AVCOMM Technologies Inc.

8008TX DIN Rail Industrial Fully Managed **8GT** L2+/L3 +Cyber Security Switch
8008GX2 DIN Rail Industrial Fully Managed **6GT + 2GF** L2+/L3 +Cyber Security Switch
8010TX DIN Rail Industrial Fully Managed **10GT** L2+/L3 +Cyber Security Switch
8010GX2 DIN Rail Industrial Fully Managed **8GT + 2GF** L2+/L3 +Cyber Security Switch
8010GX4 DIN Rail Industrial Fully Managed **6GT + 4GF** L2+/L3 +Cyber Security Switch
8012GX2 DIN Rail Industrial Fully Managed **10GT + 2GF** L2+/L3 +Cyber Security Switch
8012GX4 DIN Rail Industrial Fully Managed **8GT + 4GF** L2+/L3 +Cyber Security Switch
8014GX4 DIN Rail Industrial Fully Managed **10GT + 4GF** L2+/L3 +Cyber Security Switch
8022GX6 DIN Rail Industrial Fully Managed **16GT + 6GF** L2+/L3 +Cyber Security Switch

User Manual

About This Manual

This user manual is intended to guide a professional installer to install and to configure the 8000 Series switch. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this switch.

Disclaimer

Avcomm reserves the right to make changes to this Manual or to the product hardware at any time without notice. Information provided here is intended to be accurate and reliable. However, it might not cover all details and variations in the equipment and does not claim to provide for every possible contingency met in the process of installation, operation, or maintenance. Should further information be required, or should particular problem arise which are not covered sufficiently for the user's purposes, the matter should be referred to Avcomm. Users must be aware that updates and amendments will be made from time to time to add new information and/or correct possible unintentional technical or typographical mistakes. It is the user's responsibility to determine whether there have been any such updates or amendments of the Manual. Avcomm assumes no responsibility for its use by the third parties.

Avcomm Online Technical Services

At Avcomm, you can use the online service forms to request the support. The submitted forms are stored in server for Avcomm team member to assign tasks and monitor the status of your service. Please feel free to write to www.avcomm.us if you encounter any problems.

Table of Contents

1. Introduction

1.1. Overview

8000 series is designed for industrial environments requiring high security and high-quality Ethernet/Fiber communication, such as industrial automation, road traffic control, etc. It provides up to 22-port full-gigabit Ethernet including 16-port Gigabit RJ45 and 6-port 100M/1G SFP.

8000 series provides wire-speed witching, Cyber Security, network redundancy…L2+ management software features. Full Gigabit capability and rugged industrial design ensures system high performance and reliability in harsh environments.

Its L3 additionally supports L3 switching and VLAN/IP Routing features. You can implement the site-to-site IP Routing network, restricts the network access and security by IP rules through the L3 switch. For convenient traffic control and zero packet loss data transmission, the switch offers contemporary management and security functions.

1.2. Major features

following are the major features of the Switch:

- o 8000 Series: up to 22-port Full Gigabit L2+/L3 Managed Ethernet Switch with 16-port RJ-45 and 6-port SFP
- o SFP ports support 100/1000 Mbps with Digital Diagnostic Monitoring (DDM) to monitor long distance fiber quality
- o ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS) provides sub-50ms protection and recovery switching for Ethernet traffic.
- o Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP),
- o Advanced management features: LACP, VLAN, Private VLAN, GVRP, QoS, IGMP Snooping, Rate Control, Strom Control, Online Multi-Port Mirror, DHCP server/Option82
- o Advanced Security system by Port Security, MAC/IP ACL, 802.1, TACAS+, DHCP Snooping, IP Source Guard, Dynamic ARP Inspection
- o L3 supports L3 Routing protocols, RIPv2, OSPFv2, Static Multicast Route, VRRPv2, DVMPR*, PIM*
- o L3 supports 64 L3 IP Route Table for wire-speed L3 Switching
- o Industrial Modbus TCP monitoring in field
- o Event Notifications through E-mail, SNMP trap and Syslog
- o IEEE 802.1AB LLDP and optional NMS software for auto-topology and group management
- o CLI interface, Web, SNMP/RMON for network Management
- o Multiple event relay output for enhanced alarm control
- o Steel Metal with Aluminum for heat dissipation
- o Wide range operating temperature -40~70˚C
- o IP31/41 ingress protection

2. Hardware installation

This chapter introduces hardware and contains information on installation and configuration procedures.

2.1. Hardware dimension

Dimensions of **8008TX/8008GX2/8010TX/8010GX2/8010GX4/8012GX2/8012GX4/8014GX4** : 78 mm x 155 mmx 125 mm(W x H x D) / without DIN Rail Clip

8008TX has 8-ports, 8GT
8008GX2 has 8-ports, 6GT+2x100/1000M SFP
8010TX has 10-ports, 10GT
8010GX2 has 10-ports, 8GT+2x100/1000M SFP
8010GX4 has 10-ports, 6GT+4x100/1000M SFP
8012GX2 has 12-ports, 10GT+2x100/1000M SFP
8012GX4 has 12-ports, 8GT+4x100/1000M SFP
8014GX4 has 14-ports, 10GT+4x100/1000M SFP

*Avcomm provides X-Type Heat Sink in both sides.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024
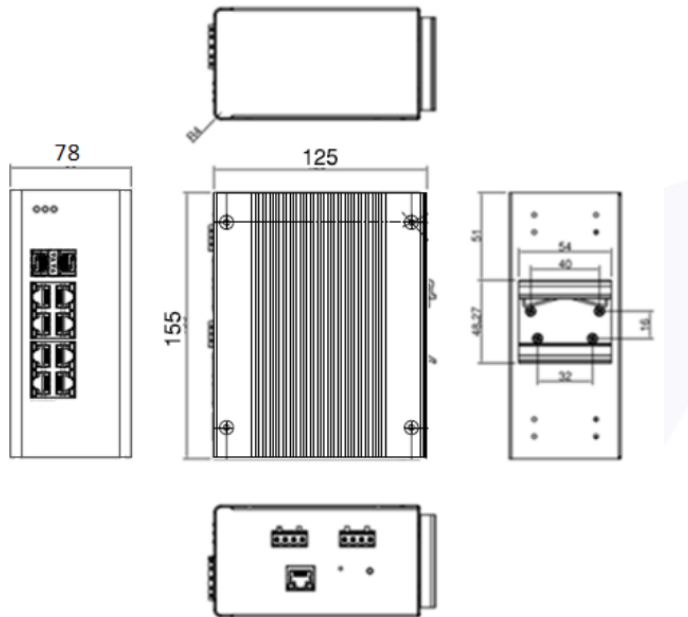
The front panel from 8010GX2 switches includes 8 ports Giga Ethernet, 2 SFP ports, System LED, RJ-45 diagnostic console, 2 x 4-pin terminal block connector (4 pin for power inputs, 2 pin for digital input and 2 pin for alarm relay output) and 1 chassis grounding screw.

8010GX2
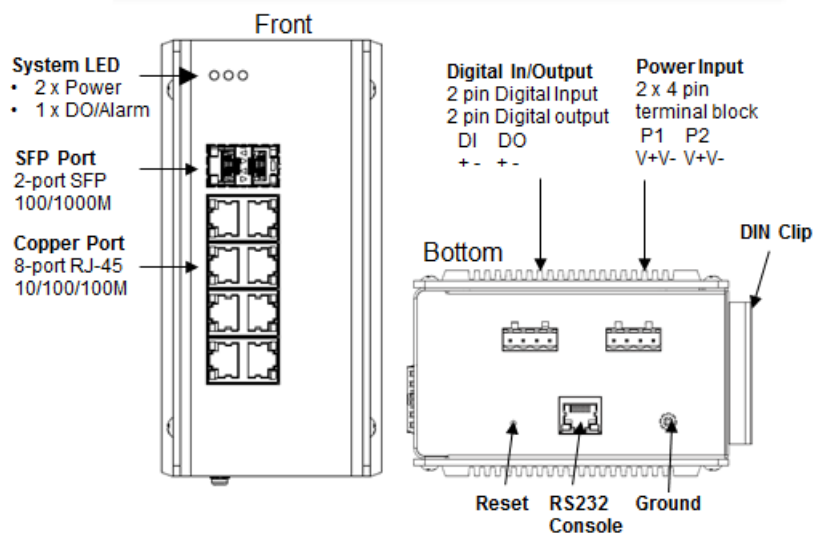
Dimensions of **8022GX6**: 78 mm x 150 mmx 125 mm(W x H x D) / without DIN Rail Clip
8022GX6 has 22-ports, 16GT+6x100/1000M SFP
*Avcomm provides X-Type Heat Sink in both sides.
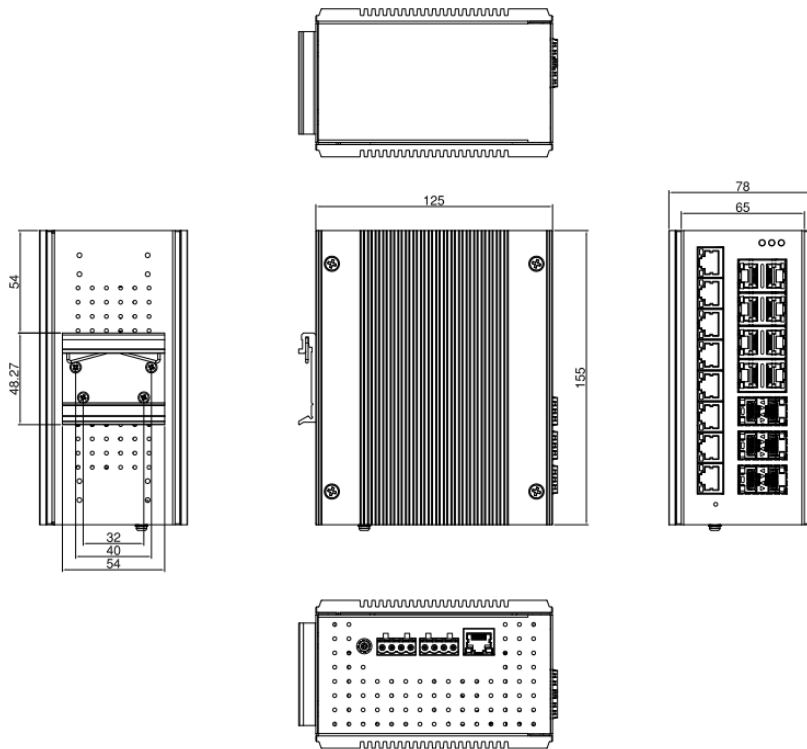
Front Panel Layout

The front panel from 8022GX6 switches includes 16 ports Giga Ethernet, 6 SFP ports, System LED, RJ-45 diagnostic console, 1 x 8-pin terminal block connector (4 pin for power inputs, 2 pin for digital input and 2 pin for alarm relay output) and 1 chassis grounding screw.

8022GX6/8022GX6-L3
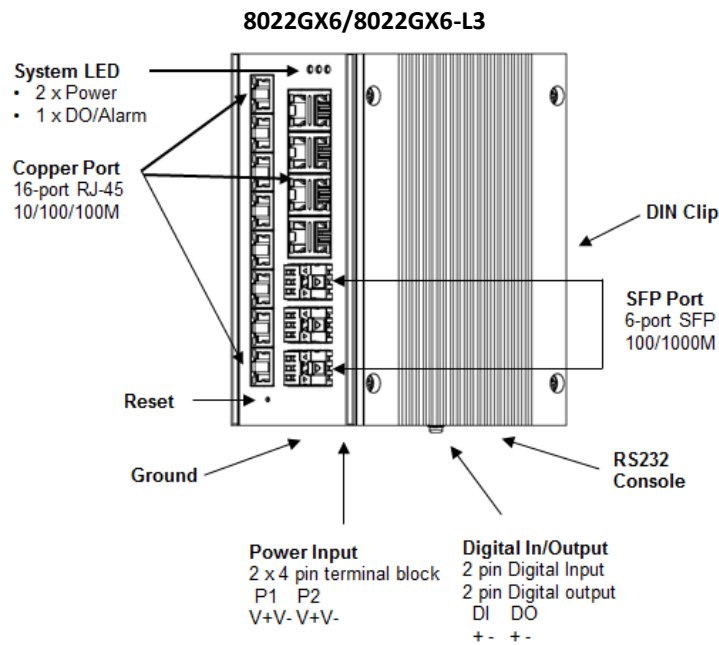
LED Indication

LED	Status	Description
PWR	Green On	DC-IN Power is On
(P1/P2)	Off	No Power in DC-IN

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

|			LED	Status	Description
Alarm (DO)	Red On	Any failures in port link, ping, power, DO and DI State by SW control			
	Off	No failure occurs			
			RJ45 Port	Green On	Links established
				Green Blinking	Packets transmitting/receiving
				Green Off	Link is inactive
				Amber On	Link Speed 1000M
				Amber Off	Link Speed 100M
			SFP Port	Green On	Links established
				Green Blinking	Packets transmitting/receiving
				Green Off	Link is inactive
				Amber On	Link Speed 1000M
				Amber Off	Link Speed 100M

2.2. Wiring the power inputs

Power Input port in the switch provides 2 sets of power input connections (P1 and P2) on the terminal block. x On the picture below is the power connector.

Wiring the Power Input

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.

> **WARNING:** Turn off AC power input source before connecting the Power to the terminal block connectors, for safety purpose. Don not turn-on the source of AC/DC power before all the connections were well established.

3. Connect the power wires to suitable AC/DC Switching type power supply.
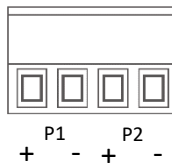
2.3. Wiring the alarm relay output (DO)

The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened. The fault conditions such as power failure, Ethernet port link break or other pre-defined events which can be configured in the switch. Screw the DO wire tightly after digital output wire is connected.
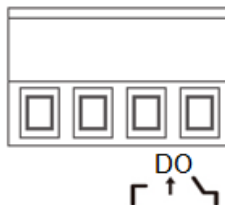
> **NOTE:** The relay contact only supports 0.5 A current, DC 24V. Do not apply voltage and current higher than the specifications.

2.4. Wiring the digital input (DI)

The Digital Input accepts one external DC type signal input that consists of two contacts on the terminal block connector on the switch's top panel. And can be configured to send alert message through Ethernet when the signal

is changed. The signal may trigger and generated by external power switch, such as door open trigger switch for control cabinet. The switch's Digital Input accepts DC signal and can receive Digital High Level input DC 11V~30V and Digital Low Level input DC 0V~10V.

Here are the steps to wire the Digital Input:

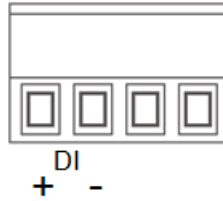**STEP 1**: Insert the negative and positive wires into the -/+ terminals, respectively.

STEP 2: To keep the wires from pulling loose, tighten the wire-clamp screws on the front of the terminal block connector.

STEP 3: Insert the terminal block connector prongs into the terminal block receptor, which is located on the switch's top panel.

2.5. Connecting the grounding screw

Grounding screw is located on the front side of the switch. grounding Screw helps limit the effects of noise due to electromagnetic interference (EMI) such as lighting or surge protection. Run the ground connection from the ground screw to the grounding surface prior to connecting devices. And tighten and wire to chassis grounding for better durability.

2.6. DIN Rail mounting

The EN50022 DIN-Rail plate should already attached at the back panel of the switch screwed tightly. If you need to reattach the DIN-Rail attachment plate to the switch, make sure the plate is situated towards the top, as shown by the following figures.
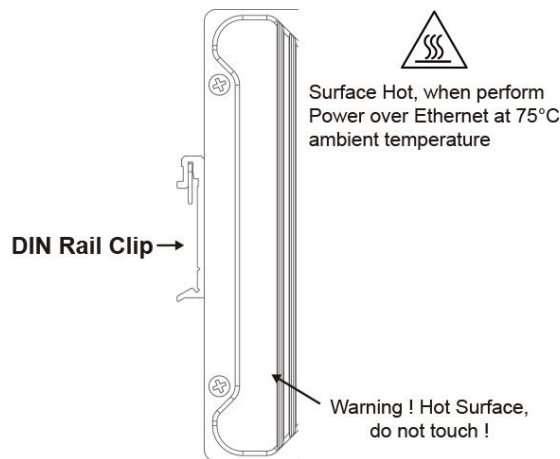
To mount the switch on DIN Rail track, do the following instruction:

1. Insert the top side of DIN Rail track into the slot of DIN Rail clip.
2. Lightly clip the bottom of DIN-Rail to the track and make sure it attached well.
3. To remove the switch from the track, reverse the steps.

2.7 Console

There is no attached console cable, you can wire the RS232 DB9 to Ethernet RJ45 connector by Cat.5/5E/6 cable. You can also contact our sales to buy one.

The Console pin Define in RJ45: 3: TxD, 6:RxD, 5:GND

Below is an example of the wiring table of the console cable.
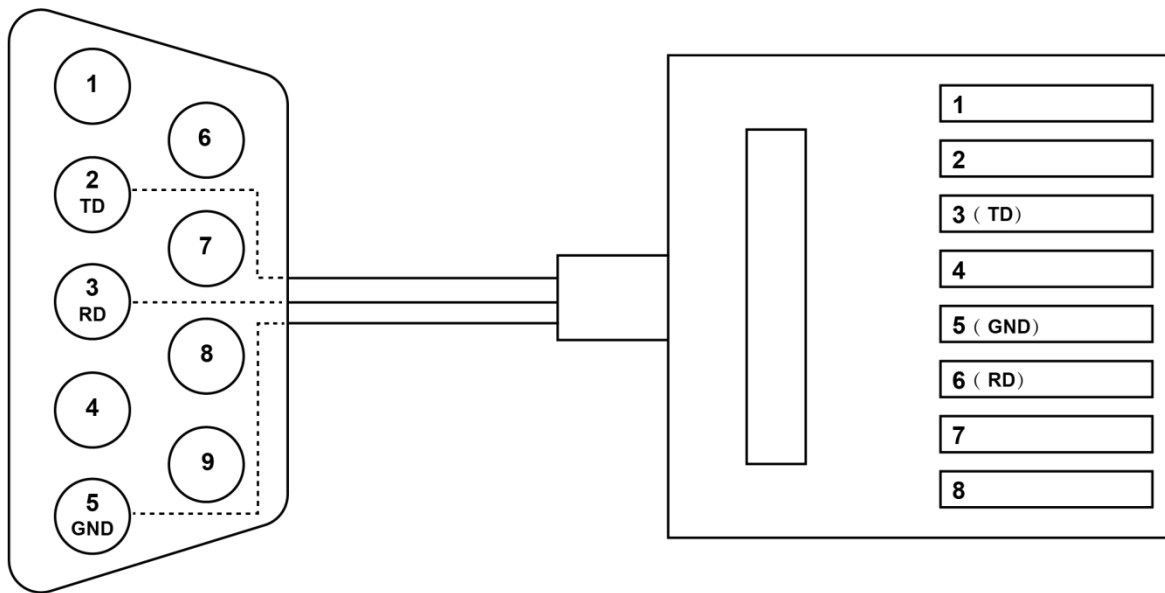
3. Web management configuration

To access the management interface, Avcomm has several ways access mode through a network; they are web management, console management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a switch interface offering status information and a subset of switch commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using console and telnet management which is offer configuration way through CLI Interface. Avcomm also provide excellent alternative by configure the switch via RS232 console cable if user doesn't attach user admin PC to the network, or if user loses network connection to Managed Switch. This manual describes the procedures for Web Interface and how to configure and monitor the managed switch only. For the CLI management interface please refers to the *CLI Command User Manual*.

PREPARATION FOR WEB INTERFACE MANAGEMENT

Avcomm provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the switch management on the network.

1. Plug the DC power to the switch and connect switch to computer.
2. Make sure that the switch default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the switch. For example, the PC and the switch are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the switch is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter** and the login page will appear.
7. For security concern, the system will ask you enter **New Username, Privilege**, **New Password and Confirm Password** at first Login, please follow the indication to enter new username, Privilege, and password. You must add New Username with **Privilege 15 (Administrator privilege)** at first login.
8. Type New username and the password, then click **Login**.

In this Web management for Featured Configuration, user will see all Avcomm Switch's various configuration menus at the left side from the interface. Through this web management interface user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all the standard web-browser to configure and access the switch on the network.

