User Manual

GSW-1005MS

Managed Gigabit Ethernet CPE Switch

CTC UNION TECHNOLOGIES CO., LTD.

LEGAL

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.
ActiPHY™ and VeriReach™ are registered trademarks of Vitesse® Semiconductor

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

WARNING:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006+A1:2007, Class A, EN55024:2010, and EN60950-1:2006

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60, Zhouzi St.
Neihu, Taipei, 114
Taiwan
Phone: +886-2-2659-1021
FAX: +886-2-2799-1355

GSW-1005MS
Managed Gigabit Ethernet CPE Switch

User Manual
Version 0.9a October 2013 (Draft)

This manual supports the following models:
GSW-1005MS Managed Gigabit Ethernet 5TP+1FX CPE Switch

This document is the current official release manual. Please check CTC Union's website for any updated manual or contact us by E-mail at sales@ctcu.com. Please address any comments for improving this manual or to point out omissions or errors to marketing@ctcu.com. Thank you.

Table of Contents

Chapter 1. Introduction

1.1 Welcome

Welcome and thank you for purchasing this "world class" product from CTC Union. We hope this product is everything you wanted and more. Our Product Managers and R&D team have placed a "quality first" motto in our development of this series of Gigabit Ethernet switches with the desire of providing a highly stable and reliable product that will give years of trouble free operation.

In this chapter we will introduce this series, for Gigabit Ethernet applications. These models can be either wall mounted or placed on a shelf/desktop. Chapter 2 will describe the mounting and installation methods. All the models in this series utilize almost identical management interfaces, whether Telnet, SSH, HTTP (Web GUI) or SNMP (Simple Network Management Protocol). Chapter 3 will cover the basic operation using Telnet CLI. Chapter 4 will detail all of the configuration settings by using an easy to point and click Web interface which can be accessed from any available web browser. Chapter 5 will give details on how these models can be managed using SNMP. Chapter 6 will be a general "Miscellaneous" section which includes troubleshooting, PC settings for TCP/IP, and other reference material of value.

1.2 Product Description

GSW-1005MS is a Managed Gigabit Ethernet CPE switch designed to make conversion between 5-Port 10/100/1000Base-T RJ-45 and 1 port 100/1000Base-X fiber optics with SFP optical modules. Traditionally, transmission distance of Gigabit Ethernet over fiber interface can be extended from 550m to 100km using the flexibility of any third party pluggable SFP modules. **GSW-1005MS** has an optional cable tray which allows the installer to enclose the excessive fiber loop within the tray housing, providing protection for the sensitive fiber at subscriber site. **GSW-1005MS** is fully compliant with IEEE 802.3, 802.3u, 802.3ab and 802.3z standards. End users can simply connect their devices, such as Ethernet home gateway, wireless access point or NIC on PC/laptop via 10/100/1000Base-T twisted pair to the RJ-45 ports of the CPE switch. No Ethernet crossover cables are required and link status can be easily monitored from the comprehensive LED display.

When **GSW-1005MS** is deployed as a stand-alone solution, it incorporates an easy to use Web user interface for operation, administration and maintenance both local and remotely. All of the enabled Layer 2 features and functions of **GSW-1005MS** can be configured and monitored via web interface and SNMP management. **GSW-1005MS** is the most suitable solution for deploying and provisioning the FTTX service of operators or service providers.

1.3 Product Features

- 5 x 10/100/1000Base-T(X) RJ-45 with 1 x 100/1000Base-X SFP Fiber
- 12VDC input via universal switching adapter
- UL60950-1, CE, FCC Certified
- Cable diagnostic, length measurement, cable OK or broken point distance
- Supports IEEE802.3az EEE (Energy Efficient Ethernet) Management to optimize power consumption
- QoS, Traffic classification QoS, CoS, Band width control for Ingress and Egress, broadcast storm control, DiffServ, IEEE802.1q VLAN, port based VLAN, MAC based VLAN, IP subnet based VLAN, Protocol based VLAN, VLAN translation, MVR, IGMP/MLD snooping V1/V2/V3, IGMP Filtering / Throttling, IGMP query, IGMP proxy reporting, MLD snooping
- Security : Port based and MAC based IEEE802.1X, RADIUS, ACL, TACACS+, HTTP/HTTPS, SSL/SSH v2
- Cisco® like CLI, Web based management, SNMP v1/v2c/v3, Telnet server for management
- Software upgrade via TFTP and HTTP, dual partitioned flash for quick recovery from upgrade failure
- DHCP client/Relay/Snooping/Snooping option 82/Relay option 82
- RMON, MIB II, port mirroring, event syslog, DNS, NTP/SNTP, IEEE802.1ab LLDP
- Supports IPv6 Telnet server /ICMP v6, SNMP, HTTP, SSH/SSL, NTP/SNTP, TFTP, QoS, AC

