Client MAC Address	IP Address	Modify

No Message

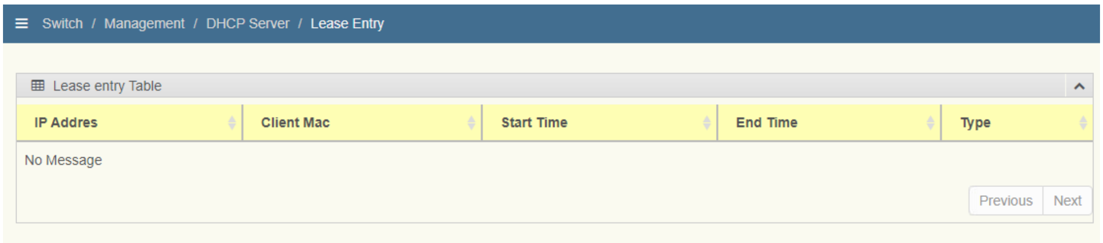
Figure 4.191 Management > DHCP Server > Client MAC Settings

Item	Description
Previous	Click **Previous** to display the preceding entry list.
Next	Click **Next** to display the following entry list.

4.10.3.7 Lease Entry

To access this page, click **Management** > **DHCP Server** > **Lease Entry**.

Lease entry Table are informational only as shown in the following:



Lease entry Table

IP Addres	Client Mac	Start Time	End Time	Type

No Message

Figure 4.192 Management > DHCP Server > Lease Entry

Item	Description
Previous	Click **Previous** to display the preceding entry list.
Next	Click **Next** to display the following entry list.

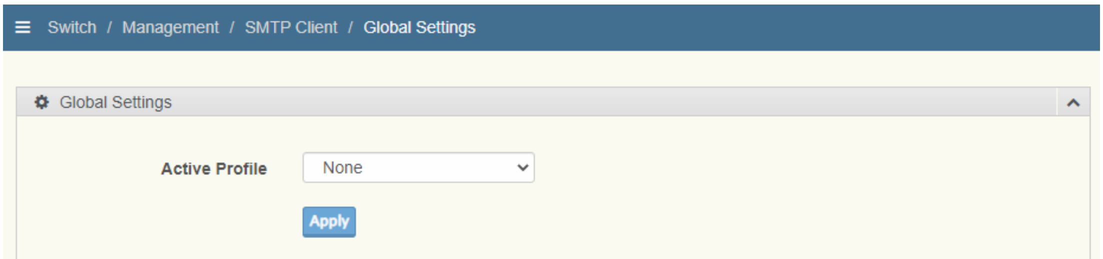
4.10.4 SMTP Client

Simple Mail Transfer Protocol (SMTP) is a protocol to send e-mail messages between servers. SMTP is used to send messages from a mail client to a mail server. SMTP by default uses TCP port 25.

4.10.4.1 Global Settings

The Global Settings page allows you to set the active profile for the SMTP client.

To access this page, click **Management** > **SMTP Client** > Global Settings.



☰ Switch / Management / SMTP Client / Global Settings

Global Settings

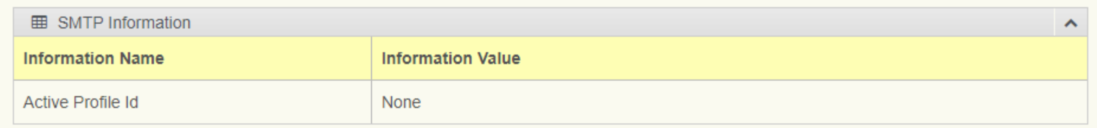
Active Profile: None

Figure 4.193 Management > SMTP Client > Global Settings

The following table describes the items in the previous figure.

Item	Description
Active Profile	Click the drop-down menu to select the profile status (None, 1 or 2).
Apply	Click **Apply** to save the values and update the screen.

SMTP Information are informational only as shown in the following:



SMTP Information

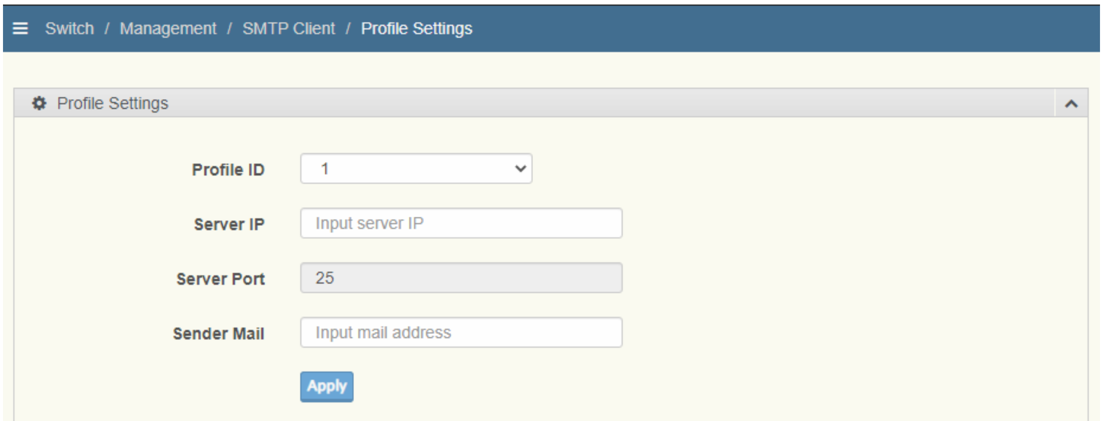
Information Name	Information Value
Active Profile Id	None

Figure 4.194 Management > SMTP Client > Global Settings

4.10.4.2 Profile Settings

The Profile Settings page allows you to select the server IP, the server port, and sender mail for the listed profile.

To access this page, click **Management** > **SMTP Client** > **Profile Settings**.



☰ Switch / Management / SMTP Client / Profile Settings

Profile Settings

Profile ID: 1

Server IP: Input server IP

Server Port: 25

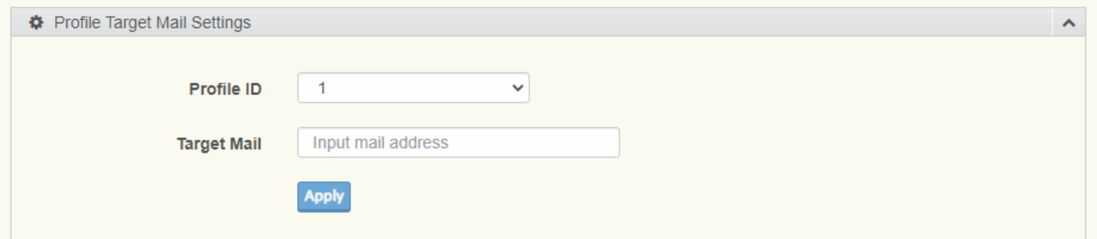
Sender Mail: Input mail address

Figure 4.195 Management > SMTP Client > Profile Settings > Profile Settings

The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Server IP	Enter the IP address to designate the server host.
Server Port	Enter the port number to designate the port associated with the server IP address.
Sender Mail	Enter the email address of the sender client.
Apply	Click **Apply** to save the values and update the screen.

Profile Target Mail Settings are described in the following:



Profile Target Mail Settings

Profile ID: 1

Target Mail: Input mail address

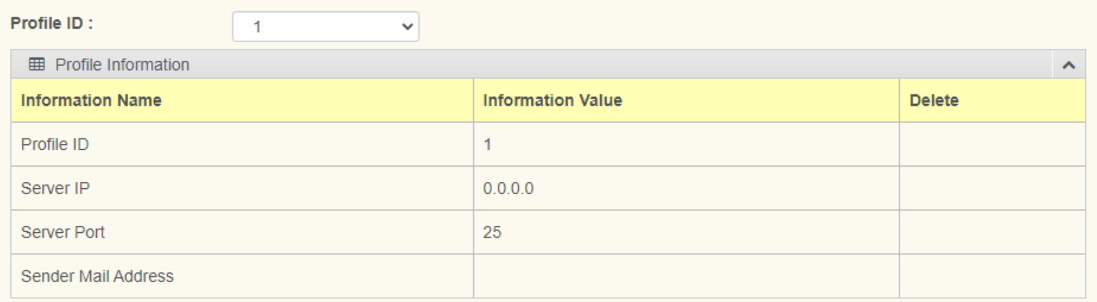
Figure 4.196 Management > SMTP Client > Profile Settings > Profile Settings

The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Target Mail	Enter the email address of the target client.
Apply	Click **Apply** to save the values and update the screen.

Profile Information menu is informational only as shown in the following.

Click on the **Profile ID** drop-down menu to select and display an existing profile.



Profile ID : 1

Profile Information

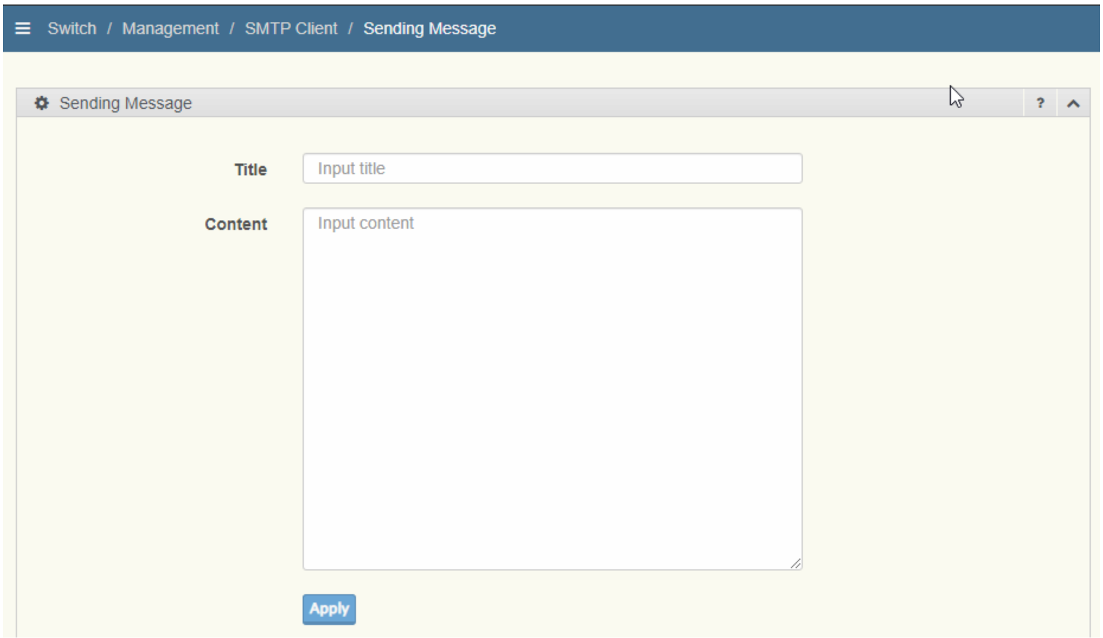
Information Name	Information Value	Delete
Profile ID	1	
Server IP	0.0.0.0	
Server Port	25	
Sender Mail Address		

Figure 4.197 Management > SMTP Client > Profile Settings > Profile Settings

4.10.4.3 Sending Message

The Sending Message page allows you to setup the log message for use with the SMTP client.

