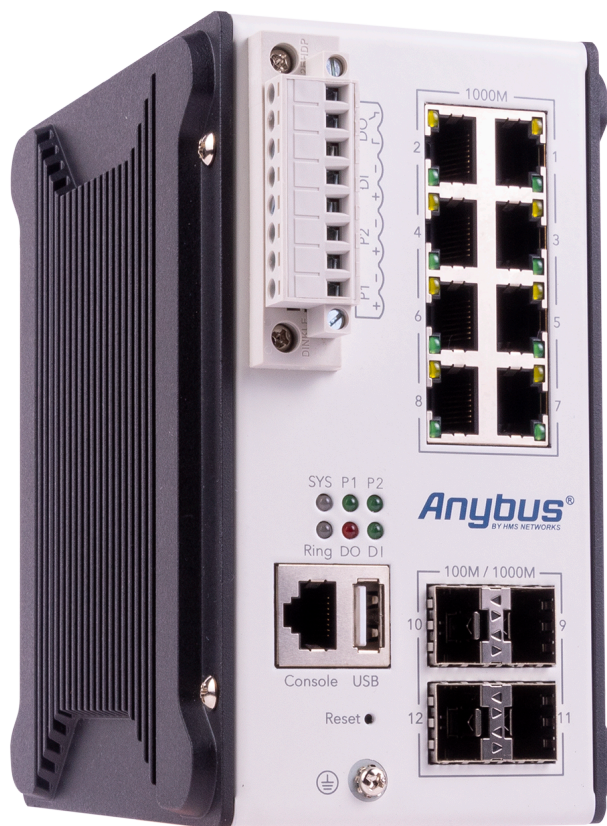


Anybus[®] Managed Industrial L3 Switch

USER MANUAL

SCM-1202-151 1.1 en-US ENGLISH



Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Industrial Networks of any inaccuracies or omissions found in this document. HMS Industrial Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Industrial Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Industrial Networks and is subject to change without notice. HMS Industrial Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Industrial Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

Page

1	Preface	5
1.1	About This Document	5
1.2	Document Conventions	5
1.3	Trademarks	5
2	Safety	6
2.1	Intended Use	6
2.2	General Safety	6
3	Preparation	7
3.1	Support and Resources	7
4	Installation	8
4.1	DIN Rail Mounting	8
4.2	Connecting Ground Screw	9
4.3	Terminal Block Connector	10
4.4	Installing Terminal Block	10
4.5	Connecting Digital Output Wires	11
4.6	Connecting Digital Input Wires	12
4.7	Connecting Power Wires	13
4.8	Connecting to Ethernet Network	14
4.9	Connecting to Fiber Network	14

5	Configuration	15
5.1	Before You Begin Configuration	15
5.2	Accessing the Web Management Interface	15
5.3	Web Interface Overview	16
5.4	System Information	17
5.5	User Account	18
5.6	IP Settings	21
5.7	Date and Time	24
5.8	DHCP Server	26
5.9	Ethernet Port	35
5.10	Redundancy	46
5.11	VLAN	58
5.12	Quality of Service (QoS)	65
5.13	Multicast	69
5.14	Routing	72
5.15	SNMP	84
5.16	Security	87
5.17	Warning	96
5.18	Diagnostics	101
6	Verify Operation	106
6.1	System LED Indicators	106
6.2	Ethernet LED Indicators	106
6.3	SFP Port LED Indicators	107
7	Maintenance and Troubleshooting	108
7.1	USB Port	108
7.2	Backup and Restore	108
7.3	Firmware Upgrade	110
7.4	Reset To Default	111
7.5	Factory Reset Button	112
8	Technical Data	113
8.1	Technical Specifications	113
A	About DHCP Option 82	115
B	About Port Trunk	116
B.1	Port Trunk Concept	116

C	About Connectivity Fault Management (CFM)	117
D	About Redundancy	118
D.1	Spanning Tree Protocol (STP)	118
D.2	Rapid Spanning Tree Protocol (RSTP)	118
D.3	Multiple Spanning Tree Protocol (MSTP)	118
E	About Ethernet Ring Protection Switching (ERPS)	120
F	About Virtual Local Area Network (VLAN)	121
G	About Open Shortest Path First (OSPF)	122
H	About Simple Network Management Protocol (SNMP)	123

This page intentionally left blank

1 Preface

1.1 About This Document

This manual describes the installation and configuration of Anybus Managed Industrial L3 Switch.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.anybus.com/support.

1.2 Document Conventions

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information
- An action
 - and a result

User interaction elements (buttons etc.) are indicated with bold text.

Program code and script examples

Cross-reference within this document: [Document Conventions, p. 5](#)

External link (URL): www.hms-networks.com



WARNING

Instruction that must be followed to avoid a risk of death or serious injury.



Caution

Instruction that must be followed to avoid a risk of personal injury.



Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.



Additional information which may facilitate installation and/or operation.

1.3 Trademarks

Anybus® is a registered trademark of HMS Industrial Networks. All other trademarks mentioned in this document are the property of their respective holders.

2 Safety

2.1 Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

2.2 General Safety

**Caution**

Ensure that the power supply is turned off before connecting it to the equipment.



Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type.

3 Preparation

3.1 Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.anybus.com/support.



Have the product article number available, to search for the specific product page. You find the product article number on the product cover.

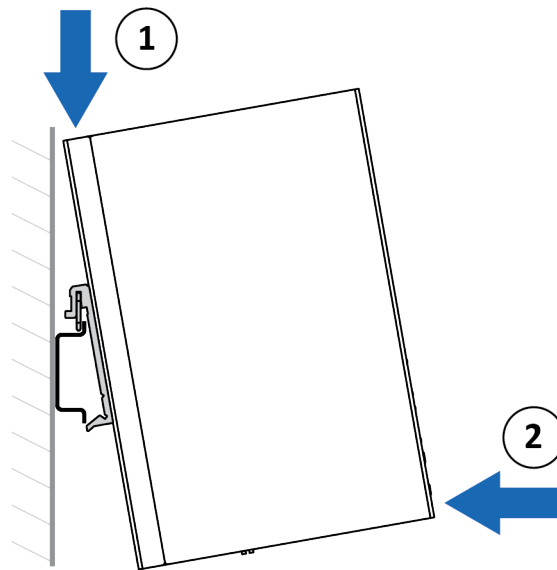
4 Installation

4.1 DIN Rail Mounting



Mount the switch on a *DIN rail* in accordance with the EN 50022 standard.

Procedure



Mount the switch on a DIN rail:

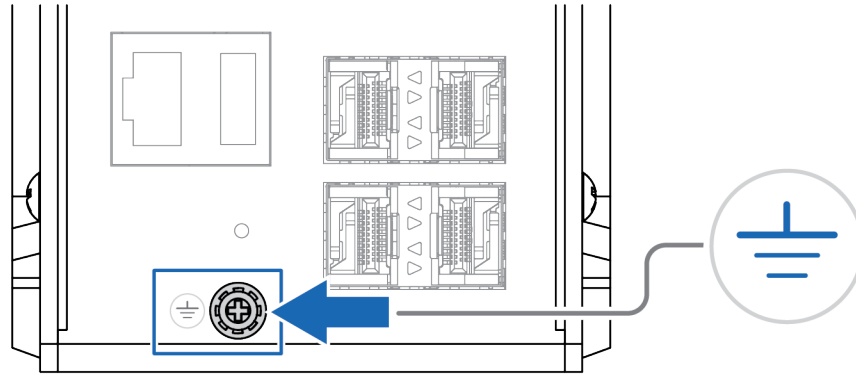
1. Insert the upper end of the *DIN rail clip* into the DIN rail.
2. Push the bottom of the *DIN rail clip* into the DIN rail.

4.2 Connecting Ground Screw



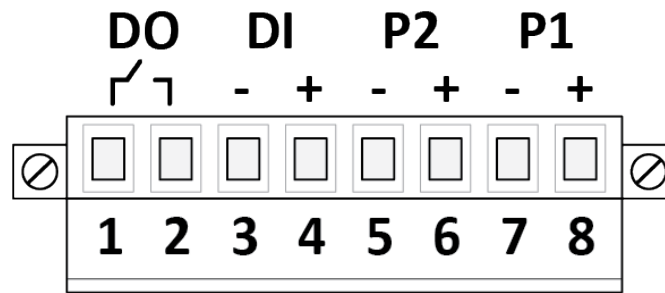
To avoid system damage, the equipment should be connected to ground.

Procedure



1. Establish a direct connection between the ground screw and the grounding surface prior to connecting devices.

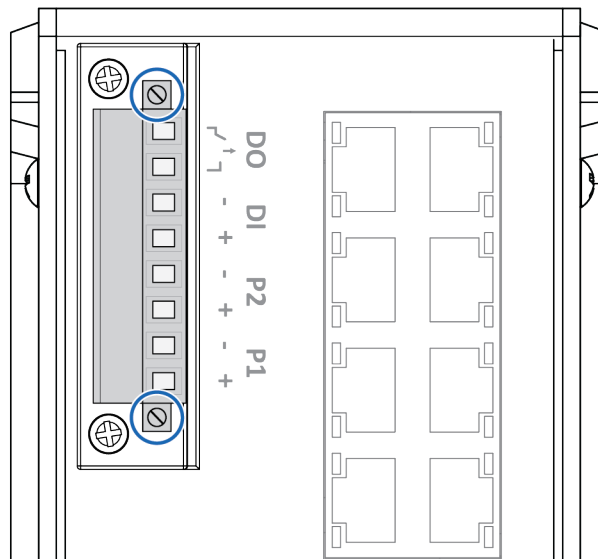
4.3 Terminal Block Connector



Contact Number	Description
1	DO, Digital Output
2	
3	DI, Digital Input –
4	DI, Digital Input +
5	P2, Power Input 2 –
6	P2, Power Input 2 +
7	P1, Power Input 1 –
8	P1, Power Input 1 +

4.4 Installing Terminal Block

Procedure



1. Attach the terminal block to the contact on the switch.
2. Fasten the terminal block with the 2 screws included.

4.5 Connecting Digital Output Wires

Before You Begin

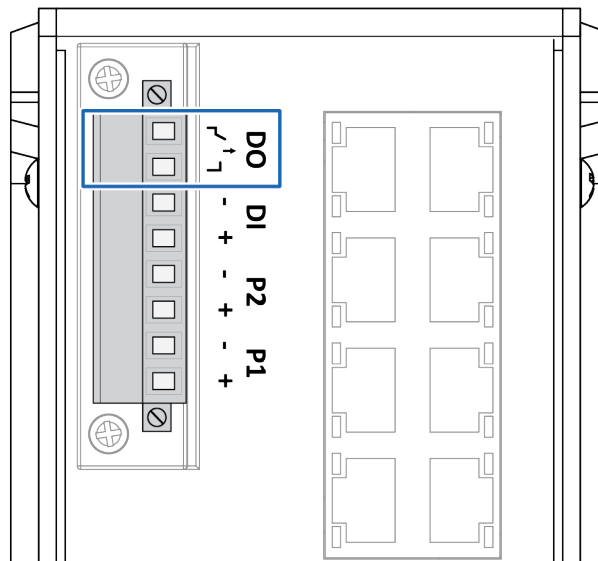
The relay output is used to detect user-configured events.

When a user-configured event is triggered, the two wires attached to the *DO*, fault contacts, form a close circuit.

The fault circuit remains opened until a user-configured event occur.

Procedure

Connect the Digital Output (DO):

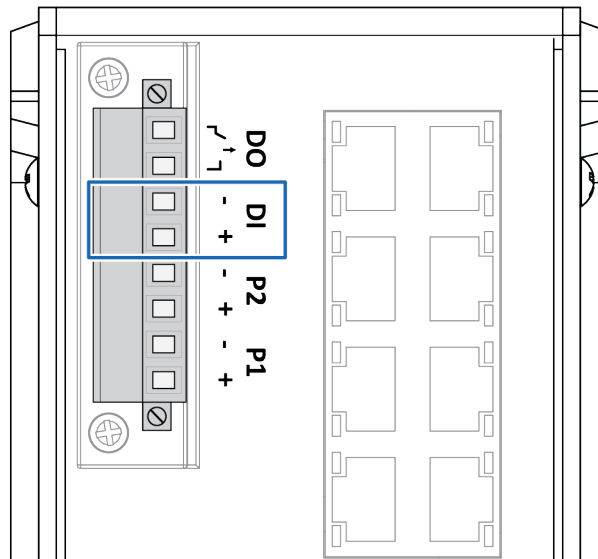


1. Insert the wires into the 2 pin *DO* contact on the *8 pin terminal block*.
2. Tighten the *wire-clamp screws*.

4.6 Connecting Digital Input Wires

Procedure

Connect the Digital Input (DI):



1. Insert the wires into the 2 pin *DI -* and *DI +* contact on the *8 pin terminal block*.
2. Tighten the *wire-clamp screws*.

4.7 Connecting Power Wires



Caution

Ensure that the power supply is turned off before connecting it to the equipment.



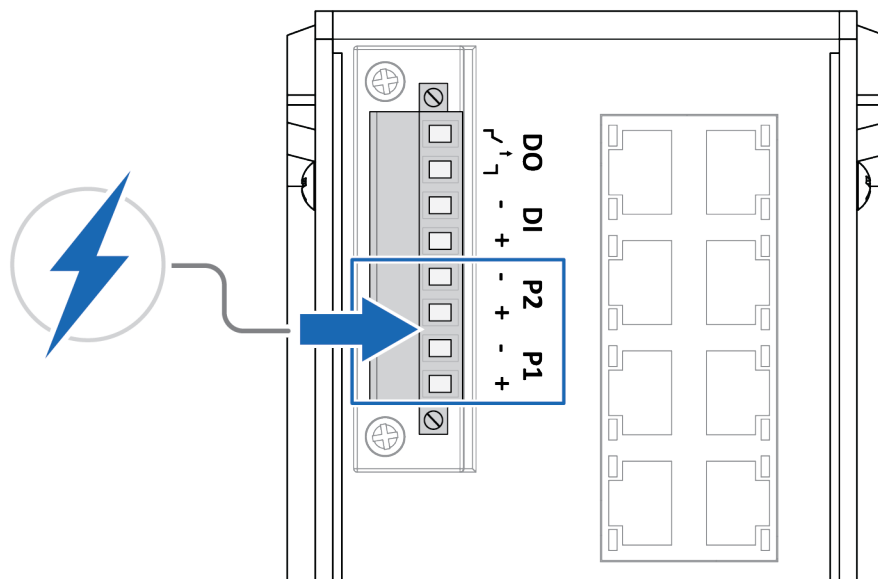
Use a power supply of 24 VDC (10-60 VDC) to power the switch.

Max power consumption: 16.08 W.



The relay contact supports 0.5 A current, 24 VDC.

Procedure

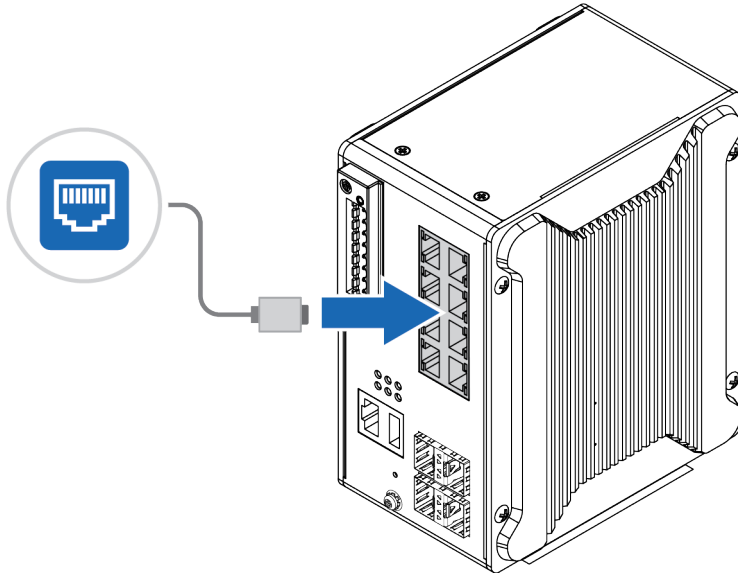


1. **Connecting to main power supply P1:** Insert the positive and negative wires into the *P1+* and *P1-* contact on the *8 pin terminal block*.
2. **Connecting to redundant power supply P2:** Insert the positive and negative wires into the *P2+* and *P2-* contact on the *8 pin terminal block*.
3. Tighten the *wire-clamp screws*.
4. Connect the power wires to a *DC switching type power supply*.

4.8 Connecting to Ethernet Network

Optional

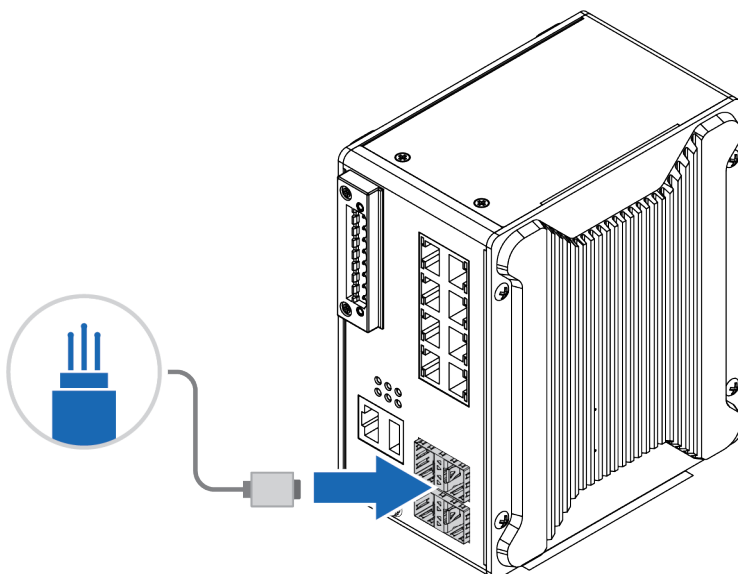
Connect the switch to an Ethernet network.



4.9 Connecting to Fiber Network

Optional

Connect the switch to a network via the *SFP* port.



5 Configuration

5.1 Before You Begin Configuration

The switch is configured through *web management* or *console management*.

The switch can also be configured through *Telnet management* or *SSH management*.



The switch default IP address is **http://192.168.10.1/**.



The default switch login user name is **admin** and the password is **admin**.

5.2 Accessing the Web Management Interface

Prepare for configuring the switch settings via the web management interface.