After the setting is changed on the configuration page/tab, user clicks on the "Submit" button at the bottom of the page to active the new settings. To save the changed settings permanently, user must click on "**Save**" at the top of the configuration page and click "**Yes**" to save all the submitted changes. Without "Save", the settings will be discarded if the switch is rebooted.
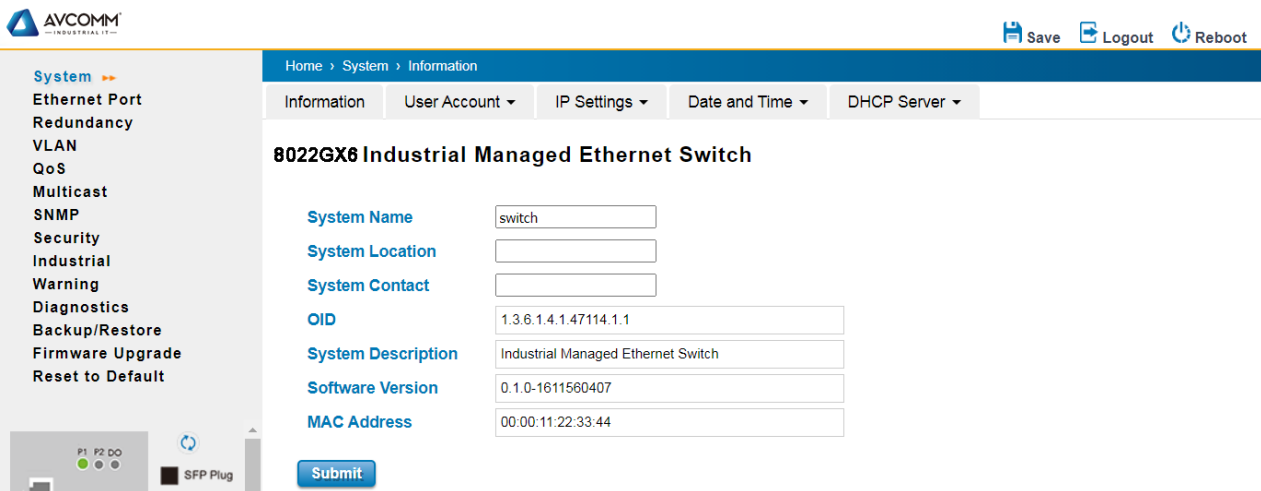
3.1. System

When the user login to the switch, user will see the system section appear. This section provides all the basic setting and information or common setting from the switch that can be configured by the administrator.

3.1.1. Information

Information section, this section shows the basic information from the switch to make it easier to identify different switches that are connected to User network. The figure below shows the interface of the Information section.

The description of the Information's interface is as below:

TERMS	DESCRIPTION
System Name	**Default: switch** Set up a name to the switch device.
System	**Default: Blank**

Location	User can specify the switch's physical location.
System Contact	**Default: Blank** User can specify the contact person here. User can type the name, mail address or other information of the administrator.
OID	Indicates the Object ID of the switch.
System Description	Display the name of the product.
Software Version	Display the firmware latest version that installed in the device.
MAC Address	Display the hardware's MAC address that assigned by the manufacturer.

NOTE: For any kind of changes in configuration settings always remember to click on **Save** to save the settings. Otherwise, all of settings User has made will be lost when the switch is powered off or restarted.

After finishing the configuration, click on **Submit** to apply User settings.

3.1.2. User account

Avcomm' switch supports the management accounts; with the Name default setting is **admin** and the authority allow user to configure all of configuration parameters. Below is the **User Account** section that consists of two interfaces, Local User and Radius Interface.

NOTE: For security consideration, please change the password after first log in.

3.1.2.1. Local user

Home › System › Local User

Information	User Account ▾	Network Settings	Date and Time ▾	DHCP Server ▾

Local User

Name [   ]

Privilege [0 ▾]

New Password [   ]

Confirm Password [   ]

[Submit] [Cancel]

Local User List

Select	User	Privilege
	admin	15
☐	admin2	15
☐	guest	0

[Remove Selected] [Cancel]

Authentication Order

Order [Local   ▾]

[Submit]

The Local User interface describes how to configure the system username, privilege and password for the web management login. To change the Name, privilege and Password, user just needs to input a new Name, select the Privilege and New Password then confirm the new password in this Local User section. After finished, click **Submit** to apply the changes. Don't forget to **Save** the settings. Try to re-login with the new Username and Password.

Privilege: The privilege 15 represent for administrator privilege, user can read and configure the new settings. The privilege 0 represent for Read-Only privilege. You must have a**t least one Username with Privilege 15 (Administrator privilege) in local user list,** otherwise you can't change the switch setting any more.

Once you try change the new setting with "0" privilege, the system will prompt error message as below:

Your permission is not enough to perform the action!

OK

Remove the user: you can Select the checkbox of the user, click "Remove Selected" to apply the change. You will see the below prompt message.

The settings were successfully changed!

OK

Authentication Order: Select the order of the authentication types. Click "Submit" to apply the change.

Authentication Order

Order

Local ▼
Local
RADIUS -> Local
TACACS+ -> Local

Submit

The description of the Local User interface is as below:

TERMS	DESCRIPTION
Name	**Default: admin** Key in new username here.
Privilege	**15:** Administrator, Read and Write the new configuration **0:** Guest, read-only
New Password	**Default: admin** Key in new password here.
Confirm Password	Re-type the new password again to confirm it.

After finished setting up the Username and Password, click on **Submit** to apply the configuration.

3.1.2.2.   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 fundamental 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.

| Information | User Account ▾ | IP Setting ▾ | Date and Time ▾ | DHCP Server ▾ |

RADIUS Authentication

RADIUS Server 1

RADIUS Server IP
Shared Key
Server Port

RADIUS Server 2

RADIUS Server IP
Shared Key
Server Port

Submit

How to set up a RADIUS server:

a.   Enter the IP address of the RADIUS server in **Server IP Address**
b.   Enter the **Shared Secret** of the RADIUS server
c.   Enter the **Server port,** if necessary, by default RADIUS server listens to port 1812
d.   Click **Submit**

The description of the RADIUS Authentication interface is as below:

TERMS	DESCRIPTION
RADIUS Server IP	Radius Server IP Address
Shared Key	Shared keys are 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	Set communication port of an external RADIUS server as the authentication database. The general value is 1812

3.1.2.3.   TACTACS+

The Terminal Access Controller Access Control System (TACACS+) security protocol is a recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Below TACAS+ server setting allows you to configure TACAS+ Server settings.

TACACS+ Settings

TACACS+ Server 1

TACACS+ Server IP
Shared Key
Server Port

TACACS+ Server 2

TACACS+ Server IP
Shared Key
Server Port

TACACS+ Settings

Authentication Type PAP
Server timeout(s) 5

Submit

How to set up a TACACS+ server:
a.   Select the **Authentication Type.**
b.   Enter the **Authentication Timeout** in seconds.
c.   Enter the IP address of the TACACS+ server in **Server IP Address.**
d.   Enter the **Shared Secret** of the TACACS+ server.
e.   Enter the **Server port,** if necessary, by default **TACACS+** server listens to port 49.
f.   Click **Submit**

The description of the TACAS+ interface is as below:

TERMS	DESCRIPTION
TACAS+ Server IP	TACACS+ Server IP Address. The system allows 2 TACAS+ servers
Share Key	Specifies the shared key for TACACS+ communications between the device and the TACACS+ server. The shared key must match the encryption used on the TACACS+ server.
Server Port	Set communication port of an external TACACS+ server as the authentication database. The general value is 49
Authentication Type	Type: PAP, ASCII, CHAP Select the authentication type to authenticate to the server.
Server Timeout	**Default: 5** The maximum number of seconds allowed establishing a TCP connection between the device and the TACACS+ server.

3.1.3.   IP settings

IP Setting section allows users to configure both IPv4 and IPv6 values for management access over the network. Avcomm switch supports both IPv4 and IPv6 and can be managed through either of these address types.

3.1.3.1.   IPV4

DHCP Client

When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default IP address will be replaced by the one assigned by DHCP server. If DHCP Client is disabled, the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. The description of the columns is as below:

TERMS	DESCRIPTION
DHCP Client	Select to **Enable** or **Disable** to activate or deactivate the DHCP Client function.

IPv4 Configuration

The IPv4 Configuration includes the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server. Configure the managed switch's IP settings. The figure below shows the user interface of IPv4 Configuration.

The description of the columns is as below:

TERMS	DESCRIPTION
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User switch. If DHCP Client function is enabled, no need to assign an IP address to switch as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Default Gateway	Assign the gateway for the switch here.
DNS Server 1, DNS Server 2	Specifies the IP address of the DNS server 1 and 2 that used in user network.

3.1.3.2.   IPV6

IPv6 Setting

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

IPV6 Setting

IPv6 Address | Prefix Length

[   ] | [   ]

[Add]

IPv6 Default Gateway

[   ]

[Submit]

	IPv6 Address
☐	fe80::9666:e7ff:fe12:933/64

[Remove] [Reload]

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 Ipv6 address is 128bits. An example of an Ipv6 address is: fe80::212:77ff:feff:1acb/64.

The description of the columns is as below:

TERMS	DESCRIPTION
Ipv6 Address	Add the 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's MAC address).
Prefix Length	The size of subnet or network, and it equivalent to the subnet mask, but written in different. Then click **Add** to apply new address to the system.
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.
Ipv6 Address	**The default IP address of the Switch: fe80::212:77ff:feff:1acb/64** Select existed Ipv6 address and click **Remove** to delete IP address. Click **Reload** to refresh and reload list.

Neighbor Cache

The IPv6 neighbor table includes the neighboring node's IPv6 address, Interface, MAC Address, and the current state of the entry.

Neighbor Cache

IPv6 Address	Interface	Link Layer (MAC) Address	State
[ ]	[ ]	[ ]	[ ]

[Reload]

The description of the columns is as below:

TERMS	DESCRIPTION

Neighbor Cache	The system will update Neighbor Cache automatically, and user also can click **Reload** to refresh the table.

3.1.4. Date and time

3.1.4.1. Date and time setting

The Avcomm' switch has a time calibration function 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.

NOTE: The Avcomm' switch does not have a real-time clock. The user must update the Current Time to set the initial time for the Avcomm' switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.

Date and Time

Current Time	Yr 2017 Mon 01 Day 1 Hr 05 Mn 34 Sec 28
	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	1st ▾ Sun ▾ in Jan ▾ at 00 ▾ 00 ▾
Daylight Saving End	1st ▾ Sun ▾ in Jan ▾ at 00 ▾ 00 ▾

Submit   Cancel

The description of the columns is as below:

TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. User also can click the **Get Time from PC** to get PC's time setting.
Time Zone	Choose the Time Zone section to adjust the time zone based on the user area.
NTP	**Enable NTP Client update** by checking this box. The system will send request packet to acquire current time from the NTP server that assigned. ***Make sure that the switch also has the internet connection.**
1st Time Server & 2nd Time Server	Choose from NTP Server List, to adjust User system time.
Daylight Saving Time	Enable the Daylight-Saving Function and the setting of function start and end time or disable it.
Daylight Saving Start &	Allows user to set the Start and End time individually.

Daylight-Saving End	

After finished configuring, click on **Submit** to activate the configuration.

IEEE 1588 PTP

IEEE 1588

IEEE 1588 was published in 2002, expands the performance capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks and enforces the specific timing requirements in such power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the protocol is intended to be administration free."

How Does an Ethernet Switch Affect 1588 Synchronization?

An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. When these fluctuations are incorrect, it will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognize significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be good design means to achieve the highest time accuracy.

Can Ethernet switches be designed to avoid the effects of these fluctuations?

A switch can be designed to support IEEE 1588 while avoiding the effects of queuing. In this case two modifications to the usual design of an Ethernet switch are necessary:

1. The **Boundary Clock and Transparent Clock** functionalities defined by IEEE 1588 must be implemented in the switch.

2. The switch must be configured so that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

Such an Ethernet switch will synchronize clocks directly connected to one of its ports to the highest possible accuracy.

The main function of IEEE 1588 is to synchronize the clocks of different end devices over a network at speeds faster than one Micro-second. After time synchronized, the system time will display the correct time of the PTP server.

3.1.4.2.   PTP setting

The PTP can be set in this PTP Setting webpage in which the user can configure PTP. The top part of this figure allows the users to enable or disable the PTP function. To enable PTP on the managed switch, please choose Enable. Note that the PTP functions will not active if the operation is disabled. Please see description of PTP Setting in table description. Note that after setting the desired PTP Setting, please click Apply button to allow the configuration take effect.

PTP Setting

Operation	Disable ▼
Operation Mode	Auto Elect ▼
Synchronization Interval	0(1s) ▼
Announce Interval	1(2s) ▼
Announce Receipt Timeout	6
Minimum Delay Request Interval	1(2s) ▼
Domain Number	0
Priority 1	128
Priority 2	128
Delay Mechanism	E2E ▼

Apply

The description of the columns is as below:

TERMS	DESCRIPTION
Operation	**Default: Disable** Enable/Disable the PTP function. This is the main option that needs to be enabled so that the PTP function will work
Operation Mode	**Default: Auto Elect** Choose Mode (Auto Elect, Preferred Master Clock or Slave)
Synchronization Interval	**Default: 0 (1s)** Set the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network.
Announce Interval	**Default: 1 (2s)** Sets the announce message interval
Announce Receipt Timeout	**Default: 6** The multiple of announce message receipt timeout by the announce message interval.
Minimum Delay Request Interval	**Default: 1 (2s)** Minimal delay request message interval
Domain Number	Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages
Priority 1	**Default: 128** 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.
Priority 2	**Default: 128** 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.
Delay Mechanism	**Default: E2E** 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

3.1.5. DHCP server

DHCP Server Setting

Avcomm' switch has DHCP Server Function that will provide a new IP address to DHCP Client. After enable DHCP Server function, set up the Network IP address for the DHCP server IP address, Subnet Mask, Default Gateway address and Lease Time for client. Below is the DHCP Server Setting interface

The description of the columns is as below:

TERMS	DESCRIPTION
Global Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
Address Pool Add	Add address pool to local DHCP Server. Select the IP address/mask in **Activated Subnet** and Click "**Add".** After applied, you can see the new Pool in Address Pool List.
Address Pool List	Choose the address pool setting that has been entered. You can "Delete" it in the list.
Pool Name	Add address pool name to local DHCP Server
Network	Enter the starting IP addresses for the DHCP server's IP assignment.
Mask	Assign the subnet mask for the IP address here.
Default Gateway	Enter the ending IP addresses for the DHCP server's IP assignment.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

21

DNS Server	Type the Primary, Secondary DNS Server's IP address.
Lease Time	The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 60-31536000 seconds)

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When user turns the computers on, they will automatically load the proper TCP/IP settings provided by the switch. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

Excluded Address List

The figure below shows the **Excluded Address List,** the IP address that is listed in the **Excluded Address List** table will not be assigned to the network devices.

The description of the columns is as below:

TERMS	DESCRIPTION
Excluded Address List	Type a specific address into the **Excluded IP** field for the DHCP server reserved IP address. Then click **Add,** to remove an IP address from the list click **Remove**. To refresh the list, click **Reload**.

Static Port/IP Binding List

The figure below is the web interface for **Static Port/IP Binding List**.

Type the specific Port and IP address, and then click **Add** to add a new Port & IP address binding rule for a specific client. The description of the columns is as below:

TERMS	DESCRIPTION
Port	The port that wishes binding.
IP Address	The IP address that will assign to the device with the Binding MAC address.

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

Static MAC/IP Binding List

The figure below is the web interface for **Static MAC/IP Binding List**.

Type the specific MAC and IP address, and then click **Add** to add a new MAC & IP address binding rule for a specific client.

The description of the columns is as below:

TERMS	DESCRIPTION
MAC Address	The MAC address of the device that wishes binding.
IP Address	The IP address that will assign to the device with the Binding MAC address.

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

Option 82/IP Binding List

The figure below is the web interface for **Option 82/IP Binding List**.

Type the specific Circuit ID, Remote ID, and IP address, and then click **Add** to add a new binding rule for a specific client.

The description of the columns is as below:

TERMS	DESCRIPTION
Circuit ID	The Circuit ID of the device that wishes binding.
Remote ID	The Remote ID of the device that wishes binding.
IP Address	The IP address that will assign to the device with the binding MAC address.

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

Option 82/IP Binding List

The figure below is the web interface for **Option 82/IP Binding List**.

Option82/IP Binding List

Circuit ID	01000101
Remote ID	COA87FFD
IP Address	192.168.10.9

Add

Index	Circuit ID	Remote ID	IP Address
☐ 1	01000101	COA87FFD	192.168.10.9

Remove **Reload**

Type the specific Circuit ID, Remote ID and IP address, and then click **Add** to add a new binding rule for a specific client.

The description of the columns is as below:

TERMS	DESCRIPTION
Circuit ID	The Circuit ID of the device that wishes binding.
Remote ID	The Remote ID of the device that wishes binding.
IP Address	The IP address that will assign to the device with the Binding MAC address.

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

DHCP Option 82

The DHCP Relay Agent (or DHCP Option 82) makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

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.

DHCP Option 82

DHCP Relay Agent [Enable ▼]

Submit

Helper Address

Helper Address [ ]

Add

☐	Helper Address 1	192.168.10.19
☐	Helper Address 2	
☐	Helper Address 3	
☐	Helper Address 4	

Remove

The description of the columns is as below:

TERMS	DESCRIPTION

DHCP Option 82	Select to **Enable** or **Disable** to activate or deactivate DHCP relay agent function, and then select the modification type of option 82.
Helper Address	There are 4 fields for the DHCP server's IP address. Fill the field with preferred IP address of DHCP Server.

And click **Submit** to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port. When **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).

Relay Policy

Replace - Replaces the existing option 82 field and adds new option 82 field. (This is the default setting).
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.

Circuit ID & Remote ID

The DHCP Option 82 information also 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. To activate this section, please make sure that DHCP Relay Agent is enabled.

The format of the **Circuit ID** is shown above: 00–01–00–01, this is where 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. For example: 00–01–00–01 is the **Circuit ID** of port number 1 with port VLAN ID 1.

The **Remote ID** identifies the relay agent itself and can be one of the following:
1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.

4. A user-defined string.

DHCP Leased Entries

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by switch.

DHCP Leased Entries

Index	IP Address	MAC Address	Leased Time Remains
1	192.168.10.3	ac22.0b70.cd13	55

Reload

Click the **Reload** button to refresh the list.
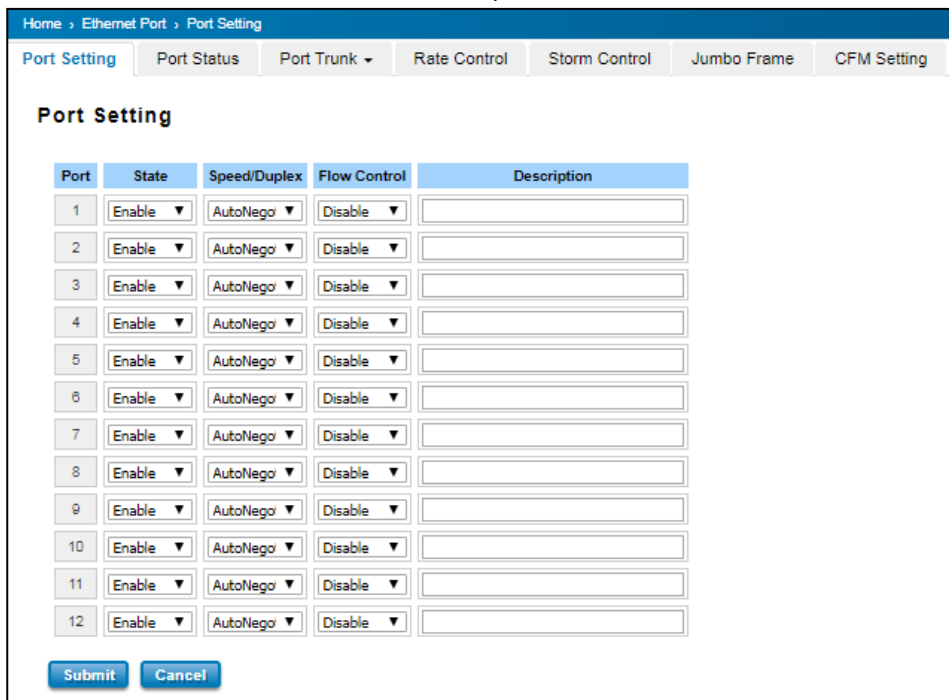
The description of the columns is as below:

TERMS	DESCRIPTION
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

3.2. Ethernet port

Ethernet Port section is used to access the port configuration and rate limit control. It also allows User to view port status and port trunk information.