To access this page, click **Management** > **SMTP Client** > **Sending Message**.



Title: Input title

Content: Input content

Figure 4.198 Management > SMTP Client > Sending Message

The following table describes the items in the previous figure.

Item	Description
Title	Enter a string to assign the title of the message. The maximum length is 20 characters: alphanumeric characters, symbols (. , _, - and spaces).
Content	Enter the content to create the body of the outgoing email message. The maximum length is 64 characters: alphanumeric characters, symbols (. , _, - and spaces).
Apply	Click **Apply** to save the values and update the screen.

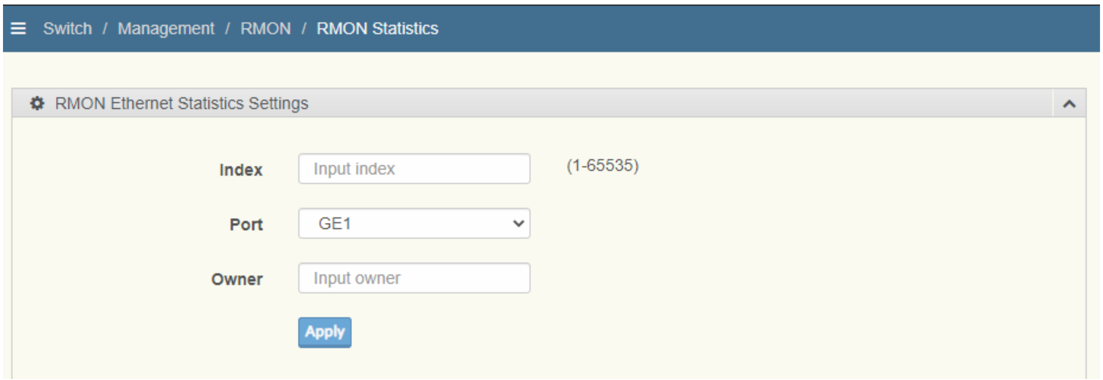
4.10.5 RMON

Remote monitoring (RMON) uses a client-server model to monitor/manage remote devices on a network. RMON delivers pertinent information from the RMON groups of monitored elements, including specific sets of data for common network-monitoring requirements.

4.10.5.1 RMON Statistics

The RMON Statistics page allows you to view information regarding packet sizes and information for physical layer errors. The information displayed is according to the RMON standard.

To access this page, click **Management** > **RMON** > **RMON Statistics**.



≡ Switch / Management / RMON / RMON Statistics
RMON Ethernet Statistics Settings
Apply

Index: Input index (1-65535)

Port: GE1

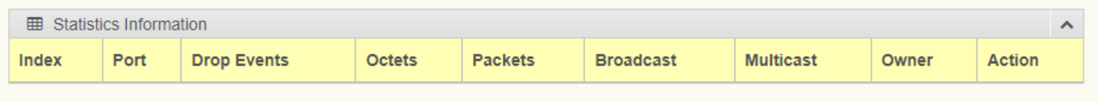
Owner: Input owner

Figure 4.199 Management > RMON > RMON Statistics

The following table describes the items in the previous figure.

Item	Description
Index	Enter an entry selection (1 to 65535) to display its statistical information.
Port	Enter the respective port number for the selected entry.
Owner	Enter the name of the owner of the RMON group.
Apply	Click **Apply** to save the values and update the screen.

Statistics Information settings are informational only as shown in the following.



Statistics Information

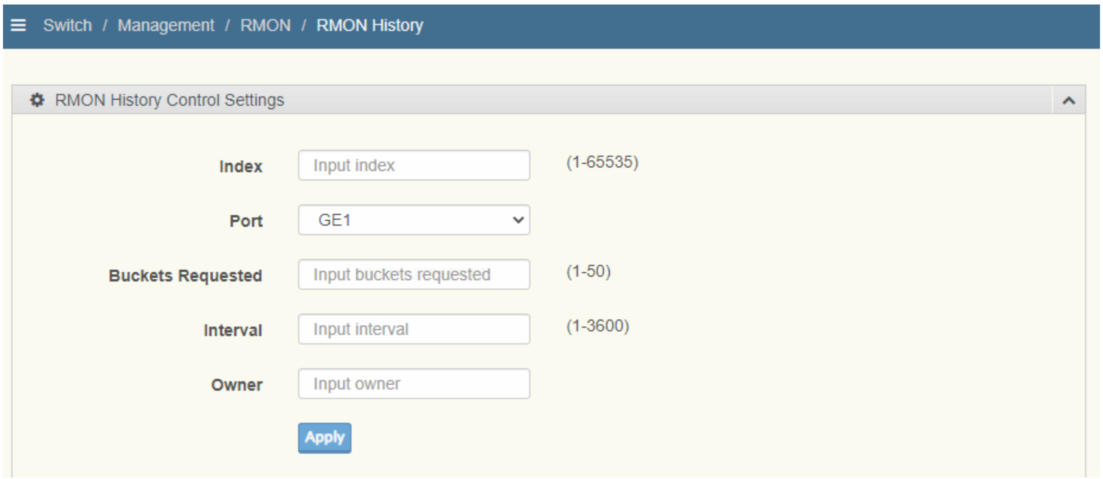
Index	Port	Drop Events	Octets	Packets	Broadcast	Multicast	Owner	Action

Figure 4.200 Management > RMON > Rmon Statistics

4.10.5.2 RMON History

The RMON History page allows you to configure the display of history entries.

To access this page, click **Management** > **RMON** > **RMON History**.



Switch / Management / RMON / RMON History

RMON History Control Settings

Index: Input index (1-65535)

Port: GE1

Buckets Requested: Input buckets requested (1-50)

Interval: Input interval (1-3600)

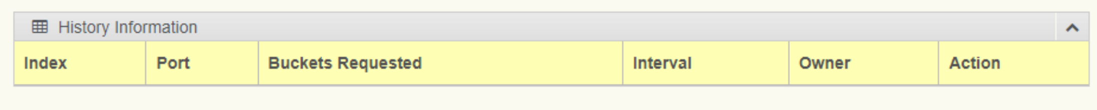
Owner: Input owner

Figure 4.201 Management > RMON > RMON History

The following table describes the items in the previous figure.

Item	Description
Index	Enter an entry selection (1 to 65535) to display its statistical information.
Port	Enter the respective port number for the selected entry.
Bucket Requested	Enter the specific (1-50) number of samples to store.
Interval	Enter value in seconds (1 to 3600) to designate a specific interval time for the collection of samples.
Owner	Enter the name of the owner of the RMON history group.
Apply	Click **Apply** to save the values and update the screen.

History Information settings are informational only as shown in the following.



History Information

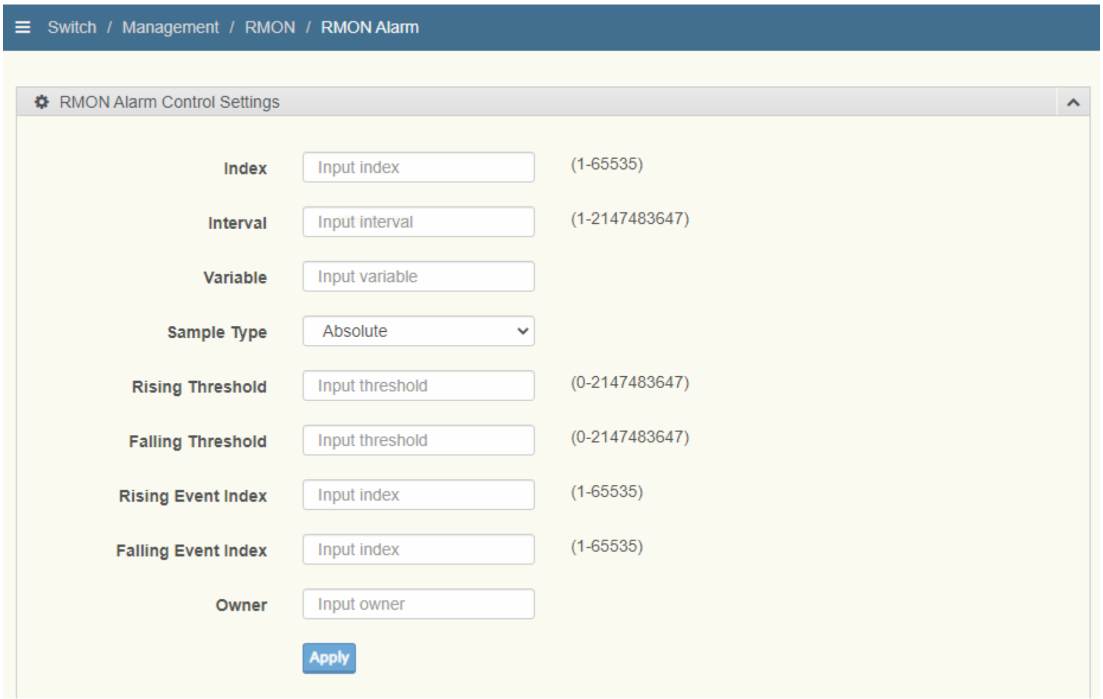
Index	Port	Buckets Requested	Interval	Owner	Action

Figure 4.202 Management > RMON > RMON History

4.10.5.3 RMON Alarm

The RMON Alarm page allows you to configure RMON statistics group and alarm groups.