Before You Begin

- ▶ Connect the switch to your computer.
- ▶ Connect the switch to power.
- ▶ To link your computer with the switch, make sure that the IP address of the computer is located in the same subnet as the switch default IP address.

Procedure

Access the web management interface:

1. In your browser, type **http://IP address** and press **Enter**.
 - The web-based management interface login screen appears.
2. In the login screen, enter user name and password.
3. Click **OK**.
 - The web-based management interface welcome page appears.

To Do Next

- ▶ Configure the switch.

5.3 Web Interface Overview

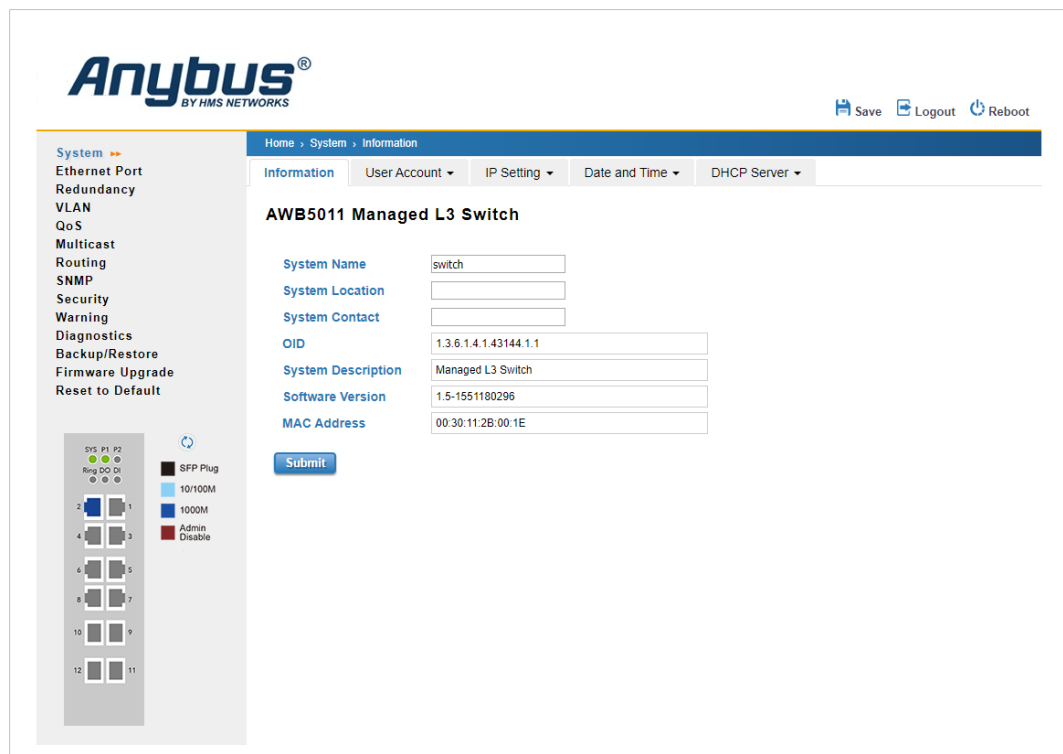


Fig. 1 Web Interface Overview

5.3.1 To Save Settings



Unsaved settings will be lost when the switch is powered off or restarted.

- ▶ To apply changes made on a configuration page/tab, click **Submit** at the bottom of the page.
- ▶ To cancel the changes, click **Cancel**.
Some pages have additional buttons that are described in the respective sections in this manual.
- ▶ To save changed settings permanently, click **Save** in the configuration page top menu.
The recent changes will otherwise be discarded if the switch is rebooted.

5.3.2 To Logout From the Web Interface

To manually logout from the system:

1. In the web interface top menu, click **Logout**.
2. To confirm, click **Yes**.

5.3.3 To Reboot the Switch



Unsaved settings will be lost when the switch reboot.

Some changes to the settings require the user to reboot the switch.

To manually reboot the switch:

1. In the web interface top menu, click **Reboot**.
 2. To confirm, click **Yes**.
- The switch will reboot immediately.

5.4 System Information

The Information page shows the basic switch information.

Home > System > Information

Information User Account IP Setting Date and Time DHCP Server

AWB5011 Managed L3 Switch

System Name:

System Location:

System Contact:

OID:

System Description:

Software Version:

MAC Address:

Fig. 2 Switch information

Configure the switch information:

System Name	Name of the unit that will be shown on the network Default: switch
System Location	Specify the physical location of the switch. Default: blank
Software Contact	Specify a contact person. Enter name, mail address or other information. Default: blank
OID	Switch Object ID.
System Description	Product name
Software Version	Latest installed firmware version.
MAC Address	MAC address of the Ethernet network interface

To apply the settings, click **Submit**.

5.5 User Account

The User Account page consists of two interfaces, Local User and RADIUS Interface.



The default authority allows the user to configure all configuration parameters.



For security consideration, please change the password after first login to the web interface.



*The default switch login user name is **admin** and the password is **admin**.*

5.5.1 Local User

Home > System > Local User

Information User Account IP Setting Date and Time DHCP Server

Local User

Name

Privilege

New Password

Confirm Password

Local User List

select	User	Privilege
<input type="checkbox"/>	admin	15

Authentication Order

Order

Fig. 3 Local User

Configure the Local User settings:

Name	Default: admin Enter a new user name here.
Privilege	Select the local user privilege level.
New Password	Default: admin Enter a new password here.
Confirm Password	Re-enter the new password to confirm it.

To apply the settings, click **Submit**.

To cancel the changes, click **Cancel**.

5.5.2 RADIUS Server

The Remote Authentication Dial In User Service (RADIUS) mechanism is a centralized "AAA" (Authentication, Authorization and Accounting) system for connecting to network services.

The purpose of RADIUS is to provide an efficient and secure mechanism for user account management.

RADIUS server system allows you to access the switch through secure networks against unauthorized access.

Fig. 4 RADIUS Setting

Configure the RADIUS server settings:

RADIUS Server IP	Enter the IP address of the RADIUS server in Server IP Address.
Shared Key	Enter the Shared Secret of the RADIUS server. Shared key is used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared key. Shared key also verify that the RADIUS message has not been modified in transit (message integrity).
Server Port	If applicable, enter the Server port. Set communication port of an external RADIUS server as the authentication database. By default, the RADIUS server listens to port 1812.

To apply the settings, click **Submit**.

5.6 IP Settings

5.6.1 IPv4

Fig. 5 IP Setting

DHCP Client

Configure the DHCP Client settings:

DHCP Client	<p>Select Enable or Disable to activate or deactivate the DHCP Client function.</p> <p>If DHCP Client is Disabled, the configured IP settings will be used.</p> <p>When the DHCP Client function is Enabled, an IP address will be assigned to the switch from the network DHCP server.</p> <p>The DHCP client will announce the configured System Name as hostname to provide DNS lookup.</p>
-------------	--

To apply the settings, click **Submit**.

IPv4 Configuration

Configure the IPv4 settings:

IP Address	<p>Default: 192.168.10.1</p> <p>Set up the IP address reserved by User network for User switch.</p> <p>If the DHCP Client function is enabled, do not assign an IP address to the switch as it will be overwritten by the DHCP server.</p>
Subnet Mask	<p>Default: 255.255.255.0</p> <p>Assign the subnet mask for the IP address.</p> <p>If the DHCP Client function is enabled, do not assign the subnet mask.</p>
Default Gateway	<p>Assign the gateway for the switch here.</p>
DNS Server 1 DNS Server 2	<p>Specifies the IP address of the DNS server 1 and 2 used in user network.</p>

To apply the settings, click **Submit**.

5.6.2 IPv6

IPv6 address

- An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets).
- The groups are separated by colons.
- The length of an IPv6 address is 128 bits.
- IPv6 address, example: fe80::212:77ff:feff:1acb/64.

IPv6 Setting

[Home](#) > [System](#) > [IPv6 Setting](#)

[Information](#) | [User Account](#) ▾ | [IP Setting](#) ▾ | [Date and Time](#) ▾ | [DHCP Server](#) ▾

IPv6 Setting

IPv6 Address

Prefix Length

Add

IPv6 Default Gateway

Submit

☐

IPv6 Address

☐

fe80::230:11ff:fe2b:1e/64

Remove

Reload

Reload

Fig. 6 IPv6 Setting

Configure the IPv6 settings:

IPv6 Address	Enter an IPv6 address. The network portion of the address can be configured by specifying the Prefix and using a EUI-64 interface ID in the low order 64 bits. The host portion of the address is automatically generated using the modified EUI-64 form of the interface identifier (Switch MAC address).
Prefix Length	Enter the Prefix Length. The size of the subnet or network, and equivalent to the subnetmask. To add the address, click Add .
IPv6 Default Gateway	The prefix value must be formatted according to the RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. To apply the settings, click Submit .
IPv6 Address	To delete an address, select the address and click Remove . To reload the information, click Reload .

Neighbor Cache**View Neighbor Cache:**

Neighbor Cache	The IPv6 neighbor table includes the neighboring node IPv6 address, Interface, MAC Address, and the current state of the entry. The system will update Neighbor Cache automatically.
----------------	---

To reload the information, click **Reload**.

5.7 Date and Time

5.7.1 Date and Time Setting

The time calibration function is based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.



The switch has no real-time clock. When there is no NTP server on the LAN or Internet connection, Current Time must be set manually after each reboot.

Home > System > Date and Time Setting

Information User Account IP Setting Date and Time DHCP Server

Date and Time Setting

Current Time
 Yr 2018 Mon 01 Day 1 Hr 00 Mn 19 Sec 15
 Get PC Time

Time Zone
 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

NTP
☐ Enable NTP client update

1st Time Server
 N/A

2st Time server
 N/A

Daylight saving Time
 Disable

Daylight Saving Start
 in at

Daylight Saving End
 in at

Submit Cancel

Fig. 7 Date and Time Setting

Configure the Date and Time settings:

Current Time	Set the time manually or click Get Time from PC to get the PC time setting.
Time Zone	To adjust the time zone based on the user area, select a Time Zone .
NTP	To Enable NTP Client update, select the checkbox. Make sure that the switch is connected to the internet. The system will send request packet to acquire current time from the NTP server that assigned.
1st Time Server 2nd Time Server	Select the NTP Server from the list, which should adjust the User system time.
Daylight Saving Time	Enable or Disable Daylight Saving Time.
Daylight Saving Start Daylight Saving End	When Daylight Saving Time is Enabled, set the Start and End time.

To apply the settings, click **Submit**.

To cancel the changes, click **Cancel**.

5.7.2 PTP Setting

Home > System > PTP Setting

Information User Account IP Setting Date and Time DHCP Server

PTP Setting

Operation Disable ▼

Operation Mode Auto Elect ▼

Synchronization Interval 0(1s) ▼

Announce Interval 1(2s) ▼

Announce Receipt Timeout 6

Minimum Path Delay Request Message Interval 1(2s) ▼

Domain Number 0

First Priority 128

Second Priority 128

Delay Mechanism E2E ▼

Submit

Fig. 8 PTP Setting

Configure the PTP settings:

Operation	Default: Disable Enable or Disable the PTP function. Operation must be enabled for the PTP function to work.
Operation Mode	Select Operation Mode from the drop-down menu, Auto Elect, Preferred Master Clock or Slave. Default: Auto Elect
Synchronization Interval	Set the interval of the sync packet transmitted time. A small interval causes higher load to the device and network. Default: 0 (1s)
Announce Interval	Set the announce message interval. Default: 1 (2s)
Announce Receipt Timeout	The multiple of announce message receipt timeout by the announce message interval. Default: 6
Minimum Path Delay Request Message Interval	Minimal delay request message interval Default: 1 (2s)
Domain Number	Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages.
First Priority	Set the clock priority 1 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm, 0 = highest priority, 255 = lowest priority. Default: 128

Second Priority	Set the clock priority 2 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority. Default: 128
Delay Mechanism	Configures the delay mechanism in boundary clock mode. E2E: The delay request or response mechanism used in the boundary clock mode. P2P: The peer-to-peer mechanism used in the boundary clock mode. Default: E2E

To apply the settings, click **Submit**.

5.8 DHCP Server

5.8.1 DHCP Server Setting

Home > System > DHCP Server Setting

Information User Account IP Setting Date and Time DHCP Server

DHCP Server Setting

Global Setting Disable ▾

Submit

Address Pool Add

Pool Name

Add

Address Pool List

Pool Name ▾

Select **Delete**

Address Pool Setting

Pool Name

Network

Mask

Default Gateway

Lease Time

Submit

Fig. 9 DHCP Server Setting

Configure the DHCP Server settings:

Global Setting	To activate and deactivate DHCP Server function, select Enable or Disable . To apply the setting, click Submit .
Address Pool Add	The address pool to local DHCP Server. Enter the Pool Name and click Add .
Address Pool List	Select a Pool Name from the Address Pool List and click Select . To delete the setting, click Delete .
Network	Enter the starting IP addresses for the DHCP server IP assignment.
Mask	Assign the subnet mask for the IP address.
Default Gateway	Enter the ending IP addresses for the DHCP server IP assignment.
Lease Time	The maximum length of time for the IP address lease. Enter the Lease time in minutes. Lease Time range: 60-31536000 seconds.

To apply the settings, click **Submit**.

Setting Up Computers as DHCP Clients

When DHCP Server is enabled, it will automatically assign IP addresses to the computers connected to the LAN/private network.

Set the computers to be DHCP clients by setting their TCP/IP settings to Obtain an IP Address Automatically.

When the user turn on the computer/device, the TCP/IP settings, provided by the switch, are automatically loaded.

If the users manually assigns IP addresses to the computers/devices, make sure that the IP addresses are outside the DHCP server address range or users may have an IP conflict.

5.8.2 Excluded Address List

IP addresses that should not be assigned to the devices connected to the network are listed in the Excluded Address List.



Fig. 10 Excluded Address List

Configure the Excluded Address settings:

Excluded Address List	Enter a IP address and click Add . To remove an IP address from the list, click Remove . To reload the information, click Reload .
-----------------------	---

5.8.3 Static Port/IP Binding List

Static Port/IP Binding List

Port

IP Address

Add

Index

Port

IP Address

Remove

Reload

Fig. 11 Static Port/IP Binding List

Configure the Static Port/IP Binding settings:

Port	Enter the port number.
IP Address	The IP address that will assign to the device with the Binding MAC address. Enter the IP address and click Add .

To remove a binding rule from the list, click **Remove**.

To reload the information, click **Reload**.

5.8.4 Static MAC/IP Binding List

Static MAC/IP Binding List

MAC Address

IP Address

Add

Index

MAC Address

IP Address

Remove

Reload

Fig. 12 Static MAC/IP Binding List

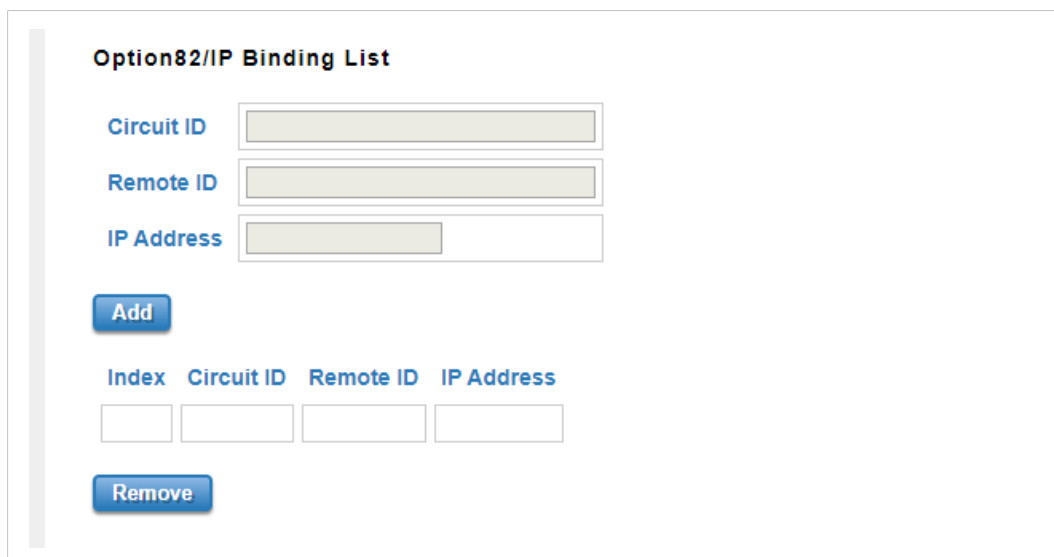
Configure the MAC/IP Binding settings:

MAC Address	Enter the MAC address.
IP Address	The IP address that will assign to the device with the Binding MAC address. Enter the IP address and click Add .

To remove a binding rule from the list, click **Remove**.

To reload the information, click **Reload**.

5.8.5 Option 82/IP Binding List



The image shows a web-based configuration interface titled "Option82/IP Binding List". It contains three input fields: "Circuit ID", "Remote ID", and "IP Address", each with a corresponding text box. Below these fields is a blue "Add" button. Underneath the button is a table with four columns: "Index", "Circuit ID", "Remote ID", and "IP Address". The table currently has one empty row. Below the table is a blue "Remove" button.

Fig. 13 Option 82/IP Binding List

Configure the Option 82/IP Binding settings:

Circuit ID	Enter the Circuit ID of the device that wishes binding.
Remote ID	Enter the Remote ID of the device that wishes binding.
IP Address	Enter the IP address that will assign to the device with the Binding MAC address. Click Add .

To remove a binding rule from the list, click **Remove**.

5.8.6 DHCP Option 82

Home > System > DHCP Option 82

Information User Account IP Setting Date and Time DHCP Server

DHCP Option 82

DHCP Relay Agent Disable ▾

Submit

Helper Address

Helper Address

Add

<input type="checkbox"/>	Helper Address 1	<input type="text"/>
<input type="checkbox"/>	Helper Address 2	<input type="text"/>
<input type="checkbox"/>	Helper Address 3	<input type="text"/>
<input type="checkbox"/>	Helper Address 4	<input type="text"/>

Remove

Fig. 14 DHCP Option 82 Setting

Configure the Option 82 settings:

DHCP Option 82	<p>Select the modification type of option 82.</p> <p>To activate or deactivate DHCP relay agent function, select Enable or Disable .</p> <p>Click Submit.</p> <p>When Option 82 is enabled, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address).</p> <p>The DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port.</p>
Helper Address	Enter a DHCP Server IP address and click Add .

To remove a binding rule from the list, select the checkbox and click **Remove**.