3.2.1. Port setting

Port Settings section allows users to enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.
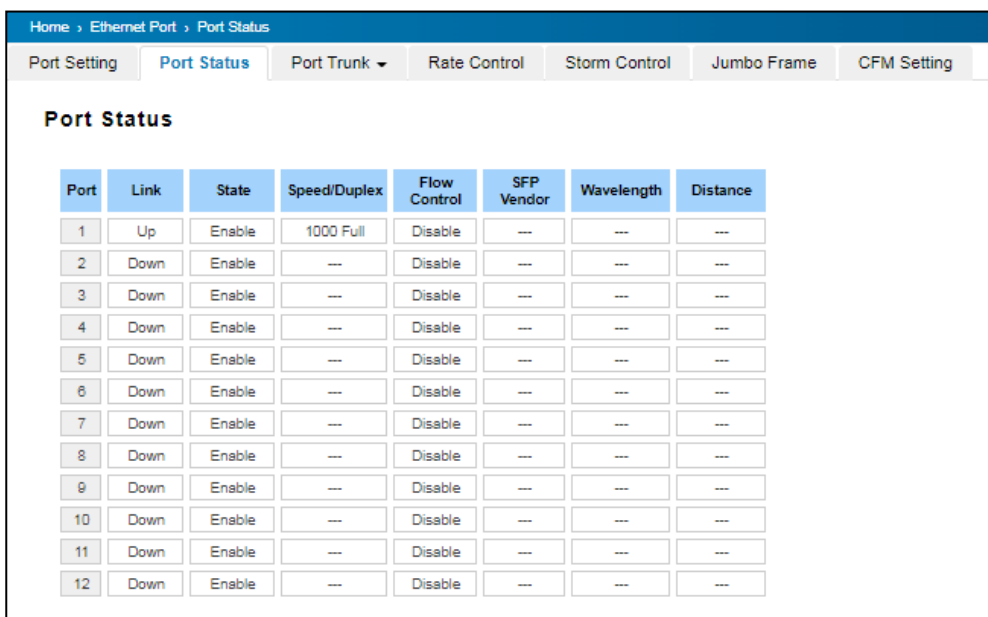

The description of the columns is as below:

TERMS	DESCRIPTION
Port	Shows port number
State	**Default: Enable** Enable or disable a port
Speed/Duplex	**Default: Auto Negotiation** Users can set the bandwidth of each port as Auto-negotiation, 100

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

	full,100 half,10 full,10 half mode for **Giga Ethernet Port 1~8 (ge1~ge8)**. For **Gigabit Ethernet Fiber Port 9~12: (ge9~ge12)**, it can be set up to 100M Full Duplex (100 Full) only.
Flow Control	**Default: Disable** **Enable** means that User need to activate the flow control function to let the flow control of that corresponding port on the switch to work. **Disable** means that User doesn't need to activate the flow control function, as the flow control of that corresponding port on the switch will work anyway.
Description	The description of interface.

After finished configuring the settings, click on **Submit** to save the configuration.

3.2.2. Port status

Port Status provides current port status.

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	Enable	1000 Full	Disable	---	---	---
2	Down	Enable	---	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

Avcomm Industrial Switch supports the SFP module with digital diagnostics monitoring (DDM) function. This technology allows the user to monitor 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. This section shows and configures the operational status, such as Scan/Eject the SFP, Enable/Disable SFP DDM, Temperature degree, Tx Power statistics, Rx Power Statistics in real time.

From the figure above, the real-time diagnostic parameters can be monitored to alert the system when the

transceiver's specified operating limits are exceeded, and compliance cannot be ensured. Basically, the SFP DDM has its own specification, as we can see from the table it is showed the temperature, Tx Power and Rx Power range. If all the current values are higher or lower than the available range or does not meet the SFP vendor specification, there would be a problem for the fiber connection.

The description of the Port Status and SFP DDM columns is as below:

TERMS	DESCRIPTION
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.

Click **Reload** to reload all port information, click **Scan All** to scan the SFP transceiver module and display the statistics. **Eject All** to eject the SFP transceiver that User has selected or plugged. User can eject one port or eject all by click the **Eject All** button. Click **Apply** to apply the configuration that just made.

3.2.3. 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. Avcomm' industrial managed switches 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.

Port Trunk Concept

Port trucking 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 User network while configuring a trunk, first disable or disconnect all ports that User want to add to the trunk or remove from the trunk. After User finish 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 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.

After port trunk has been activated, User can configure these items again for each trunk port.

Port Trunk Setting

The switch can support up to 8 trunk groups with 2 trunk members. Since the member ports should use same speed/duplex, max trunk members would be 8 for 100Mbps, and 2 members for Gigabit.

The description of the columns is as below:

TERMS	DESCRIPTION
Group ID	Default: 0 Group ID is the ID for the port trunk group. Ports with same group ID are in the same group.
Type	Default: Blank Static and LACP. Each Trunk Group can only support Static or LACP. Choose the type of User need here.

Click on Submit to apply the configuration and reload to refresh the table.

Load Balance Setting

Load Balance Type: Each Trunk Group can support several Load Balance types that can be seen from the table below:

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

Click **Submit** to apply your settings.

Port Trunk Status

This page shows the status of port aggregation. Once the aggregation ports are negotiated well, User will see following status. The figure below is the Port Trunk Status interface.

The description of the columns is as below:
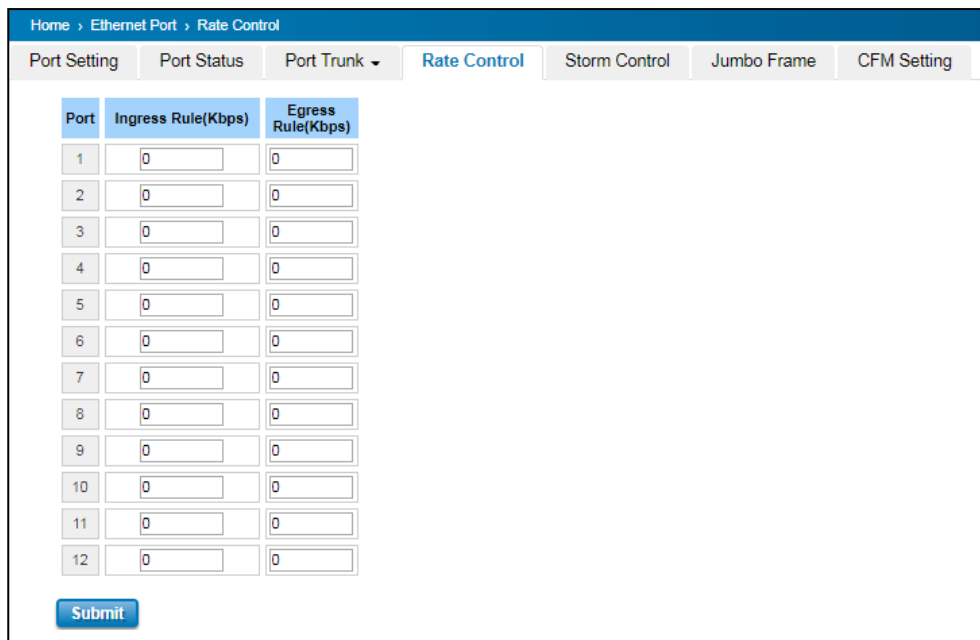
TERMS	DESCRIPTION

Group ID	Display Trunk 1 to Trunk 5 setup in Aggregation Setting.
Type	Static or LACP setup in Aggregation Setting.
Aggregated Ports	When LACP links well, User can see the member ports in aggregated column.
Individual Ports	When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column.
Link Down	When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column.

To refresh the list, click **Reload**.

3.2.4. Rate control

Rate control is a form of flow control used to enforce a strict bandwidth limit at a port. User can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types.

The description of the columns is as below:

TERMS	DESCRIPTION
Packet Type	Select the packet type that wanted to filter.
Ingress	The packet types of the Ingress Rule listed here include **Broadcast Only / Broadcast and multicast / Broadcast, Multicast and Unknown Unicast** or **All**.
Egress	The packet types of the Egress Rule (outgoing) only support **all** packet types.
Rate (Ingress & Egress)	**Default value Ingress:0 Kbps** **Default value Egress: 0 Kbps (**0 stands for disabling the rate control for the port.**)** The step of the rate is 64kbps.

Click on **Submit** to apply the configuration.

3.2.5. 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. In this page, user can configure the storm control for each port. Click Submit to apply the configuration.

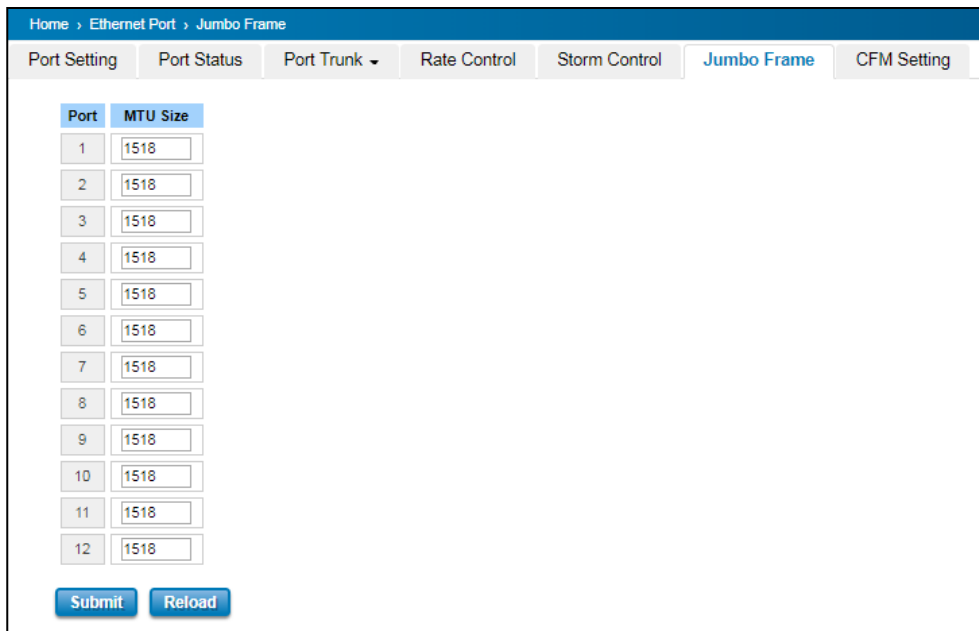| TERMS	DESCRIPTION
Broadcast	Default: Disable Set enable to control Broadcast Packets
DLF	Default: Disable Set enable to control Destination Lookup Failure packets
Multicast	Default: Disable Set enable to control Multicast Packets
Rate (Packet/Sec)	Rate limit value 0~262142 packet/sec

3.2.6. Jumbo frame

The switch allows user to configure the size of the Maximum Transmission Unit. The default value is 1,518bytes. The maximum Jumbo Frame size is 9,216 bytes.
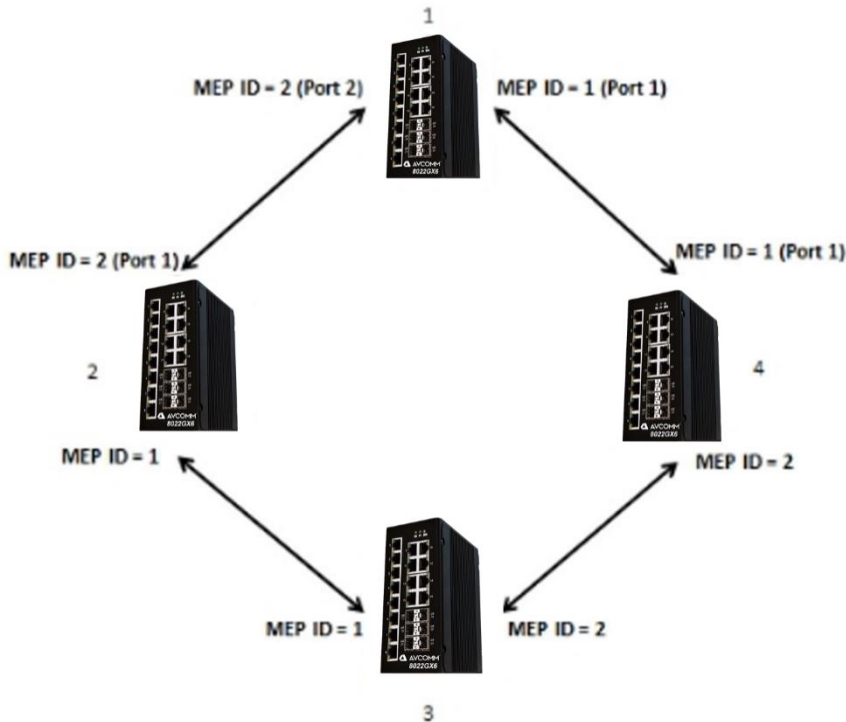

3.2.7. CFM setting

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 Ether type is 0x8902 and it has its own MAC address) to validate the health of the service instance.

Continuity Check Protocol (CCP): "Heart beating" 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 10ms.

1

MEP ID = 2 (Port 2)   MEP ID = 1 (Port 1)

MEP ID = 2 (Port 1)   MEP ID = 1 (Port 1)

2   4

MEP ID = 1   MEP ID = 2

MEP ID = 1   MEP ID = 2

3

The MEP ID in a link connection should be the same. For the example above the ERPS Ring, the port 1 from device one, the MEP ID is 1 and the port 1 from device 4, the MEP ID is also 1. In one device the MEP ID cannot be the same, it can be used only for a port. Below is the CFM CCP configuration page. In this page user may configure the Maintenance Domain, Maintenance Association, and the Maintenance association End Point setting.

Add Domain

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 the Domain name and the MD level then click **Add.**

TERMS	DESCRIPTION
MD Level	Select the MD Level from 0~7 The eight levels range from 0 to 7. A hierarchical relationship exists between domains based on levels. The larger the domain, the higher the level value. Recommended values of levels are as follows: Customer Domain: Largest (e.g., 7) Provider Domain: In between (e.g., 3) Operator Domain: Smallest (e.g., 1)
Domain Name	Enter a new Domain Name. Domain name, maximum of 43 characters

Add Association

Add Association

Domain Name	
Association Name	
VLAN	VLAN 1
Transmit Interval (ms)	3

Add

Choose the Domain Name from the list that has been added up then add a new Association Name for the Maintenance Association. After that choose the VLAN, please create VLAN first, and each port set to be "tagged" Add the Domain association name, end point type, port number and the MEP ID then click **Add.**

TERMS	DESCRIPTION
Domain Name	Choose the Domain Name that has been added
Association Name	Enter the Association Name. Association name, maximum of 45 characters
VLAN	Choose VLAN that has been assigned
Domain Name	Enter a new Domain Name. Domain name, maximum of 43 characters

Add Endpoint

Add Endpoint

Domain Association Name	
Endpoint Type	Local Endpoint
Port	Port 1
MEP ID	1

Add

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.
All the configurations above will directly appear at the three tables below, Domain Table, Association Table and the Endpoint Table.

TERMS	DESCRIPTION
Domain Association Name	Choose the Domain Association Name that has been added
Endpoint Type	**Default: Local Endpoint** 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.
Port	**Default: Port 1** Choose port that need to be assigned
MEP ID	**Default: 1** Choose the MEP ID. One MEP refer to one MEP ID

Domain Table

	Domain Name	MD Level
☐	1	0

Remove Selected   Cancel

Domain Table
This section shows the Domain entry. User may delete the list, by select the list and click **Remove Selected**

Association Table

	Domain Name	MD Level	Association Name	VLAN	Transmit Interval (ms)
	1	0	1	2	3 ▼

Association Table

Submit   Remove Selected   Cancel

This section shows the Association entry. In this table, user can configure the Configure Continuity Check Message transmit interval (default 3 ms), and after that click Submit to apply the setting. User may delete the list, by select the list and click **Remove Selected**

Endpoint Table

This section shows the Endpoint entry. User may delete the list, by select the list and click **Remove Selected**

Endpoint Table

	Domain Name	MD Level	Association Name	Port	Endpoint Type	MEP ID
	1	0	1	1	Remote	1

Remove Selected   Cancel

3.3. POWER OVER ETHERNET (PoE MODELS ONLY)

Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally. AVCOMM' industrial DIN Rail PoE Switch compliant with IEEE 802.3af and IEEE 802.3at. All of AVCOMM' switches adapt 8-Port PoE injectors in port 1 to port 8, each port with the ability to deliver 30W to compatible IEEE 802.3at standard and provides 240W power budget for hall system.

Power over Ethernet can be used with:

• Surveillance cameras

• Security I/O sensors

• Industrial wireless access points

• Emergency IP phones

3.3.1. PoE STATUS

The PoE Status page shows the system PoE status and the operating status of each PoE Port. The information includes PoE mode, Operation status, and PD class, Power Consumption, Voltage and Current. For example, in the figure below,

Home › PoE › PoE Status

PoE Status | PoE Control ▾ | PoE Schedule | Alive Check | PoE Event

PoE Status

Total Power Budget	240 W
Total Output Power	3.10 W
Utilization	1 %
Event	Normal

Port	Mode	Status	Class	Budget(w)	Consumption(W)	Voltage(V)	Current(mA)
1	Disable	Off	---	---	0.00	0.0	0.0
2	Disable	Off	---	---	0.00	0.0	0.0
3	Disable	Off	---	---	0.00	0.0	0.0
4	Disable	Off	---	---	0.00	0.0	0.0
5	Disable	Off	---	---	0.00	0.0	0.0
6	Disable	Off	---	---	0.00	0.0	0.0
7	Enable	Powering	Class2	7.70	3.10	47.8	65.4
8	Disable	Off	---	---	0.00	0.0	0.0

Reload

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

Port 7 was enabled and is supplying power to a Class 2 Powered Device (PD) indicated under the Classification column. The PD device is rated at 47.8V and 65.4mA. The total power consumption for this PD is 3.10W with Budget 7.70W. To check the status of the PoE port, please click on the Reload button.
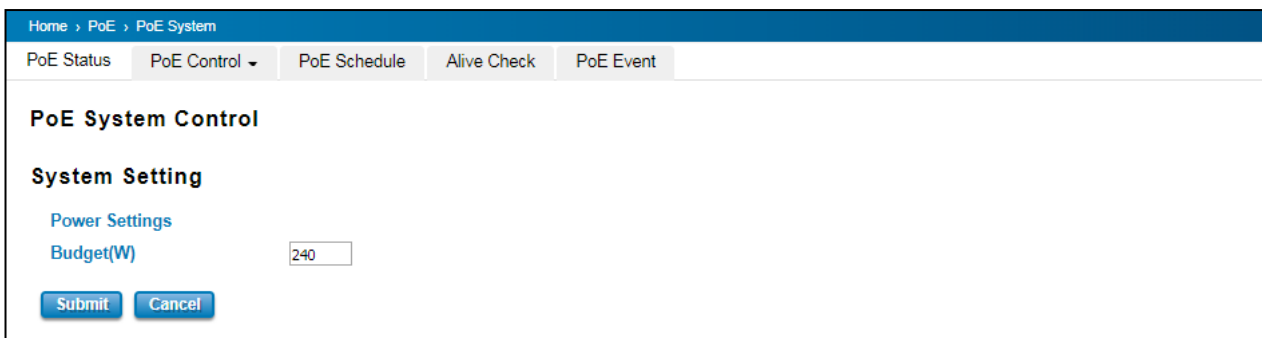
The description of the columns is as below:

TERMS	DESCRIPTION
Mode	Enable/Disable/Schedule Indicates the PoE port status
Status	Default: Off PoE status is included Off, Powering, and Searching. Off – PoE is inactive. Powering – PoE is enabled and powering the PD. Searching – Searching the PD which need the power.
Class	Indicates the PD included in which PoE class.
Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (mA)	Indicates the actual Current consumed value for PoE port

3.3.2. PoE CONTROL

The PoE control includes 3 parts, **System Setting**, **Port setting** and **PD status detection**. The following section will introduce the function.

System Setting

Home › PoE › PoE System
PoE Status   PoE Control ▾   PoE Schedule   Alive Check   PoE Event

PoE System Control

System Setting

Power Settings
Budget(W)   240

Submit   Cancel

The figure above is **System Setting** interface. In this section, user can enable or disable the PoE function.

The description of the columns is as below:

TERMS	DESCRIPTION
PoE System	Enable or disable system's PoE function.
Budget (W)	Default: 240W The power supply maximum output budget.

After finished configuring the settings, click on **Submit** to save the configuration.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

PoE Port Control

The description of the columns is as below:

TERMS	DESCRIPTION
Mode	Enable/Disable/Schedule port's PoE function.
Powering Mode	802.3af, 802.3at (LLDP), 802.3at (2-event) and forced mode. ***Forced mode will ignore the classification behaviors and apply power onto the RJ-45, uses the forced mode must be carefully.**
Budget Mode	Choose budget mode as auto or manual. If auto the budget would be delivered automatically based on the end device requirement. If user choose manual, user can input the number at the budget text box.
Budget (W)	Input the budget.

If the system PoE consumption is over the system budget control, the PoE system will turn off low priority port PoE function, until the consumption is becomes smaller than the system budget. After finished configuring the settings, click on **Submit** to save the configuration.

To enable the IEEE 802.3at High Power PoE function, the power input voltage should be DC 50 ~57V to obtain better performance. Applies DC 48V to PoE Switch and perform 30W high power output may cause the PoE disable automatically. To avoid this issue, we suggest adjust the power supply output to 50V DC or higher. In usually, the Switching power supply adopted adjust resistor for voltage fine tune.

> **WARNING:** During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating.