To access this page, click **Management** > **RMON** > **RMON Alarm**.



☰ Switch / Management / RMON / RMON Alarm

RMON Alarm Control Settings

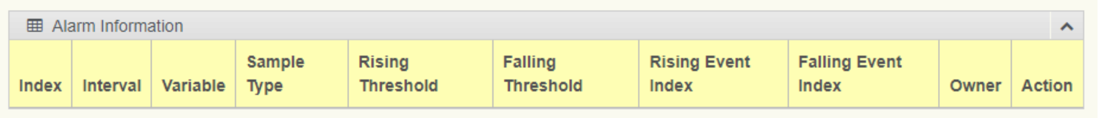
Index	Input index	(1-65535)
Interval	Input interval	(1-2147483647)
Variable	Input variable	
Sample Type	Absolute	
Rising Threshold	Input threshold	(0-2147483647)
Falling Threshold	Input threshold	(0-2147483647)
Rising Event Index	Input index	(1-65535)
Falling Event Index	Input index	(1-65535)
Owner	Input owner	

Figure 4.203 Management > RMON > RMON Alarm

The following table describes the items in the previous figure.

Item	Description
Index	Enter the index entry (1 to 65535) to define a specific Alarm Collection history entry.
Interval	Enter a value (1 to 2147483647) to define the interval value for the Alarm Collection history.
Variable	Enter the alarm variables to define the monitoring triggers.
Sample Type	Click the drop-down menu to select the sample type: Absolute (default) or Delta.
Rising Threshold	Enter the rising alarm threshold trigger.
Falling Threshold	Enter the falling alarm threshold trigger.
Rising Event Index	Enter the rising event index (1-65535) to define the alarm group.
Falling Event Index	Enter the falling event index (1-65535) to define the alarm group.
Owner	Enter the name of the owner of the RMON alarm group.
Apply	Click **Apply** to save the values and update the screen.

Alarm Information settings are informational only as shown in the following.



Alarm Information

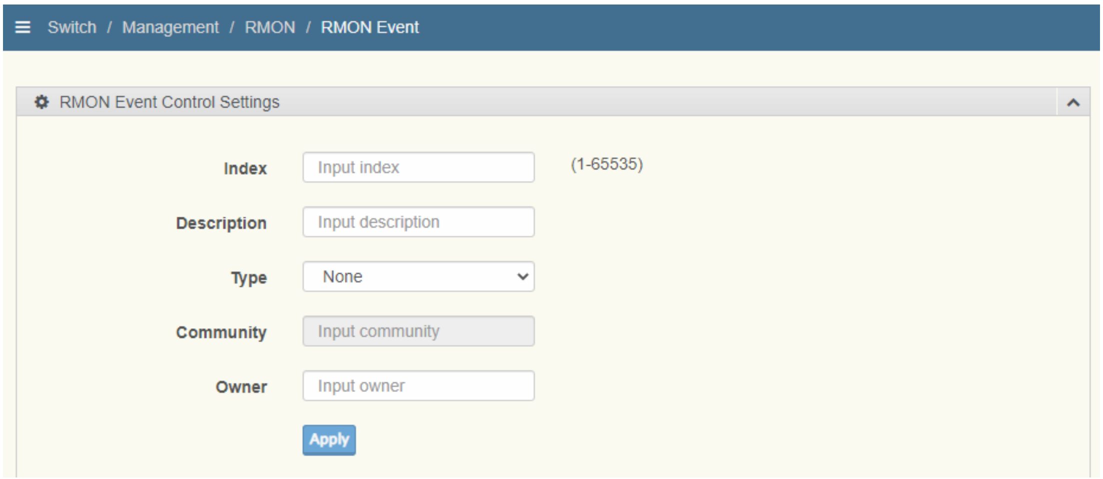
Index	Interval	Variable	Sample Type	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Action

Figure 4.204 Management > RMON > RMON Alarm

4.10.5.4 RMON Event

The RMON Event page is used to configure RMON event groups.

To access this page, click **Management** > **RMON** > **RMON Event**.



☰ Switch / Management / RMON / RMON Event

RMON Event Control Settings

Index: Input index (1-65535)

Description: Input description

Type: None

Community: Input community

Owner: Input owner

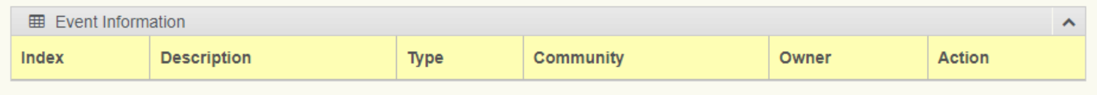
Apply

Figure 4.205 Management > RMON > RMON Event

The following table describes the items in the previous figure.

Item	Description
Index	Enter the index entry (1 to 65535) to define a specific RMON event.
Description	Enter a value (1 to 2147483647) to define the interval value for the Alarm Collection history.
Type	Click the drop-down menu to define the event type: None, Log, SNMP Trap, Log and Trap.
Community	Enter the community string to be passed for the specified event.
Owner	Enter the name of the owner of the RMON event.
Apply	Click **Apply** to save the values and update the screen.

Event Information settings are informational only as shown in the following.



Event Information

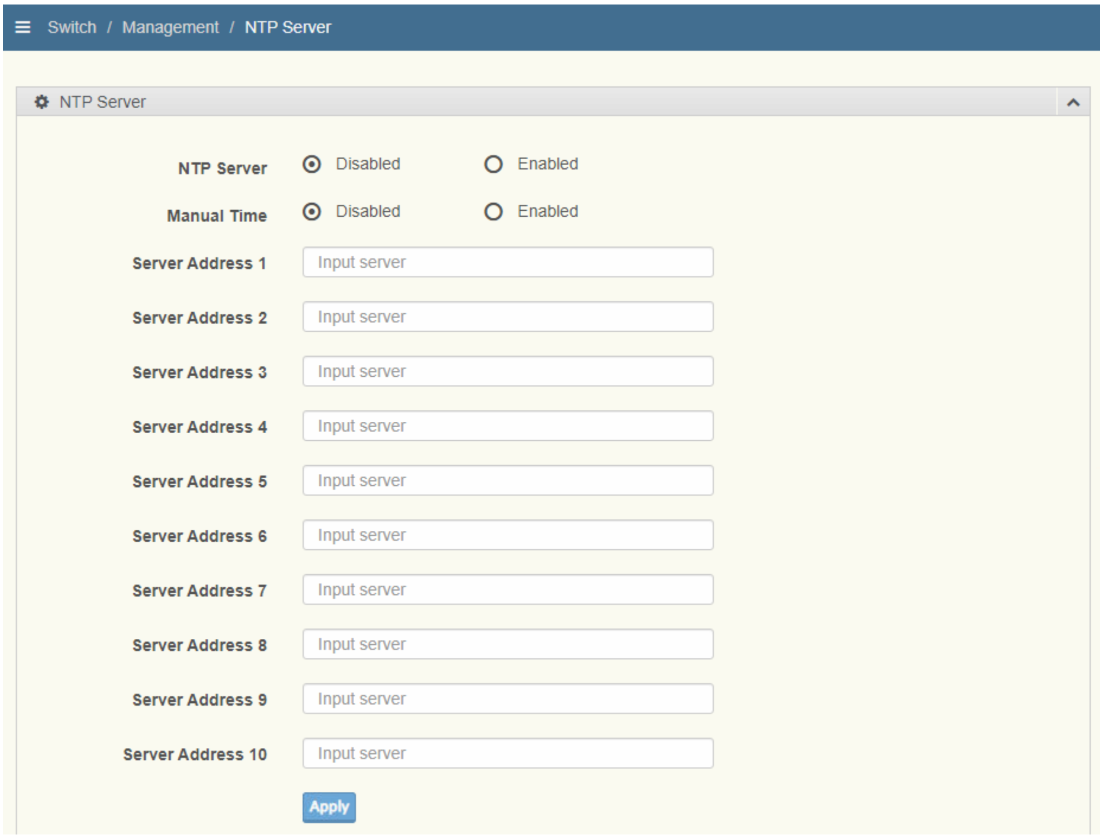
Index	Description	Type	Community	Owner	Action

Figure 4.206 Management > RMON > RMON Event

4.10.6 NTP Server

The NTP Server settings allow you to manually synchronize the devices on the network. See the following information for further details.

To access this page, click **Management** > **NTP Server**.



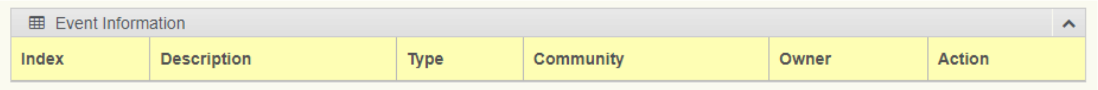
NTP Server	● Disabled	○ Enabled
Manual Time	● Disabled	○ Enabled
Server Address 1	Input server	
Server Address 2	Input server	
Server Address 3	Input server	
Server Address 4	Input server	
Server Address 5	Input server	
Server Address 6	Input server	
Server Address 7	Input server	
Server Address 8	Input server	
Server Address 9	Input server	
Server Address 10	Input server	

Figure 4.207 Management > NTP Server

The following table describes the items in the previous figure.

Item	**Description**
NTP Server	Click the radio button to enable or disable the NTP server function.
Manual Time	Click the radio button to enable or disable the manual time function.
Server Address 1 ~ Server Address 10	Enter the address of the NTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a NTP server.
Apply	Click **Apply** to save the values and update the screen.

Event Information settings are informational only as shown in the following.



Index	Description	Type	Community	Owner	Action

Figure 4.208 Management > NTP Server

4.10.7 TTDP

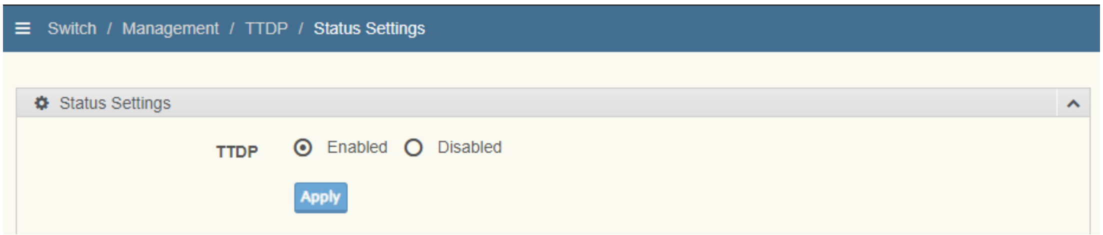
This section describes the Train Topology Discovery Protocol (TTDP). The functions dynamically discovers the backbone routers (ETBNs) and consist networks (ECNs) in a train and the related connections.