5.8.7 Relay Policy

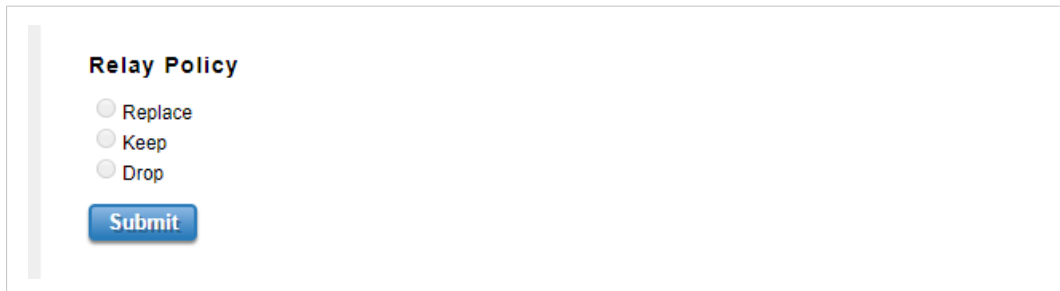
The image shows a web-based configuration interface for the Relay Policy. It features a title "Relay Policy" at the top. Below the title are three radio button options: "Replace", "Keep", and "Drop". The "Replace" option is selected, indicated by a filled radio button. At the bottom of the form is a blue "Submit" button.

Fig. 15 Relay Policy Setting

Configure the Relay Policy settings:

Replace	Default setting. Replaces the existing option 82 field and adds new option 82 field.
Keep	Keeps the original option 82 field and forwards to server.
Drop	Drops the option 82 field and do not add any option 82 field.

To apply the settings, click **Submit**.

5.8.8 Circuit ID and Remote ID

The DHCP Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server.

Circuit ID

▼

☐ Default (VLAN/Port)
 ☐ User Defined

Submit

Port	Circuit ID	HEX value
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>

Remote ID

☐ Default (MAC Address)
 ☐ IP Address
 ☐ User Defined

Submit

Remote ID	HEX value
<input type="text"/>	<input type="text"/>

Fig. 16 Circuit ID and Remote ID Setting

Circuit ID

The Circuit ID is a 4-byte number generated by the Ethernet switch.

Before you begin, ensure that the DHCP Relay Agent function is enabled, refer to [DHCP Option 82, p. 30](#).

The format of the Circuit ID is 00–01–00–01.

The first byte is "00", the second and the third byte "01-00" is formed by the port VLAN ID, and the last byte "01" is formed by the port number.

Example: 00-01-00-01 is the Circuit ID of port number 1 with port VLAN ID 1.

To apply the settings, click **Submit**.

Remote ID

The Remote ID identifies the relay agent itself and can be one of the following:

- The IP address of the relay agent.
- The MAC address of the relay agent.
- A combination of IP address and MAC address of the relay agent.
- A user-defined string.

To apply the settings, click **Submit**.

5.8.9 DHCP Leased Entries

The DHCP Leased Entries table shows the MAC address and IP address assigned by the switch.

Home > System > DHCP Leased Entries

Information User Account IP Setting Date and Time DHCP Server

DHCP Leased Entries

Index	IP Address	MAC Address	Leased Time Remains

Reload

Fig. 17 DHCP Leased Entries Settings

Configure the DHCP Leased Entries settings:

IP Address	IP address that was assigned by switch.
MAC Address	MAC address that was assigned by switch.
Leased Time Remains	Remains time for the IP address leased

To reload the information, click **Reload**.

5.9 Ethernet Port

5.9.1 Port Setting

In the Port Setting page you can access the port configuration and rate limit control.

You can also view port status and port trunk information.

Port	State	Speed/Duplex	Flow Control	Description
1	Enable	AutoNegotiation	Disable	
2	Enable	AutoNegotiation	Disable	
3	Enable	AutoNegotiation	Disable	
4	Enable	AutoNegotiation	Disable	
5	Enable	AutoNegotiation	Disable	
6	Enable	AutoNegotiation	Disable	
7	Enable	AutoNegotiation	Disable	
8	Enable	AutoNegotiation	Disable	
9	Enable	AutoNegotiation	Disable	
10	Enable	AutoNegotiation	Disable	
11	Enable	AutoNegotiation	Disable	
12	Enable	AutoNegotiation	Disable	

Submit Cancel

Fig. 18 Port Setting

Configure the Port settings:

Port	Shows the port number.
State	Enable or disable a port. Default: Enable
Speed/Duplex	Set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode for Giga Ethernet Port 1–8 (ge1–ge8). For Gigabit Ethernet Port 9–12: (ge9–ge12), it can be set up to 100M Full Duplex(100 Full) only. Default: AutoNegotiation
Flow Control	Enable: Activate the flow control function to let the flow control of that corresponding port on the switch to work. Disable: The flow control of the corresponding port on the switch will work automatically. Default: Disable
Description	The description of the interface.

To apply the settings, click **Submit**.

To cancel the changes, click **Cancel**.

5.9.2 Port Status

Home > Ethernet Port > Port Status

Port Setting
Port Status
Port Trunk
Rate Control
Storm Control
Jumbo Frame
CFM Setting

Port Status

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Down	Enable	---	Disable	---	---	---
2	Up	Enable	1000 Full	Disable	---	---	---
3	Down	Enable	---	Disable	---	---	---
4	Down	Enable	---	Disable	---	---	---
5	Down	Enable	---	Disable	---	---	---
6	Down	Enable	---	Disable	---	---	---
7	Down	Enable	---	Disable	---	---	---
8	Down	Enable	---	Disable	---	---	---
9	Down	Enable	---	Disable	---	---	---
10	Down	Enable	---	Disable	---	---	---
11	Down	Enable	---	Disable	---	---	---
12	Down	Enable	---	Disable	---	---	---

SFP DDM

Port	SFP Scan/Eject	SFP DDM	Temperature (degree)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
9	---	Enable	---	---	---	---	---	---
10	---	Enable	---	---	---	---	---	---
11	---	Enable	---	---	---	---	---	---
12	---	Enable	---	---	---	---	---	---

Reload
Apply
Scan All
Eject All

Fig. 19 Port Status Page

SFP module with digital diagnostics monitoring (DDM)

The switch supports the SFP module with digital diagnostics monitoring (DDM) function.

This feature enables monitoring the real-time parameters of the fiber optic transceivers, like optical input/output power, temperature, and transceiver supply voltage of an SFP module via SFP DDM section.

The real-time diagnostic parameters can be monitored to alert the system when the transceiver specified operating limits are exceeded and compliance cannot be ensured.

SFP DDM

Configure the SFP DDM settings:

SFP Scan/Eject	Scan the SFP module or Eject the SFP module.
SFP DDM	Enable/Disable the DDM function.
Temperature	The specific temperature range and current temperature detected of DDM SFP transceiver.
Tx Power (dBm)	The range and current transmit power of DDM SFP transceiver.
Rx Power (dBm)	The range and current received power of DDM SFP transceiver.

For the settings to take effect, click **Apply**.

To reload the information, click **Reload**.

To scan the SFP transceiver module and show the statistics, click **Scan All**.

To eject selected SFP transceivers or plug SFP transceivers, click **Eject All**.

5.9.3

Port Trunk

Port Trunk Setting

The screenshot shows the 'Port Trunk Setting' configuration page. At the top, there is a breadcrumb trail: 'Home > Ethernet Port > Port Trunk Setting'. Below this is a tabbed interface with tabs for 'Port Setting', 'Port Status', 'Port Trunk', 'Rate Control', 'Storm Control', 'Jumbo Frame', and 'CFM Setting'. The 'Port Trunk' tab is selected. The main content area is titled 'Port Trunk Setting' and contains a table with 12 rows, each representing a port. Each row has three columns: 'Port', 'Group ID', and 'Trunk Type'. The 'Port' column lists ports from 1 to 12. The 'Group ID' column has a dropdown menu with '0' selected for all ports. The 'Trunk Type' column has a dropdown menu with 'Static' selected for all ports.

Port	Group ID	Trunk Type
1	0	Static
2	0	Static
3	0	Static
4	0	Static
5	0	Static
6	0	Static
7	0	Static
8	0	Static
9	0	Static
10	0	Static
11	0	Static
12	0	Static

Fig. 20 Port Trunk Setting

Configure the Port settings:

The switch can support up to 8 trunk groups with 2 trunk members.

Since the member ports should use the same speed/duplex, max trunk members would be 8 for 100Mbps, and 2 members for Gigabit.

Group ID	Group ID is the ID for the port trunk group. Ports with same group ID are in the same group. Default: 0
Type	Static and LACP. Each Trunk Group can only support Static or LACP. Default: Blank

Load Balance Setting

Load Balance Setting

Group ID	Type
1	src-dst-mac ▼
2	src-dst-mac ▼
3	src-dst-mac ▼
4	src-dst-mac ▼
5	src-dst-mac ▼
6	src-dst-mac ▼
7	src-dst-mac ▼
8	src-dst-mac ▼

SubmitReload

Fig. 21 Load Balance Setting

Configure the Balance settings:

Load Balance Type	Description
src-mac	Load distribution is based on the source MAC address.
dst-mac	Load distribution is based on the destination-MAC address.
src-dst-mac	Load distribution is based on the source and destination MAC address.
src-ip	Load distribution is based on the source IP address.
dst-ip	Load distribution is based on the destination IP address.
src-dst-ip	Load distribution is based on the source and destination IP address.

To apply the settings, click **Submit**.

To reload the information, click **Reload**.

Port Trunk Status

On the Port Trunk Status page you can view the status of port aggregation.

Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
1	N/A			
2	N/A			
3	N/A			
4	N/A			
5	N/A			
6	N/A			
7	N/A			
8	N/A			

Reload

Fig. 22 Port Trunk Status

View the Port Truck settings:

Group ID	Display Trunk groups 1-8 setup in Aggregation Setting.
Type	Static or LACP setup in Aggregation Setting.
Aggregated Ports	When LACP link is well, the member ports are shown in the aggregated column.
Individual Ports	When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports are shown in the Individual column.
Link Down Ports	When LACP is enabled, member ports of LACP group which are not linked up are shown in the Link Down column.

To reload the information, click **Reload**.

5.9.4 Rate Control

Rate control is a type of flow control used to enforce a strict bandwidth limit at a port.

Separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port can be programmed.

Home > Ethernet Port > Rate Control

Port Setting Port Status Port Trunk ▾ **Rate Control** Storm Control Jumbo Frame CFM Setting

Rate Control

Port	Ingress Rule(Kbps)	Egress Rule(Kbps)
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0

Submit

Fig. 23 Rate Control

Configure the Rate Control settings:

Rate (Ingress & Egress)	Default value, Ingress rule: 0 kbps Default value, Egress rule: 0 kbps (0 stands for disabling the rate control for the port.) Valid values are increments of 64 kbps from 64-1 000 000 kbps.
-------------------------	---

To apply the settings, click **Submit**.

5.9.5 Storm Control

A LAN storm appears when packets flood the LAN, creating excessive traffic and degrading network performance.

Errors in the implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm.

Storm control prevents traffic on a LAN from being disrupted by a broadcast, DLF, or multicast storm on a port.

Home > Ethernet Port > Storm Control

Port Setting Port Status Port Trunk ▾ Rate Control **Storm Control** Jumbo Frame CFM Setting

Storm Control

Port	Broadcast	Rate(packet/sec)	DLF	Rate(packet/sec)	Multicast	Rate(packet/sec)
1	Disable ▾	0	Disable ▾	0	Disable ▾	0
2	Disable ▾	0	Disable ▾	0	Disable ▾	0
3	Disable ▾	0	Disable ▾	0	Disable ▾	0
4	Disable ▾	0	Disable ▾	0	Disable ▾	0
5	Disable ▾	0	Disable ▾	0	Disable ▾	0
6	Disable ▾	0	Disable ▾	0	Disable ▾	0
7	Disable ▾	0	Disable ▾	0	Disable ▾	0
8	Disable ▾	0	Disable ▾	0	Disable ▾	0
9	Disable ▾	0	Disable ▾	0	Disable ▾	0
10	Disable ▾	0	Disable ▾	0	Disable ▾	0
11	Disable ▾	0	Disable ▾	0	Disable ▾	0
12	Disable ▾	0	Disable ▾	0	Disable ▾	0

Submit

Fig. 24 Storm Control Setting

Configure the Storm Control for each port.

Broadcast	Set enable to control Broadcast Packets. Default: Disable
DLF	Set enable to control Destination Lookup Failure packets. Default: Disable
Multicast	Set enable to control Multicast Packets. Default: Disable
Rate(Packet/Sec)	Rate limit value 0-262142 packet/sec.

To apply the settings, click **Submit**.

5.9.6 Jumbo Frame

Home > Ethernet Port > Jumbo Frame

Port Setting | Port Status | Port Trunk ▾ | Rate Control | Storm Control | **Jumbo Frame** | CFM Setting

Jumbo Frame

Port	MTU Size
1	1518
2	1518
3	1518
4	1518
5	1518
6	1518
7	1518
8	1518
9	1518
10	1518
11	1518
12	1518

Submit **Reload**

Fig. 25 Jumbo Frame Settings

Configure the Jumbo Frame settings:

Enter the size of the Maximum Transmission Unit (MTU).

The default value is 1,518 bytes.

The maximum Jumbo Frame size is 9,216 bytes.

To apply the settings, click **Submit**.

To reload the information, click **Reload**.

5.9.7 CFM Setting

Home > Ethernet Port > CFM Setting

Port Setting | Port Status | Port Trunk ▾ | Rate Control | Storm Control | Jumbo Frame | **CFM Setting**

CFM Setting

Add Domain

MD Level: 0 ▾

Domain Name:

Add

Add Association

Domain Name: ▾

Association Name:

VLAN: VLAN 1 ▾

Transmit Interval (ms): 3 ▾

Add

Add Endpoint

Domain Association Name: ▾

Endpoint Type: Local Endpoint ▾

Port: Port 1 ▾

MEP ID: 1 ▾

Add

Fig. 26 CFM Setting

Add Domain

Configure the domain settings:

MD Level	<p>Select the MD Level from 0-7</p> <p>A hierarchical relationship exists between domains based on levels. The larger the domain, the higher the level value.</p> <p>Recommended values of levels:</p> <ul style="list-style-type: none"> Customer Domain: Largest Provider Domain: In between (e.g., 3) Operator Domain: Smallest
Domain Name	<p>Enter a Domain Name.</p> <p>Maximum: 43 characters</p>

To add the settings, click **Add**.

Add Association

Configure the Association settings:

Domain Name	Select the Domain Name from the list.
Association Name	Enter the Association Name. Association name, maximum of 45 characters
VLAN	Select the assigned VLAN. Please create VLAN first, and each port set to be tagged.
Transmit Interval (ms)	Select the Transmit Interval from the list.

To add the settings, click **Add**.

Add Endpoint

Points at the edge of the domain, define the boundary for the domain.

A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

Domain Association Name	Choose the Domain Association Name that has been added
Endpoint Type	Choose between Local Endpoint and Remote Endpoint Local Endpoint: Set the port as the Continuity Check Message (CCM) sender. Remote Endpoint: Set the port as the Continuity Check Message (CCM) receiver. Default: Local Endpoint
Port	Choose port that need to be assigned Default: Port 1
MEP ID	Choose the MEP ID. One MEP refer to one MEP ID Default: 1

To add the settings, click **Add**.

Domain Table



The screenshot shows a web interface titled "Domain Table". It contains a table with two columns: "Domain Name" and "MD Level". Below the table, there are two buttons: "Remove Selected" and "Cancel".

Fig. 27 Domain Table

The Domain Table shows the Domain entry.

To remove the list, click **Remove Selected**.

To cancel settings, click **Cancel**.

Association Table

	Domain Name	MD Level	Association Name	VLAN	Transmit Interval (ms)

Fig. 28 Association Table

Configure the Transmit Interval. The default value is 3 ms.

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

To remove the list, select the list and click **Remove Selected**.

Endpoint Table

	Domain Name	MD Level	Association Name	Port	Endpoint Type	MEP ID

Fig. 29 Endpoint Table

View the endpoint entry.

To remove the list, select the list and click **Remove Selected**.

To cancel settings, click **Cancel**.

5.10 Redundancy

5.10.1 RSTP Bridge Setting

Fig. 30 RSTP Bridge Setting

STP Mode

The default mode is RSTP enabled.

For more information about the STP Modes, refer to [About Redundancy, p. 118](#).

1. Select STP mode, STP, RSTP, MSTP or Disable.
2. Depending on which mode selected:
 - STP or RSTP mode, configure the Bridge settings for STP and RSTP.
 - MSTP mode, configure the MSTP settings, refer to [MSTP Setting, p. 50](#).

Bridge Configuration



Follow the rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$

Configure the Bridge settings:

Bridge Address	Shows the switch MAC address.
Bridge Priority	<p>Enter a value from 0 to 61440.</p> <p>RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. The bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will become the root bridge.</p> <p>The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority.</p> <p>The Web GUI allows you to select the priority number directly. This is the convenient of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly. Follow the $n \times 4096$ rules for the Bridge Priority.</p>

Max Age	Enter a value from 6 to 40 seconds. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.
Hello Time	Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status. The root bridge of the spanning tree topology periodically sends out a hello message to other devices on the network to check if the topology is normal. The hello time is the amount of time the root has waited during sending hello messages.
Forward Delay Time	Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

To apply the settings, click **Cancel**.

RSTP Port Setting

Home > Redundancy > RSTP Port Setting

RSTP Settings ▾ MSTP Settings ▾ ERPS Settings ▾

RSTP Port Setting

Port	STP State	Path Cost	Port Priority	Link Type	Edge Port	BPDU Filter	BPDU Guard
1	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
2	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
3	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
4	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
5	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
6	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
7	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
8	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
9	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
10	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
11	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾
12	Enable ▾	20000	128 ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾

Submit Cancel

Fig. 31 RSTP Bridge Setting

Configure the RSTP Bridge settings:

STP State	Enable or Disable the STP function. Default: Enable
Path Cost	Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port.
Priority	Enter a value between 0 and 240, using multiples of 16. This value decides which port should be blocked by priority in a LAN.
Link Type	There are 3 types for user selects Auto, P2P and Share. Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. <ul style="list-style-type: none"> Auto - means to auto select P2P or Share mode. P2P - means P2P is enabled; the 2 ends work in full duplex mode. Share - means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.
Edge Port	A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the Enable state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.
BPDU Filter	BPDU filter is used to filter sending or receiving BPDUs on a switch port. Enable or Disable the BPDU Filter function.
BPDU Guard	BPDU Guard is used to protect the Layer 2 Spanning Tree Protocol (STP) Topology from BPDU related attacks. Enable or Disable the BPDU Guard function.