3.3.3. PoE SCHEDULING

For energy saving or power recycle powered devices, the PoE managed switch's **PoE scheduling** interface allows users to appoint any date and time to enable or disable PoE functions for each PoE port. User need to configure **PoE Scheduling** and select a target port manually to enable this function. The figure below is PoE Schedule interface.

PoE Schedule

PoE Schedule [Disable ▽] on [Port 1   ▽]

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	☐	☐	☐	☐	☐	☐	☐
01:00	☐	☐	☐	☐	☐	☐	☐
02:00	☐	☐	☐	☐	☐	☐	☐
03:00	☐	☐	☐	☐	☐	☐	☐
04:00	☐	☐	☐	☐	☐	☐	☐
05:00	☐	☐	☐	☐	☐	☐	☐
06:00	☐	☐	☐	☐	☐	☐	☐
07:00	☐	☐	☐	☐	☐	☐	☐
08:00	☐	☐	☐	☐	☐	☐	☐

The PoE schedule supports hourly and weekly base PoE schedule configuration. **Enable** and select the target port and marking the time frame, then click **Submit** to activate the PoE scheduling function on selected port.

3.3.4. ALIVE CHECK

PD Alive Check

PD Alive Check

☐ **Enable PD Alive Check**

PD	IP Address	Cycle Time(s)	Delete
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐

[Submit] [Cancel]

AVCOMM' Switches support a useful function that help user to maintain the PD's status and help use to saving the maintenance time and money. Once user defined this function, the PoE Switch will request PD system and turn-off PoE power if PD system does not echo the request. After the duration time (cycle time), the PoE switch will start request PD again.
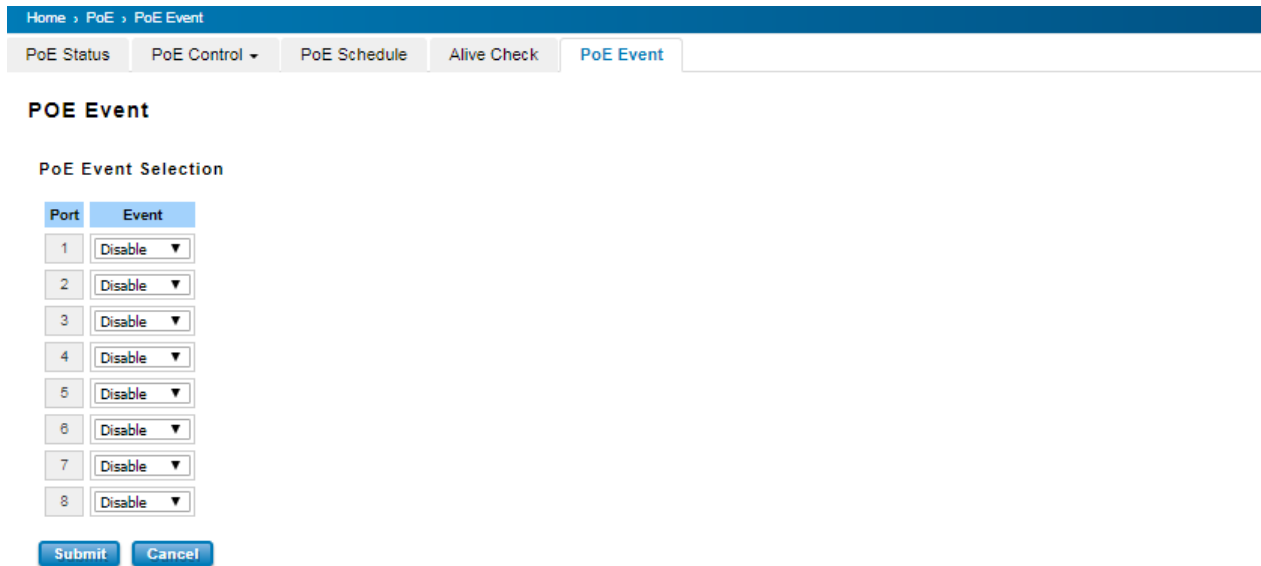
The description of the columns is as below:

TERMS	DESCRIPTION
IP address	PD's IP-address that installed on the port.
Cycle time	User measured the PD system boots duration time.

	*Most of PD system – IP camera will take at least 40~50 seconds. Here, we suggest that user sets the cycle time to 90 seconds.
Delete	Delete PD's IP-address that has been selected.

After finished configuring the settings, click on **Submit** to save the configuration.

3.3.5. PoE EVENT

In this section, user is allowed to configure the PoE Event, the value is Enable and Disable. When the status is enabled PoE itself will detect the PD, then it will deliver the power when the PD is detected.

3.4. 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 if a cable is inadvertently disconnected or damaged. This 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-50ms 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.

3.4.1. RSTP

This page allows select the RSTP mode and configuring the global RSTP Bridge Configuration.

The STP mode includes the **STP**, **RSTP**, **MSTP** and **Disable**. User can select the STP mode for user system first. The default mode is RSTP enabled. After user selects the STP or RSTP mode; user should continue to configure the global Bridge parameters for STP and RSTP. If user selects the MSTP mode, user need go to MSTP Configuration page.

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.

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.

MSTP (Multiple Spanning Tree Protocol)

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. MSTP can provide multiple forwarding paths and enable load balancing. By understand the architecture, allow you 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 is from 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 because 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 enabled MSTP mode, user can go to the MSTP Settings page.

Bridge Configuration

Bridge Address: This shows the switch's MAC address.

Priority (0-61440): 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. So that 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 then become the root bridge.

Max Age (6-40): Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait

> **NOTE:**
>
> 1. The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority.
> 2. The Web GUI allows user selects the priority number directly. This is the convenient of the GUI design. When user configures the value through the CLI or SNMP, user may need to type the value directly. Please follow the n x 4096 rules for the Bridge Priority.

without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

Hello Time (1-10): 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 (4-30): 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.

Once user has completed user configuration, click on **Submit** to apply user settings.

> **NOTE:** User must follow the rule to configure Hello Time, Forwarding Delay, and Max Age parameters.
>
> **2× (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)**

RSTP Port Settings

Select the port user wants to configure and user will be able to view current setting and status of the port.

The description of the columns is as below:

TERMS	DESCRIPTION
STP State	Default: Enable

		To enable or disable STP function.
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 is the value that 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. **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.

Once user finished user configuration, click on **Submit** to save user settings.

RSTP Status

This page allows user to see the information of the root switch and port status.

Root Status: User can see 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

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port	Aggregated(ID/Type)
1	Disabled	Disabled	200000	128	P2P	Edge	/
2	Disabled	Blocking	200000	128	P2P	Edge	/
3	Disabled	Blocking	200000	128	P2P	Edge	/
4	Disabled	Disabled	200000	128	P2P	Edge	/
5	Disabled	Disabled	200000	128	P2P	Edge	/
6	Disabled	Disabled	200000	128	P2P	Edge	/
7	Disabled	Disabled	200000	128	P2P	Edge	/
8	Disabled	Disabled	200000	128	P2P	Edge	/
9	Disabled	Disabled	20000	128	P2P	Edge	/
10	Disabled	Disabled	20000	128	P2P	Edge	/

Reload

Port Status: User can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode and Aggregated (ID/Type).

3.4.2. MSTP

MSTP Region Configuration

This page allows 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.

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

Once user finished user configuration, click on **Submit** to apply user settings.

Add MSTP Instance

This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page. **After** finishing the configuration, click on **Add** to apply user settings.

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

MST Instance Configuration

This page allows user to see the current MST Instance Configuration user added. Click on **Submit** to apply the setting. User can **Remove** the instance in this page.

MSTP Port Setting

This page allows configure the Port settings. Choose the Instance ID user wants to configure. The MSTP enabled and linked up ports within the instance will be listed in this table. Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.

The description of the columns is as below:

TERMS	DESCRIPTION
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. Path cost value is derived from the media speed of an interface. 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. 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.

Port Priority	Enter a value between 0 and 240. This is the value that 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. **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.

Once user finished user configuration, click on **Submit** to save user settings.

MSTP Status

This page allows user to see the current MSTP status. Choose the **Instance ID** first. If the instance is not added, the information remains blank. The **Root Information** shows the setting of the Root switch.

Root Status: User can see 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

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1	Disabled	Blocking	200000	128	P2P	Edge
2	Designated	Forwarding	200000	128	P2P	Edge
3	Designated	Forwarding	200000	128	P2P	Edge
4	Disabled	Blocking	200000	128	P2P	Edge
5	Designated	Forwarding	200000	128	P2P	Edge
6	Disabled	Blocking	200000	128	P2P	Edge
7	Designated	Forwarding	200000	128	P2P	Edge
8	Disabled	Blocking	200000	128	P2P	Edge
9	Disabled	Blocking	20000	128	P2P	Edge
10	Disabled	Blocking	20000	128	P2P	Edge

Reload

Port Status: User can see port Role, Port State, Path Cost, Port Priority, Link Type, and the Edge Port within the instance. Click **Reload** to refresh the information display.

3.4.3. ERPS

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms 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.
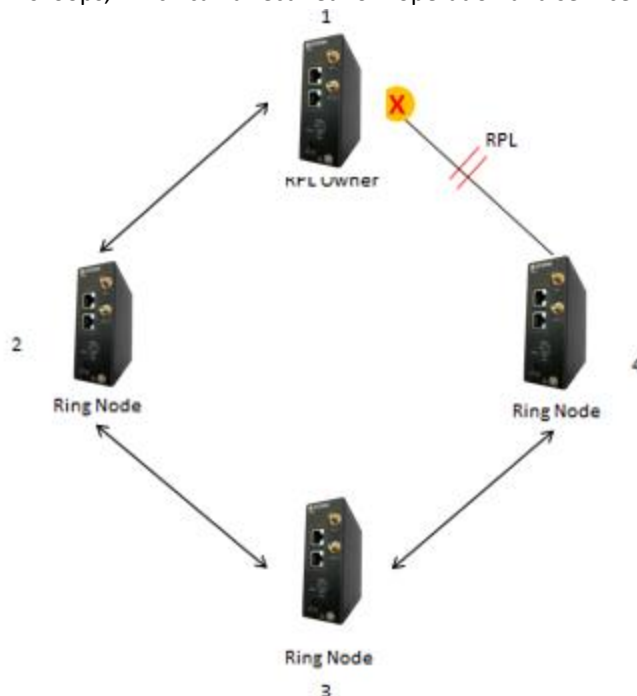
The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This link 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. Thus, 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.

Avcomm managed switches provide several Ethernet ring protocols. The ERPS/Ring section is subdivided into two menus, which are: ERPS Setting and ERPS Status.

3.4.3.1.   ERPS setting

ERPS Setting

Add ERPS Instance is a section for mapping the VLAN to Instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page.

After clicking the **Add** button, the Instance ID and the VLAN group information will directly display in the **ERPS Instance Setting** section.

TERMS	DESCRIPTION
Instance ID	Select the Instance ID, the available number is 1-15.
VLAN Group	Type the VLAN ID that user wants mapping to the instance.

Add ERPS Ring

Add ERPS Ring is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will be directly created in the **ERPS Ring Setting** section. The ERPS Ring Setting section is a table that used to set up the ERPS Ring configuration.

Below is the description table.

TERMS	DESCRIPTION
Ring ID	Display the Ring ID

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enable - Ring Status is enable Disable - Ring Status is disable
Node Role	It can be either RPL owner or RPL Neighbor or Ring Node.
Control Channel	**Default: 1** Control channel is implemented using a VLAN. Each ERP instance uses a tag-based VLAN for sending and receiving R-APS messages. (1-4094)
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	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)
Ring Port 0	This will create a Port 0 of the switch in the Ring. Choose 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. Choose the port number that belongs to Ring port 1.
Ring Port 0 RMEP ID	**Default: None** The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please check the CFM Setting (MEP ID)
Ring Port 1 RMEP ID	**Default: None** The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please Check the CFM Setting (MEP ID).
RPL Port	This allows you to select the Ring Port 0 or Ring Port 1 as the RPL block.
Revertive Mode	**Default: Revertive** **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.
Instance	Select the Instance ID, the available number is 1-15.
Manual Switch	**Default: None** In the absence of a failure or FS, 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.
Force Switch	**Default: None** 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.

ERPS Timer Setting

TERMS	DESCRIPTION
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.

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
0	v2	Enabled	Major Ring	Idle	RPL Owner	1	False	2	Link Up / Forwarding	Link Up / Blocking	None	None	1	Revertive		

3.4.3.2. ERPS status

In this section, user can check the ERPS Status, Timer Status and Statistics from the Ring.

TERMS	DESCRIPTION
Ring ID	Display the Ring ID
Version	ERPS Protocol Version - v1 or v2.
Ring State	**Default: Disable** Enabled - Ring Status is enable Disabled - Ring Status is 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	**Default: False** **True** – if have a virtual channel **False** – if doesn't have any virtual channel
Virtual Channel of Sub Ring	**Default: 1** Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)
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
Ring Port 0 RMEP ID	Show the remote MEP id that CFM monitored of ERPS ring port detection.
Ring Port 1 RMEP ID	Show the remote MEP id that CFM monitored of ERPS ring port detection.

RPL Port	The port status as the RPL block.
Revertive Mode	**Default: Revertive** **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.
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

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)
1	not running	5	0	not running	5100	0	not running	100	0

TERMS	DESCRIPTION
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.

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
1	0	0	15	12	0	0	0	8432	22	72	10

Reload

TERMS	DESCRIPTION
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.

3.5. 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 VLANs, User can segment User network without being restricted by physical connections—a limitation of traditional network design. With VLANs User can segment User network into:

• **Departmental groups**—User could have one VLAN for the marketing department, another for the finance department, and another for the product development department.

• **Hierarchical groups**—User could have one VLAN for directors, another for managers, and another for general staff.

• **Usage groups**—User could have one VLAN for email users and another for multimedia users.

Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides User with three other benefits:

• **VLANs ease the relocation of devices on networks:** With a VLAN setup, if a host originally on the Marketing VLAN, is moved to a port on another part of the network, and retains its original subnet membership, User only needs to specify that the new port is on the Marketing VLAN. User does not need to do any re-cabling.

• **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.

• **VLANs help control traffic:** VLANs increase the efficiency of User network because each VLAN can be set up to contain only those devices that need to communicate with each other.

This 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.

TERMS	DESCRIPTION
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.

3.5.1. VLAN setting

To configure 802.1Q VLAN and port based VLANs on the Avcomm switch, use the VLAN Settings page to configure the ports., User can assign Management VLAN, create the static VLAN, and assigns the Egress rule for the member ports of the VLAN.

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

VLAN Setting

Management VLAN ID `1`

[Submit]

Static VLAN

VLAN ID	NAME

[Add]

The description of the columns is as below:

TERMS	DESCRIPTION
Management VLAN ID	**Default: 1.** The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch.
Static VLAN	User can assign a VLAN ID and VLAN Name for new VLAN here.
VLAN ID	**Default: 1** Used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094.
Name	A reference for network administrator to identify different VLANs. The available character is 12 for User to input. If User don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID).

The steps to create a new VLAN: Type in VLAN ID and NAME, and press **Add** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Configuration table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

NOTE:

1. Before User changed the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise, the administrator can't access the switch via the network.
2. Avcomm switch supports max 256 groups VLAN.

Static VLAN Configuration

Static VLAN Configuration table is presented on the figure below. User can see the created VLANs and specify the egress (outgoing) port rule to be **Untagged or Tagged** here.

Static VLAN Setting

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12
☐ 1	VLAN1	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾
☐ 2	VLAN2	-- ▾	-- ▾	T ▾	T ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾

Submit   Remove Selected   Reload

The description of the columns is as below:

TERMS	DESCRIPTION
--	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.

Steps to configure Egress rules:

Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to **U** or **T**. Press **Submit** to apply the setting. If User wants to remove one VLAN, select the VLAN entry. Then press **Remove** button.

3.5.2. VLAN port setting

| VLAN Setting | VLAN Port Setting | VLAN Status | PVLAN Setting | PVLAN Port Setting | PVLAN Status | GVRP 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 ▾

VLAN Port Setting allows User to setup VLAN port parameters to specific port.

The description of the columns is as below:

TERMS	DESCRIPTION
PVID	The abbreviation of the **Port VLAN ID**. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 0 to 4095. But 0 and 4095 are reserved. User can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column.
Tunnel Mode	**Default: None** **None**: This is Port that no using Q in Q

	802.1Q Tunnel: As the Ingress port, is connected to the client port. Configures Q in Q tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network. 802.1Q Tunnel Uplink: As the egress port, that is, the middle switch port. Configures Q in Q tunneling for an uplink port to another device within the service provider network. 802.1Q Tunnel Uplink-Add-PVID: Assign second VLAN tag for specify VLANs.
Ether Type	Default: 0x8100 It is used to indicate which protocol is encapsulated in the payload of the frame.
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. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped.

3.5.3. VLAN status

This table shows User status of User VLAN, including VLAN ID, Name, Status, and Egress rule of the ports.

The description of the columns is as below:

TERMS	DESCRIPTION
VLAN ID	ID of the VLAN.
Name	Name of the VLAN.
Status	Static shows this is a manually configured static VLAN. This VLAN is not workable yet. Dynamic means this VLAN is learnt by GVRP.

After created the VLAN, the status of this VLAN will remain in unused status until User adds ports to the VLAN.

3.5.4. PVLAN setting

The figure above is PVLAN Setting interface. PVLAN Configuration allows User to assign Private VLAN type. After created VLAN in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN User wants to configure.

The description of the columns is as below:

TERMS	DESCRIPTION
None	The VLAN is not included in Private VLAN.
Primary	The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.
Isolated	The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.
Community	The VLAN is the Community VLAN. The member ports of the VLAN can communicate with each other.

3.5.5. PVLAN port setting

PVLAN Port Setting page allows to configure Port and Private VLAN Association.

Port Configuration
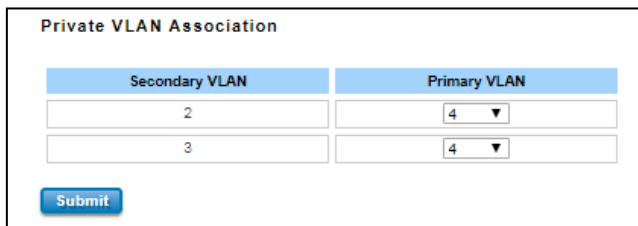
The description of the columns is as below:

TERMS	DESCRIPTION
PVLAN Port Type	**Normal:** The Normal port is None PVLAN ports; it remains its original VLAN setting.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

	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 (PVLAN)

Secondary VLAN: Secondary VLAN is included Isolated and Community VLAN Type that assigned in Private VLAN Configuration section. User can select the Secondary VLAN ID here.

Primary VLAN: Primary VLAN is included the Primary VLAN Type that assigned in Private VLAN Configuration section. User can select the Primary VLAN ID here.

Before configuring PVLAN port type, the Private VLAN Association should be done first.

For example:
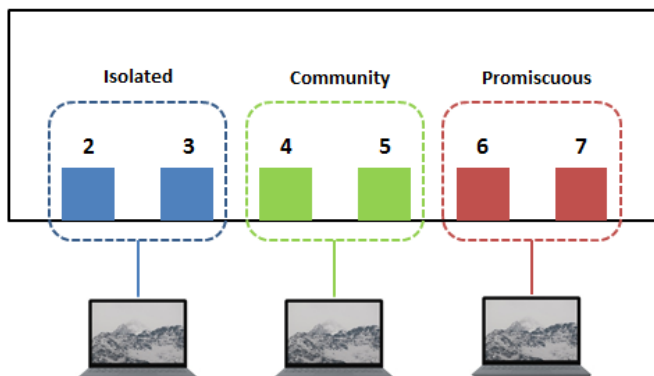
1. Create VLAN and Assign the Private VLAN Type:

The very first thing that user need to do is create the VLAN and make sure that the ports are assigned to specific VLAN. After created VLAN, assign the Private VLAN type for each VLAN, for example: VLAN 2 -> Isolated (Secondary VLAN), VLAN 3 -> Community (Secondary VLAN) and VLAN 4 -> Primary.

2. Associate the Secondary VLAN to Primary VLAN:

After creating the VLAN and assign the Private VLAN Type, then associate the secondary VLAN, VLAN 2 and 3 to VLAN 4 as the Primary VLAN in Private VLAN Association section.