1.4 Product Specifications

Standards	IEEE 802.3	10Base-T 10Mbit/s Ethernet
	IEEE 802.3u	100Base-TX, 100Base-FX, Fast Ethernet
	IEEE 802.3ab	1000Base-T Gbit/s Ethernet over twisted pair
	IEEE 802.3z	1000Base-X Gbit/s Ethernet over Fiber-Optic
	IEEE 802.1d	STP (Spanning Tree Protocol)
	IEEE 802.1w	RSTP (Rapid Spanning Tree Protocol)
	IEEE 802.1s	MSTP (Multiple Spanning Tree Protocol)
	IEEE 802.1Q	Virtual LANs (VLAN)
	IEEE 802.1X	Port based Network Access Control, Authentication
	IEEE 802.3x	Flow control for Full Duplex
	IEEE 802.1ad	Stacked VLANs, Q-in-Q
	IEEE 802.1p	LAN Layer 2 QoS/CoS Protocol for Traffic Prioritization
	IEEE 802.1ab	Link Layer Discovery Protocol (LLDP)
	IEEE 802.3az	EEE (Energy Efficient Ethernet)
Switch	VLAN Groups	up to 4096
	Switching Fabric	12Gbps
	Data Processing	Store and Forward
	Flow Control	IEEE 802.3x for full duplex mode, back pressure for half duplex mode
	MTU	9600 Bytes (Jumbo Frames)
	MAC Table	8K
	LAN	5 x RJ-45 10/100/1000BaseT(X) auto detect speed, auto negotiate duplex, auto MDI/MDI-X function, Full/Half duplex
	Fiber	1 X 100/1000 BaseX dual speed mode SFP slot, supporting DDMI
Connectors	Network Cable	UTP/STP Cat.5e cable or above
	EIA/TIA-568	100-ohm (100m)
Ethernet	Protocol	CSMA/CD
	Reverse polarity	auto detect/correct
	Protection	Present
	Overload current protection	Present
	CPU Watch Dog	Present
	Power Supply	External AC adapter, 12VDC 1A capacity
	LED per unit	Power (Green), Fault (Amber), CPU Act (Green), Ring Master (Yellow)
Power	LED per RJ-45 port	10/100 Link/Active (Green), 1000 Link/Active (Amber)
LEDs	LED per SFP port	Link/Active (Green)

Chapter 2. Installation

2.1 Introduction

GSW-1005MS is designed for placing on a desktop or optionally can be used with fiber cable tray. The units come without fiber tray from the factory.

2.1.1 Mounting

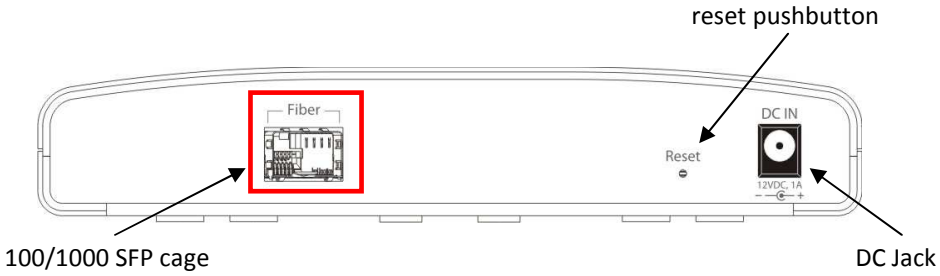
The fiber tray installation will be written here.

2.1.2 Un-mounting

2.2 Connections

2.2.1 Power

GSW-1005MS uses an external AC power adapter that supports wide voltage range input and is of a 'green' power efficiency design. Plug the power adapter's DC plug into the GSW-1005MS prior to plugging the adapter into the AC power source.



Back View

2.2.2 Fiber Connections

Refer to the graphic drawing above. **GSW-1005MS** utilizes an SFP module for fiber transmission. The fiber port has an associated status LED (viewed from the top) to indicate the presence or absence of fiber link and will also flash when there is Ethernet activity on the port. The SFP cage may insert any standard SFP module and be configured for 100M or 1000M operation. There is no 'lock out' mechanism, so any third party SFP, compliant with MSA, can be used in **GSW-1005MS**.

2.2.2.1 Inserting a Bale Clasp SFP Module into a SFP cage

Step 1 Close the bale clasp upward before inserting the SFP module.
Step 2 Line up the SFP module with the port, and slide it into the cage.

2.2.2.2 Removing a Bale Clasp SFP Module

Step 1 Open the bale clasp on the SFP module. Press the clasp downward with your index finger.
Step 2 Grasp the SFP module between your thumb and index finger and carefully remove it from the SFP cage.