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**

RSTP Status

Home > Redundancy > RSTP Status

RSTP Settings ▾ MSTP Settings ▾ ERPS Settings ▾

RSTP Status

Root Status

Root Address

0030.112b.001e

Root Priority

32768

Root Port

N/A

Root Path Cost

0

Max Age

20 second(s)

Hello Time

2 second(s)

Forward Delay

15 second(s)

Port Status

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port	Aggregated(ID/Type)
1	Disabled	Disabled	20000	128	P2P	Edge	/
2	Designated	Forwarding	20000	128	P2P	Edge	/
3	Disabled	Disabled	20000	128	P2P	Edge	/
4	Disabled	Disabled	20000	128	P2P	Edge	/
5	Disabled	Disabled	20000	128	P2P	Edge	/
6	Disabled	Disabled	20000	128	P2P	Edge	/
7	Disabled	Disabled	20000	128	P2P	Edge	/
8	Disabled	Disabled	20000	128	P2P	Edge	/
9	Disabled	Disabled	20000	128	P2P	Edge	/
10	Disabled	Disabled	20000	128	P2P	Edge	/
11	Disabled	Disabled	20000	128	P2P	Edge	/
12	Disabled	Disabled	20000	128	P2P	Edge	/

Reload

Fig. 32 Root Status

Root Status

View the root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Status

View the port Role, Port State, Path Cost, Port Priority, Link Type, Edge Port and Aggregated (ID/Type).

To reload the information, click **Reload**.

5.10.2 MSTP Setting

MSTP Region Configuration

Home > Redundancy > MSTP Setting

RSTP Settings ▾ MSTP Settings ▾ ERPS Settings ▾

MSTP Setting

MSTP Region Configuration

Region Name

Revision

Add MSTP Instance

Instance ID

VLAN Group

Instance Priority

MSTP Instance Configuration

Instance ID	VLAN Group	Instance Priority
<input type="text"/>	<input type="text"/>	<input type="text"/>

Fig. 33 MSTP Setting

Configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration.

The network can be divided virtually to different Regions.

The switches within the Region should have the same Region and Revision level.

Region Name	The name for the Region. Maximum length: 32 characters.
Revision	The revision for the Region. Range: 0-65535 Default: 0

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

Add MSTP Instance

Map VLAN to Instance and assign priority to the instance.

Before mapping VLAN to Instance, create VLAN and assign the member ports, refer to the VLAN setting page.

Instance ID	Select the Instance ID, the available number is 1-15.
VLAN Group	Enter the VLAN ID that user wants mapping to the instance.
Instance Priority	Assign the priority to the instance. (0-61440)

To add the settings, click **Add**.

MST Instance Configuration

The table shows the current MST Instance Configuration added.

To apply the settings, click **Submit**.

To delete an instance, select the instance and click **Remove Selected**.

To cancel settings, click **Cancel**.

MSTP Port Setting

Home > Redundancy > MSTP Port Setting

RSTP Settings ▾ MSTP Settings ▾ ERPS Settings ▾

MSTP Port Setting

Instance ID 0 ▾

Port	Path Cost	Port Priority	Link Type	Edge Port
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Fig. 34 MSTP Port Setting

Enabled MSTP and linked up ports within the instance are listed in the Instance ID table.

The ports that do not belong to the Instance, or the ports not MSTP activated are not shown.

Path Cost	<p>Enter a number between 1 and 200,000,000.</p> <p>This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port.</p> <p>Path cost value is derived from the media speed of an interface.</p> <p>If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. Lower cost values can be assigned to interfaces that selected first and higher cost values that selected last.</p> <p>If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.</p>
Port Priority	<p>Enter a value between 0 and 240. This is the value that decides which port should be blocked by priority in a LAN.</p>
Link Type	<p>There are 3 types for user selects Auto, P2P and Share.</p> <p>Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively.</p> <ul style="list-style-type: none">• Auto - means to auto select P2P or Share mode.• P2P - means P2P is enabled; the 2 ends work in full duplex mode.• Share - means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.
Edge Port	<p>A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the Enable state.</p> <p>When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.</p>

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

MSTP Status

View the current MSTP status.

Home > Redundancy > MSTP Status

RSTP Settings ▾ MSTP Settings ▾ ERPS Settings ▾

MSTP Status

Instance ID 0 ▾

Root Status

Root Address	--
Root Priority	--
Root Port	--
Root Path Cost	--
Max Age	--
Hello Time	--
Forward Delay	--

Port Status

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						

[Reload](#)

Fig. 35 MSTP Status

Instance ID

Select an **Instance ID**.

If the instance is not added, the information remains blank.

Root Status

View Root Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch based on the Instance ID.

Port Status

View Port, Role, Port State, Path Cost, Port Priority, Link Type and the Edge Port within the instance.

To reload the information, click **Reload**.

5.10.3 ERPS Setting

The switch provide a number of Ethernet ring protocol.

The ERPS/Ring page is subdivided into two menus; ERPS Setting and ERPS Status.

Fig. 36 ERPS Setting

Before mapping VLAN to Instance, create VLAN and assign the member ports, refer to [VLAN Setting, p. 58](#).

Add ERPS Instance

Map the VLAN to Instance.

Instance ID	Select the Instance ID and click Add . The available number is 1-15.
VLAN Group	Type the VLAN ID that user wants mapping to the instance.

ERPS Instance Setting

When the ERPS Instance is added, the Instance ID and the VLAN group information are shown in the ERPS Instance Setting.

To apply the settings, click **Submit**.

To delete an instance, select the instance and click **Remove Selected**.

To cancel settings, click **Cancel**.

ERPS Ring Setting

1. To add ERP Ring, select a Ring ID and click **Add**.

A new row is added in the ERPS Ring Setting section.

The maximum numbers of ERPS Protection Groups are 32.

2. Configure the selected ERPS Ring:

Ring ID	Display the Ring ID Integer value between 0 and 31.
Version	ERPS Protocol Version - v1 or v2.
Ring State	Enable - Ring Status is enable Disable - Ring Status is disable Default: Disable
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	Control channel is implemented using a VLAN. Each ERP instance uses a tag-based VLAN for sending and receiving R-APS messages. (1-4094) Default: 1
Sub Ring without Virtual Channel	Default: False True – if doesn't have a virtual channel False – if have any virtual channel
Virtual Channel of Sub Ring	Sub-rings can have a virtual channel on the interconnected node. Select the number based on the VLANs Range (1-4094) Default: 1
Ring Port 0	This will create a Port 0 of the switch in the Ring. Select the port number that belongs to Ring port 0
Ring Port 1	This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Select the port number that belongs to Ring port 1.
RPL Port	This allows you to select the Ring Port 0 or Ring Port 1 as the RPL block.
Revertive Mode	Revertive mode, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. Default: Revertive
Instance	Select the Instance ID, the available number is 1-15.
Manual Switch	In the absence of a failure, Manual Switch command forces a block on the ring port where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1. Default: None
Force Switch	Forced Switch command forces a block on the ring port where the command is issued. Choose 0 or 1, refers to Ring Port 0 or Ring Port 1. Default: None


To apply the settings, click **Submit**.

To delete a ring, select the ring and click **Remove Selected**.

To clear settings, select the ring and click **Clear Selected**.

To cancel settings, click **Cancel**.

ERPS Timer Setting



ERPS Timer Setting

Ring ID	Guard Timer(ms)	WTR Timer(m)
<input type="text"/>	<input type="text"/>	<input type="text"/>

Fig. 37 ERPS Timer Setting

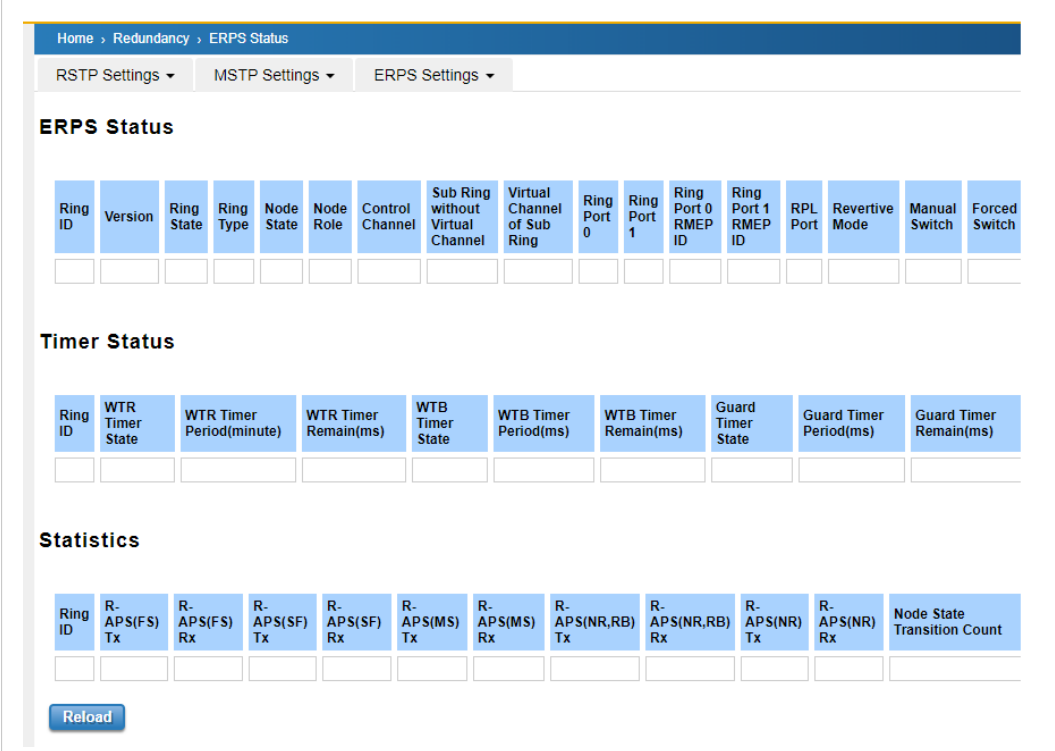
Configure the ERPS Timer settings:

Guard Timer (ms)	Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2000 ms, with a default value of 100 ms.
WTR Timer (m)	The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 1 and 12 minutes with a default value of 5 minutes.

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

5.10.4 ERPS Status



Home > Redundancy > ERPS Status

RSTP Settings ▾
 MSTP Settings ▾
 ERPS Settings ▾

ERPS Status

Ring ID	Version	Ring State	Ring Type	Node State	Node Role	Control Channel	Sub Ring without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 0	Ring Port 1	Ring Port 0 RMEP ID	Ring Port 1 RMEP ID	RPL Port	Revertive Mode	Manual Switch	Forced Switch
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Timer Status

Ring ID	WTR Timer State	WTR Timer Period(minute)	WTR Timer Remain(ms)	WTB Timer State	WTB Timer Period(ms)	WTB Timer Remain(ms)	Guard Timer State	Guard Timer Period(ms)	Guard Timer Remain(ms)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Statistics

Ring ID	R-APS(FS) Tx	R-APS(FS) Rx	R-APS(SF) Tx	R-APS(SF) Rx	R-APS(MS) Tx	R-APS(MS) Rx	R-APS(NR,RB) Tx	R-APS(NR,RB) Rx	R-APS(NR) Tx	R-APS(NR) Rx	Node State Transition Count
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Fig. 38 ERPS Status

View the ERPS Status:

Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	Enabled - Ring Status is enable Disabled - Ring Status is disable Default: Disable
Node State	Status from the Ring is Idle, Protection, Manual Switch, Force Switch or Pending.
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	Control Channel is referred to the VLANs number (1-4094)
Sub Ring without Virtual Channel	True – if have a virtual channel False – if doesn't have any virtual channel Default: False
Virtual Channel of Sub Ring	Sub-rings can have a virtual channel on the interconnected node. Select the number based on the VLANs Range (1-4094) Default: 1
Ring Port 0	The status from the port Link up/link down and Forwarding/Blocking
Ring Port 1	The status from the port Link up/link down and Forwarding/Blocking
RPL Port	The port status as the RPL block.
Revertive Mode	Revertive mode, after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is, blocked on the RPL. In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. Default: Revertive
Manual Switch	Status from the Ring Port 0 and 1 or None
Force Switch	Status from the Ring Port 0 and 1 or None

Timer Status

View the Timer Status:

Ring ID	Display the Ring ID
WTR Timer State	Running or not Running status
WTR Timer Period (minute)	WTR timeout in milliseconds.
WTR Timer Remain (ms)	Remaining WTR timeout in milliseconds.
WTB Timer State	Running or not Running status
WTB Timer Period (ms)	WTB timeout in milliseconds.
WTB Timer Remain (ms)	Remaining WTB timeout in milliseconds.
Guard Timer State	Running or not Running status
Guard Timer Period (ms)	Guard Timer timeout in milliseconds.
Guard Timer Remain (ms)	Remaining Guard Timer timeout in milliseconds.

View the Statistics:

Ring ID	Display the Ring ID.
R-APS(FS) Tx	The number of R-APS messages with Forced Switch (FS) being sent.
R-APS(FS) Rx	The number of R-APS messages with Forced Switch (FS) being received.
R-APS(SF) Tx	The number of R-APS messages with Signal Fail (SF) being sent.
R-APS(SF) Rx	The number of R-APS messages with Signal Fail (SF) being received.
R-APS(MS) Tx	The number of R-APS messages with Manual Switch (MS) being sent.
R-APS(MS) Rx	The number of R-APS messages with Manual Switch (MS) being received.
R-APS(NR, RB) Tx	The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being sent.
R-APS(NR, RB) Rx	The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being received.
R-APS(NR) Tx	The number of R-APS messages with a No Request (NR) being sent.
R-APS(NR) Rx	The number of R-APS messages with a No Request (NR) being received.
Node State Transition Count	The number of state transition that detected in the Ring.

To reload the information, click **Reload**.

5.11 VLAN

5.11.1 VLAN Setting



Before changing the management VLAN ID by Web or Telnet.

Remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can not access the switch via the network.

The switch supports max 256 VLAN groups.

Home > VLAN > VLAN Setting

VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status

GVRP Setting

VLAN Setting

Static VLAN

VLAN ID	Name
<input type="text"/>	<input type="text"/>

Add

Static VLAN Setting

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/> 1	VLAN1	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼

Submit **Remove Selected** **Reload**

Fig. 39 VLAN Setting

Configure the Static VLAN settings:

VLAN ID	The VLAN ID is used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094. Default: 1
Name	A reference for network administrator to identify different VLANs. Maximum 12 characters. If no VLAN name is set, the system automatically assign a VLAN name. The rule is VLAN (VLAN ID).

To add the settings, click **Add**.

The new VLAN is shown in the Static VLAN Setting table.

The VLAN remain in status Unused until ports are added to the VLAN.

Static VLAN Setting

Configure the Static VLAN settings:

--	Not available
U/Untag	Indicates that egress/outgoing frames are not VLAN tagged.
T/Tag	Indicates that egress/outgoing frames are to be VLAN tagged.

To configure Egress rules:

1. Select the VLAN ID. The entry of the selected VLAN turns to light blue.
2. Assign the Egress rule of the ports to U or T.
3. To apply the settings, click **Submit**.

To delete a ring, select the ring and click **Remove Selected**.

To reload the information, click **Reload**.

5.11.2 VLAN Port Setting

Home > VLAN > VLAN Port Setting

VLAN Setting | **VLAN Port Setting** | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status

GVRRP Setting

VLAN Port Setting

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None	0x8100	Admit	Disable
2	1	None	0x8100	Admit	Disable
3	1	None	0x8100	Admit	Disable
4	1	None	0x8100	Admit	Disable
5	1	None	0x8100	Admit	Disable
6	1	None	0x8100	Admit	Disable
7	1	None	0x8100	Admit	Disable
8	1	None	0x8100	Admit	Disable
9	1	None	0x8100	Admit	Disable
10	1	None	0x8100	Admit	Disable
11	1	None	0x8100	Admit	Disable
12	1	None	0x8100	Admit	Disable

Submit

Fig. 40 VLAN Port Setting

Setup VLAN port parameters to specific port.

PVID	<p>The abbreviation of the Port VLAN ID.</p> <p>PVID allows the switches to identify which port belongs to which VLAN.</p> <p>It is recommended that PVID is equivalent to VLAN IDs.</p> <p>The values of PVIDs are from 0 to 4095.</p> <p>0 and 4095 are reserved, and can not be used.</p> <p>1 is the default value.</p> <p>2 to 4094 are valid and available in this column.</p>
Tunnel Mode	<p>Default: None</p> <ul style="list-style-type: none"> None: Not used. 802.1Q Tunnel: As the Ingress port, is connected to the client port. <p>Configures Q in Q tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.</p> <ul style="list-style-type: none"> 802.1Q Tunnel Uplink: As the egress port, that is, the middle switch port. <p>Configures Q in Q tunneling for an uplink port to another device within the service provider network.</p> <ul style="list-style-type: none"> 802.1Q Tunnel Uplink-Add-PVID: Assign second VLAN tag for specify VLANs.

Accept Frame Type	This column defines the accepted frame type of the port. There are 2 modes User can select, Admit All and Tag Only. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.
Ingress Filtering	Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. Example: If a tagged frame from Management VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Management VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped.

To apply the settings, click **Submit**.

5.11.3 VLAN Status

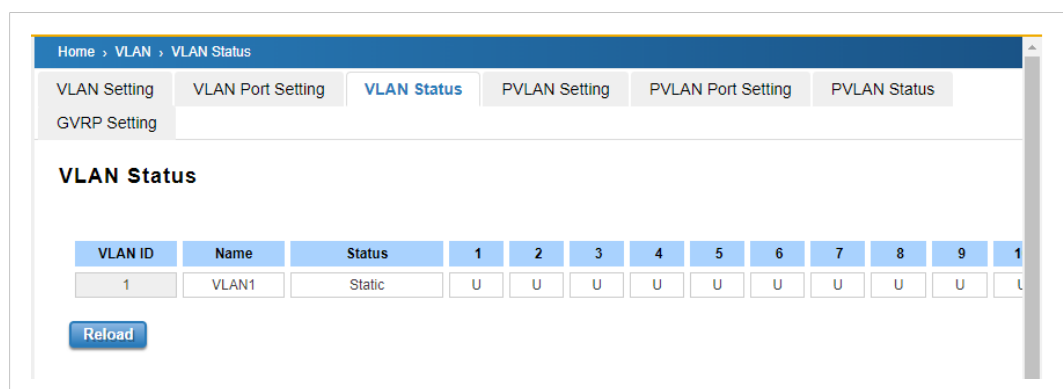


Fig. 41 VLAN Status

View the current status of the VLAN, including VLAN ID, Name, Status, and Egress rule of the ports.