3. Configure the Private VLAN Port:

● VLAN 4 – **Primary** -> The member port of VLAN 4 is Promiscuous port. (Port 6 and 7)
● VLAN 2 – **Isolated** -> Map the Host port to VLAN 2. (Port 2 and 3)
● VLAN 3 – **Community** -> Map the Host port to VLAN 3. (Port 4 and 5)

5. Result (See 3.5.6 PVLAN Status):

● VLAN 4 -> VLAN 2 and 3; member ports (6 & 7) can communicate with ports in secondary VLAN.
● VLAN 2 -> VLAN 4; member ports (2 & 3) are isolated and cannot communicate each other, but they can communicate with Primary VLAN ports.
● VLAN 3 -> VLAN 4; member ports (4 & 5) within the community can communicate with each other and communicate with Primary VLAN ports.
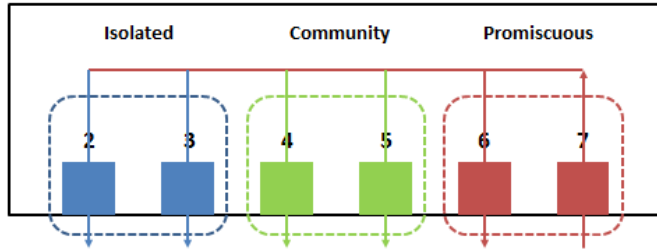
3.5.6. PVLAN status

This page allows User to see the Private VLAN status information.

3.5.7. 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. GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. The description of the columns is as below:

TERMS	DESCRIPTION
GVRP Protocol	**Default: Disable** Allow user to enable / disable GVRP function globally.
State	**Default: Disable**

	After enable GVRP globally, here 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

3.6. 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 guarantees are 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. This section allows User to configure Quality of Service settings for each port by configure the priorities to provide a smooth data traffic.

3.6.1. QoS setting

The figure below shows QoS Setting.
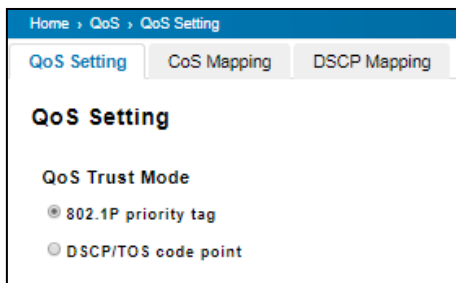
QoS Trust Mode

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.
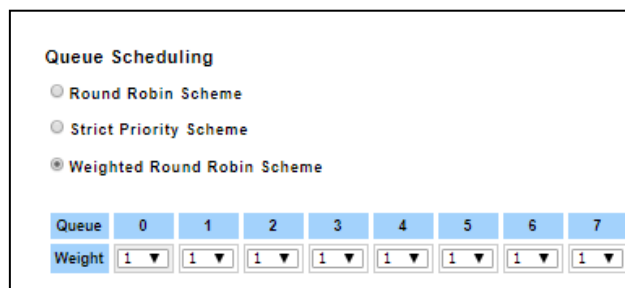
Queue Scheduling

User may select the Queue Scheduling rule:
- o **Use Round Robin Scheme:** The Round Robin scheme means all the priority has the same privilege; the traffic is forward cyclic from highest to lowest.

o **Use strict priority scheme:** The priority here always the higher queue will be processed first, except the higher queue is empty.
o **Use 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

Choose 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. Click the **Submit** button to apply the configuration changes.

3.6.2. CoS mapping

This section allows user to change CoS values to Physical Queue mapping table. In Avcomm switch, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Below is the interface.

The service classes (CoS) are assigned to the queues as default as follows:
● COS 0 → Queue 0
● COS 1 → Queue 1
● COS 2 → Queue 2
● COS 3 → Queue 3
● COS 4 → Queue 4
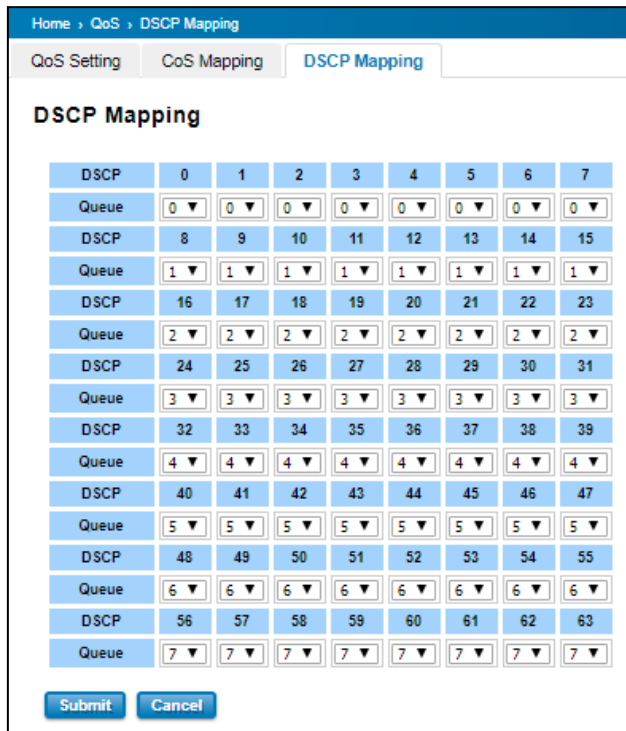● COS 5 → Queue 5
● COS 6 → Queue 6
● COS 7 → Queue 7
For the step-in configuration
1. For each value in the **CoS** column, select the queue from the **Queue** drop-down list.
2. Click the **Submit** button.

3.6.3. DSCP mapping

This page is to change DSCP values to Physical Queue mapping table. Users should therefore assign how to map DSCP value to the level of the physical queue. Users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.

After configuration, press **Submit** to enable the settings.

DSCP Value and Priority Queues Setting	Description	Factory Default
0 to 7	Maps different TOS 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

3.7. Multicast
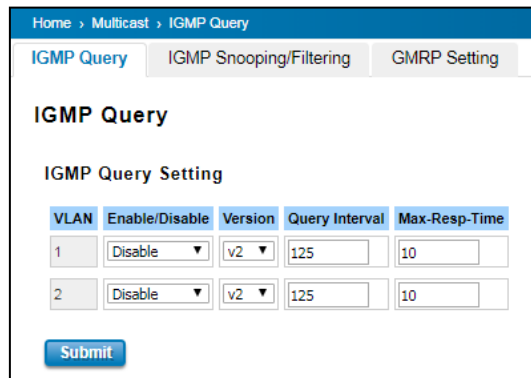
Multicasts are like broadcasts; they are sent to all end stations on a LAN or VLAN that belong to the multicast group. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations. For multicast filtering, Avcomm switch uses 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.

3.7.1. IGMP Query

This page allows users to configure **IGMP Query** feature. Since the device can only be configured by member

ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If User wants to run IGMP Snooping feature in several VLANs, User should notice that whether each VLAN has its own IGMP Querier first.

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.

TERMS	DESCRIPTION
Enable	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.

Once User finished configuring the settings, click on **Submit** to apply User configuration.

3.7.2. IGMP snooping

This page is to enable IGMP Snooping feature. After enable the feature, user may assign IGMP Snooping function to specific VLAN, and the IGMP Snooping table will show the specific multicast group from dynamic learnt or manual input. By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets,

and manage multicast traffic through the switch.

TERMS	DESCRIPTION
IGMP Snooping Global Setting	User can select **Enable** or **Disable** this function here. After enabling IGMP Snooping, User can then enable IGMP Snooping for specific VLAN.
IGMP Snooping	Select the **Enable** to activate the IGMP Snooping. In the same way, User can also **Disable** IGMP Snooping for certain VLANs.
Filtering Mode	It allows the switch to filter the unknown-multicast data flow. Multicast Filtering Mode is Flood unknown, discard unknown and source only learning. 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.

IGMP Snooping Table: User can see several information such as multicast IP address, VLAN ID from the multicast group, and the interface member ports of the multicast group (256 multicast groups)

3.7.3. 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.

3.8. Routing

The chapter is applied for 8010GX2/8012GX4-L3 L3 Managed Ethernet Switch.
Routing Feature is the most important feature of the Layer 3 Switch. Layer 3 routing feature is requested since the hosts located in different broadcast domain can't communicate each other once there is a need to communicate among the different VLANs. Avcomm Switch combines Layer 2 switching and Layer 3 routing within the single platform. In the Routing Configuration pages allows users create the Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy, and check the related routing information.

3.8.1. IP interface setting

Through this page, user is allowed to enable the IP Routing interface and assign the IP Address. First create the VLAN Interface and assign the member port to the VLAN before creating IP Interface, please refer to the VLAN Configuration page. The IP Interface table listed all the created VLAN automatically; user can change the setting for each VLAN here.

IP Interface

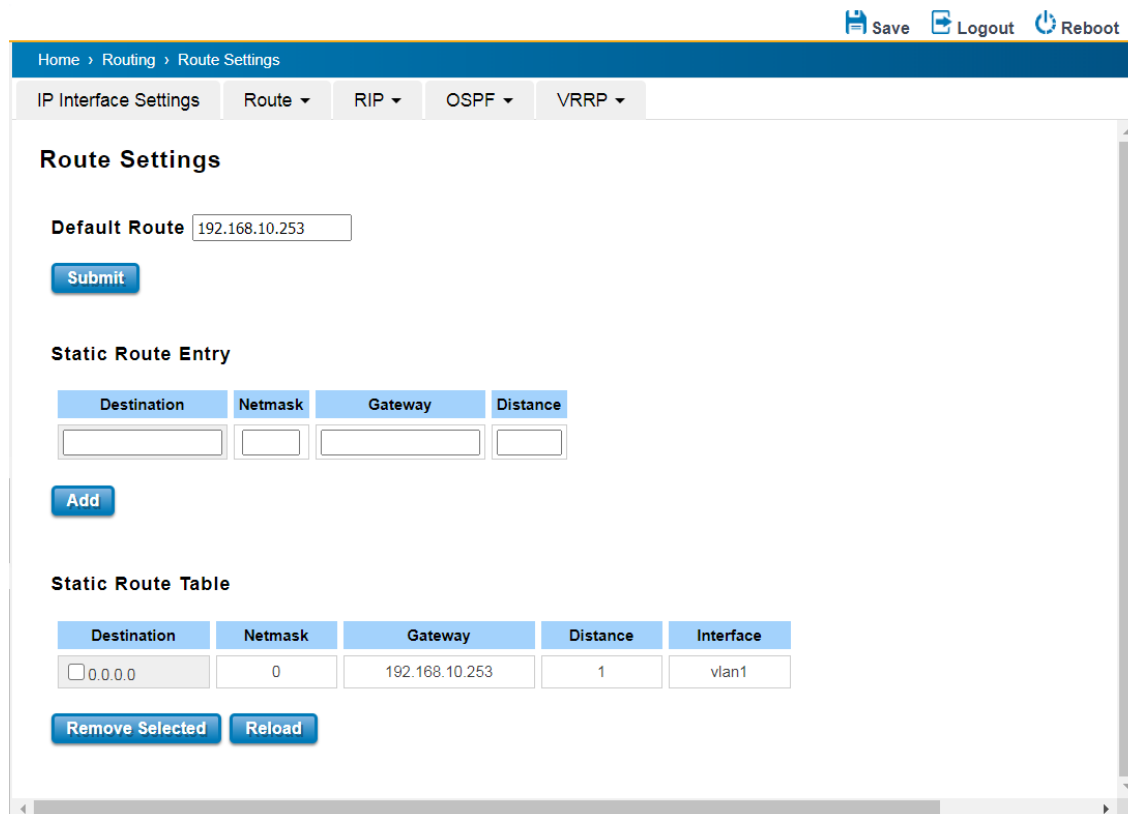| TERMS	DESCRIPTION
Interface	The name of the IP interface.
Status	After enabled the routing state, the Status shows **Up**. The routing state is enabled while the member ports of the interface relate to another switch or end device. After disabled the routing state, the status shows **Down**
State	Enable or disable the IP Routing Interface state. After disabled, the interface just works as a layer 2 VLAN. After enabled, the interface can support IP routing feature.
IP Address	Assign the IP Address for the target IP Interface.
Subnet Mask	Choose the subnet mask here. For 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.

Alias IP Table

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

Click the **Add** to add an alias IP address for the selected interface. Click the **Remove Selected** to remove the selected alias IP address of an interface.

3.8.2. Route setting

This configuration page allowed user to configure the route entry and display the route table.
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 and run their own routing protocols, however, while they want to communicate with unknown network, the traffic will be forwarded to the default route. While configuring Default Route, the IP address of the next hop router/switch is the only setting needs to be specified.

Static Route Entry

Static route entries go to and go from a stub network to another stub network. The static route is usually configured to connect the neighbor router/switch; both routers/switches then can communicate through the route.
While configuring Static Route, all the fields in Route entry like the destination network and its netmask, the valid route interface to the destination and distance are needed to be specified.

TERMS	DESCRIPTION
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.

Click the **Add** button to add a static route entry.

Static Route Table

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

TERMS	DESCRIPTION
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.
Metric	The metric of static route entry.
Interface	The IP interface of static route entry.

Click the **Remove Selected** button to remove selected route entry. Click the **Reload** button to reload Route Entry Table information.

Route Table

Once the routing interfaces changed, the system maintains information and updates the routing table. It is important to find out the possible and best route in the field especially when troubleshooting the network problem.

TERMS	DESCRIPTION
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.

3.8.3. RIP

The Industrial L3 managed switch also implements a dynamic routing protocol to allow automatically learning and updating of routing table. In this subsection, one of the dynamic routing protocols can be setup by the users. Routing Information Protocol (RIP) is a distance vector-based routing protocol that can make decision on which interface the L3 managed switch should forward Internet Protocol (IP) packet 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 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 also be used to automatically build up a routing table.

RIP Setting

RIP Settings

RIP Protocol [Version 2 ▾]

[Submit]

Routing for Networks

Network Address [192.168.1.0] / [24] (A.B.C.D/M)

[Add]

Index	Network Address
☐ 1	192.168.20.0/24

[Remove Selected] [Reload]

TERMS	DESCRIPTION
RIP Protocol	Choose the RIP protocol **Version 1** or **Version 2** or **Disable** RIP protocol in here. Click the **Submit** button to apply RIP protocol setting.
Routing for Networks	All the networks no matter directly connected or learnt from other router/switch should be added to the switch. The format is IP Network/bit mask. For example, 192.168.20.0/24. After type the network address, click the **Add** to add a routing network.

Click the **Add** button to add a routing network. Click the **Remove Selected** button to remove selected network address. Click the **Reload** button to reload RIP information.

RIP Interface Setting

TERMS	DESCRIPTION
Interface	The IP interfaces.
RIP Version	RIP version of IP interface. (RIPv1, RIPv2 and Both)

Click the **Submit** button to apply RIP interface settings. Click the **Reload** button to reload RIP interface configuration.
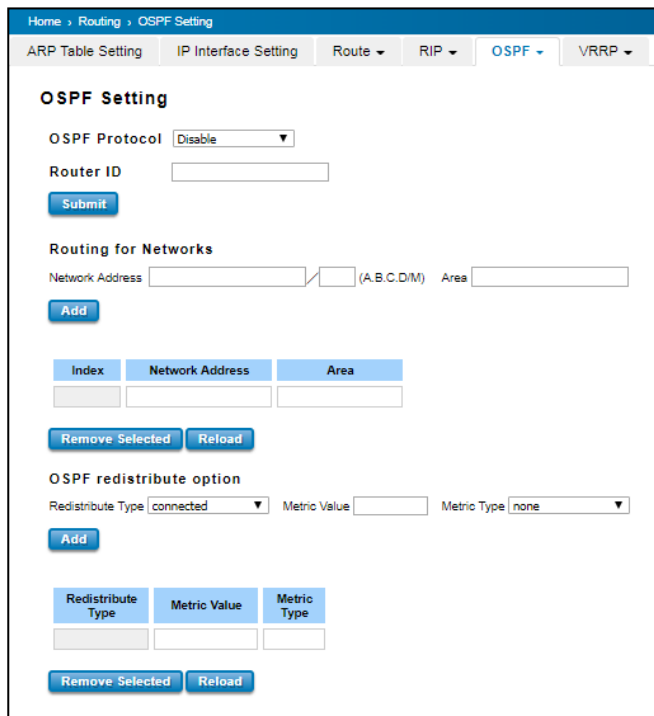
3.8.4. OSFP

Open Shortest Path First is a link-state protocol that equips the IP, mask, the type of network, the routers connected to that network. The State is its relationship to its neighboring routers. 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 switches. When compared with RIP (Routing Information Protocol) 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 ISP (Internet Service Provider) backbone and

enterprise networks.

The OSPF is a complex protocol which defines the role of the router/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. The routers within the same area update its routing table. Any change in routing information is flooded to all routers in the same area

Avcomm Layer3 Managed Switch design comforts to the OSPF Version 2 specification. Typically, the switch acts as the Internal Router, a router within the area; the Designated Router, the Master router in the same broadcast domain within the area; the Area Board Router which is the boundary router between different area. While configuring the OSPF network, the area ID should be configured with the same IP address or the same area ID.
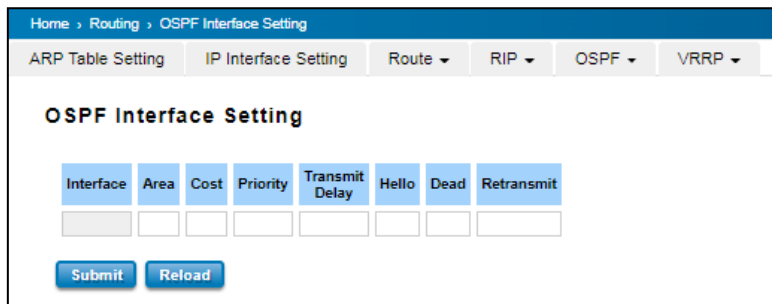
OSPF Setting

TERMS	DESCRIPTION
OSPF Protocol	**Enable** or **Disable** the OSFP 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.
Routing for Network	Type the **Network Address** and the **Area** ID in the field.

Click **Add** to apply the setting then the new entry will appear in the network table below. Click the **Remove Selected** button to remove the selected network. Click the **Reload** button to reload the table.

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

OSPF Interface Setting

TERMS	DESCRIPTION
Interface	The VLAN Interface name.
Area	The area ID of the 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 is identified depends on what the bandwidth is by the system. 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.

Once finish configuring the settings, click on "Apply" to apply configuration.

OSPF Area Setting

This page allows user to configure the OSPF Area information. 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 Avcomm Switch is usually installed as internal router of a single Area environment. While there are multiple areas in the network, this page allows modify the Area information and Virtual Link.

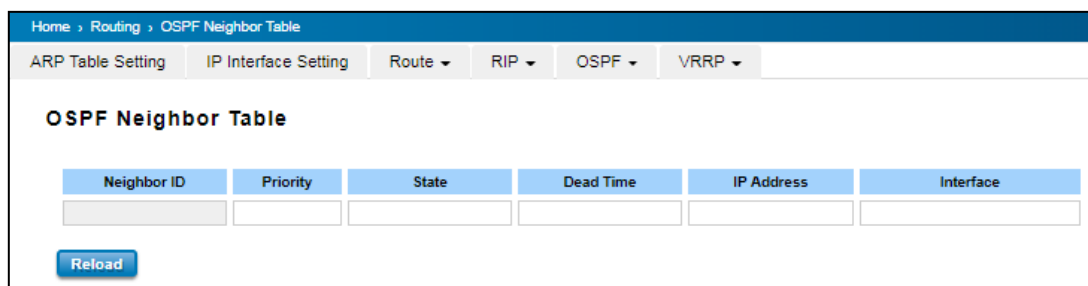
TERMS	DESCRIPTION
Area	This field indicates the area ID. Select the ID you want to modify here.
Default Cost	The default cost of the area ID.
Shortcut	No Defined, Disable, Enable. This indicates whether the area is the OSPF ABR shortcut mode.
Stub	Represents whether the specified Area is a stub area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

Click the **Apply** button to apply OSPF area settings. Click the **Remove Selected** button to remove selected area.

Click the **Reload** button to reload OSPF area configurations.

OSPF Neighbor Table

This page allows user to see the OSPF Neighbor information. The Neighbor interface and its state will be listed here.

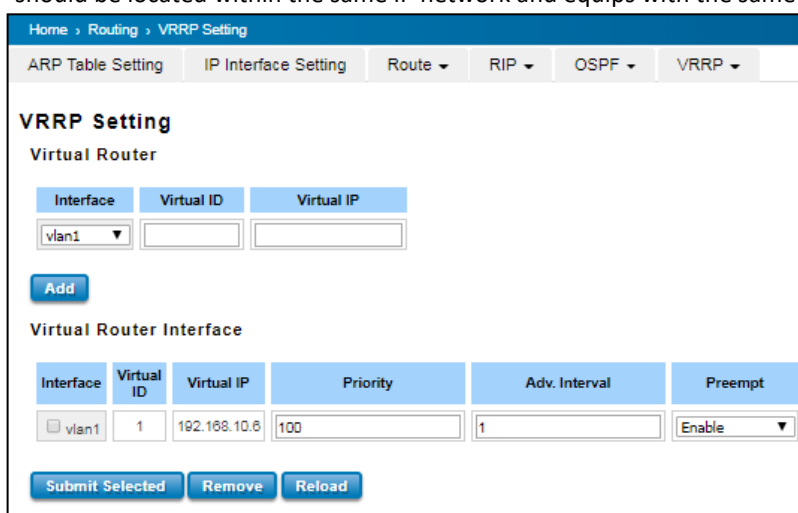| TERMS	DESCRIPTION
Neighbor ID	Display the Router ID of the Neighbor routers/switches.
Priority	Show the priority of the link.
State	While the **State** is changed to **Full**, which means the exchange progress is done.
Dead Time	The activated time of the link.
IP Address	Shows the learnt IP interface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

Click **Reload** to update the information from the table.