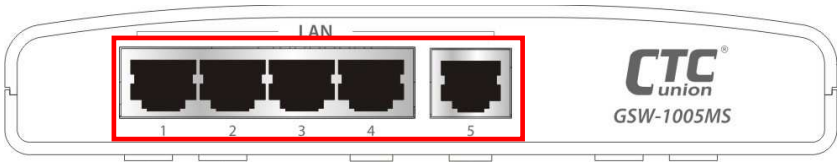
Within the management interfaces of the **GSW-1005MS**, the fiber port is numbered after the five electrical ports. So, that port is seen as ports 6 by the internal switch and as viewed in management.

2.2.3 Reset

There is a recessed pushbutton switch used to reset **GSW-1005MS** or to return it to factory defaults. Pressing the reset momentarily once will "warm boot" the switch. Pressing and holding the pushbutton switch for more than 3 seconds and then releasing will set the running configuration to the original factory default settings, including the original factory default IP address followed by a "warm boot". If the IP address of the switch is unknown, it may be necessary to do a factory default reset. The IP address will then be the known default.

2.2.4 LAN Connections

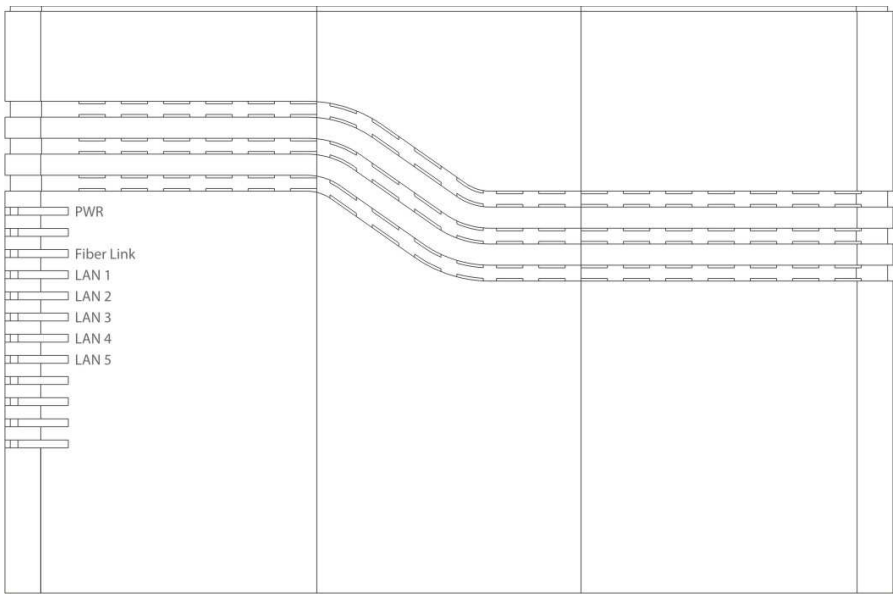
There are 5 shielded RJ-45 that provide LAN connections from **GSW-1005MS** Switch. These ports support Ethernet speeds of 10M/100M/1000M automatically. Each of these five LAN ports has associated LEDs, located on the top, which indicate the active link state and the detected speed of the interface. A green indicates a link and a speed of 10M or 100M, while amber color indicates a link and speed of 1000M.



10/100/1000 RJ-45 LAN ports

Front View

2.2.5 LED Indicators



Top of unit

Chapter 3. Configuration and Operation

3.1 Introduction

The **GSW-1005MS** Managed Gigabit Ethernet CPE switch provides a number of configuration/management methods. The first method of configuration/management uses a Web Browser. This requires that networking be configured so that the device can be accessed via a LAN port. Accessing the **GSW-1005MS** from a network allows for both local and remote management.

The Telnet/SSH access, using a command line (CLI), is familiar to most network engineers. For engineers that are not comfortable using CLI, this device should be managed using any standard Web Browser in a more user friendly 'point-and-click' method. Therefore, in most configuration scenarios, Telnet/SSH will only be used by experienced networking engineers.

After the device has been properly configured for the application and placed into service, a third method of configuration/management can be employed using Simple Network Management Protocol (SNMP). The operator will use SNMP management software to manage and monitor the **GSW-1005MS** switches on a network. This requires some configuration of the device to allow SNMP management. In addition, the network management platform will need to import and compile the proprietary MIB (management information base) file so that the management software knows "how" to manage the **GSW-1005MS**.