The VLAN remain in status Unused until ports are added to the VLAN.

VLAN ID	ID of the VLAN.
Name	Name of the VLAN.
Status	Static: Shows that this is a manually configured static VLAN. This VLAN is not workable yet. Dynamic: The VLAN is learnt by GVRP.

To reload the information, click **Reload**.

5.11.4 PVLAN Setting

Home > VLAN > PVLAN Setting

VLAN Setting | VLAN Port Setting | VLAN Status | **PVLAN Setting** | PVLAN Port Setting | PVLAN Status

GVRP Setting

PVLAN Setting

VLAN ID	Private VLAN Type
<input type="text"/>	<input type="text"/>

Submit

Fig. 42 PVLAN Setting

Enter the VLAN ID and the Private VLAN Type for each VLAN you want to configure.

To apply the settings, click **Submit**.

5.11.5 PVLAN Port Setting

Port Configuration

Home > VLAN > PVLAN Port Setting

VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | **PVLAN Port Setting** | PVLAN Status

GVRP Setting

PVLAN Port Setting

Port Configuration

Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Normal	None
3	Normal	None
4	Normal	None
5	Normal	None
6	Normal	None
7	Normal	None
8	Normal	None
9	Normal	None
10	Normal	None
11	Normal	None
12	Normal	None

Private VLAN Association

Secondary VLAN	Primary VLAN
<input type="text"/>	<input type="text"/>

Submit

Fig. 43 PVLAN Port Setting

Before configuring the PVLAN port type, ensure that the Private VLAN Association is configured.

PVLAN Port Type	Normal: The Normal port is None PVLAN ports; it remains its original VLAN setting. Host: The Host type ports can be mapped to the Secondary VLAN. Promiscuous: The promiscuous port can be associated to the Primary VLAN.
VLAN ID	After assigned the port type, the web UI display the available VLAN ID the port can associate to.

Private VLAN Association

Secondary VLAN	Secondary VLAN is included Isolated and Community VLAN Type is assigned in the Private VLAN Configuration section.
Primary VLAN	Primary VLAN is included the Primary VLAN Type is assigned in the Private VLAN Configuration section.

To apply the settings, click **Submit**.

5.11.6 PVLAN Status

Home > VLAN > PVLAN Status

VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | PVLAN Port Setting | **PVLAN Status**

GVRP Setting

PVLAN Status

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Reload

Fig. 44 PVLAN Status

View the Private VLAN status information.

To reload the information, click **Reload**.

5.11.7 GVRP Setting

Home > VLAN > GVRP Setting

VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status

GVRP Setting

GVRP Protocol Disable ▾

Port	State	Join Timer	Leave Timer	Leave All Timer
1	Disable ▾	20	60	1000
2	Disable ▾	20	60	1000
3	Disable ▾	20	60	1000
4	Disable ▾	20	60	1000
5	Disable ▾	20	60	1000
6	Disable ▾	20	60	1000
7	Disable ▾	20	60	1000
8	Disable ▾	20	60	1000
9	Disable ▾	20	60	1000
10	Disable ▾	20	60	1000
11	Disable ▾	20	60	1000
12	Disable ▾	20	60	1000

Note: The timer unit is centisecond.

Submit

Fig. 45 GVRP Setting

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network.

GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data.

This allows network devices to dynamically exchange VLAN configuration information with other devices.

With GVRP, VLANs can be set-up automatically rather than manual configuration on every port of every switch in the network.

Configure the GVRP Protocol settings:

GVRP Protocol	Default: Disable Enable or Disable the GVRP function globally.
State	Default: Disable After enable GVRP globally, you still can enable/disable GVRP by port.
Join Timer	Default: 20 Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis
Leave Timer	Default: 60 Control the time to release the GVRP reservation after received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state.
Leave All Timers	Default: 1000 Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis

5.12 Quality of Service (QoS)

Quality of Service (QoS) is the ability from the switch to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow.

QoS is important if the network capacity is insufficient, especially for real-time streaming multimedia applications.

QoS can also help to reduce traffic problems and control the traffic by deliver the high priority first.

Configure the Quality of Service settings for each port by setting the priorities in order to provide a smooth data traffic.

5.12.1 QoS Setting

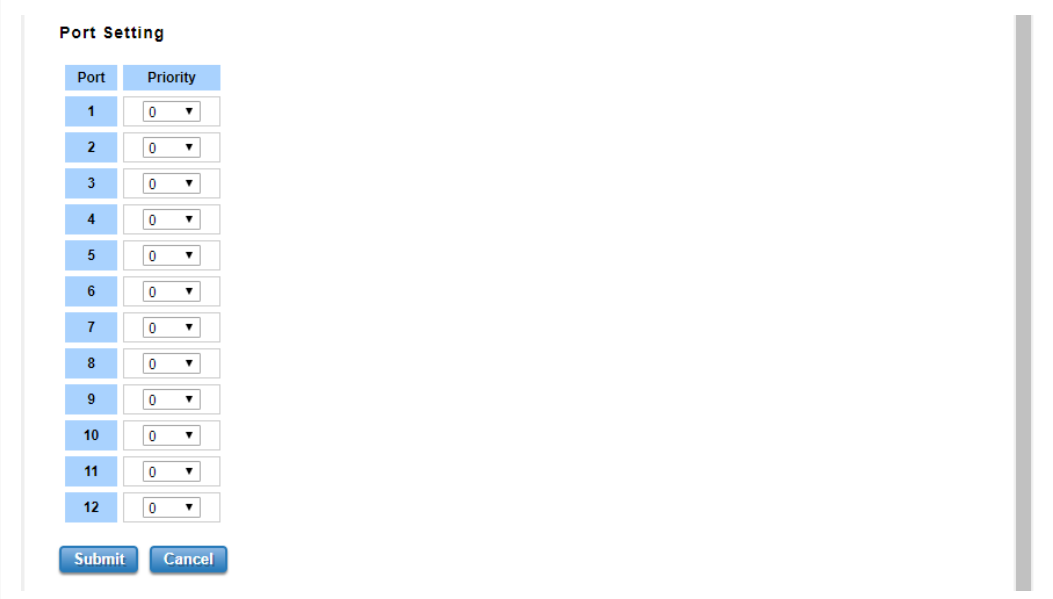
Fig. 46 QoS Setting

Select QoS Trust Mode:

802.1P Priority Tag	If 802.1P is selected the switch relies on a packet's CoS information to determine priority. This is related to the settings in the CoS-Queue Mapping page
DSCP/TOS Code Point	If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the DSCP-Priority Mapping page.

Select Queue Scheduling rule:

Round Robin Scheme	The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.
Strict priority scheme	The priority here always the higher queue will be processed first, except the higher queue is empty.
Weighted Round Robin scheme	This scheme allows users to assign new weight ratio from 1 to 10 for each class where 10 is the highest ratio.



Port Setting

Port	Priority
1	0 ▼
2	0 ▼
3	0 ▼
4	0 ▼
5	0 ▼
6	0 ▼
7	0 ▼
8	0 ▼
9	0 ▼
10	0 ▼
11	0 ▼
12	0 ▼

Fig. 47 Port Setting

Configure the Port Setting:

Select the Queue value of each port, the port then has its default priority.

The Queue 7 is the highest port-based queue, 0 is the lowest queue.

The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch.

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

5.12.2 CoS Mapping

Change CoS values to Physical Queue mapping table.

Assign the mapping table freely or follow the suggestion of the 802.1p standard.

CoS	0	1	2	3	4	5	6
Queue	0	1	2	3	4	5	6

Submit Cancel

Fig. 48 CoS Mapping

As default, the service classes (CoS) are assigned to the queues as follows:

- COS 0 → Queue 0
- COS 1 → Queue 1
- COS 2 → Queue 2
- COS 3 → Queue 3
- COS 4 → Queue 4
- COS 5 → Queue 5
- COS 6 → Queue 6
- COS 7 → Queue 7

For each value in the **CoS** column, select the queue from the **Queue** drop-down list.

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

5.12.3 DSCP Mapping

Change DSCP values to Physical Queue mapping table.

Assign how to map DSCP value to the level of the physical queue. Change freely in the mapping table or follow the upper layer 3 switch or router DSCP setting.

Home > QoS > DSCP Mapping

QoS Setting CoS Mapping **DSCP Mapping**

DSCP Mapping

DSCP	0	1	2	3	4	5	6	7
Queue	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼
DSCP	8	9	10	11	12	13	14	15
Queue	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼
DSCP	16	17	18	19	20	21	22	23
Queue	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼
DSCP	24	25	26	27	28	29	30	31
Queue	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼
DSCP	32	33	34	35	36	37	38	39
Queue	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼
DSCP	40	41	42	43	44	45	46	47
Queue	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼
DSCP	48	49	50	51	52	53	54	55
Queue	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼
DSCP	56	57	58	59	60	61	62	63
Queue	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼

Submit Cancel

Fig. 49 DSCP Mapping

Configure the DSCP Mapping settings:

DSCP Value and Priority Queues Setting	Description	Factory Default
0 to 7	Maps different types of services values to one of 8 different egress queues.	0
8 to 15		1
16 to 23		2
24 to 31		3
32 to 39		4
40 to 47		5
48 to 55		6
56 to 63		7

To apply the settings, click **Submit**.

To cancel settings, click **Cancel**.

5.13 Multicast

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN that belong to the multicast group.

Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups.

With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

For multicast filtering, the switch uses Internet Group Management Protocol (IGMP) Snooping technology. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

In effect, it manages multicast traffic by making use of switches, routers, and hosts that support IGMP.

5.13.1 IGMP Query

Configure the IGMP Query feature. The switch can only be configured by member ports of the management VLAN, so the IGMP Query can only be enabled on the management VLAN.

If you want to run IGMP Snooping feature in several VLANs, ensure that each VLAN has its own IGMP Querier.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it.

For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

VLAN	Enable/Disable	Version	Query Interval	Max-Resp-Time
1	Disable	v2	125	10

Fig. 50 IGMP Query

Configure the IGMP Query settings:

Enable/Disable	Default: Disable Enable the IGMP Query function
Version	Default: V2 V1 means IGMP V1 General Query V2 means IGMP V2 General Query.
Query Interval(s)	The interval period of querier to send the query.
Query Maximum Response Time (s)	The response time for querier detects to confirm there are no more directly connected group members on a LAN.

To apply the settings, click **Submit**.

5.13.2 IGMP Snooping/Filtering

IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch.

Fig. 51 IGMP Snooping/Filtering

IGMP Snooping Global Setting

When IGMP Snooping is enabled, you can assign IGMP Snooping to a specific VLAN.

The IGMP Snooping table shows the specific multicast group from dynamic learnt or manual input.

Select to Enable or Disable IGMP Snooping Global Setting and click **Submit**.

IGMP Snooping VLAN Setting

Configure the IGMP Snooping VLAN settings:

IGMP Snooping	Select to Enable or Disable IGMP Snooping and click Submit .
Filtering Mode	<p>It allows the switch to filter the unknown-multicast data flow. Multicast Filtering Mode is Flood unknown, discard unknown and source only learning.</p> <ul style="list-style-type: none"> Flood Unknown: The switch would filter the unknown packets that transmit through the network and the packets will be flooded to the member ports of the same VLAN. Discard Unknown: Non-member ports will not receive the unknown packets because the filter discards the unknown multicast. Source Only Learning: The switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast ports.

To apply the settings, click **Submit**.

IGMP Snooping Table

The IGMP Snooping Table show multicast IP address, VLAN ID from the multicast group, and the interface member ports of the multicast group (256 multicast groups).

To reload the information, click **Reload**.

5.13.3 GMRP Setting

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping.

GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P.

The GMRP Setting allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services.

Home > Multicast > GMRP Setting

IGMP Query IGMP Snooping/Filtering **GMRP Setting**

GMRP Setting

GMRP Global Setting Disable ▼

Submit

GMRP Port Setting

Port	State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable

Submit

Fig. 52 GMRP Setting

Configure the GMRP settings:

GMRP Global Setting	Select Enable or Disable and click Submit .
GMRP Port Setting	Select to Enable or Disable GMRP Port Setting and click Submit .

5.14 Routing

The switch combines Layer 2 switching and Layer 3 routing within the single platform.

You can create Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy and check the related routing information.

5.14.1 ARP Table Setting

Address Resolution Protocol (ARP) is a network layer protocol that query by broadcast and reply by unicast packet format.

ARP assists IP protocol to get the MAC address of an IP destination due to the unique MAC address in the network.

It is important to find the destination MAC address so that the traffic can be correctly and smoothly directed to the destination.

Fig. 53 ARP Table Setting

Configure the ARP Table settings:

Aging Time (secs)	Default: 14400 seconds Set the Age time for the ARP entry. Once there is no packet (IP+MAC) hit the entry within the time, the entry will be aged out. Short ARP age time leads the entry aged out easier and re-learn often, the re-learn progress lead the communication stop.
Total Entry Count	Count of total entries from the ARP Table.
Static Entry Count	Count the static entries that user configured.
Dynamic Entry Count	Count the ARP table dynamically learnt.

To apply the settings, click **Submit**.

To reload the information in the ARP Table, click **Reload**.

5.14.2 Interface Setting

Enable the IP Routing interface and assign the IP Address.

Before creating the IP Interface, create the VLAN Interface and assign the member port to the VLAN, refer to the VLAN Configuration.

All the created VLANs are automatically listed in the IP Interface table.

Fig. 54 IP Interface Setting

IP Interface

Configure the IP Interface settings:

Interface	The name of the IP interface.
Status	When the routing state is enabled, the Status shows Up. When the routing state is disabled, the Status shows Down
State	Enable or Disable the IP Routing Interface state. When disabled, the interface work as a layer 2 VLAN. When enabled, the interface can support IP routing feature.
IP Address	Assign the IP Address for the target IP Interface.
Subnet Mask	Select subnet mask. Example: 255.255.255.0 represents for the typical Class C, or so-call 24-bits mask. There are 256 IP Addresses within the range.

To apply the settings, click **Submit**.

Alias IP Table

Configure the IP Table settings:

Interface	Select the interface.
Alias IP Address (A.B.C.D/M)	The alias IP and its subnet mask

To add the interface, click **Add**.

To delete the interface, click **Remove Selected**.

5.14.3 Route

Static Route Entry Setting

Fig. 55 Static Route Entry Setting

Default Route

The default route allows the stub network to reach all unknown networks through the route.

The stub area has only one way and one route to other networks.

Within the stub area, there are multiple networks that run their own routing protocols. When these networks want to communicate with an unknown network, the traffic will be forwarded to the default route.

When configuring the Default Route, the IP address of the next hop router/switch is the only setting that need to be specified.

For the settings to take effect, click **Apply**.

Static Route Entry

Static route entries go to and go from a stub network to another stub network.

The static route is configured to connect the neighbor router/switch. Both routers/switches then can communicate through the route.

When configuring the Static Route, all the fields in Static Route Entry must be specified:

Destination	The destination address of static route entry.
Netmask	The destination address netmask of static route entry.
Gateway	The gateway IP address of static route entry.
Distance	The distance of static route entry.

To add the settings, click **Add**.

Static Route Table

This table displays the routing table information after user adds the static route entry form.

Destination	The destination address of the static route entry.
Netmask	The destination address netmask of the static route entry.
Gateway	The gateway IP address of the static route entry.
Distance	The distance of the static route entry.
Metric	The metric of the static route entry.
Interface	The IP interface of the static route entry.

To delete the entry, select the checkbox and click **Remove Selected**.

To reload the information, click **Reload**.

Route Table

When the routing interfaces is changed, the system maintains information and updates the routing table.

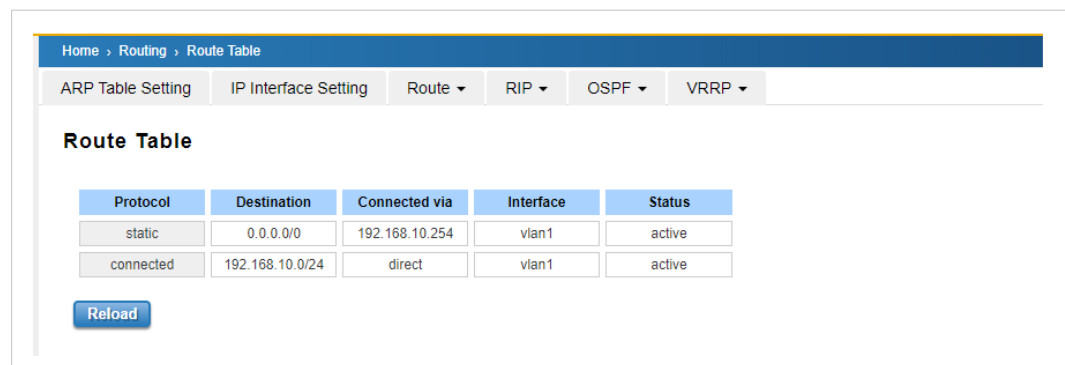


Fig. 56 Route Table

Protocol	The field shows the entry is a local interface or learnt from the routing protocol. The connected represents for the local interface. The OSPF shows the entry is learnt from the routing protocol, OSPF.
Destination	The destination address of static route entry.
Connected via	The IP interface wherever the network learnt from. The interface is usually the next hop's IP address.
Interface	Show the VLAN Interface wherever the network connected to or learnt from.
Status	Shows the entry status is active or not.

To reload the information, click **Reload**.

5.14.4 RIP

The Industrial L3 managed switch also implements a dynamic routing protocol to allow automatically learning and updating of routing table.

Routing Information Protocol (RIP) is a distance vector-based routing protocol that can make decision on which interface the switch should forward Internet Protocol (IP) packet to and can share information about how to route traffic among network devices that use the same routing protocol.

RIP sends routing-update messages periodically every 30 seconds and when there is a change in the network topology.

RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.

RIP can be used to automatically build up a routing table.