3.8.5. VRRP

A VRRP (Virtual Router Redundancy Protocol) 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

The fields allow you to create the Virtual Router Interface. All the layer 3 switches within the same VRRP domain should be located within the same IP network and equips with the same Virtual ID and Virtual IP address.

Virtual Router

TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain.
Virtual ID	This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

Click **Add** once finish the configuration. Then a new entry is created in the Virtual Router Interface Configuration page. After the VRRP interface is created, user can see the new entry and adjust the settings to decide the policy of the VRRP domain.
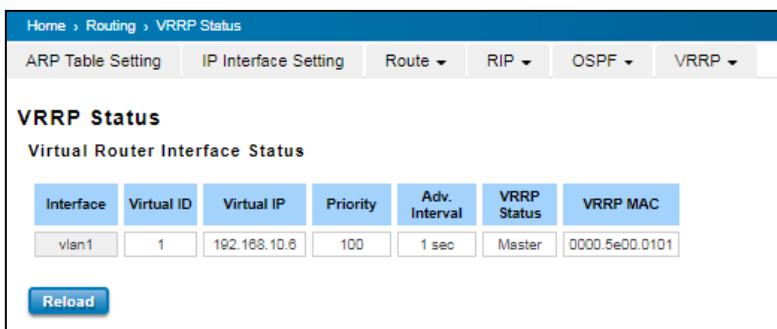
Virtual Router Interface

TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain.
Virtual ID	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.
Priority	The priority of the entry of this switch. In VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings and choose who should be the VRRP Master switch. The switch equips with the highest priority will be selected as the VRRP master. 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	While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who should be the Master? The Preempt decide whether the VRRP master should be recovered or not. While the Preempt is **Enable** and the interface is VRRP Master, the interface will be recovered. While 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 restart the switches.

Click the **Submit Selected** button to apply the configuration. Click the **Remove Selected** button to remove selected setting. Click the **Reload** button to reload table.

VRRP Status

The VRRP represent for the Virtual Router Redundancy Protocol. 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.

TERMS	DESCRIPTION
Interface	Select the interface for the VRRP domain.
Virtual ID	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.

Priority	The priority of the entry of this switch. In VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings and choose who should be the VRRP Master switch. The switch equips with the highest priority will be selected as the VRRP master. 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.
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.

3.8.6. Example: IP routing

Here is an example of how to start the IP Routing environment.

3.8.6.1.   IP Routing setting Example: Purpose/Question

The purpose is to let the two client PCs which are in different VLANs to communicate with each other. You can think the answer of below target environment, practice, and find the answer in next page.

IP Routing Setup Example - Purpose

VLAN Status (L3 Switch A)
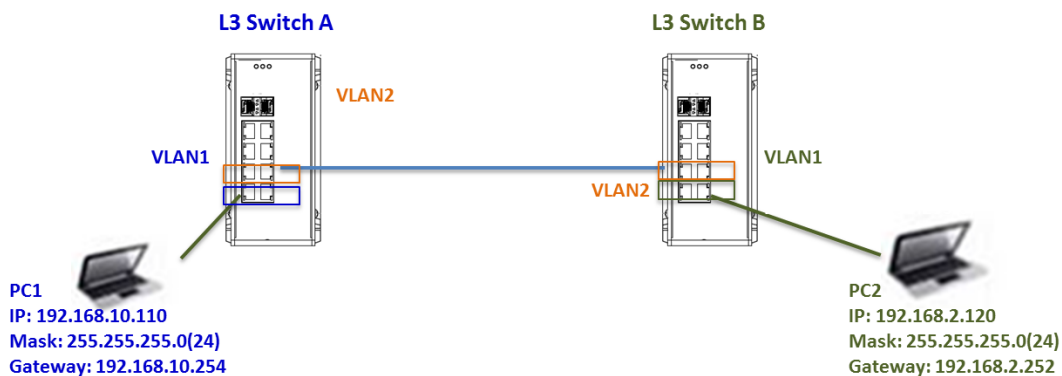
VLAN ID	Name	Status	1	2	3	4	5	6	7	8
1	VLAN1	Static	U	U	-	-	-	-	-	-
2	VLAN2	Static	-	-	U	U	-	-	-	-
3	VLAN3	Static	-	-	-	-	-	-	U	U

Reload

VLAN Status (L3 Switch B)

VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9
1	VLAN1	Static	U	U	-	-	U	U	U	U	U
2	VLAN2	Static	-	-	U	U	-	-	-	-	-

Reload

In above figure, the PC1 is connected to the member port of VLAN 1 in L3 Switch A. PC2 is connected to the member port of VLAN 1 in L3 Switch B. The VLAN ID is not concern in L3 environment.

First create the VLAN Interface and assign the member port to the VLAN before creating IP Interface, please refer to the VLAN Configuration page.

First create the IP Interface and assign the, please refer to the IP INTERFACE CHECKING configuration page.

For enable dynamic routing, you can configure RIP or OSPF, please refer to the RIP/OSPF configuration page.

3.8.6.2.   IP Routing setting Example: IP setting/Answers

IP Routing Setup Example – IP Settings

Apply IP address, Subnet Mask for the two VLANs and check the Route Table.

L3 Switch A:

The IP address/Subnet Mask of VLAN1: 192.168.10.254/24. This is also the IP address of PC1's default gateway.

The IP address/Subnet Mask of VLAN2: 192.168.1.254/24. This is the direct connect interface to Switch B.

The IP address/Subnet Mask of VLAN3: 192.168.20.254/24. This is just a non-active VLAN interface.

L3 Switch B:

The IP address/Subnet Mask of VLAN1: 192.168.2.252/24. This is also the IP address of PC2's default gateway.

The IP address/Subnet Mask of VLAN2: 192.168.1.252/24. This is the direct connect interface to Switch A.

Connect L3 Switch A and B through the IP subnet: 192.168.1.0/24. The IP address and subnet mask of the connected interface in Switch A and B Must be located within the same subnet.

If all the L3 interfaces are "direct connect" interface and the status is "UP", you can communicate with other PC in different VLANs without enable dynamic routing protocol.

If there are more L3 switch and some of VLAN interface are not directly connect, you can type Static Route or enable the dynamic Routing protocol, for example the RIP protocol. Below figure show how to enable the RIP protocol, you need to enable the RIP protocol for the connected IP interface of Switch A and B. Then the two L3 switch can exchange the information of their owned IP interfaces.

The figure shows the RIP Settings in L3 Switch A.
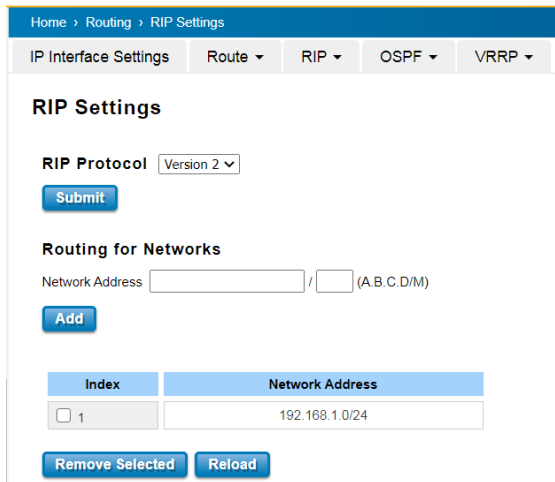
The figure shows the Route Table after RIP protocol enabled in Switch A. You can see the IP subnet 192.168.1.0/24 is direct connected in Switch A. The IP subnet 192.168.2.0/24 in Switch B is leant by RIP protocol.
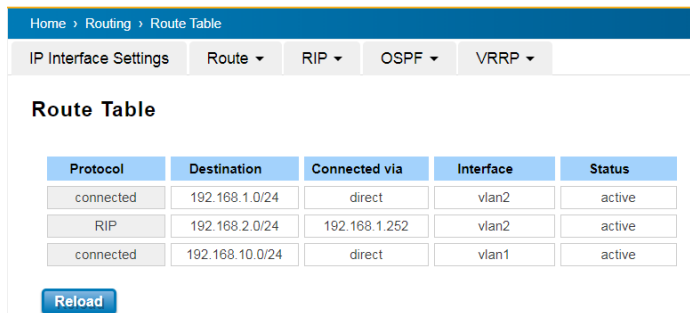
To check whether the setup is correctly, you can ping the directly connected interface first, and ping the other activated interfaces of the connected switch, and finally the IP of the destination PC. This is the common steps every time when you diagnostic the L3 network setting.

Example of PC1 in Switch A ping PC2 in Switch B: PC1 start ping the 192.168.10.254 first, then ping the 192.168.1.254, then ping the 192.168.1.252(connected interface of Switch B), then ping 192.168.2.252(active interface in switch B), then the destination PC2 192.168.2.120. You can see "Reply from 192.168.2.120…" It means the IP VLAN Routing setting is correctly.
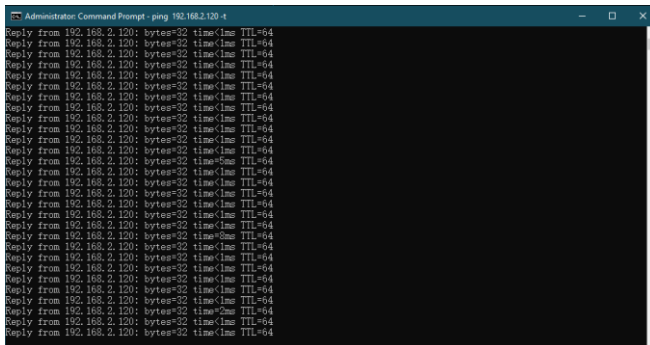
3.8.6.3. *IP Routing setting Example: Site to Site L3 network through Fiber Uplink*

Below figure simulate a site-to-site communication among the different machines. The Switch A is represented for machine A, Switch B is represented for machine B…etc. In this network, there are more IP interfaces, and they are connected through the Fiber optic link. The advantage is that the end customers are connected to different IP network, and they don't know each other, you can restrict connections by IP address, add IP based access control rule…etc. In this application, you must enable the L3 Route function for the switches.

There are some technical tips to configure such environment.

IP Routing Setup Example 2 – L3 Fiber Network
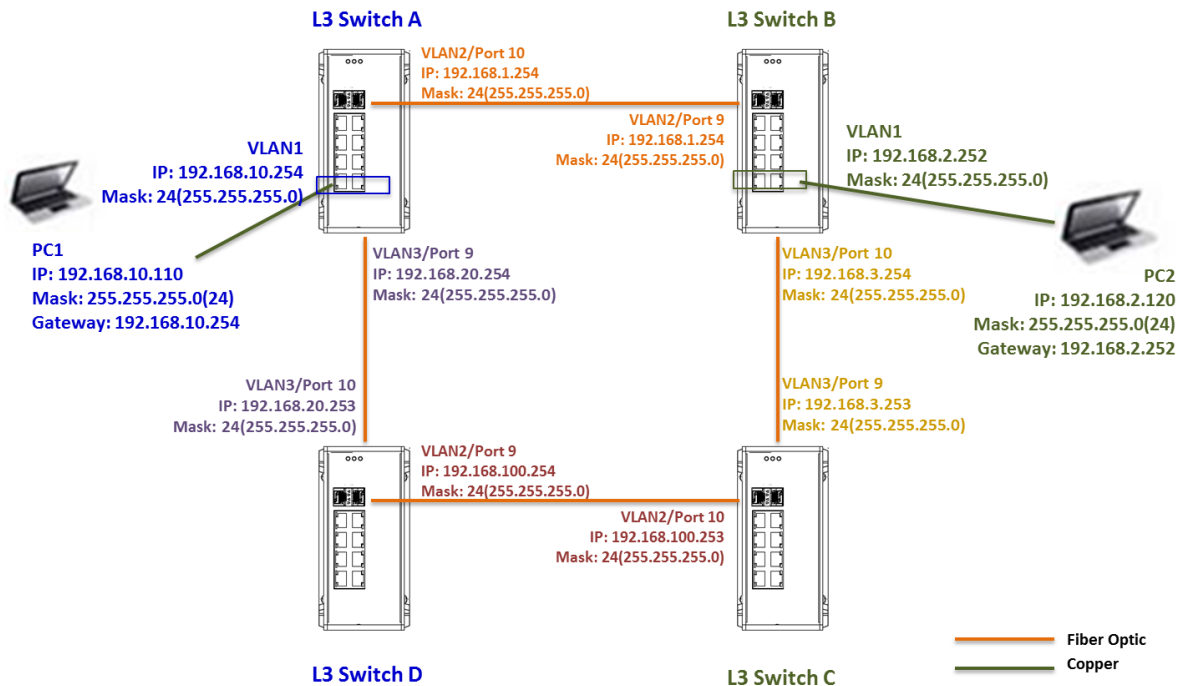
The IP interface is bind with VLAN. Configure member ports for each VLAN and apply the IP Interface for each VLAN. The setting should be applied to all client devices and Fiber uplink ports.

The IP address of each IP interfaces can Not be the same.

The connected IP interfaces between the 2 switches Must be located within the same subnet.

There are some non-direct connect interfaces, for example the Switch A do not know any IP interface setting of Switch C, you MUST enable the dynamic Routing protocol or configured the correct static IP route path for all switches.

To check whether the setup is correctly, you can ping the directly connected interface first, then ping the other activated interface of the connected switch, then ping the uplink interface and activated interfaces of the neighbor switch, step by step to ping the IP of the destination PC. If you find any Ping Reply Timeout, check the IP Interface Settings, Route Table status… Then you can find out the problem and resolve. This is the common steps every time when you diagnostic the L3 network setting.

The DS610/612 series supports maximum 64 available IP subnets, do not configure more than 64 IP subnets within the same network.

3.9. SNMP

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. Avcomm Managed Switch support SNMP v1 and v2c and V3.

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.

3.9.1. SNMP V1/V2c setting

In this page allows users to define the new community string set and remove the unwanted community string. The community string can be viewed as the password because SNMP V1/V2c doesn't request User to enter password before User tries to access SNMP agent. The community includes 2 privileges, Read Only and Read and Write.

PRIVILEGE	DESCRIPTION
Read Only	User only can read the values of MIB tables. Default community string is Public.
Read and write	User can read and set the values of MIB tables. Default community string is Private.

Avcomm Managed Switch allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Submit**.

NOTE: When User first installs the device in User network, we highly recommend user to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.

3.9.2. SNMP V3

SNMPv3 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.

SNMP V1/V2c   **SNMP V3**   SNMP Trap

SNMP V3

SNMP V3

User Name	[ ]
Security Level	None ▼
Authentication Level	MD5 ▼
Authentication Password	[ ]
DES Password	[ ]

Add

SNMP V3 Users

	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐						

Remove   **Reload**

TERMS	DESCRIPTION
Username	Set up the username.
Security Level	**Default: None** Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.
Authentication Level	**Default: MD5** MD5 (Message-Digest algorithm 5) is a widely used 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	Here the user enters the SNMP v3 user authentication password.
DES Password	Here the user enters the password for SNMP v3 user DES Encryption.

3.9.3. SNMP TRAP

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version. Below is the SNMP Trap Interface.

SNMP V1/V2c   SNMP V3   **SNMP Trap**

SNMP Trap

SNMP Trap [Disable ▼]

[Submit]

SNMP Trap Server

Server IP [   ]

Community [   ]

Version [V1 ▼]

[Add]

Trap Server Profile

	Server IP	Version	Community

[Remove] [Reload]

TERMS	DESCRIPTION
SNMP Trap	**Default: Disable** Enable / Disable SNMP Trap
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.

After configuration, Click **Add** then User can see the change of the SNMP pre-defined standard traps.

3.10. Security

Avcomm Switch provides several security features for User to secure access to its management functions and it can be remotely managed (monitored and configured).
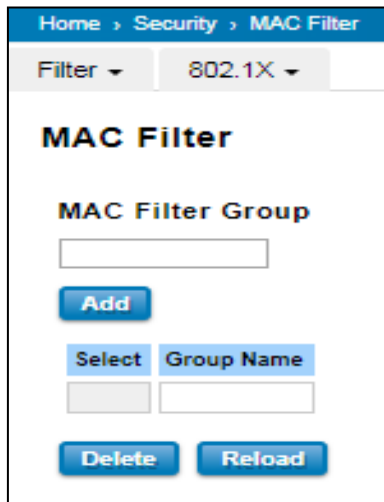
3.10.1. Filter

Filter is known as Access Control List feature. There are 2 major types; one is MAC Filter that allows user to define the access rule based on the MAC address flexibility. Another one is IP Filter. It includes the IP security, IP Standard access list and advanced IP based access lists.

MAC Filter
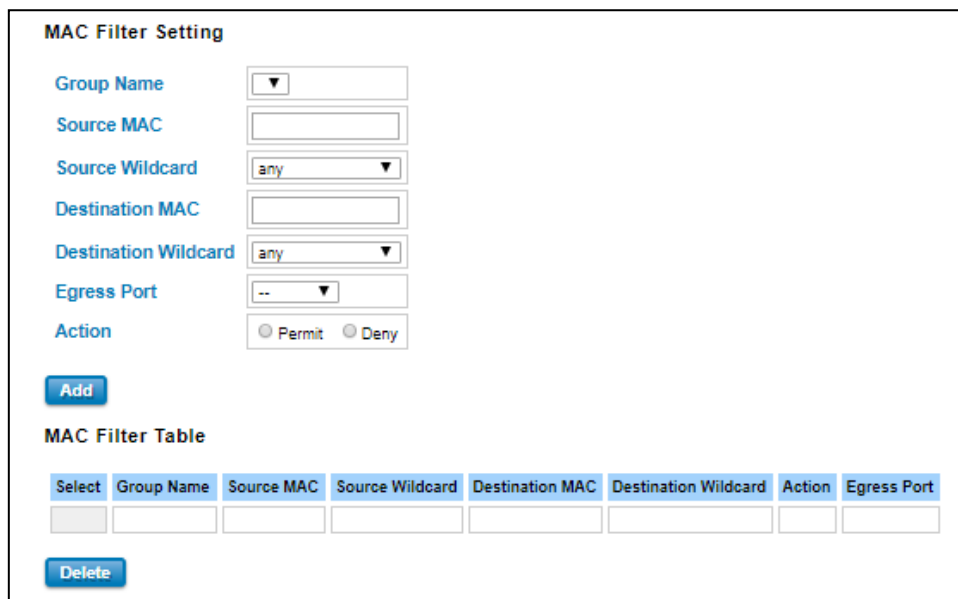
Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. Mac Filter feature allows User to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in the list can access the switch and transmit/receive traffic. This is a simple way to secure User network environment and not to be accessed by hackers.

MAC Filter Group

Create a group of MAC Filters by entering a name and clicking the **Add** button to create a new Filter Group. The MAC Filter Group table provides the following information. **Select** the entry and click the **Delete** button then the Filter Group is deleted. Click the **Reload** button to reload the MAC Filter Group table.

MAC Filter Setting
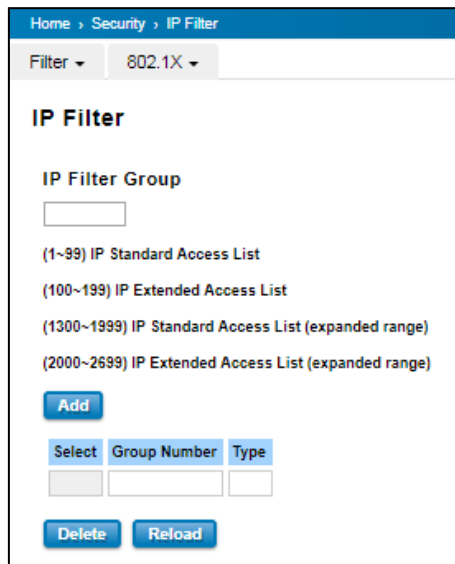
In this form user may configure the MAC Filter Setting. The description of the columns is as below:

TERMS	DESCRIPTION
Group Name	This is the name of the MAC Filter Group.
Source MAC	This is the source MAC Address of the packet.
Source Wildcard	This is the mask of the MAC Address.
Destination MAC	This is the destination MAC Address of the packet.
Destination Wildcard	This is the mask of the MAC Address.
Egress Port	This is 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.

Once User finishes configuring the settings, click on **Submit/Add** to apply User configuration.