TTDP assigns IP addresses to ETBNs and ECNs establishing routing and NAT entries on the assigned IP assignments.

The section provides a further description of the available features.

4.10.7.1 Status Settings

To access this page, click **Management** > **TTDP > Status Settings**.



≡ Switch / Management / TTDP / Status Settings

Status Settings

TTDP ● Enabled ○ Disabled

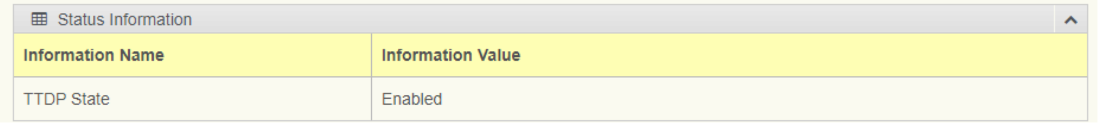
Apply

Figure 4.209 Management > TTDP > Status Settings

The following table describes the items in the previous figure.

Item	Description
TTDP	Click the radio button to enable or disable the Train Topology Discovery Protocol function.
Apply	Click **Apply** to save the values and update the screen.

Status Information settings are informational only as shown in the following.

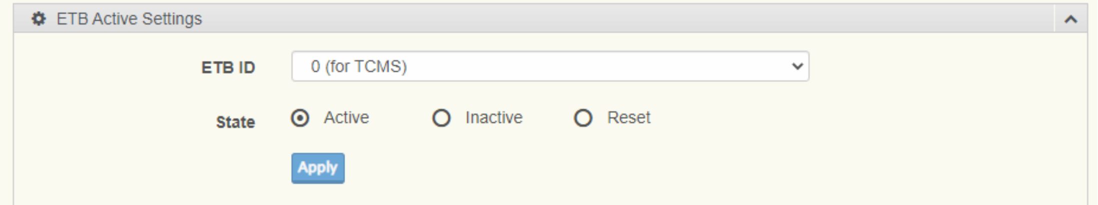


Status Information

Information Name	Information Value
TTDP State	Enabled

Figure 4.210 Management > TTDP > Status Settings

ETB Active Settings are informational only as shown in the following.



ETB Active Settings

ETB ID: 0 (for TCMS)

State ● Active ○ Inactive ○ Reset

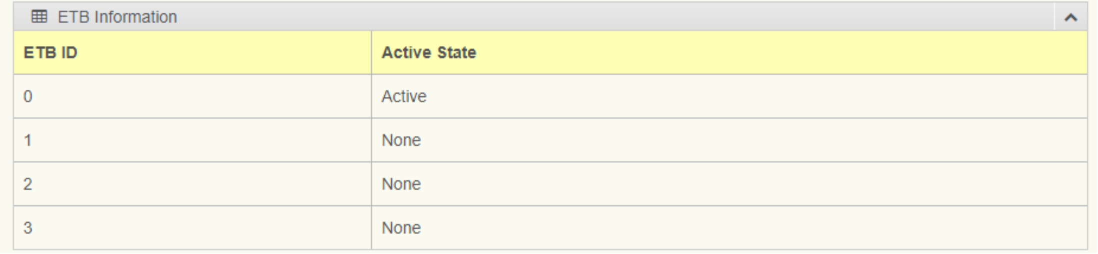
Apply

Figure 4.211 Management > TTDP > Status Settings

The following table describes the items in the previous figure.

Item	Description
ETB ID	Click the drop-down menu to select the interface on the ETBN.
State	Click the radio button to apply the state on the selected interface: **Active**, Inactive, Reset.
Apply	Click **Apply** to save the values and update the screen.

ETB Information settings are informational only as shown in the following.



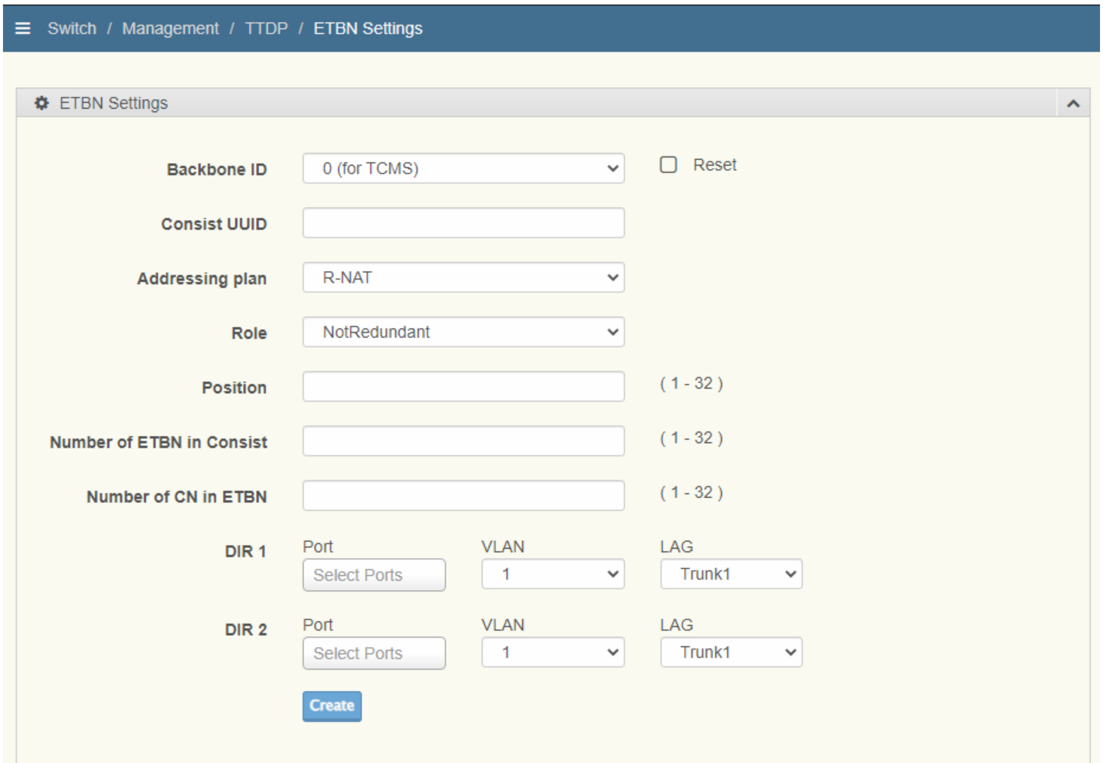
ETB Information

ETB ID	Active State
0	Active
1	None
2	None
3	None

Figure 4.212 Management > TTDP > Status Settings

4.10.7.2 ETBN Settings

To access this page, click **Management** > **TTDP > ETBN Settings**.



Backbone ID: 0 (for TCMS) □ Reset

Consist UUID:

Addressing plan: R-NAT

Role: NotRedundant

Position: (1 - 32)

Number of ETBN in Consist: (1 - 32)

Number of CN in ETBN: (1 - 32)

DIR 1: Port: Select Ports; VLAN: 1; LAG: Trunk1

DIR 2: Port: Select Ports; VLAN: 1; LAG: Trunk1

Figure 4.213 Management > TTDP > ETBN Settings

The following table describes the items in the previous figure.

Item	Description
Backbone ID	Click the drop-down menu to select the setting identifier from displayed options. Reset: Click the **Reset** radio button to initiate a reset of the selected setting.
Consist UUID	Enter the Universally Unique Identifier (UUID) to map the order/ position of the ETBN on the train backbone.
Addressing plan	Click the drop-down menu to select the type of IP assignment topology: ■ Absolute: ■ R-NAT (default): Railway-NAT translates IP addresses and populated dynamically based on the subnet allocation.
Role	Click the drop-down menu to select the role of the device: ■ Master: defines the device as the master router with the highest priority. ■ Backup: defines the device as the backup router in case the master fails. ■ NotRedundant: defines the device to operate on a non redundant scheme.
Position	Enter the string (1 - 32) to define the position of the
Number of CN in ETBN	Enter the string to identify the CN subset in each ETBN. The value is used to build train IP mapping, train routing definition, NAT rules.
Dir 1	Click the drop-down menu to define the following Dir1 and Dir2 settings: ■ Port: select from GE1 to GE12 ■ VLAN: select from 1, 492, 500, 1000 ■ LAG: select from Trunk1 to Trunk8

Item	Description
Dir 2	Click the drop-down menu to define the following Dir1 and Dir2 settings: ■ Port: select from GE1 to GE12 ■ VLAN: select from 1, 492, 500, 1000 ■ LAG: select from Trunk1 to Trunk8
Create	Click **Create** to set up the defined setting.

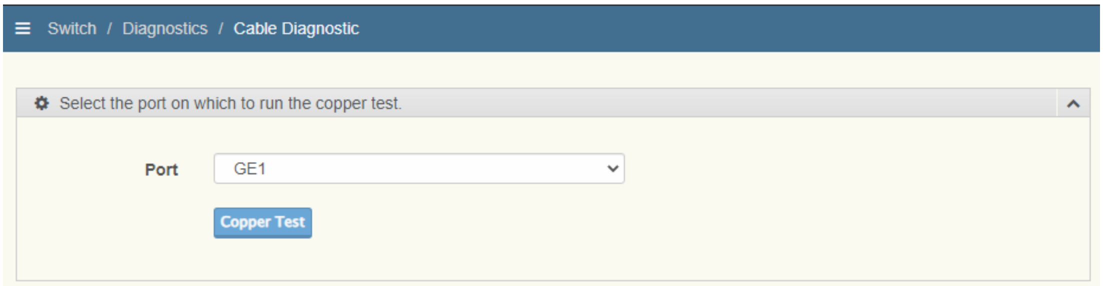
4.11 Diagnostics

Through the Diagnostics function configuration of settings for the switch diagnostics is available.