RIP Setting

Fig. 57 RIP Setting

Configure the RIP Settings:

RIP Protocol	Choose the RIP protocol Version 1 or Version 2 or Disable RIP protocol in here. To apply RIP protocol setting, click Submit .
Routing for Networks	All networks, directly connected or learnt from other router/switch, should be added to the switch. The format is IP Network/bit mask. Example: 192.168.10.0/24. To add a routing network, enter the network address and click Add .

To delete the selected network address, click **Remove Selected**.

To reload the RIP information, click **Reload**.

RIP Interface Setting



Home > Routing > RIP Interface Setting

ARP Table Setting IP Interface Setting Route RIP OSPF VRRP

RIP Interface Setting

Interface	RIP Version
<input type="text"/>	<input type="text"/>

Fig. 58 RIP Interface Setting

Configure the RIP Interface settings:

Interface	The IP interface.
RIP Version	RIP version of IP interface. (RIPv1, RIPv2 or Both)

To apply the settings, click **Submit**.

To reload the RIP interface configuration, click **Reload**.

5.14.5 OSPF

OSPF Setting

Fig. 59 OSPF Setting

OSPF Protocol

OSPF Protocol	Enable or Disable the OSPF routing protocol.
Router ID	The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier. Router ID is used while connected multiple OSPF routers/switches to the same broadcast domain. The lowest Router ID will be selected as the Designated Router in the network. To apply the settings, click Submit .

Routing for Network



*All the Area ID of the router/switch within the same area should use the same IP address or ID.
All the network addresses should be added.*

Routing for Network	Enter the Network Address and the Area ID and click Add .
---------------------	--

To delete the network address and area, click **Remove Selected**.

To reload the information, click **Reload**.

OSPF redistribute option

Redistribute Type	Redistribute routes learned from another routing process to OSPF. Select connected, static or rip.
Metric Value	Enter a metric value.
Metric Type	Select none, 1 or 2.

To add a the settings, click **Add**.

To delete the settings, click **Remove Selected**.

To reload the information, click **Reload**.

OSPF Interface Setting

Fig. 60 OSPF Interface Setting

Configure the OSPF Interface settings:

Interface	The VLAN Interface name.
Area	The Area ID of the OSPF Interface you added. The Area ID must be the same for all routers/switches on a network.
Cost	The distance of this link/Interface. The default distance identified, depends on the system bandwidth. The value can be changed to decide the best router.
Priority	The priority of this link/Interface. Set priority to help find the OSPF designated router for a network. The default is 1. The range is 0 to 255.
Transmit Delay	The transmit delay timer of this link/Interface. Transmit Delay is the estimated number of seconds to wait before sending a link state update packet. The default value is 1 second.
Hello	The Hello timer of this link/Interface. The value must be the same for all routers/switches on a network. The default value is 10 seconds. The min. value is 1.
Dead	The Dead Interval Timer of this link/Interface. The Dead timer is the time to identify whether the interface is down or not, before the neighbors declare the OSPF router to be down. The default value is 4 times (40 seconds) than the Hello interval (default is 10).
Retransmit	The count of Retransmit of this link/Interface. The Retransmit time specifies the number of seconds between link state advertisement transmissions. The default value is 5 seconds.

To apply the settings, click **Submit**.

To reload the information, click **Reload**.

OSPF Area Setting

An OSPF domain is divided into different areas.

Areas are logical grouping of hosts and networks, including their routers having interfaces connected to any of the included networks.

Each area maintains its own link state database.

In OSPF, all areas must be connected to a backbone area. The backbone area is responsible for distributing routing information between non-backbone areas.

The switch is usually installed as internal router of a single Area environment. When there are multiple areas in the network, you can modify the Area information and Virtual Link.

Home > Routing > OSPF Area Setting

ARP Table Setting IP Interface Setting Route RIP OSPF VRRP

OSPF Area Setting

OSPF Area Table

Area	Default Cost	Shortcut	Stub

Submit Reset Selected Reload

OSPF Range Table

Area	Range (A.B.C.D/M)

Add

Area	Range

Remove Selected

OSPF Virtual Link Table

Area	Virtual Link (A.B.C.D)

Add

Area	Virtual Link

Remove Selected

Fig. 61 OSPF Area Setting

Configure the OSPF Area settings:

Area	This field indicates the area ID. Select the ID you want to modify.
Default Cost	The default cost of the area ID.
Shortcut	No Defined, Disable, Enable. This indicates whether the area is the OSPF ABR shortcut mode.
Stub	Represents whether the specified Area is a stub area or not. The possible values are No Defined, No Summary and Summary. Summary is used to advertise summary routes

To apply the settings, click **Submit**.

To reset the settings, click **Reset Selected**.

To reload the information, click **Reload**.

OSPF Neighbor Table

Fig. 62 OSPF Neighbor Table Page

View the OSPF Neighbor settings:

Neighbor ID	Display the Router ID of the Neighbor routers/switches.
Priority	Show the priority of the link.
State	While the State is changed to Full, which means the exchange progress is done.
Dead Time	The activated time of the link.
IP Address	Shows the learnt IP interface of the next hops.
Interface	Shows the connected local interface.

To reload the information, click **Reload**.

OSPF Database

Fig. 63 OSPF Database Page

To reload the information, click **Reload**.

5.14.6 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol aimed to eliminate the single point of failure by automatically assigning available IP routers to participating hosts.

Using a virtual router ID (VRID) address and virtual router IP (VRIP) address to represent itself, a virtual router consists of two or more physical routers, including one master router and one or more backup routers.

All routers in the virtual router group share the same VRID and VRIP.

The master router provides primary routing and the backup routers monitor the status of the master router and become active if the master router fails.

VRRP Setting

Create the Virtual Router Interface. All nodes within the same VRRP domain should be located within the same IP network and equips with the same Virtual ID and Virtual IP address.

Fig. 64 VRRP Setting

Virtual Router

Configure the Virtual Router settings:

Interface	Select the interface for the VRRP domain.
VirtualID	This is a virtual ID range from 1-255. The switches within the same VRRP domain should have the same Virtual ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

To add a the settings, click **Add**.

A new entry is created in the Virtual Router Interface section.

Virtual Router Interface

Configure the Virtual Router Interface settings:

Priority	The priority of the entry of this switch. In the VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings. The switch with the highest priority will be selected as the VRRP Master switch. The priority setting field can be manually changed, the range is from 1-254, 255 for virtual IP owner and 100 for backup by default.
Adv. Interval	This field indicates how often the VRRP switches exchange the VRRP settings.
Preempt	If the VRRP Master link is fails, the VRRP Backup will take over the job immediately. If the VRRP master link is recovered, the Preempt decide whether the VRRP master should be recovered or not. If the Preempt is Enabled and the interface is the VRRP Master, the interface will be recovered. If the Preempt is Disable and the interface is VRRP Master, there is no change while the link is recovered. The VRRP backup acts as the Master before restarting the switches.

To apply the settings, click **Submit Selected**.

To delete the setting, click **Remove**.

To reload the information, click **Reload**.

VRRP Status

To further ensure the high reliability of an environment, the Layer 3 switch supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without the default gateway configuration change.

Fig. 65 VRRP Status

View VRRP Status:

VRRP Status	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately
VRRP MAC	This field indicates the VRRP MAC in this configuration entry.

To reload the information, click **Reload**.

5.15 SNMP

5.15.1 SNMP V1/V2c Setting



When installing the switch on the network, it is highly recommend to change the community string.

Most SNMP management application uses Public and Private as their default community name.

Fig. 66 SNMP V1/V2c Setting

Configure the SNMP V1/V2c settings:

The community includes 2 privileges, Read Only and Read and Write.

The community string can be viewed as the password because SNMP V1/V2c does not request the user to enter password before accessing the SNMP agent.

Read Only	User only has the ability to read the values of MIB tables. Default community string is Public.
Read and Write	User has the ability to read and set the values of MIB tables. Default community string is Private.

The switch allows users to assign 4 community strings.

To assign a community string, enter a string and select the privilege.

To apply the settings, click **Submit**.

To delete the setting, select the checkbox and click **Remove**.

5.15.2 SNMP V3 Setting

SNMP V3 provides network monitoring and control through SNMP protocol, that provides secure access to devices by a combination of authenticating (MD5 & SHA) and encrypting packets over the network to ensure the secure communication.

The security model that is used by SNMPv3 is an authentication strategy that is set up for a user and user group.

A security level is the permitted level of security within a security model.

A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

Fig. 67 SNMP V3 Setting

Configure the SNMP V3 settings:

User Name	Set up the user name.
Security Level	Default: None Select the security level: None, User Authentication, and Authentication with privacy.
Authentication Level	Default: MD5 MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation.
Authentication Password	Enter the SNMP v3 user authentication password.
DES Password	Enter the password for SNMP v3 user DES Encryption.

To add a the settings, click **Add**.

To delete the settings, click **Remove**.

To reload the information, click **Reload**.

5.15.3 SNMP Trap

SNMP Trap is the notification feature defined by SNMP protocol.

All the SNMP management applications can understand trap messages generated by the switch.

If no trap manager is defined, no traps will be issued.

Fig. 68 SNMP Trap

Configure the SNMP Trap settings:

To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

SNMP Trap	Default: Disable Enable or Disable SNMP Trap and click Submit .
Server IP	Enter the IP address of the trap manager.
Community	Enter the community string for the trap station.
Version	Select the SNMP trap version type, v1 or v2c.

To add a the settings, click **Add**.

To delete the settings, click **Remove**.

To reload the information, click **Reload**.

5.16 Security

5.16.1 Filter

Filter is known as Access Control List feature.

There are 2 major types:

- MAC Filter allows you to define the access rule based on the MAC address flexibility.
- IP Filter includes the IP security, IP Standard access list and advanced IP based access lists.

MAC Filter

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC Filter feature stops the MAC address learning for a specific port.

After stopping MAC learning, only the MAC address listed in the list can access the switch and transmit/receive traffic. This is a simple way to secure User network environment.

MAC Filter Group

Home > Security > MAC Filter

Filter ▾ 802.1X ▾ DHCP Snooping ▾ IP Source Guard DAI ▾

MAC Filter

MAC Filter Group

Add

Select **Group Name**

Delete **Reload**

MAC Filter Setting

Group Name

Source MAC

Source Wildcard

Destination MAC

Destination Wildcard

Egress Port

Action ☐ Permit ☐ Deny

Add

MAC Filter Table

Select	Group Name	Source MAC	Source Wildcard	Destination MAC	Destination Wildcard	Action	Egress Port
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Delete

Fig. 69 MAC Filter Group

To add a MAC Filter Group, enter a name and click **Add**.

To delete a group, click **Delete**.

To reload the information, click **Reload**.

MAC Filter Setting

Configure the MAC Filter settings:

Group Name	The name of the MAC Filter Group.
Source MAC	The source MAC Address of the packet.
Source Wildcard	The mask of the MAC Address.
Destination MAC	The destination MAC Address of the packet.
Destination Wildcard	The mask of the MAC Address.
Egress Port	The outgoing (exiting) port number.
Action	The filter action, which is to deny or permit the packet. Permit: Permit traffic from specified sources. Deny: Deny traffic from those sources.

To add a the settings, click **Add**.

To delete the setting, click **Delete**.

IP Filter

Home > Security > IP Filter

Filter ▾ 802.1X ▾ DHCP Snooping ▾ IP Source Guard DAI ▾

IP Filter

IP Filter Group

(1~99) IP Standard Access List
(100~199) IP Extended Access List
(1300~1999) IP Standard Access List (expanded range)
(2000~2699) IP Extended Access List (expanded range)

Add

Select	Group Number	Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Delete **Reload**

IP Filter Setting

Group Number

Protocol

Source IP

Source Wildcard

Source Port

Destination IP

Destination Wildcard

Destination Port

Egress Port

Action ☐ Permit ☐ Deny

Add

Fig. 70 IP Filter

To create a IP Filter Group, add a Group Number and click **Add**.

The following Group Numbers are available:

- 1 - 99: IP Standard Access List
- 100 – 199: IP Extended Access List
- 1300 – 1999: IP Standard Access List (expanded range)
- 2000 – 2699: IP Extended Access List (expanded range)

To delete a group, click **Delete**.

To reload the information, click **Reload**.

IP Filter Setting

Group Number	Number of the Filter Group.
Protocol	The L4 protocol (IP/TCP/UDP/ICMP).
Source IP	The source IP address of the packet.
Source Wildcard	The mask of the IP address.
Source Port	The source port of L4 protocol (TCP/UDP)
Destination IP	The destination IP address of the packet.
Destination Wildcard	The mask of the IP address.
Destination Port	The destination port of L4 protocol (TCP/UDP).
Egress Port	The outgoing (exiting) port number.
Action	This is the filter action, which is to deny or permit the packet. Permit: to permit traffic from specified sources. Deny: to deny traffic from those sources.

To add a the settings, click **Add**.

IP Filter List

The screenshot shows a web-based configuration interface titled "IP Filter List". It features a table with the following columns: "Select", "Group Number", "Type", "Protocol", "Source IP", "Source Wildcard", "Source Port", "Destination IP", "Destination Wildcard", and "Destination Port". Each column has a corresponding input field below it. A "Delete" button is located below the table. The table is currently empty.

Fig. 71

View the IP Filter settings:

Select	Selected the entry for delete. To delete the setting, click Delete .
Group Number	Number of the Filter Group.
Type	The filter group type (standard or extended).
Protocol	The L4 protocol (IP/TCP/UDP/ICMP).
Source IP	The source IP address of the packet.
Source Wildcard	The mask of the IP address.
Source Port	The source port of L4 protocol (TCP/UDP)
Destination IP	The destination IP address of the packet.
Destination Wildcard	The mask of the IP address.
Destination Port	The destination port of L4 protocol (TCP/UDP).

Action	The filter action, which is to deny or permit the packet.
Egress Port	The outgoing (exiting) port number.

To delete a filter, click **Delete**.

Filter Attach

Home > Security > Filter Attach

Filter ▾ 802.1X ▾ DHCP Snooping ▾ IP Source Guard ▾ DAI ▾

Filter Attach

Filter Attach

Port

MAC Filter

IP Filter

Filter Attach List

Port	MAC Filter	IP Filter
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Fig. 72 Filter Attach

Attach IP Filter and MAC Filter to ports on the switch:

Port	Select the port that needs to be attached the filter.
MAC Filter	Select a MAC address based filter to attach to the interface.
IP Filter	Select an IP address based filter to attach to the interface.

To apply the settings, click **Submit**.

Filter Attach List

Filters attached to the ports on the switch.

View Filter Attach List:

Port	The port number.
MAC Filter	The filter attached MAC address
IP Filter	The filter attached IP address

5.16.2 IEEE 802.1X

802.1X is an IEEE Standard for Port-based Network Access Control that provides an authentication mechanism to devices that wish to attach to a LAN or WLAN.

Port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server.

With 802.1X authentication, a username can be linked with an IP address, MAC address, and port. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses.

Radius

RADIUS is used in the authentication process.

Database of authorized users is maintained on a RADIUS server.

Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

802.1X Setting

IEEE 802.1X is the protocol that provides authentication to obtain access to IEEE 802 LANs.

It is port-base network access control. The switch can control which connection is available or not.

The screenshot displays the '802.1X Setting' configuration page. At the top, there is a breadcrumb trail: 'Home > Security > 802.1X Setting'. Below this, a navigation bar contains tabs for 'Filter', '802.1X', 'DHCP Snooping', 'IP Source Guard', and 'DAI'. The main content area is titled '802.1X Setting' and includes the following sections:

- System Auth Control:** A dropdown menu set to 'Disable'.
- Authentication Method:** A dropdown menu set to 'RADIUS'.
- Submit:** A blue button.
- RADIUS Server 1:**
 - RADIUS Server IP:** Text input field containing '192.168.10.100'.
 - Shared Key:** Text input field containing 'radius-key'.
 - Server Port:** Text input field containing '1812'.
 - Accounting Port:** Text input field containing '1813'.
- RADIUS Server 2:**
 - RADIUS Server IP:** Empty text input field.
 - Shared Key:** Empty text input field.
 - Server Port:** Empty text input field.
 - Accounting Port:** Empty text input field.
- Submit:** A blue button.
- Local RADIUS User:**
 - User Name:** Text input field.
 - Password:** Text input field.
 - VID:** Text input field.
- Submit:** A blue button.

Fig. 73 802.1X Setting

Configure the 802.1X settings:

System Auth Control	Enable or Disable the 802.1X authentication.
Authentication Method	Radius is an authentication server that provide key for authentication. If Local is selected as the authentication method, the switch uses the local user data base. To apply the settings, click Submit .
Radius Server IP	The IP address of Radius server
Shared Key	It is the password for communicate between switch and Radius Server.
Server Port	UDP port of Radius server.
Accounting Port	Port for packets that contain the information of account login or logout.
Secondary Radius Server IP	Secondary Radius Server could be set in case of the primary radius server down.
802.1X Local User	Add Account/Password for local authentication.

To apply the settings, click **Submit**.

802.1X Port Setting

After configuring the Radius Server or Local user list, you need to configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication.

Home > Security > 802.1X Port Setting

Filter ▾ 802.1X ▾ DHCP Snooping ▾ IP Source Guard ▾ DAI ▾

802.1X Port Setting

802.1X Port Setting

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
<input type="checkbox"/> 1	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 2	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 3	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 4	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 5	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 6	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 7	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 8	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 9	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 10	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 11	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾
<input type="checkbox"/> 12	Force Authorize ▾	Disable ▾	Disable ▾	2	0	Single ▾	Both ▾

Fig. 74 802.1X Port Setting

802.1X Timeout Setting

Port	Re-Auth Period(s)	Quiet Period(s)	Tx period(s)	Supplicant Timeout(s)	Server Timeout(s)
1	3600	60	30	30	30
2	3600	60	30	30	30
3	3600	60	30	30	30
4	3600	60	30	30	30
5	3600	60	30	30	30
6	3600	60	30	30	30
7	3600	60	30	30	30
8	3600	60	30	30	30
9	3600	60	30	30	30
10	3600	60	30	30	30
11	3600	60	30	30	30
12	3600	60	30	30	30

Fig. 75 802.1X Timeout Setting

Configure the 802.1X Port settings:

Port control	Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control.
MAB	MAC Authentication Bypass (MAB) Enable or Disable the 802.1X MAC Authentication Bypass. When MAB is enabled on a port, that port will first try to check if the connected device is 802.1X compliant.
Re-authentication	Default: 3600 seconds If enable this field, switch will ask client to re-authenticate.
Max Request	The maximum times that the switch allow client request.
Guest VLAN	0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN.
Host Mode	If there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the devices can access this port once any one of them pass the authentication.
Admin Control Direction	Determined devices can end data out only or both send and receive.
Re-Auth Period	Control the Re-authentication time interval, 1-65535 are available.
Quiet Period	When authentication failed, Switch will wait for a period and try to communicate with radius server again.
Tx period	The time interval of authentication request.
Supplicant Timeout	The timeout for the client authenticating
Sever Timeout	The timeout for server response for authenticating.