IP Filter

User can create a group of IP Filters with following numbers.
1 - 99: IP Standard Access List
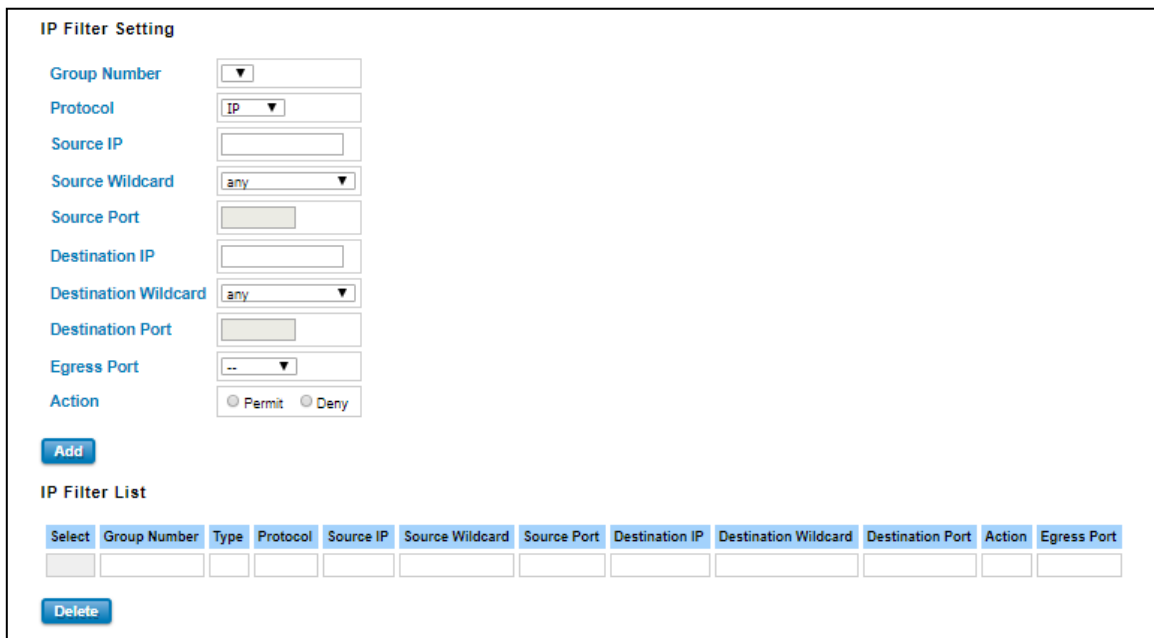
100 – 199: IP Extended Access List

1300 – 1999: IP Standard Access List (expanded range)

2000 – 2699: IP Extended Access List (expanded range)

After entering the IP Filter Group number, click the **Add** to create the new Filter Group.

IP Filter Setting

TERMS	DESCRIPTION
Group Number	Number of the Filter Group.
Protocol	This is the L4 protocol (IP/TCP/UDP/ICMP).
Source IP	This is the source IP address of the packet.
Source Wildcard	This is the mask of the IP address.
Source Port	This is the source port of L4 protocol (TCP/UDP)
Destination IP	This is the destination IP address of the packet.
Destination Wildcard	This is the mask of the IP address.

Destination Port	This is the destination port of L4 protocol (TCP/UDP).
Egress Port	This is 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.

IP Filter List

TERMS	DESCRIPTION
Select	Selected the entry for delete.
Group Number	Number of the Filter Group.
Type	This is the filter group type (standard or extended).
Protocol	This is the L4 protocol (IP/TCP/UDP/ICMP).
Source IP	This is the source IP address of the packet.
Source Wildcard	This is the mask of the IP address.
Source Port	This is the source port of L4 protocol (TCP/UDP)
Destination IP	This is the destination IP address of the packet.
Destination Wildcard	This is the mask of the IP address.
Destination Port	This is the destination port of L4 protocol (TCP/UDP).
Action	This is the filter action, which is to deny or permit the packet. Click the **Delete** button to remove the Filter that has been selected.
Egress Port	This is the outgoing (exiting) port number.

Filter Attach

This page allows you to attach filters created on the IP Filter and MAC Filter pages to ports on the switch.

TERMS	DESCRIPTION
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.

Click the **Submit** button to apply the configurations.

Filter Attach List

This table displays what filters are currently attached to each port.

Filter Attach List

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

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

3.10.2. 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. This provides greater visibility into the network. 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. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. 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 performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, Avcomm switch could control which connection is available or not.

802.1X Setting

System Auth Control [Disable ▾]

Authentication Method [RADIUS ▾]

[Submit]

RADIUS Server

RADIUS Server IP: 192.168.10.100

Shared Key: radius-key

Server Port: 1812

Accounting Port: 1813

Secondary RADIUS Server

RADIUS Server IP: [   ]

Shared Key: [   ]

Server Port: [   ]

Accounting Port: [   ]

[Submit]

Local RADIUS User

User Name	Password	VID

[Submit]

Local RADIUS User List

User	Name	Password	VID

[Delete]

The description of the columns is as below:

TERMS	DESCRIPTION
System Auth Control	To enable or disable the 802.1X authentication.
Authentication Method	Radius is an authentication server that provide key for authentication, with this method, user must connect switch to server. If user selects Local for the authentication method, switch use the local user data base which can be created in this page for authentication.
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	Here User can add Account/Password for local authentication.
802.1X Local User List	This is a list shows the account information; User also can remove selected account.

802.1X Port Setting

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.

The description of the columns is as below:

TERMS	DESCRIPTION
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.
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.

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

802.1X Port Status

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

Home › Security › 802.1X Port Status

Filter ▾   802.1X ▾

802.1X Port Status

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

Reload

3.10.3. DHCP snooping

DHCP snooping is a security feature of DHCP and is mainly applied to switches.
The purpose of DHCP Snooping is to block illegal DHCP servers in the access network. That is, after the DHCP Snooping function is enabled, clients on the network can only obtain IP addresses from the DHCP server specified by the administrator. Due to the lack of authentication mechanism in DHCP protocol, if there is an illegal DHCP server in the network, the administrator will not be able to guarantee that the client obtains a legal address and the client may obtain the wrong IP address from the illegal DHCP server.

The description of the column is as below:

TERMS	DESCRIPTION
DHCP Snooping	Enable the DHCP Snooping function.
MAC Verify	Enable MAC Verify to start checking.
DHCP Snooping VLAN Setting	Enable DHCP Snooping for specific VLAN interface. DHCP Snooping should be enabled first then it's available to Enable the DHCP Snooping for specific VLAN.
DHCP Snooping Statistics	The column shows the Drop Type and Drop Packets. It can help you check the status of your environment.

DHCP Snooping Binding

The Static Entry in DHCP Snooping Binding table allows to add tracking the specific IP Address and MAC Address for specific VLAN ID and LAN port. The DHCP Snooping Binding List table includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on untrusted switch ports. The Trust/Untrust port setting can be configured in IP Source Guard page.

DHCP Snooping Binding

Add Static Entry

IP Address	192.168.10.253
MAC Address	9466.E700.0002
VLAN	1 ▾
Interface	Port 8 ▾

Submit

DHCP Snooping Binding List

Select	MAC Address	IP Address	Lease Time	VLAN	Interface	Type
☐	9466.e700.0002	192.168.10.253	0	1	Port 8	static

Remove Selected   Reload

DHCP Snooping Write Interval

Interval	300	(secs)
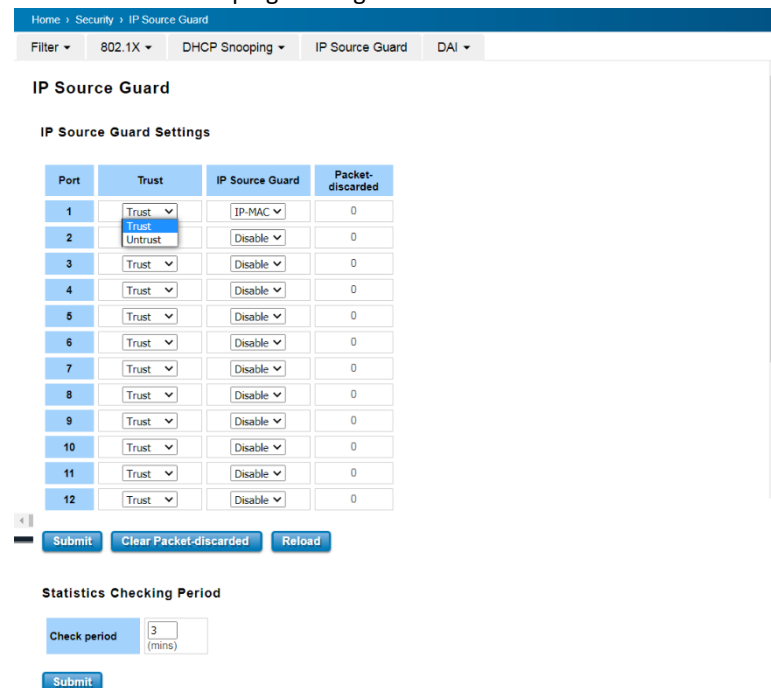
Submit

The description of the column is as below:

TERMS	DESCRIPTION
IP Address	Type the IP address to bind the MAC Address of selected server.
MAC Address	Type the MAC address of the selected IP Address. The format should be like '0060.b312.3456'.
VLAN	Select the VLAN you'd like to apply.
Interface	Select the Port (LAN port) you'd like to apply.
DHCP Snooping Write Interval	Default: 300 secs

3.10.4. IP source guard

IP source guard can prevent the illegal use of IP by others, which is also a headache for many network managers. IP Source Guard is a security feature that restricts IP/IP-MAC traffic on untrusted L2 LAN ports by filtering traffic based on the DHCP snooping binding database.

The description of the column is as below:

TERMS	DESCRIPTION
Trust	Select Trust/Untrust for each LAN port.
IP Source Guard	Select the Filter Type of IP or IP-MAC traffic.
Packet-discarded	The entry shows the discarded packet count of the port. You can manually click "Reload" to update the count. Or the system will update it based on the time of Statistic Checking Period.
Statistics Checking Period	It's the time to update the count of discarded traffic.

3.10.5. Dynamic ARP inspection (DAI)

DAI (Dynamic ARP Inspection) provides IP address and MAC address binding on the switch and dynamically establishes a binding relationship. DAI is based on the DHCP Snooping binding table. For individual machines that do not use DHCP, you can use statically added ARP access-list. The DAI configuration is for VLANs. For interfaces in the same VLAN, DAI can be enabled or disabled. DAI can control the number of ARP request packets on a certain port. With this configuration, the problem of ARP attacks can be solved, and network security and stability can be better improved.

The description of the column is as below:

TERMS	DESCRIPTION
VLAN	Display the VLAN ID.
Configuration	Enable or disable the DAI of the VLAN
Operation	Display the DAI operation state of the VLAN
Gateway Verify	Enable/Disable verify the Gateway
Gateway IP	Assign the target IP of Gateway Verify
ACL-Match	Select the target ARP filter rule. Need to set the rule in ARP Filter.

		VLAN	Configuration	Operation	Gateway Verify	Gateway IP	ACL-Match
		1	Enable ▼	Active	Enable ▼	192.168.10.1	▼
		2	Disable ▼	Inactive	Disable ▼	0.0.0.0	test

Interface Configuration Port	The LAN Port ID
Trust	Select Trust/Untrust for each LAN port.
Rate	Configure the DAI rate limit of incoming ARP packets
Statistic Checking Period	It's the time to update the count of DAI Statistics.

ARP Filter

Add the ARP Filter Name and then apply the ARP Filter Rule for it. Then you can see the Name/Rules in ARP Filter List table.

The description of the column is as below:

TERMS	DESCRIPTION
ARP Filter Group/Filter	Type "Name" of ARP Filter and click "Add". The entry can be added in ARP Filter Group.
ARP Filter Rule Setting/Filter	Select the ARP Filter Entry then assign the parameters in below columns.
Action	Permit or deny
Source IP	Configure specific IP Address for the rule.

	Blank/Any: All the coming source IP address.
Source MAC	Configure specific MAC Address for the rule. Blank/Any: All the coming source IP address.
Destination IP	Configure specific IP Address for the rule. Blank/Any: All the coming source IP address.
Destination MAC	Configure specific MAC Address for the rule. Blank/Any: All the coming source IP address.
Egress Port	Select the target Egress Port for the ARP Filter Entry.

Dynamic ARP Inspection Statistics

Below figures display the statistics of the Interface and VLAN for your reference. With the info, it can help you identify the overall status of the connected port and VLAN, this is used for network security diagnostic.

Dynamic ARP Inspection Statistics

Interface Statistics

Port	Received	Forwarded	Dropped	Invalid IP	Mismatch MAC	DHCP Dropped	Invalid GW IP	Invalid Opcode	Mismatch Src Port	No Dst Port	ACL Dropped
1	386	0	386	0	0	0	0	0	0	0	386
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0

[Clear Statistics] [Reload]

VLAN Statistics

VLAN	Forwarded	Dropped	DHCP Dropped	ACL Dropped	DHCP Permits	ACL Permits	Source MAC Dropped	Source MAC Dropped	Destination MAC Dropped	Invalid IP
1	0	386	0	386	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0

[Clear Statistics] [Reload]

3.11. Warning

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

3.11.1. Relay output

Avcomm switch provides 1 alarm relay output, also known as Digital Output. These settings in Relay Output section control the events that will trigger the alarm output. The OK 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 Output configuration interface has shown as below:

The condition or term described as following table.
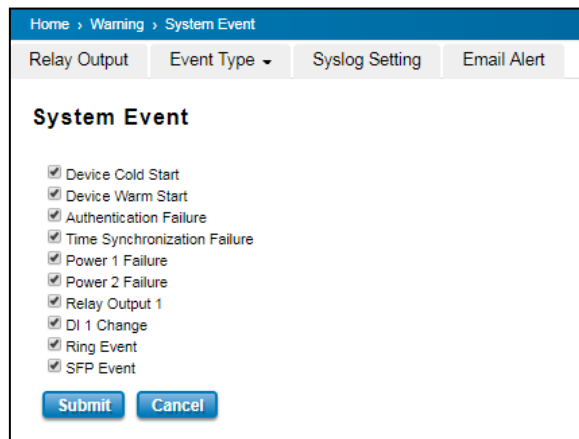
TERMS	CONDITION	DESCRIPTION
Power Failure	Power ID 1 Power ID 2 Any	Detect power input status. If one of condition occurred, relay triggered.
Link Failure	Port number	Monitoring port link down event
Ring	Ring failure	If ring topology changed
Ping Failure 1	**IP Address:** remote device's IP address.	If target IP does not reply ping request, then relay 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. Note: 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	Relay trigger when DI states change to Hi or Low

	1 DI)	

The relay supports multiple event trigger function; click and select type of event and setting the detail information, and then clicks **Submit** to activate the relay alarm function.

3.11.2. 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
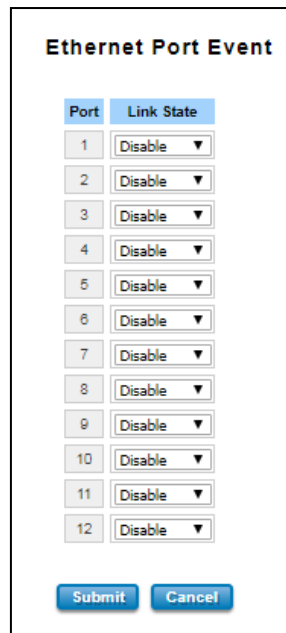
Once User finishes configuring the settings, click on Submit to apply User configuration.

The description of the columns is as below:

System Event Selection	Warning Event is sent when…..
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	The power input is failure.
Relay Output 1	The Digital Output is on.
DI 1 Change	The Digital Input change
Ring Event	Ring Status has changed, or backup path is activated.
SFP Event	The SFP transceiver's state is abnormal.
Port Event	**Warning Event is sent when….**
Up	The port is connected to another device
Down	The port is disconnected (e.g., the cable is pulled out, or the opposing devices turns down)
Both	The link status changed.

3.11.3. Syslog setting

System Log can provide the switch events history by locally or remotely monitor. There are 3 System Log modes provided by the switch, local mode, remote mode and both.

Local Mode: In this mode, the device will print the selected events in the Event Selection page to System Log table of the switch.
Remote Mode: In this mode, User should assign the IP address of the System Log server. Then the selected occurred events will be sent to System Log server User assigned.
Both: Above 2 modes can be enabled at the same time.
Once User finishes configuring the settings, click on **Submit** to apply User configuration.

3.11.4. Email alert

Avcomm switch provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). 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. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system. On this page, you can configure SMTP servers and the four corresponding e-mail addresses.

The description of the columns is as below:

TERMS	DESCRIPTION
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
Username	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
User can set up to 4 email addresses to receive email alarm from the switch	
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)

Once User finishes configuring the settings, click on **Submit** to apply User configuration.
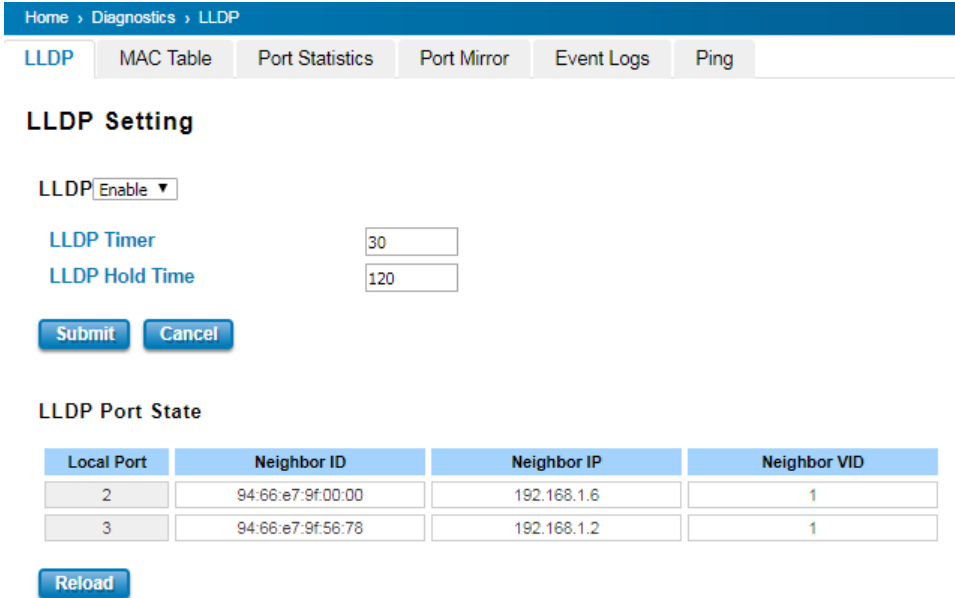
3.12.   Diagnostics

Avcomm Switch provides several types of features for User to monitor the status of the switch or diagnostic for User to check the problem when encountering problems related to the switch.

3.12.1. 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 Avcomm managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP. From the switch's web interface, User can enable or disable LLDP, and User can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows to automatically display the neighbor ID and IP leant from the connected devices.

The configuration and settings explain as following.

TERMS	DESCRIPTION
LLDP	Select to enable/disable LLDP function.
LLDP Timer	**Default: 30 seconds** The interval time of each LLDP and counts in second; the valid number is from 5 to 254.
LLDP Hold time	**Default: 120 seconds** The TTL (Time to Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time.
Local port	The 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.

3.12.2. MAC table

In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Submit** to change the value.

Aging Time (Sec)

Each switch Fabric has limit size to write the learnt MAC address. To save more entries for 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. The Aging Time can be modified in this page.

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

MAC Address Table

Aging Time(secs) [300]

[Submit]

Static Unicast MAC Address

In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, User can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.

Static Unicast MAC Address

MAC Address	VID	Port
		Port 1 ▼

[Add]

MAC Address Table

At this table, all the MAC Addresses learnt by the switch will be shown here. Use the MAC address table to ensure the port security. The MAC Address Table can be displayed based on the MAC Address Type and based on the Port.

MAC Address Table [All ▼]

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
☐ 708b.cd03.b567	Dynamic Unicast	1	V									
☐ 0100.5e00.00fb	Dynamic Multicast	1	V									
☐ 0100.5e00.00fc	Dynamic Multicast	1	V									
☐ 0100.5e7f.fffa	Dynamic Multicast	1	V									

[Remove] [Reload]

Click on **Remove** to remove the selected static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

3.12.3. Port statistics

This page displays the number of error packets that is received and sent from the port. This level of detail is not available from the Dashboard graphs. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.