4.11.1 Cable Diagnostics

The Cable Diagnostics page allows you to select the port for applying a copper test.

To access this page, click **Diagnostics** > **Cable Diagnostics**.


Switch / Diagnostics / Cable Diagnostic

Select the port on which to run the copper test.

Port: GE1

Figure 4.214 Diagnostics > Cable Diagnostics

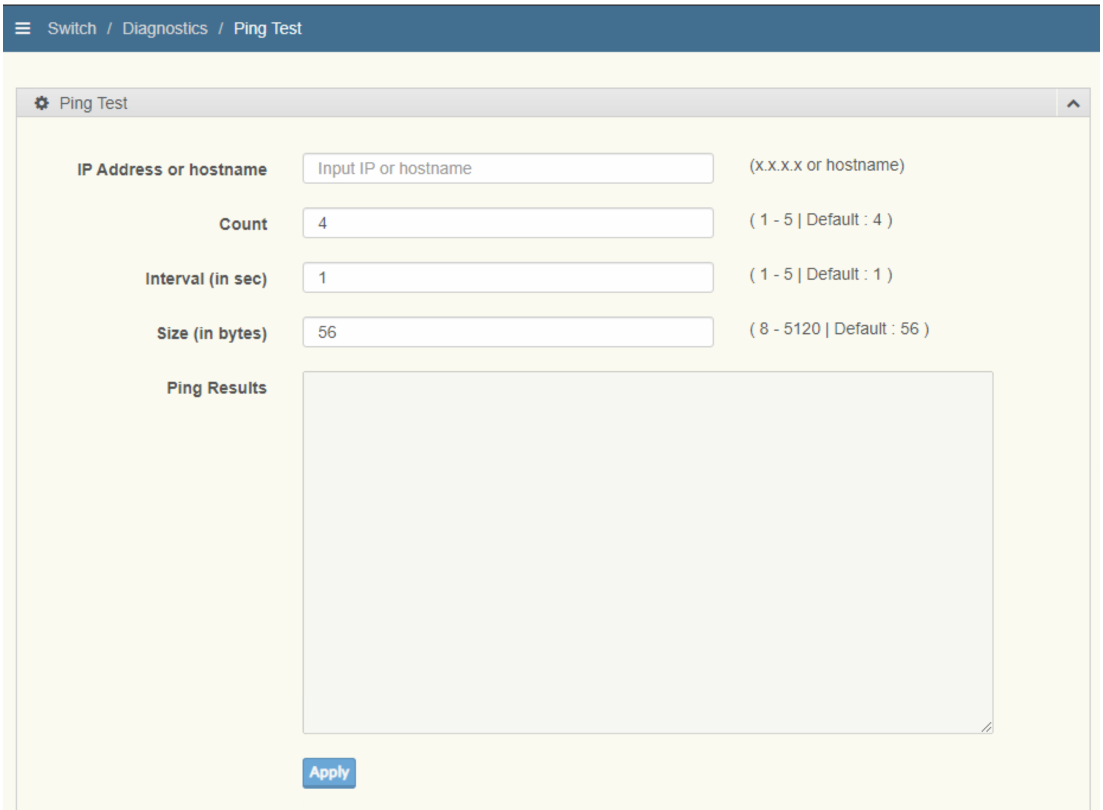
The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a pre-defined port for diagnostic testing.
Copper Test	Click **Copper Test** to display the test result for the selected port.

4.11.2 Ping Test

The Ping Test page allows you to configure the test log page.

To access this page, click **Diagnostics** > **Ping Test**.


Switch / Diagnostics / Ping Test

Ping Test

IP Address or hostname: Input IP or hostname (x.x.x.x or hostname)

Count: 4 (1 - 5 | Default : 4)

Interval (in sec): 1 (1 - 5 | Default : 1)

Size (in bytes): 56 (8 - 5120 | Default : 56)

Ping Results

Figure 4.215 Diagnostics > Ping Test

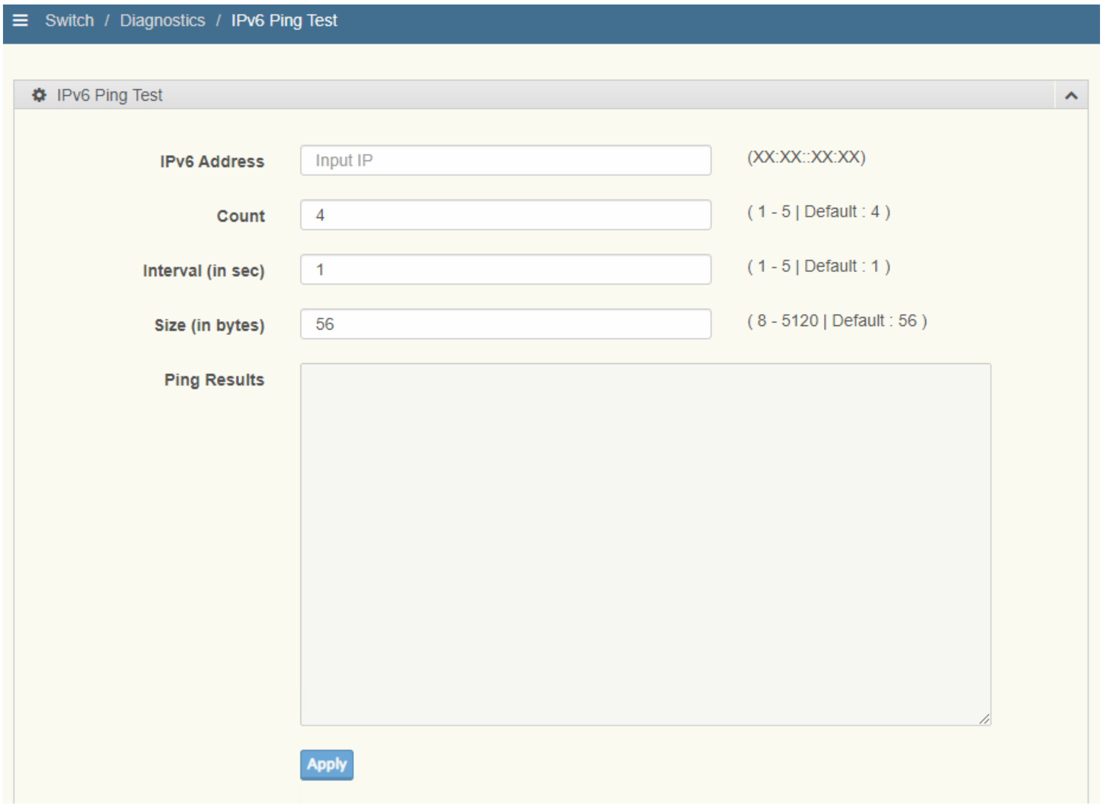
The following table describes the items in the previous figure.

Item	Description
IP Address or hostname	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Count	Enter the number of echo requests to send. The default value is 4. The value ranges from 1 to 5. The count entered is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval entered is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size entered is not retained across a power cycle.
Ping Results	Display the reply format of ping. An example is provided as follows: PING 172.17.8.254 (172.17.8.254): 56 data bytes --- 172.17.8.254 ping statistics --- 4 packets transmitted, 0 packets received, 100% packet loss Or PING 172.17.8.93 (172.17.8.93): 56 data bytes 64 bytes from 172.17.8.93: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=3 ttl=128 time=0.0 ms --- 172.17.8.93 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
Apply	Click **Apply** to display ping result for the IP address.

4.11.3 IPv6 Ping Test

The IPv6 Ping Test page allows you to configure the Ping Test for IPv6.

To access this page, click **Diagnostics** > **IPv6 Ping Test**.



IPv6 Address	Input IP	(XX:XX::XX:XX)
Count	4	(1 - 5 | Default : 4)
Interval (in sec)	1	(1 - 5 | Default : 1)
Size (in bytes)	56	(8 - 5120 | Default : 56)
Ping Results		

Figure 4.216 Diagnostics > IPv6 Ping Test

The following table describes the items in the previous figure.

Item	Description
IPv6 Address	Enter the IP address or host name of the station you want the switch to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 64 characters.
Count	Enter the number of echo requests you want to send. The default value is 4. The value ranges from 1 to 5. The count you enter is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval you enter is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size you enter is not retained across a power cycle.

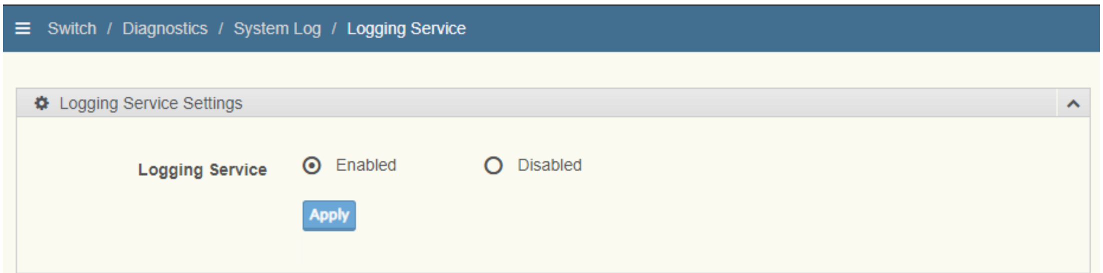
Item	Description
Ping Results	Display the reply format of ping. An example is provided as follows: PING 2222:777 (2222:777): 56 data bytes --- 2222:777 ping statistics --- 4 packets transmitted, 0 packets received, 100% packet loss Or PING 2222:717 (2222:717): 56 data bytes 64 bytes from 2222:717: icmp6_seq=0 ttl=128 time=10.0 ms 64 bytes from 2222:717: icmp6_seq=1 ttl=128 time=0.0 ms 64 bytes from 2222:717: icmp6_seq=2 ttl=128 time=0.0 ms 64 bytes from 2222:717: icmp6_seq=3 ttl=128 time=0.0 ms --- 2222:717 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/2.5/10.0 ms
Apply	Click **Apply** to display ping result for the IP address.

4.11.4 System Log

4.11.4.1 Logging Service

The Logging Service page allows you to setup the logging services feature for the system log.

To access this page, click **Diagnostics** > **System Log** > **Logging Service**.