- To apply the settings, click **Submit**.
- To set the authorize state of selected port to initialize status, click **Initialize Selected**.
- To send EAP Request to supplicant to request re-authentication, click **Re-authenticate Selected**.
- To reset the configurable 802.1X parameters of selected port to the default values, click **Default Selected**.

802.1X Port Status

Observe the port status for Port control, Authorized Status, Authorized Supplicant and Open Control Direction from each port.

Port	Port Control	MAB	Authorized Status	Authorized Supplicant	Oper Control Direction
1	Force Authorized	Disable	AUTHORIZED	NONE	Both
2	Force Authorized	Disable	AUTHORIZED	NONE	Both
3	Force Authorized	Disable	AUTHORIZED	NONE	Both
4	Force Authorized	Disable	AUTHORIZED	NONE	Both
5	Force Authorized	Disable	AUTHORIZED	NONE	Both
6	Force Authorized	Disable	AUTHORIZED	NONE	Both
7	Force Authorized	Disable	AUTHORIZED	NONE	Both
8	Force Authorized	Disable	AUTHORIZED	NONE	Both
9	Force Authorized	Disable	AUTHORIZED	NONE	Both
10	Force Authorized	Disable	AUTHORIZED	NONE	Both
11	Force Authorized	Disable	AUTHORIZED	NONE	Both
12	Force Authorized	Disable	AUTHORIZED	NONE	Both

Reload

Fig. 76 802.1X Port Status

To reload the information, click **Reload**.

5.17 Warning

The switch provides several types of Warning feature for remote monitoring of end devices status or network changes.

5.17.1 Relay Output

The switch provides 1 alarm relay output, Digital Output.

The Relay Output settings control the events that trigger the alarm output.

The discrete output is on during normal conditions and turned off in the event of an alarm condition.

The relay output supports multiple event relay binding function.

The relay supports multiple event trigger function.

Fig. 77 Relay Output Page

Configure the Relay Output settings:

Power Failure	Power ID 1 Power ID 2 Any	Detect power input status. If one of the conditions occur, the relay is triggered.
Link Failure	Port number	Monitoring port link down event.
Ring	Ring failure	If ring topology changed.
Ping Failure 1	IP Address: remote device's IP address.	If target IP does not reply ping request, the relay is active.
Ping Failure 2	IP address: remote device's address. Restart Period: duration of output open. Hold Period: duration of Ping hold time.	Ping target device and trigger relay to emulate power reset for remote device, if remote system crash. Once perform Ping Restart; the relay output will form a short circuit.
Dry Output	On period: duration of relay output short (close). Off period: duration of relay output open.	Relay continuous perform On/Off behavior with different duration.
DI Change	DI number	The switch supports 1 DI. Relay trigger when DI states change to Hi or Low.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

To reload the information, click **Reload**.

5.17.2 Event Type

Event Types can be divided into two basic groups: System Event and Port Event.

System Event are related to the overall function of the switch, whereas Port Event related to the activity of specific ports.

Fig. 78 System Event

Configure the System Event settings:

Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Power 1/ 2 Failure	Power input failure.
Relay Output 1	Digital Output is on.
DI 1 Change	Digital Input change
Ring Event	Ring Status has changed or backup path is activated.
SFP Event	SFP transceiver state is abnormal.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

Home > Warning > Port Event

Relay Output | Event Type ▾ | Syslog Setting | Email Alert

Ethernet Port Event

Port	Link State
1	Disable ▾
2	Disable ▾
3	Disable ▾
4	Disable ▾
5	Disable ▾
6	Disable ▾
7	Disable ▾
8	Disable ▾
9	Disable ▾
10	Disable ▾
11	Disable ▾
12	Disable ▾

Submit Cancel

Fig. 79 Ethernet Port Event

Configure the System Event settings:

Up	The port is connected to another device.
Down	The port is disconnected.
Both	Link status is changed.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

5.17.3 Syslog Setting

Syslog can provide the switch events history by locally or remotely monitor.

Fig. 80 Syslog Setting

Configure the Syslog settings:

Local Mode	In this mode, the device will print the selected events in the Event Selection page to Syslog table of the switch.
Remote Mode	In this mode, User should assign the IP address of the Syslog server. Then the selected occurred events will be sent to Syslog server User assigned.
Both	Both Local Mode and Remote Mode are enabled.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

5.17.4 Email Alert

The switch can be set to automatically send an e-mail if an alarm event occurs.

The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp.

You can set up to 4 email addresses to receive email alarm from the switch.

Fig. 81 Email Alert

Configure SMTP servers and the four corresponding e-mail addresses:

Email Alert	Enable or Disable the Email Alert function.
SMTP Server IP	Enter the IP address of the email Server
Mail Account	Enter the email Server address
Authentication	Click on check box to enable password
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account
Confirm Password	Re-type the password of the email account
Email 1 To	The first email address to receive email alert from the switch. Max. 40 characters.
Email 2 To	The second email address to receive email alert from the switch. Max. 40 characters.
Email 3 To	The third email address to receive email alert from the switch. Max. 40 characters.
Email 4 To	The fourth email address to receive email alert from the switch. Max. 40 characters.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

5.18 Diagnostics

5.18.1 LLDP Setting

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a managed switch, to periodically send its system and configuration information to its neighbors.

All LLDP devices are kept informed of each other's status and configuration, and with SNMP.

Fig. 82 LLDP Setting

Configure the LLDP settings:

LLDP	Select to Enable or Disable LLDP function. When LLDP is Enabled the neighbor ID and IP learned from the connected devices are automatically shown.
LLDP Timer	Default: 30 seconds The interval time of each LLDP and counts in second. Valid number is from 5 to 254.
LLDP Hold time	Default: 120 seconds
Local port	Current port number that linked with neighbor network device.
Neighbor ID	The MAC address of neighbor device on the same network segment.
Neighbor IP	The IP address of neighbor device on the same network segment.
Neighbor VID	The VLAN ID of neighbor device on the same network segment.

To apply the settings, click **Submit**.

To cancel the settings, click **Cancel**.

To reload the information, click **Reload**.

5.18.2 MAC Table

Home > Diagnostics > MAC Table

LLDP **MAC Table** Port Statistics Port Mirror Event Logs Ping

MAC Address Table

Aging Time(secs)

Submit

Static Unicast MAC Address

MAC Address	VID	Port
<input type="text"/>	<input type="text"/>	Port 1 ▼

Add

MAC Address Table

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10	11	12
<input type="checkbox"/> 00e0.4c68.04a5	Dynamic Unicast	1		V										

Remove **Reload**

Fig. 83 Aging Time (Sec)

Aging Time (Sec)

Each switch Fabric has limit size to write the learnt MAC address.

To save more entries for a new MAC address, the switch Fabric will age out non-used MAC address entry per Aging Time timeout.

The default Aging Time is 300 seconds.

Enter the aging time and click **Submit**.

Static Unicast MAC Address and Static Multicast MAC Address

In some applications, the static Unicast MAC address to its MAC address table must be entered.

Enter the address and click **Add**.

MAC Address Table

Use the MAC address table to ensure the port security.

The MAC Address Table can be shown based on the MAC Address Type and based on the Port.

To delete an address, select the checkbox and click **Remove**.

To reload the information, click **Reload**.

5.18.3 Port Statistics

The Port Statistics page shows the number of error packets that is received and sent from the port.

The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
<input type="checkbox"/> 1	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 2	1000	Connected	Enable	3656174	0	32	20679665	0	0
<input type="checkbox"/> 3	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 4	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 5	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 6	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 7	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 8	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 9	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 10	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 11	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 12	0	Disconnected	Enable	0	0	0	0	0	0

Clear Selected Clear All Reload

Fig. 84 Port Statistics

To clear the settings, select the port checkbox and click **Clear Selected**.

To clear all settings, click **Clear All**.

To reload the information, click **Reload**.

5.18.4 Port Mirror

With the Port mirroring tool data transmitted through a specific port can be monitored. Use this feature for diagnostics, debugging, and analysis.

Set up another port (the mirror port) to receive the same data that is transmitted from, or both to and from, the port under observation.

Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

Any traffic will be duplicated at the Destination Port.

Home > Diagnostics > Port Mirror

LLDP MAC Table Port Statistics **Port Mirror** Event Logs Ping

Port Mirror

Port Mirror Disable ▾

Port	Source Port		Destination Port
	Rx	Tx	
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>

Submit

Fig. 85 Port Mirror

Configure the Port Mirror settings:

Port Mirror	Enable or Disable the Port Mirror.
Source Port	<p>The ports to be monitored.</p> <p>The traffic of all source ports will be duplicated to the destination ports.</p> <p>Select a single port, or multiple ports.</p> <p>To select the source ports, click on the Port ID, RX, Tx or Both checkbox.</p>
Destination Port	<p>Analyze the traffic of all the monitored ports at this port, without affecting the flow of traffic on the port being monitored.</p> <p>Only one RX/TX of the destination port can be selected.</p>

To apply the settings, click **Submit**.

5.18.5 Event Logs

The Event Logs page records and shows the system events log.

Home > Diagnostics > Event Logs

LLDP MAC Table Port Statistics Port Mirror **Event Logs** Ping

Event Logs

Index	Date	Time	Event Log

Clear Reload

Fig. 86 Event Logs

Index	Event index assigned to identify the event sequence.
Date	The date is updated based on how the current date is set in the Basic Setting page.
Time	The time is updated based on how the current time is set in the Basic Setting page.
Event Log	The occurred events.

To clear settings, click **Clear**.

To reload the information, click **Reload**.

5.18.6 Ping

The Ping utility in the management interface, is a tool used to troubleshooting network problems and to check if the remote device is alive or not.

Home > Diagnostics > Ping

LLDP MAC Table Port Statistics Port Mirror Event Logs **Ping**

Ping

Destination

Ping

Fig. 87 Ping

To start the ping, enter the Destination IP address of the target device and click **Ping**.

6 Verify Operation

When installation and configuration are completed, verify that the switch is in operation.

6.1 System LED Indicators

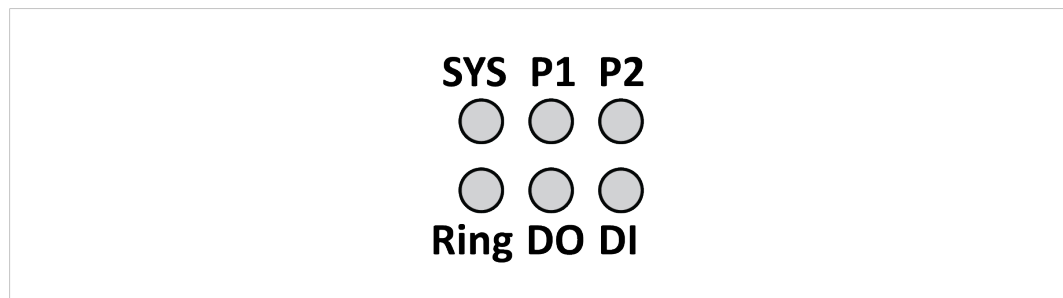


Fig. 88 System LED

LED	Status	Description
P1 and P2 Power	Green On	DC-IN Power is On
	Off	No Power in DC-IN
SYS System status	Green On	Ready
	Green blinking	Firmware updating
	Off	Not Ready
Ring Ring status	Green On	Not Owner/Normal
	Green blinking	Owner/Normal
	Amber On	Abnormal
	Amber blinking	Ring Port Failure
	Off	Ring is disabled
DO Alarm	Red On	Any failure in port link, ping, power, DO or DI State by SW control
	Off	No failure occurs
DI Digital Input	Green On	Detected Digital Input
	Off	No Digital Input

6.2 Ethernet LED Indicators

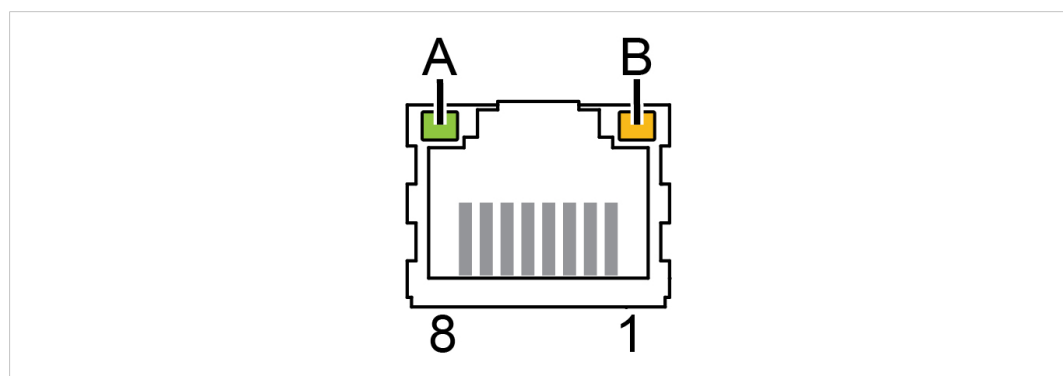


Fig. 89 RJ45 connector LED indicator

8-port 10/100/100 Base-T		
LED	Status	Description
A Status	Green On	Link established
	Green Blinking	Packets transmitting/receiving
	Green Off	Link is inactive
B Link/Activity	Amber On	Link Speed 1 Gbit/s
	Amber Off	Link speed 100 Mbit/s

6.3 SFP Port LED Indicators

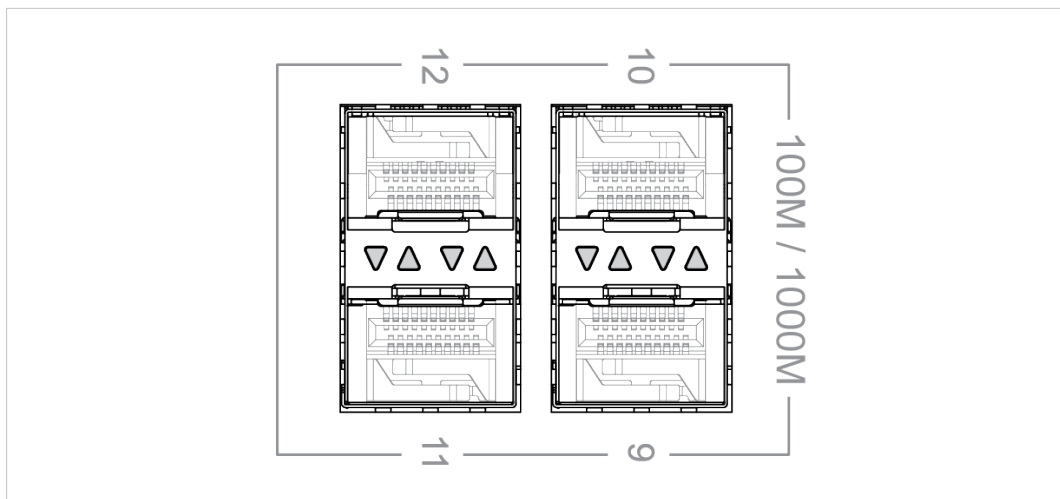


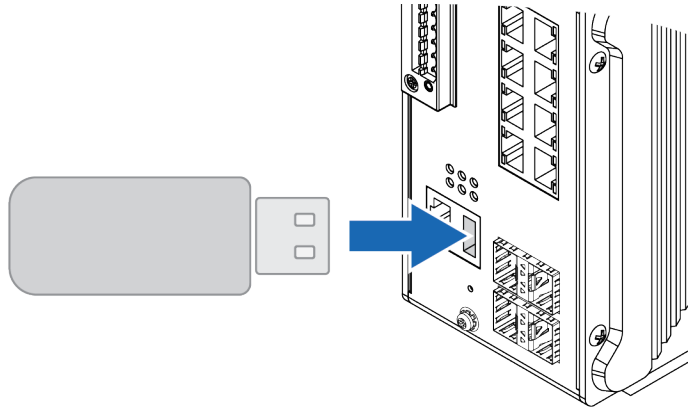
Fig. 90 SFP Port LED Indicators

4-port 100/1000 Base SFP, DDM		
LED	Status	Description
SFP Port	Green On	Link established
	Green blinking	Packets transmitting/receiving
	Green Off	Link is inactive
	Amber On	Link Speed 1 Gbit/s
	Amber Off	Link speed 100 Mbit/s

7 Maintenance and Troubleshooting

7.1 USB Port

Use the USB port in order to save or restore a configuration and to upload firmware upgrade.



7.2 Backup and Restore

Use the Backup and Restore configuration to save and load the switch configuration.

7.2.1 Web Backup and Restore

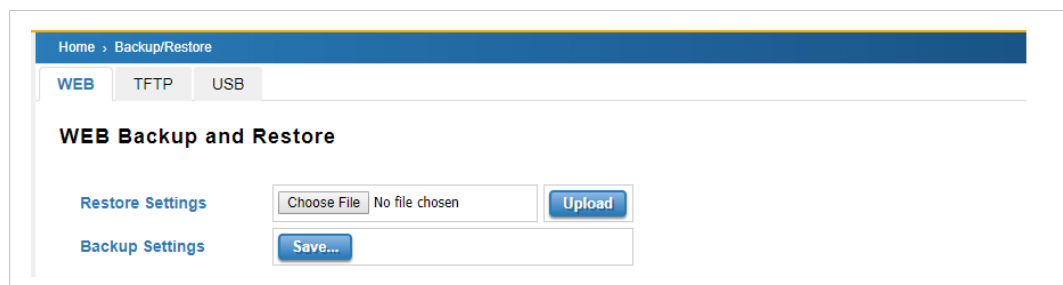


Fig. 91 Web Backup and Restore

To restore settings: Click **Choose File** and browse the target folder, then select the configuration file and click **Upload**.

To back-up settings in a configuration file: Click **Save** and browse where to save the file.

7.2.2 TFTP Backup and Restore

In the TFTP Server mode, the switch acts as TFTP client.

Home > Backup/Restore

WEB TFTP USB

TFTP Backup and Restore

TFTP Server IP

File Name

Action ☒ Load ☐ Save

Fig. 92 TFTP Backup and Restore

Ensure that the TFTP server is ready.