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

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
☐ 1	100	Connected	Enable	155947	0	94	1628434	0	0
☐ 2	100	Connected	Enable	2598107	0	52	1740950061	0	0
☐ 3	0	Disconnected	Enable	151722118	0	3841	22607856	1	0
☐ 4	1000	Connected	Enable	849857338	0	8	857672721	4	0
☐ 5	0	Disconnected	Enable	0	0	0	0	0	0
☐ 6	0	Disconnected	Enable	984	0	0	192	0	0
☐ 7	0	Disconnected	Enable	0	0	0	0	0	0
☐ 8	0	Disconnected	Enable	867764923	0	8	868123192	0	0
☐ 9	0	Disconnected	Enable	0	0	0	0	0	0
☐ 10	0	Disconnected	Enable	0	0	0	0	0	0
☐ 11	0	Disconnected	Enable	0	0	0	0	0	0
☐ 12	0	Disconnected	Enable	0	0	0	0	0	0

Clear Selected   **Clear All**   **Reload**

Click on **Clear Selected** to reinitialize the counts of the selected ports and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

3.12.4. Port mirror

Port mirroring is a tool that allows User to monitor data that being transmitted through a specific port. User can use this feature for diagnostics, debugging, and any kind of analysis. This is done by setting up another port (the mirror port) to receive the same data being 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. All of the traffics at the Destination port can be analyzed using a monitoring tool.

The configuration and settings explain as following.

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

Port Mirror

Port Mirror [Disable ▼]

Port	Source Port		Destination Port
	Rx	Tx	
1	☐	☐	◯
2	☐	☐	◯
3	☐	☐	◯
4	☐	☐	◯
5	☐	☐	◯
6	☐	☐	◯
7	☐	☐	◯
8	☐	☐	◯
9	☐	☐	◯
10	☐	☐	◯
11	☐	☐	◯
12	☐	☐	◯

Submit

TERMS	DESCRIPTION
Port Mirror	Select Enable/Disable to enable/disable Port Mirror.

AVCOMM technologies Inc.   www.avcomm.us   333 West Loop N, St 460, Houston, TX 77024

Source Port	These are the ports that User wants to monitor. The traffic of all source ports will be duplicated to destination ports. User can choose a single port, or multiple ports. Click on checkbox of the Port ID, RX, Tx, or Both to select the source ports.
Destination Port	User can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port being monitored. Only one RX/TX of the destination port can be selected.

Once User finishes configuring the settings, click on **Submit** to apply the settings.

3.12.5. Event logs

This event logs page will show and record the system events log.

Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.
The description of the columns is as below:

TERMS	DESCRIPTION
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.

3.12.6. Ping

Avcomm' provides **Ping** utility in the management interface, the function is to give users a simple but powerful tool for troubleshooting network problems and check that the remote device is still alive or not.
Type **Destination** IP address of the target device and click on **Ping** to start the ping.

3.13. Industrial

Avcomm Switch's latest firmware provides Industrial Modbus features for User to monitor the status of the switch by Modbus TCP protocol. For example, user can add the switch to their HMI dashboard and monitor the status by Modbus Read register.

Home › Indistrial › Modbus TCP

Modbus TCP

Modbus TCP

Status	Disable ▾
Listening Port	502
Max Modbus TCP Master/Client	10
Idle Timeout (ms)	3000

Submit

The description of the columns is as below:

TERMS	DESCRIPTION
Status	Select Enable/Disable to enable/disable Modbus TCP.
Listening Port	Set the TCP port for listening Modbus TCP message. The range of the number is 1 to 65535. The default is **502**.
Max Modbus TCP Master/Client	Set the maximum Modbus TCP Master/Client connection. The default is **10**.
Idle Timeout(ms)	Set the Idle Timeout for the Modbus TCP connection. The default=**3000ms**

Note: The value of Modbus TCP table in below is for reference example, different model may have different product name, description, system name…etc. Some of the new settings may be updated without earlier notice.

Run Modbus TCP poll tool to see the latest values or contact our technical window for up to date info.

The following table shows the Modbus TCP table Example:

Word Address	Data Type	Description
System Information		
0x0000	32 words	Product Name = "8010GX2" (*Depends on product name) Word 0 Hi byte = '8' Word 0 Lo byte = '0' Word 1 Hi byte = '1' Word 1 Lo byte = '0' Word 2 Hi byte = 'G'

		Word 2 Lo byte = 'X'
		Word 3 Hi byte = '2'
		….
		(Other words = 0)
0x0020	256 words	Product Description = " Industrial Managed Ethernet Switch" (*Depends on product description) Word 0 Hi byte = 'I' Word 0 Lo byte = 'n' Word 1 Hi byte = 'd' Word 1 Lo byte = 'u' Word 2 Hi byte = 's' Word 2 Lo byte = 't' Word 3 Hi byte = 'r' Word 3 Lo byte = 'i' Word 4 Lo byte = 'a' Word 4 Hi byte = 'l' ….. Word 14 Lo byte = 'S' Word 14 Hi byte = 'w' Word 15 Lo byte = 'i' Word 15 Hi byte = 't' Word 16 Lo byte = 'c' Word 16 Hi byte = 'h' Word 17 Lo byte = '\0' (Other words = 0)
0x0120	128 words	SNMP system name (string)
0x01A0	128 words	SNMP system location (string)
0x0220	128 words	SNMP system contact (string)
0x02A0	32 words	SNMP system OID (string)
0x02C0	2 words	System uptime (unsigned long)
0x02C2 to 0x02FF	62 words	Reserved address space
0x0300	2 words	Boot loader version

		Word 0 Hi byte = first number of version
		Word 0 Lo byte = second number of version
		Word 1 Hi byte = third number of version
		Word 1 Lo byte = fourth number of version
		Version = v1.0.3.0
		Word 0 Hi byte = 0x1
		Word 0 Lo byte = 0x0
		Word 1 Hi byte = 0x3
		Word 1 Lo byte = 0x0
0x0302	2 words	Firmware Version
		Word 0 Hi byte = first number of version
		Word 0 Lo byte = second number of version
		Word 1 Hi byte = third number of version
		Word 1 Lo byte = fourth number of version
		Ex: Version = v1.2
		Word 0 Hi byte = 0x1
		Word 0 Lo byte = 0x2
		Word 1 Hi byte = 0x0
		Word 1 Lo byte = 0x0
		Version = v1.2.3
		Word 0 Hi byte = 0x1
		Word 0 Lo byte = 0x2
		Word 1 Hi byte = 0x3
		Word 1 Lo byte = 0x0
		Version = v1.2.3.4
		Word 0 Hi byte = 0x1
		Word 0 Lo byte = 0x2
		Word 1 Hi byte = 0x3
		Word 1 Lo byte = 0x4
0x0304	2 words	Firmware Release Date
		Firmware was released on 2018-08-11 at 09 o'clock
		Word 0 = 0x0B09
		Word 1 = 0x1208

0x0306	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x0309 to 0x3FF	247 words	Reserved address space
0x0400	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0402	2 words	Subnet Mask
0x0404	2 words	Default Gateway
0x0406	2 words	DNS Server
0x0408 to 0x04FF	248 words	Reserved address space (IPv6 or others)
0x0500	1 word	Power1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0501	1 word	Power2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0502	1 word	Power3 0x0000:Off 0x0001:On 0xFFFF: unavailable

0x0503	1 word	Power4 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0504 to 0x050F	12 words	Reserved address space
0x0510	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0511	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0512	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0513	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0514 to 0x051F	12 words	Reserved address space
0x0520	1 word	SYS LED (Green light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0521	1 word	SYS LED(Yellow light) 0x0000:Off 0x0001:On

		0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0522	1 word	R.S. LED (Green light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0523	1 word	R.S. LED (Yellow light) 0x0000:Off 0x0001:On 0x0002: blinking 0x0003: blinking fast 0xFFFF: unavailable
0x0524 to 0x0BFF	1756 words	Reserved address space
Port Information (32 Ports)		
0x1000 to 0x101F	1 word	Operating Status 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1020 to 0x103F	1 word	Speed/Duplex 0x0000: 10M-Half 0x0001: 10M-Full 0x0002: 100M-Half 0x0003: 100M-Full 0x0004: 1000M-Half 0x0005: 1000M-Full 0xFFFF: No port
0x1040 to	1 word	Flow Control

0x105F		0x0000: off
		0x0001: on
		0xFFFF: No port
0x1060 to 0x107F	1 word	MDI/MDIX
		0x0000: MDI
		0x0001: MDIX
		0xFFFF: No port
0x1080 to 0x109F	1 word	Medium mode
		0x0000: copper
		0x0001: fiber
		0x0002: none
		0xFFFF: No port
0x10A0 to 0x10BF	1 word	STP Status
		0x0000: disabled
		0x0001: blocking
		0x0002: listening
		0x0003: learning
		0x0004: forwarDINg
		0xFFFF: No port
0x10C0 to 0x14BF	32 words	Port Description
Packet information (32 Ports)		
0x2000 to 0x203F	2 words	Tx Packets
		Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x44332211
		Word 0 = 4433
		Word 1 = 2211
0x2040 to 0x207F	2 words	Rx Packets
		Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211
		Word 0 = 4433
		Word 1 = 2211
0x2080 to 0x20BF	2 words	Tx Error Packets

		Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x20C0 to 0x20FF	2 words	Rx Error Packets Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response: 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2100 to 0x2BFF	2816 words	Reserved address space
0x2C00	1 words	Clear ROMN by bitmap of port 1 to 16 Write to clear Read to return 0x0000 To clear port 1 Word = 0x0001 To clear port 1 and 2 Word = 0x0003
0x2C01	1 words	Clear ROMN by bitmap of port 17 to 32 Write to clear Read to return 0x0000 To clear port 17 Word = 0x0001 To clear port 17 and 18 Word = 0x0003
Network Redundancy Information		
0x3000	1 word	Ring 0's Status 0x0000: none 0x0001: Disable 0x0002: Enable 0xFFFF: unavailable
0x3001	1 word	Ring 0's Version 0x0000: none

		0x0001: v1
		0x0002: v2
		0xFFFF: unavailable
0x3002	1 word	Ring 0's Node State
		0x0000: Disabled
		0x0001: Initial
		0x0002: Idle
		0x0003: Protection
		0x0004: Manual Switch
		0x0005: Forced Switch
		0x0006: PenDINg
		0xFFFF: unavailable
0x3003	1 word	Ring 0's Ring Type
		0x0000: none
		0x0001: Major Ring
		0x0002: Sub Ring
		0xFFFF: unavailable
0x3004	1 word	Ring 0's Node Role
		0x0000: none
		0x0001: Ring node
		0x0002: RPL Owner
		0x0003: RPL Neighbor
		0xFFFF: unavailable
0x3005	1 word	Ring 0's Control Channel
0x3006	1 words	Ring 0's Sub Ring without Virtual Channel
		0x0000: none
		0x0001: True
		0x0002: False
		0xFFFF: unavailable
0x3007	1 word	Ring 0's Virtual Channel of Sub Ring

0x3008	1 word	Ring 0's Ring Port 0 0x0000: none 0x0001: port 1 0x0002: port 2 … 0x001C: port 28 0xFFFF: unavailable
0x3009	1 word	Ring 0's Ring Port 1 0x0000: none 0x0001: port 1 0x0002: port 2 … 0x001C: port 28 0xFFFF: unavailable
0x300A	1 word	Ring 0's Ring Port 0 state 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x300B	1 word	Ring 0's Ring Port 1 state 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x300C	1 word	Ring 0's Ring Port 0 RMEP ID 0x0000: none 0x0001: RMEP ID = 1 0x0002: RMEP ID = 2 … 0x1FFF: RMEP ID = 8191 0xFFFF: unavailable

0x300D	1 word	Ring 0's Ring Port 1 RMEP ID 0x0000: none 0x0001: RMEP ID = 1 0x0002: RMEP ID = 2 … 0x1FFF: RMEP ID = 8191 0xFFFF: unavailable
0x300E	1 word	Ring 0's RPL port 0x0000: RPL port = Ring port 0 0x0001: RPL port = Ring port 1 0xFFFF: unavailable
0x300F	1 word	Ring 0's Revertive Mode 0x0000: Revertive 0x0001: non-Revertive 0xFFFF: unavailable
0x3010	1 word	Ring 0's Instance
0x3011	1 word	Ring 0's Manual Switch 0x0000: Manual Switch port = Ring port 0 0x0001: Manual Switch port = Ring port 1 0x0001: Manual Switch port = none 0xFFFF: unavailable
0x3012	1 word	Ring 0's Force Switch 0x0000: Force Switch port = Ring port 0 0x0001: Force Switch port = Ring port 1 0x0001: Force Switch port = none 0xFFFF: unavailable
0x3013 to 0x301F	13 words	Reserved address space
0x3020 to 0x303F		ERPS Ring 1's Information
0x3040 to		ERPS Ring 2's Information

0x305F		
0x3060 to 0x307F		ERPS Ring 3's Information
0x3080 to 0x309F		ERPS Ring 4's Information
0x30A0 to 0x30BF		ERPS Ring 5's Information
0x30C0 to 0x30DF		ERPS Ring 6's Information
0x30E0 to 0x30FF		ERPS Ring 7's Information
0x3100 to 0x311F		ERPS Ring 8's Information
0x3120 to 0x313F		ERPS Ring 9's Information
0x3140 to 0x315F		ERPS Ring 10's Information
0x3160 to 0x317F		ERPS Ring 11's Information
0x3180 to 0x319F		ERPS Ring 12's Information
0x31A0 to 0x31BF		ERPS Ring 13's Information
0x31C0 to 0x31DF		ERPS Ring 14's Information
0x31E0 to 0x31FF		ERPS Ring 15's Information
0x3200 to 0x321F		ERPS Ring 16's Information
0x3220 to 0x323F		ERPS Ring 17's Information
0x3240 to		ERPS Ring 18's Information

0x325F		
0x3260 to 0x327F		ERPS Ring 19's Information
0x3280 to 0x329F		ERPS Ring 20's Information
0x32A0 to 0x32BF		ERPS Ring 21's Information
0x32C0 to 0x32DF		ERPS Ring 22's Information
0x32E0 to 0x32FF		ERPS Ring 23's Information
0x3300 to 0x331F		ERPS Ring 24's Information
0x3320 to 0x333F		ERPS Ring 25's Information
0x3340 to 0x335F		ERPS Ring 26's Information
0x3360 to 0x337F		ERPS Ring 27's Information
0x3380 to 0x339F		ERPS Ring 28's Information
0x33A0 to 0x33BF		ERPS Ring 29's Information
0x33C0 to 0x33DF		ERPS Ring 30's Information
0x33E0 to 0x33FF		ERPS Ring 31's Information

3.14.   Backup and restore

User can use Avcomm' Backup and Restore configuration to save and load configuration through the switch. There are 3 modes for users to backup/restore the configuration file.

WEB Backup and Restore

Restore Settings	Choose File No file chosen Upload
Backup Settings	Save...

Web mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

TFTP Backup and Restore

TFTP Server IP	
File Name	DP412-9466E7ABCDEF.con
Action	● Load ○ Save Submit

TFTP Server mode: In this mode, the switch acts as TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

TERMS	DESCRIPTION
TFTP Server IP	User needs to key in the IP address of TFTP Server here.
File Name	Type the correct file name of the configuration file.
Configuration File (*.conf*)	The configuration file of the switch is a pure text file. User can open it by word/txt read file. User can also modify the file, add/remove the configuration settings, and then restore back to the switch.
Action	User can choose to Load or Save configuration

3.15.   Firmware and upgrade

Avcomm provides the latest firmware online at www.avcomm.us . The new firmware may include new features, bug fixes or other software changes. Avcomm also provide the release notes for the update as well. For technical viewpoint, Avcomm suggests user uses the latest firmware before installing the switch to the customer site.

> **NOTE:** Note that the system will be automatically rebooted after User finished upgraDINg the new firmware. Please remind the attached network users before User performs this function.

There are 3 modes for users to backup/restore the configuration file, Local File mode, USB and TFTP Server mode.

WEB Firmware Upgrade

Select File	Choose File No file chosen

Upgrade   Cancel

Web mode: The switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.

TFTP Firmware Upgrade

IP

File Name

Upgrade   Cancel

TFTP Server mode: In this mode, the switch acts as the TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

TERMS	DESCRIPTION
IP	Users need to key in the IP address of TFTP Server here.
File Name	Type the correct file name of the configuration file.

The UI also shows User the current firmware version and built date of current firmware upgrade. Please check the version number after the switch is rebooted. Input the TFTP Server IP Address and the specific File Name. Then click on **Upgrade** to start the process. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

3.16.   Reset to default

This function provides users with a quick way of restoring the Avcomm switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

Factory Default main screen

Home › Reset to Default

Load default

Load default settings?

Reset

Pop-up message screen to show User that have done the command. Click on **OK** to close the screen.

192.168.10.1 says:

Do you really want to reset the current settings to default?

OK   Cancel

Then please go to **Reboot** page to reboot the switch. Click **OK.** The system will auto reboot the device.

Home › Reset to Default

Please reboot the switch to reset to the default settings except IP address.

OK

3.17.   Save

Save option allows user to save any configuration. Powering off the switch without clicking on **Save** will cause loss of new settings. After selecting **Save**, click on **Yes** to save new configuration.

Save

Do you want to save all submitted changes?

Yes

3.18.   Logout

There are 2 logout methods. If user doesn't input any command within 30 seconds, the web connection will be logged out. The Logout command allows user to manually logout the web connection. Click on **Yes** to logout.

Logout

Do you want to logout?

Yes

3.19.   Reboot

System Reboot allows user to reboot the device. Some of the feature changes require user to reboot the system. Click on **Reboot**-to-reboot device.

Reboot main screen, to do confirmation request. Click **Yes**, then the switch will reboot immediately.

> **NOTE:** Remember to click on Save button to save configuration settings. Otherwise, the settings user made will be gone when the switch is powered off.

Reboot

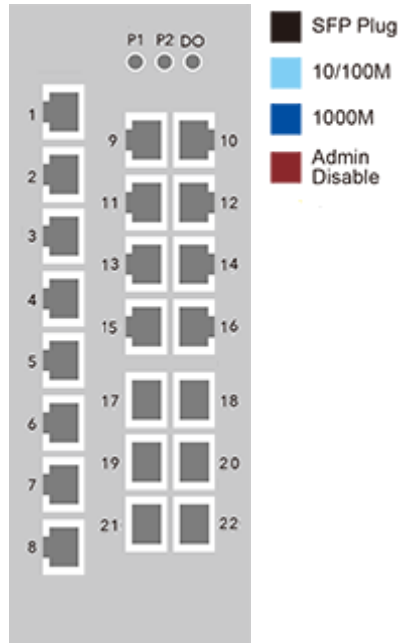Do you want to reboot?

Yes

3.20.   Front panel

Front Panel commands allow user to see LED status of the switch. User can see LED and link status of the Power, DO and Ports. Front panel interface, can be seen on the web consoles. Shown as below.

Click ⟳ button to refresh and update the latest status.

The description of the Front Panel is as below:

Feature	LED On	LED off
P1/P2	Green on: Power is on	No power
DO/ALM	Red on alarm relay active and contacts is short.	Red off: relay output contact is open.
10/100M	Light Blue on: Port is linked	Port link is down
1000M	Dark Blue on: The port is linked at 1000Mbps speed.	Not available
Admin Disable	Maroon on: Port disable	Not available

4. Major specifications

INTERFACE	8022GX6	8022GX6-L3
Ethernet Port	16 x 10/100/1000BaseTX RJ45, Auto Negotiation 6 x 100/1000 SFP , DDM	16 x 10/100/1000BaseTX RJ45, Auto Negotiation 6 x 100/1000 SFP, DDM
System LED	2 x Power: Green On 1 x DO: Red On	2 x Power: Green On 1 x DO: Red On
Ethernet Port LED	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)
SFP Port LED	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)	Link (Green On), Active (Green Blinking), Speed 1000M(Amber On), Speed 100M(Off)
Reset	System Reboot(2-6 Seconds)/Default Settings Reset(over 7 seconds)	System Reboot(2-6 Seconds)/Default Settings Reset(over 7 seconds)
Console	1 x RS232 for System Configuration. Baud Rate: 115200.n.8.1	1 x RS232 for System Configuration. Baud Rate: 115200.n.8.1

Power Input, Digital Input, Digital Output	2x 4-Pin Removable Terminal Block Connector
	Pins for Redundant Power
	Pins for DI, DO (Relay Alarm)
	Digital Output: Dry Relay Output with 0.5A /24V DC
	Digital Input with Photo-Coupler Isolation
	    Digital High: DC 11V~30V
	    Digital Low: DC 0V~10V
		2x 4-Pin Removable Terminal Block Connector
		Pins for Redundant Power
		Pins for DI, DO (Relay Alarm)
		Digital Output: Dry Relay Output with 0.5A /24V DC
		Digital Input with Photo-Coupler Isolation
		    Digital High: DC 11V~30V
		    Digital Low: DC 0V~10V

Power Requirement		
Input Voltage	24VDC (10~60VDC)	24VDC (10~60VDC)
Reverse Polarity Protect	Yes	Yes
Input Current	Typical 0.67A@24V	Typical 0.67A@24V
Power Consumption	Typical 16W@24VDC full traffic load. Max 18W@60VDC full traffic load, suggest reserving 15% tolerance	Typical 16W@24VDC full traffic load. Max 18W@60VDC full traffic load, suggest reserving 15% tolerance

Revision History

Version	Description	Date	Editor
V1.5	Add some models	June. 2022	Anya