Switch / Diagnostics / System Log / Logging Service

Logging Service Settings

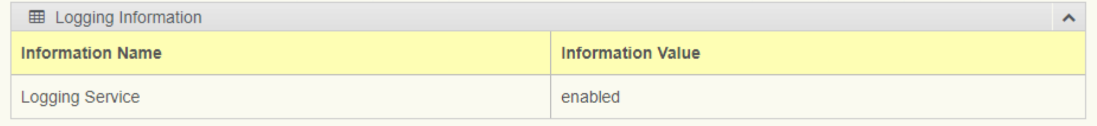
Logging Service ● Enabled ○ Disabled

Figure 4.217 Diagnostics > System Log > Logging Service

The following table describes the items in the previous figure.

Item	Description
Logging Service	Click Enabled or Disabled to set the Logging Service status.
Apply	Click **Apply** to save the values and update the screen.

Logging Information settings are informational only as shown in the following.



Logging Information

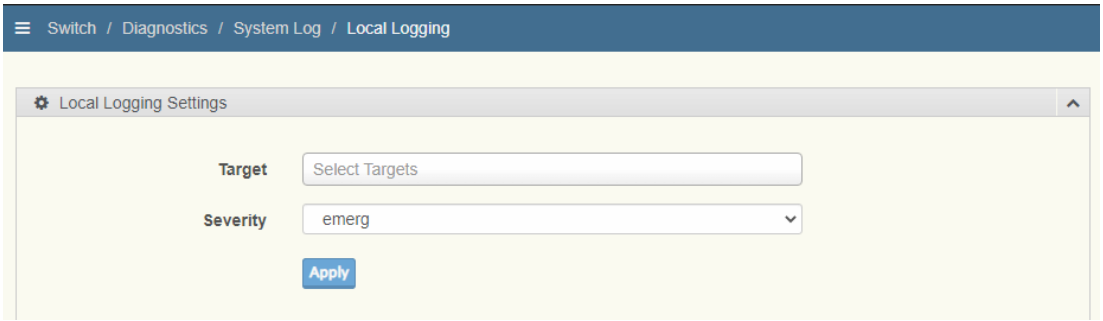
Information Name	Information Value
Logging Service	enabled

Figure 4.218 Diagnostics > System Log > Logging Service

4.11.4.2 Local Logging

The Local Logging page allows you to designate a local target when the severity criteria is reached.

To access this page, click **Diagnostics** > **System Log** > **Local Logging**.



☰ Switch / Diagnostics / System Log / Local Logging

Local Logging Settings

Target: Select Targets

Severity: emerg

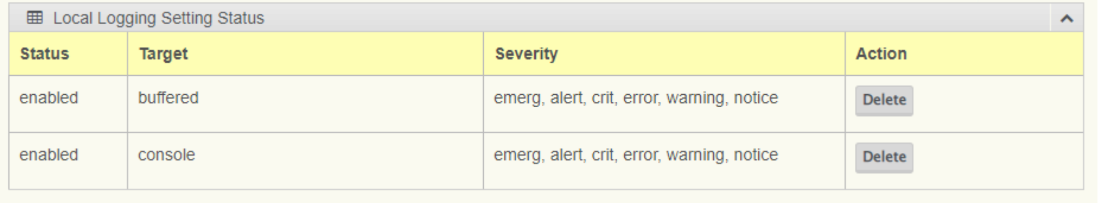
Apply

Figure 4.219 Diagnostics > System Log > Local Logging

The following table describes the items in the previous figure.

Item	Description
Target	Enter the local logging target.
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Apply	Click **Apply** to save the values and update the screen.

Local Logging Settings Status settings are described in the following.



Local Logging Setting Status

Status	Target	Severity	Action
enabled	buffered	emerg, alert, crit, error, warning, notice	Delete
enabled	console	emerg, alert, crit, error, warning, notice	Delete

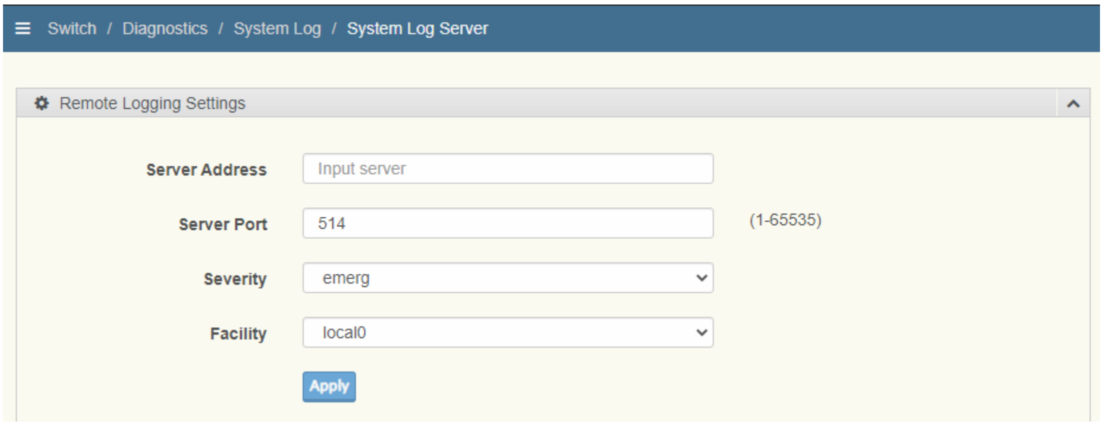
Figure 4.220 Diagnostics > System Log > Local Logging

Item	Description
Delete	Click Delete to clear the selected status log.

4.11.4.3 System Log Server

The System Log Server page allows you to configure the log server.

To access this page, click **Diagnostics** > **System Log** > **System Log Server**.



Switch / Diagnostics / System Log / System Log Server

Remote Logging Settings

Server Address: Input server

Server Port: 514 (1-65535)

Severity: emerg

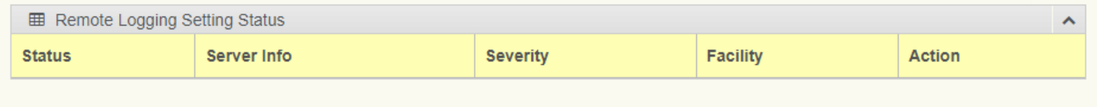
Facility: local0

Figure 4.221 Diagnostics > System Log > System Log Server

The following table describes the items in the previous figure.

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number (1 to 65535, default: 514) of the log server.
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: ■ emerg (default): Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click **Apply** to save the values and update the screen.

Remote Logging Setting Status settings are informational only as shown in the following.



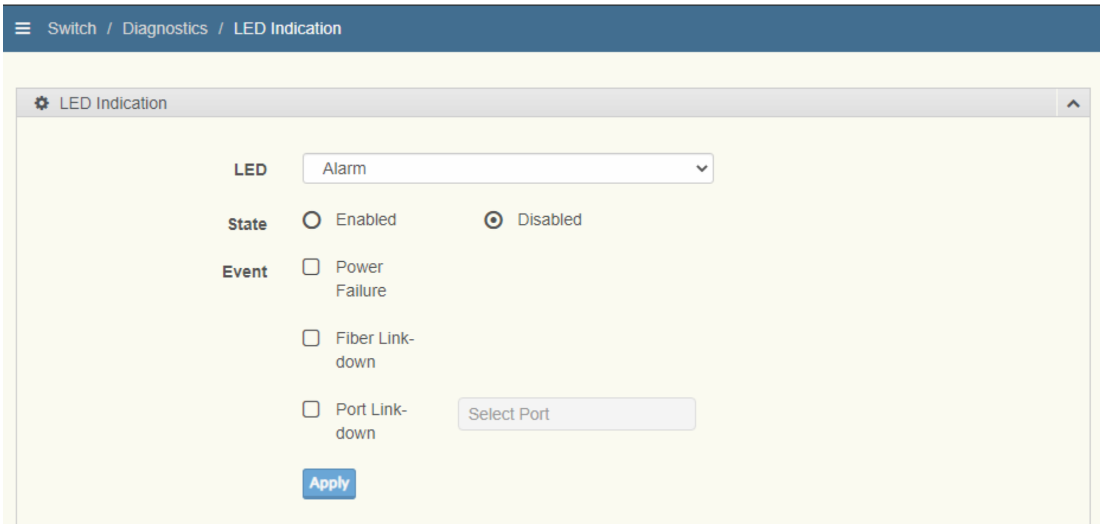
Remote Logging Setting Status

Status	Server Info	Severity	Facility	Action

Figure 4.222 Diagnostics > System Log > System Log Server

4.11.5 LED Indication

To access this page, click **Diagnostics** > **LED Indication**.



Switch / Diagnostics / LED Indication

LED Indication

LED: Alarm

State: ○ Enabled ● Disabled

Event: □ Power Failure

□ Fiber Link-down

□ Port Link-down   Select Port

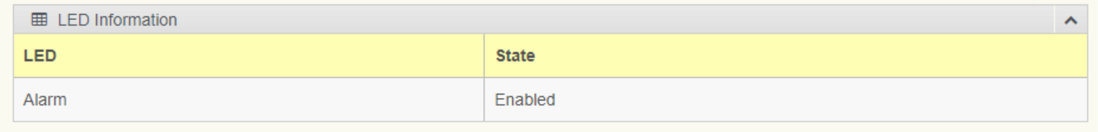
Apply

Figure 4.223 Diagnostics > LED Indication

The following table describes the items in the previous figure.

Item	Description
LED	Click the drop-down menu to select LED indicator.
State	Select **Enable** or **Disable** to enable LED alarm.
Event	Click to select the event to be of LED alarm. Power Failure: Fiber Link-down: Port Link-down: Click the drop-down menu to select a port number.
Apply	Click **Apply** to save the values and update the screen.

LED Information settings are informational only as shown in the following.