TFTP Server IP	Enter the TFTP Server IP address.
File Name	Enter the file name of the configuration file. File format: <i>.conf</i>
Configuration File	The configuration file of the switch is a pure text file. The file can be modified, add/remove the configuration settings, and then restored back to the switch.
Action	Select Load or Save configuration. Click Submit .

7.2.3 USB Backup and Restore

In the USB Mode, you can Load Setting from File or Save Setting to USB.

File format: *.conf*

Home > Backup/Restore

WEB TFTP USB

USB Backup and Restore

Load from USB

Save to USB

Fig. 93 USB Backup and Restore

Connect a USB memory to the switch.

To restore the settings from a configuration file: Click **Restore** and then browse and load the backup configuration file from the USB memory.

To save the settings in a configuration file to the USB memory: Click **Save to USB**.

7.3 Firmware Upgrade

Download the latest firmware at www.anybus.com/support.



*When a firmware upgrade is finished, the system will automatically reboot.
Before performing a firmware upgrade, inform attached network users.*

When a firmware upgrade is finished and the switch is rebooted, check that the Software Version number is updated in the System > Information page.

7.3.1 Web Firmware Upgrade

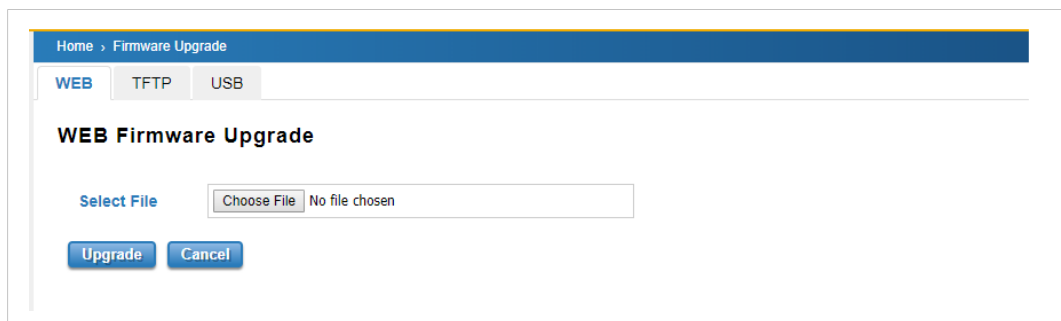


Fig. 94 Web Firmware Upgrade

To upgrade the firmware:

1. Click **Choose file** and browse the target folder.
2. Select the firmware upgrade file and click **Open**.
3. To start the firmware upgrade, click **Upgrade**.

7.3.2 TFTP Firmware Upgrade

In the TFTP Server mode, the switch acts as TFTP client.

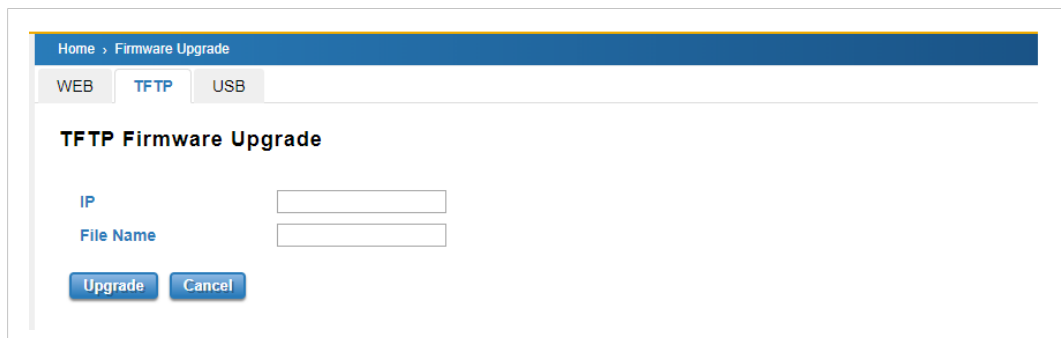


Fig. 95 TFTP Firmware Upgrade

Upgrade the firmware:

1. Ensure that the TFTP server is ready.
2. Enter the TFTP Server IP address and the firmware file name.
3. Click **Upgrade**.

After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

7.3.3 USB Firmware Upgrade

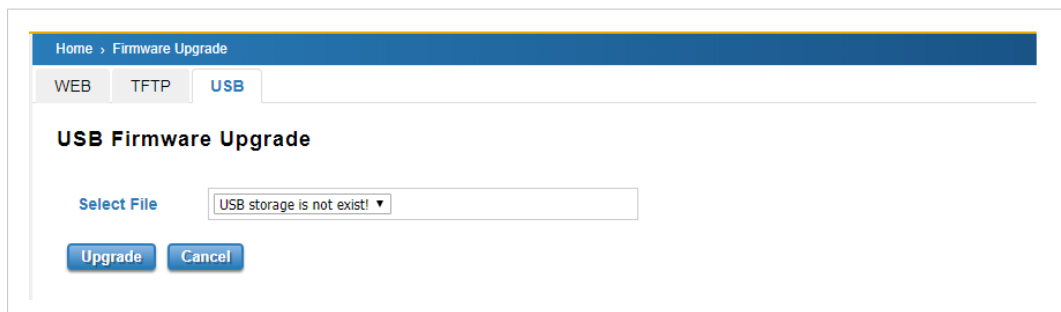


Fig. 96 USB Firmware Upgrade

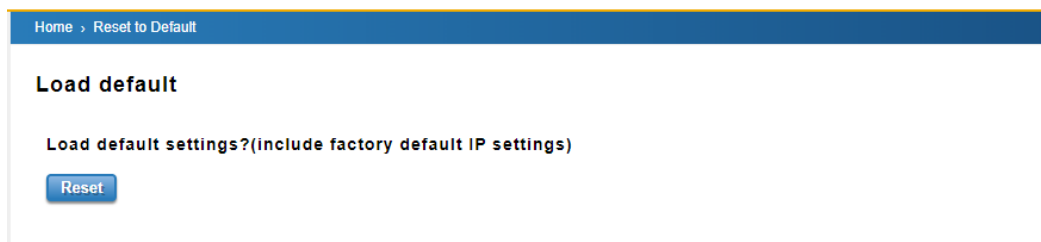
Upgrade the firmware:

1. Connect the USB memory, containing the new firmware file, to the switch.
2. Select the new firmware file from the **Selected File** menu.
3. Click **Upgrade**.

7.4 Reset To Default

Restore the switch to factory default settings.

Procedure



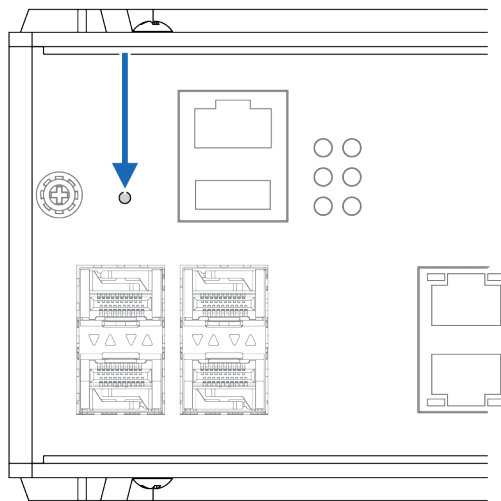
To load the default settings:

1. Click **Reset**.
2. A pop-up message appears, click **OK** to accept.
3. In the web interface top menu, click **Reboot**.
4. To reboot the switch, click **OK**.

Result

→ For the changes to take effect, the system auto reboots the switch.

7.5 Factory Reset Button



Procedure

To reset the switch to its factory settings:

1. Ensure that the switch is powered on.
2. Use a pointed object (such as a ballpoint pen) to press and hold the **reset** button for >10 seconds.

Result

- Once the **reset** button is released, the switch reboot automatically.
- When the switch has successfully rebooted, the SYS LED turns green.

8 Technical Data

8.1 Technical Specifications

Order Codes	AWB5011
Ethernet	8 x 10/100/1000Base-T RJ-45 4 x 100/1000Base SFP, DDM
Console	1 x RS232 (RJ45) 115200.n.8.1
USB	1 x USB type A
Operating temperature	-40°C-75°C , 0%-95% Non- Condensing
Data speeds	10Base-TX: 14,880pps, 100Base-TX/FX: 148,800pps, 1000Base-TX/FX: 1,488,100pps
Operating voltage	24VDC (10-60VDC)
Power Consumption	Max 16.08W
Weight	1,38 kg
Housing material	Steel & aluminium
IP protection class	IP31
Dimensions	85.5 x 150 x 126.5 (W x H x D) without DIN Rail Clip
Mounting	DIN-rail
Configuration	CGI WebGUI, Command Line Interface (CLI), SNMP
Security	IEEE 802.1X/RADIUS, Private VLAN, ACL(MAC/IP filter), HTTPS/SSH secure login
Redundancy	Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS) Virtual Router Redundancy Protocol (VRRP)
L3 Routing	Static/Dynamic IP Routing, VLAN Routing, RIP v1/v2, OSPF v1/v2, IGMP and Multicast Routing
Traffic Management	Flow Control, Port Trunk/802.3ad LACP, VLAN, Private VLAN, GVRP, GMRP, QinQ, QoS, IGMP Snooping v1/v2/v3, Rate Control, Storm
Network Management	IPv4/IPv6, SNMP v1/v2c/v3, RMON, LLDP, DHCP server/client/Option 82, SysLog
Standards	IEC60950-1 Compliance, EN61000-6-2/EN61000-6-4, CISPR 22, FCC part 15B Class A, EN61000-4-2 ESD, EN61000-4-3 RS, EN61000-4-4 EFT, EN61000-4-5, EN61000-4-6 CS, EN61000-4-8 Magnetic Field, EN50121-4

For more information, refer to datasheet at www.anybus.com/support.

This page intentionally left blank

A About DHCP Option 82

When DHCP Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The Circuit ID is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID.

B About Port Trunk

Port Trunk, also called “Link Aggregation”, is a method of combining multiple network connections in parallel to increase throughput beyond what a single connection could sustain.

The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other.

The switch support 2 types of Port Trunk. One is LACP (dynamic) and the other is Static. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. LACP mode is more flexible, and it can change modes, either trunk or single port.

Dynamic Port Trunk also provides a redundancy function, in case one of the links fails. If one of the trunk members has failed, it will still work well in LACP mode, but it will link down if using static mode. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode. Static mode is still necessary, because some devices only support static trunk.

B.1 Port Trunk Concept

Port trunking protocol that provides the following benefits:

- Flexibility in setting up User network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

To avoid broadcast storms or loops in the network while configuring a trunk, first disable or disconnect all ports that the user want to add to the trunk or remove from the trunk. After finishing the configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, this means that users can double, triple, or quadruple the bandwidth of the connection by port trunk between two switches.

When the user activates port trunk, certain settings on each port will be reset to factory default values or disabled:

- Communication redundancy will be reset.
- 802.1Q VLAN will be reset.
- Multicast Filtering will be reset.
- Port Lock will be reset and disabled.
- Set Device IP will be reset.
- Mirror will be reset.

C About Connectivity Fault Management (CFM)

Ethernet Connectivity Fault Management (CFM, IEEE 802.1ag) is an end-to-end Ethernet OAM that can cross multiple domains to monitor the health of the entire service instance.

A service instance can be a native Ethernet VLAN. CFM is a connectivity checking mechanism that uses its own Ethernet frames (its Ethertype is 0x8902 and it has its own MAC address) to validate the health of the service instance.

Continuity Check Protocol (CCP): "Heartbeating" messages for CFM. The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. CCMs are multicast messages. CCMs are confined to a domain (MD). These messages are unidirectional and do not solicit a response. Each MEP transmits a periodic multicast Continuity Check Message inward towards the other MEPs. The switch support Hardware CCM transition. The transition/receiving interval can up to 3.3ms to support detection Gigabit Ethernet cooper interface in 10 ms.

D About Redundancy

Redundancy role on the network is to help protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. Sustainable, uninterrupted data communication network is critical for industrial applications.

Network Redundancy allows user to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged.

The switch supports Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) and ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS). ERPS (Ethernet Ring Protection Switching) or ITU-T G.8032 is a loop resolution protocol, just like STP.

Convergence time is much quicker in ERPS. Unlike in STP, most of the ERPS parameters are management configured – which link to block in the start etc.

Normally ERPS is implemented with-in the same administrator domain, there by having control on the nodes participating in the Ring.

This technology provides sub-50 ms protection and recovery switching for Ethernet traffic. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable.

D.1 Spanning Tree Protocol (STP)

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network.

For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations.

Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

D.2 Rapid Spanning Tree Protocol (RSTP)

If the destination from a switch is more than one path, it will lead to looping condition that can generate broadcast storms in a network.

The spanning tree was created to combat the negative effects of message loops in switched networks.

A spanning tree algorithm is used to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path, and block the other path.

Spanning Tree Protocol (STP) introduced a standard method to accomplish this.

Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change.

D.3 Multiple Spanning Tree Protocol (MSTP)

MSTP is a direct extension of RSTP that can provide an independent spanning tree for different VLANs.

It simplifies network management by limiting the size of each region, and prevents VLAN members from being segmented from the group.

By understanding the architecture, you can effectively maintain and operate the correct spanning tree. One VLAN can be mapped to an instance. The maximum Instance of the switch is 16, with the range 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree that is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

To configure the MSTP setting, the STP Mode of the RSTP Settings page should be changed to MSTP mode first. After enabling MSTP mode, you can go to the MSTP Settings page.

E About Ethernet Ring Protection Switching (ERPS)

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings.

The protocol specifies the protection mechanism for sub-50 ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links.

ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability.

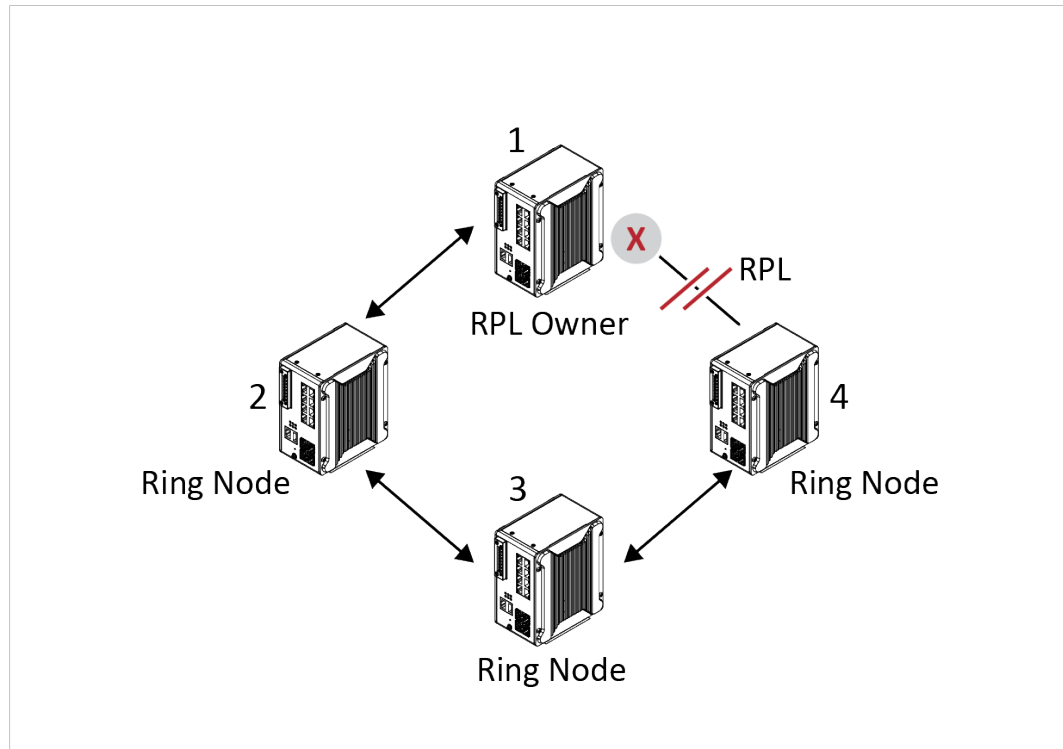


Fig. 97 Ethernet Ring Example

Each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links.

In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called Ring Protection Link (RPL).

A control message called Ring Automatic Protection Switch (R-APS) coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the Owner Node. Loops can be avoided by this mechanism.

In case an Ethernet ring failure occurs, one designated Ethernet Ring Node called the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs.

F About Virtual Local Area Network (VLAN)

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment.

With VLAN you can segment the network into:

- Departmental groups
Example: There is one VLAN for the marketing department, another for the finance department, and another for the product development department.
- Hierarchical groups
Example: There is one VLAN for directors, another for managers, and another for general staff.
- Usage groups
Example: There is one VLAN for email users and another for multimedia users.

The switch also has private VLAN functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues.

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other.

A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN.

The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs.

A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

The Private VLAN provides primary and secondary VLAN within a single switch.

Primary VLAN	The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with the Secondary VLANs.
Secondary VLAN	The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN.

G About Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a link-state protocol that equips the IP, mask, the type of network and the routers/routing switches connected to that network.

The State is its relationship to its neighboring routers/routing switches.

The Metric is the distance between the 2 links; it is usually the bandwidth of the link in link-state protocol.

The Link State Database is the collection of all these link states.

The destination network address, the shortest metric to the network and the IP address of the next hop are specified in the link state database. It propagates link-state advertisements (LSAs) to its neighbor routers/routing switches.

When compared with Routing Information Protocol (RIP), which is a distance vector based routing protocol, OSPF can provide scalable network support and faster convergence time for network routing state. OSPF is widely used in large networks such as Internet Service Provider (ISP) backbone and enterprise networks.

The OSPF is a complex protocol which defines the role of the router/routing switch when it is installed in different Areas. The Area is a group of routers, the OSPF uses flooding to exchange link-state updates between routers/routing switches. The routers/routing switches within the same area update its routing table. Any change in routers/routing switches information is flooded to all routers/routing switches in the same area.

H **About Simple Network Management Protocol (SNMP)**

Simple network management protocol (SNMP) is a standard TCP/IP protocol for network management.

Network administrators use SNMP to monitor and map network availability, performance, and error rates.

System management software uses SNMP to allow administrators to remotely monitor and manage thousands of systems on a network, often by presenting the data gathered from monitored devices in a snapshot or dashboard view.

SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format.

The manager is the console through the network.

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

[HMS Networks:](#)

[AWB5011-B](#)