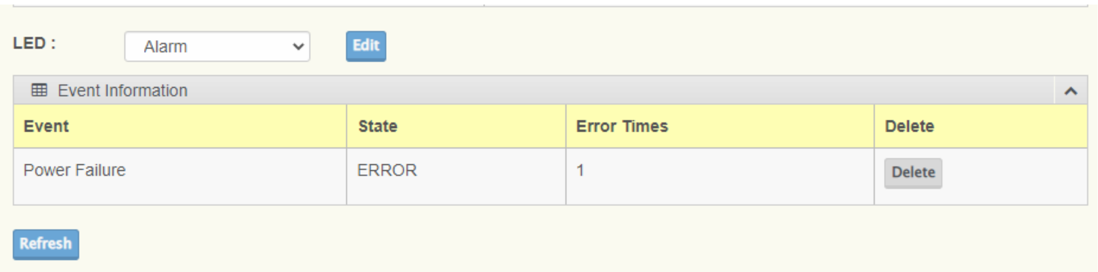


LED Information

LED	State
Alarm	Enabled

Figure 4.224 Diagnostics > LED Indication

Event Information settings are described as shown in the following.



LED : Alarm   Edit

Event Information

Event	State	Error Times	Delete
Power Failure	ERROR	1	Delete

Refresh

Figure 4.225 Diagnostics > LED Indication

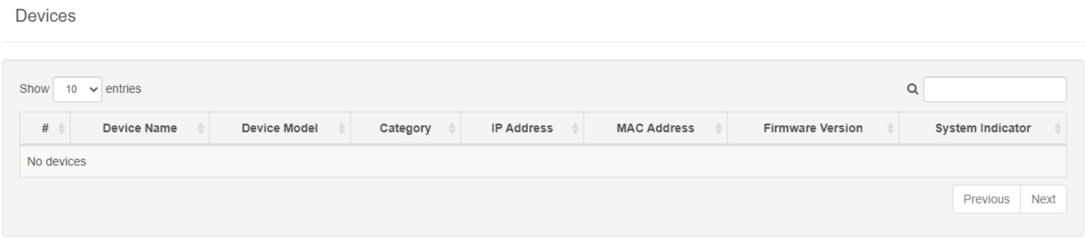
Item	Description
LED	Click the drop-down menu to select an event.
Edit	Click **Edit** to modify the selected event.
Delete	Click **Delete** to remove the listed event.
Refresh	Click **Refresh** to update the pool listing.

4.12 Tools

4.12.1 IXM

The IXM tool is an industrial Ethernet switch solution to help the users deploy industrial Ethernet switch hardware by allowing users with multiple, managed Ethernet switches in the field to eliminate the need to individually connect to each device to configure it.

To access this page, click **Tools** > **IXM**.



Devices

Show 10 entries

#	Device Name	Device Model	Category	IP Address	MAC Address	Firmware Version	System Indicator
No devices							

Figure 4.226 Tools > IXM

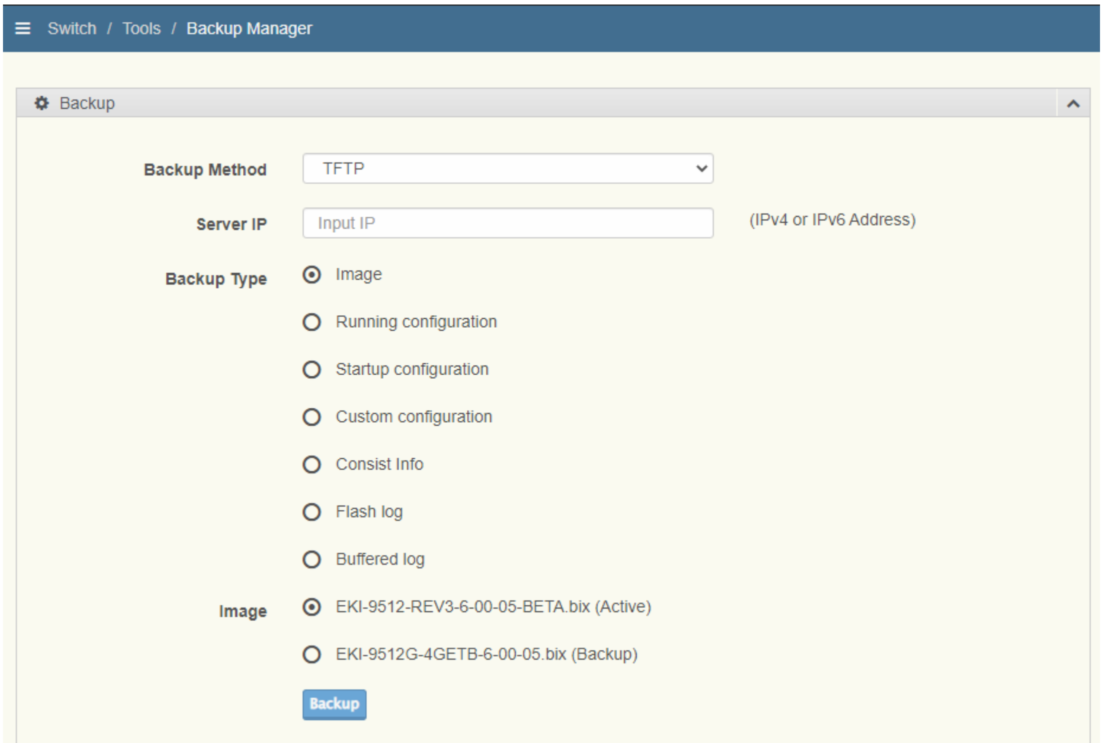
The following table describes the items in the previous figure.

Item	Description
Search Field	Enter criteria to search the IXM information.
#	Displays the reference to the device number.
Device Name	Displays the device name.
Device Model	Displays the device model type.
Category	Displays the device’s category type.
IP Address	Displays the device’s IP address.
MAC Address	Displays the device’s IP MAC address.
Firmware Version	Displays the device’s firmware version.
System Indicator	Displays the device’s system indicator.
Previous	Click Previous to back to previous page.
Next	Click Next to go to the next page.

4.12.2 Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to backup the firmware image or configuration file.

To access this page, click **Tools** > **Backup Manager**.



Switch / Tools / Backup Manager

Backup

Backup Method: TFTP

Server IP: Input IP (IPv4 or IPv6 Address)

Backup Type:
- ● Image
- ○ Running configuration
- ○ Startup configuration
- ○ Custom configuration
- ○ Consist Info
- ○ Flash log
- ○ Buffered log

Image:
- ● EKI-9512-REV3-6-00-05-BETA.bix (Active)
- ○ EKI-9512G-4GETB-6-00-05.bix (Backup)

Backup

Figure 4.227 Tools > Backup Manager

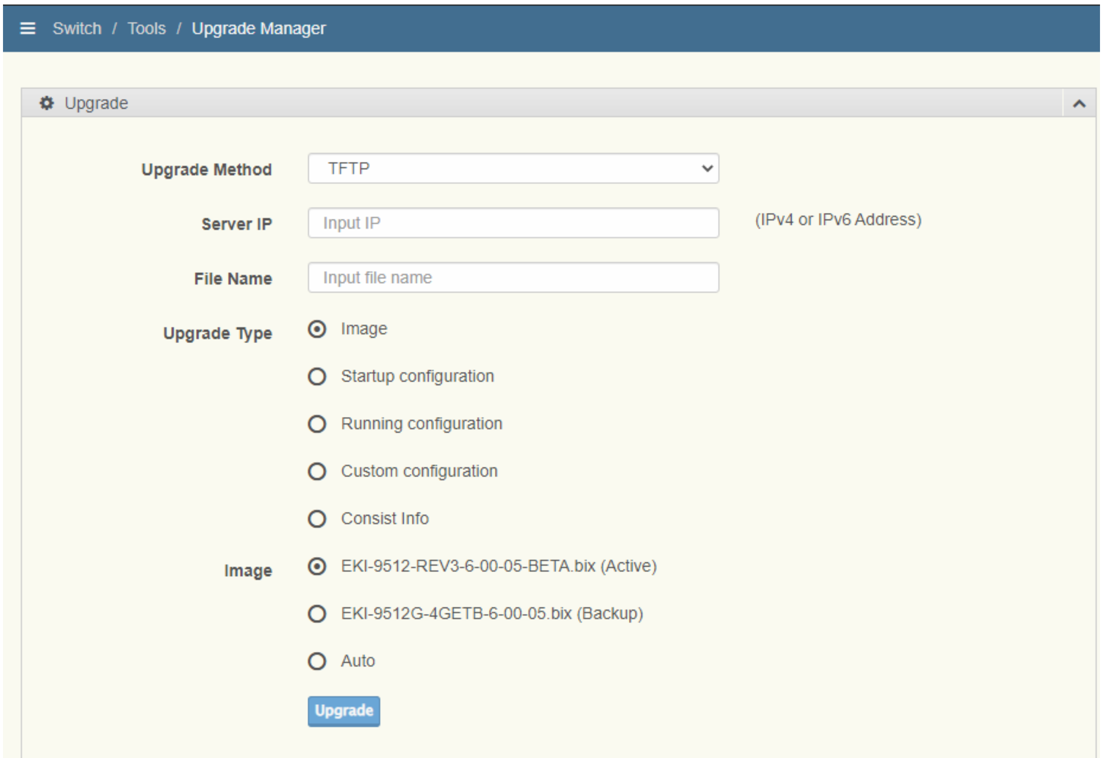
The following table describes the items in the previous figure.

Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image: running configuration, startup configuration, flash log, or buffered log.
Image	Click the format for the image type: 9612G_1_00_13.bix (Active) or vmlinux.bix (backup).
Backup	Click **Backup** to backup the settings.

4.12.3 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files.

To access this page, click **Tools** > **Upgrade Manager**.



☰ Switch / Tools / Upgrade Manager

Upgrade

Upgrade Method: TFTP

Server IP: Input IP (IPv4 or IPv6 Address)

File Name: Input file name

Upgrade Type:
● Image
○ Startup configuration
○ Running configuration
○ Custom configuration
○ Consist Info

Image:
● EKI-9512-REV3-6-00-05-BETA.bix (Active)
○ EKI-9512G-4GETB-6-00-05.bix (Backup)
○ Auto

Upgrade

Figure 4.228 Tools > Upgrade Manager

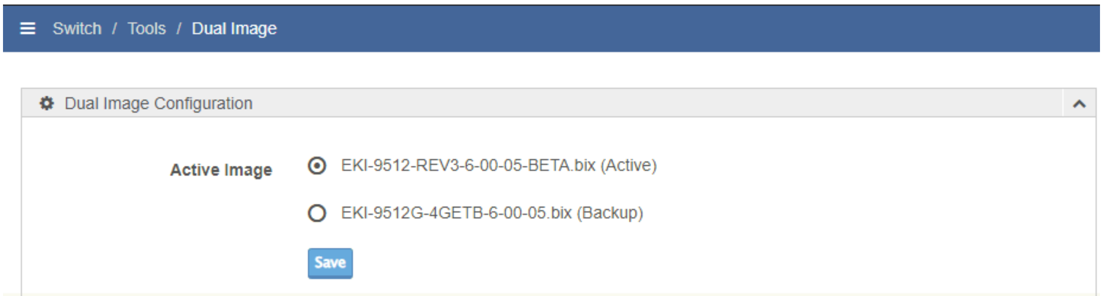
The following table describes the items in the previous figure.

Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click the radio button to define the type of upgrade function to initiate: image, startup configuration, custom configuration, or consist info.
Image	Click the radio button to select the Active, Backup, or Auto firmware image option as the upgrade source.
Upgrade	Click **Upgrade** to upgrade to the current version.

4.12.4 Dual Image

The Dual Image page allows you to setup an active and backup partitions for firmware image redundancy.

To access this page, click **Tools** > **Dual Image**.



☰ Switch / Tools / Dual Image

Dual Image Configuration

Active Image:
● EKI-9512-REV3-6-00-05-BETA.bix (Active)
○ EKI-9512G-4GETB-6-00-05.bix (Backup)

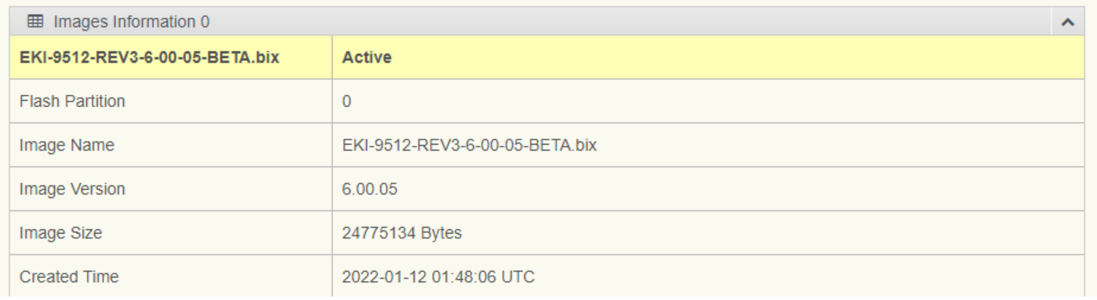
Save

Figure 4.229 Tools > Dual Image

The following table describes the items in the previous figure.

Item	Description
Active Image	Click the format for the image type: Partition0 (Active) or Partition1 (backup).
Save	Click **Save** to save and keep the new settings.

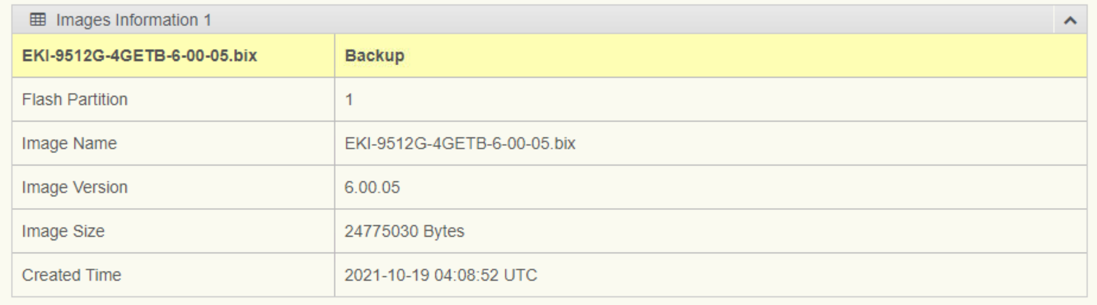
Image Information 0 settings are informational only as shown in the following.



EKI-9512-REV3-6-00-05-BETA.bix	Active
Flash Partition	0
Image Name	EKI-9512-REV3-6-00-05-BETA.bix
Image Version	6.00.05
Image Size	24775134 Bytes
Created Time	2022-01-12 01:48:06 UTC

Figure 4.230 Tools > Dual Image

Image Information 1 settings are informational only as shown in the following.



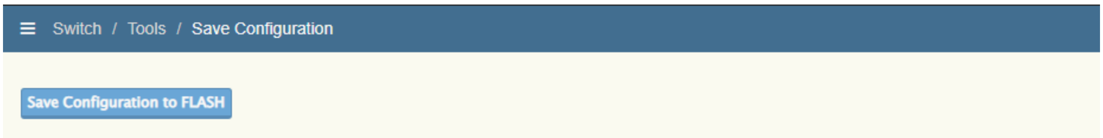
EKI-9512G-4GETB-6-00-05.bix	Backup
Flash Partition	1
Image Name	EKI-9512G-4GETB-6-00-05.bix
Image Version	6.00.05
Image Size	24775030 Bytes
Created Time	2021-10-19 04:08:52 UTC

Figure 4.231 Tools > Dual Image

4.12.5 Save Configuration

To access this page, click **Tools** > **Save Configuration**.

Click **Save Configuration to FLASH** to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.



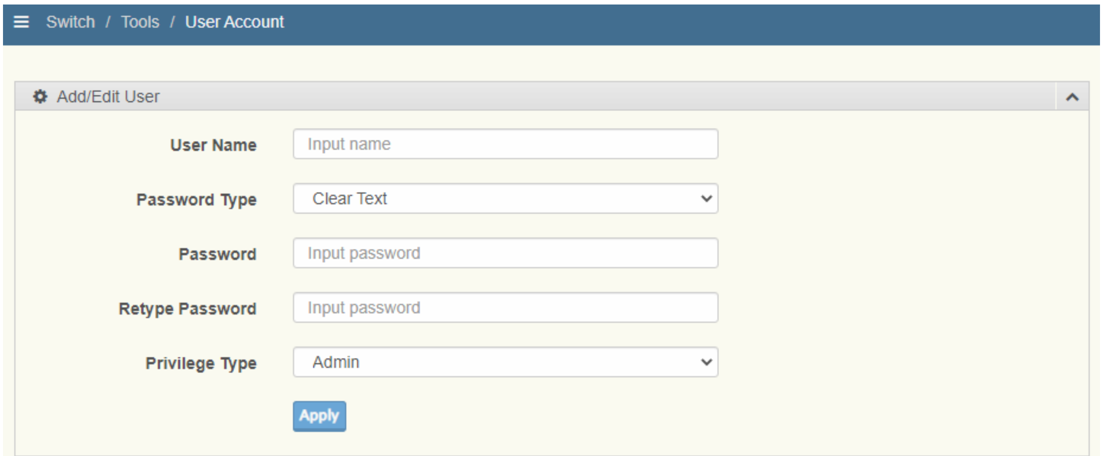
Switch / Tools / Save Configuration
Save Configuration to FLASH

Figure 4.232 Tools > Save Configuration

4.12.6 User Account

The User Account page allows you to setup a user and the related parameters.

To access this page, click **Tools** > **User Account**.



☰ Switch / Tools / User Account

Add/Edit User

User Name	Input name
Password Type	Clear Text
Password	Input password
Retype Password	Input password
Privilege Type	Admin

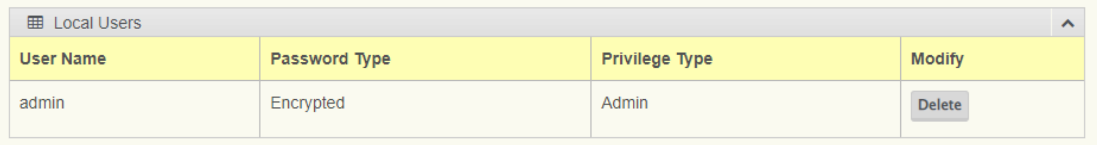
Apply

Figure 4.233 Tools > User Account

The following table describes the items in the previous figure.

Item	Description
User Name	Enter the name of the new user entry.
Password Type	Click the drop-down menu to define the type of password: **Clear Text**, **Encrypted** or **No Password**.
Password	Enter the character set for the define password type.
Retype Password	Retype the password entry to confirm the profile password.
Privilege Type	Click the drop-down menu to designate privilege authority for the user entry: **Admin** or **User**.
Apply	Click **Apply** to create a new user account.

Local Users settings are informational only as shown in the following.



Local Users

User Name	Password Type	Privilege Type	Modify
admin	Encrypted	Admin	Delete

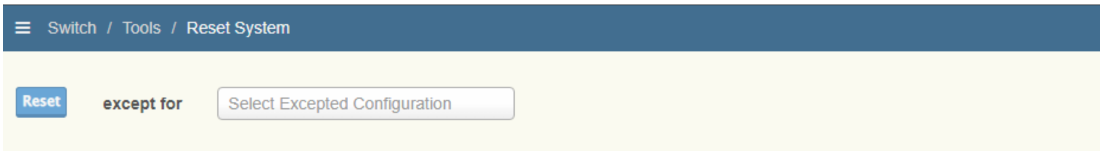
Figure 4.234 Tools > User Account

4.12.7 Reset System

To access this page, click **Tools** > **Reset System**.

Click **Reset** to have all configuration parameters reset to their factory default values. Click **except for** to select the configuration are excepted. All changes that have been made will be lost, even if you have issued a save.

Reset settings take effect after a system reboot.



☰ Switch / Tools / Reset System

Reset except for Select Excepted Configuration

Figure 4.235 Tools > Reset System

4.12.8 Reboot Device

To access this page, click **Tools** > **Reboot Device**.

Click **Reboot** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.

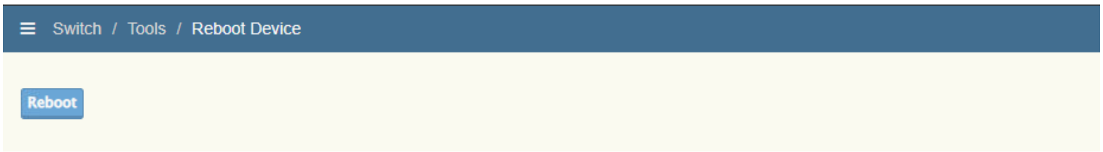


Figure 4.236 Tools > Reboot Device

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.