3.2 Telnet Operation

Default TCP/IP settings of **GSW-1005MS.**
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Default Gateway:
Username: admin
Password: None

From a cold start, the following screen will be displayed. At the "Username" prompt, enter 'admin' with no password.

```
Username: admin
Password:
Login in progress...
Welcome to CCLI (v1.2).
Type 'help' or '?' to get help.
>
```

3.2.1 CLI Online Help

While using the CLI, online help is always available by using 'help' command or typing '?' (question mark). Commands may be 'auto-completed' by pressing [TAB] and previous commands can be recalled by using the 'up/down arrow keys'.

Note: When making corrections while typing, please be aware that unless the terminal emulation program specifically issues a [CTRL-H] for [Backspace] that the backspace action must use the key combination of [CTRL-H] as the [Backspace] character is not recognized by the CLI.

```
>?
General Commands:
-----------------
Help/?: Get help on a group or a specific command
Up    : Move one command level up
Logout: Exit CCLI

Command Groups:
---------------
System        : System settings and reset options
IP            : IP configuration and Ping
Auto Provision: Auto Provision configuration
Port          : Port management
MAC           : MAC address table
VLAN          : Virtual LAN
PVLAN         : Private VLAN
Security      : Security management
STP           : Spanning Tree Protocol
Aggr          : Link Aggregation
LACP          : Link Aggregation Control Protocol
LLDP          : Link Layer Discovery Protocol
LLDPMED       : Link Layer Discovery Protocol Media
EEE           : Energy Efficient Ethernet
Thermal       : Thermal Protection
Led_power     : LED power reduction
PoE           : Power Over Ethernet
QoS           : Quality of Service
Mirror        : Port mirroring
Config        : Load/Save of configuration via TFTP
Firmware      : Download of firmware via TFTP
UPnP          : Universal Plug and Play
MVR           : Multicast VLAN Registration
Voice VLAN    : Specific VLAN for voice traffic
Loop Protect  : Loop Protection
IPMC          : MLD/IGMP Snooping
sFlow         : sFlow Agent
VCL           : VLAN Control List

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>
```

3.2.2 TCP/IP Configuration via CLI

3.2.2.1 IP Address, Subnet Mask, Default Router

syntax: IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

```
>ip setup 192.168.0.251 255.255.255.0 192.168.0.10 1
>
```

notes: The default <vlan> for untagged packets is VID 1.
Changing the IP address from Telnet will result in disconnection. Please avoid doing this and instead use web interface.

3.2.2.2 DHCP

syntax: IP DHCP [enable|disable]

```
>ip dhcp disable
>
```

note: The DHCP client is disabled by default. To set static IP on network with DHCP server, do not enable DHCP client.

3.2.2.3 DNS Server

syntax: IP DNS <dns_source>

```
>ip dns 192.168.0.1
>
```

note: The <dns_source> parameter points to the static DNS server for the network.

3.2.2.4 Display TCP/IP Settings

syntax: IP Configuration

```
>ip configuration

IP Configuration:
=================

DHCP Client       : Disabled
DHCP Option 60    : GSW-1005M
IP Address        : 192.168.0.1
IP Mask           : 255.255.255.0
IP Router         : 0.0.0.0
DNS Server        : 0.0.0.0
VLAN ID           : 1
DNS Proxy         : Disabled

IPv6 AUTOCONFIG mode   : Enabled  (Fallback in 300 seconds)
IPv6 Link-Local Address: fe80::6082:cdb9:19ab:c0e2
IPv6 Address           : ::192.168.0.16
IPv6 Prefix            : 96
IPv6 Router            : ::

Active Configuration for IPv6: (AUTOCONFIG... 300 seconds remaining)
IPv6 Address: fe80:2::6082:cdb9:19ab:c0e2/64 Scope:Link
Status:UP/RUNNING(Enabled)/MTU 1500/LinkMTU is 1500>
>
```

3.2.3 Factory Default

syntax: System Restore Default <keep_ip>

```
>system restore default
>
```

note: To restore factory default but keep TCP/IP settings, use: "system restore default keep_ip"

3.2.4 Reboot Device

syntax: System Reboot

```
>system reboot
>
```

3.2.5 Admin Password

syntax: Security Switch Users Add <username> <password> <privilege_level>

```
>security switch add admin secret 15
>
```

Note: sets the password "secret" for the admin user. (Admin user has highest privilege level of 15.)
To clear admin password, use a pair of double quotes to enter a null password.

```
>security switch add admin "" 15
>
```

3.2.6 Logout

syntax: Logout

```
>logout

Username:
```

Note: After the logout command is issued, the "Username:" login prompt will again be displayed.

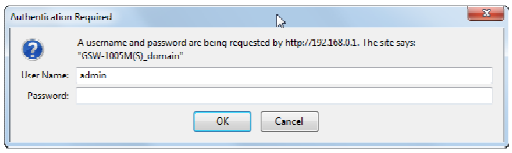
3.3 Web Operation

3.3.1 Home Page

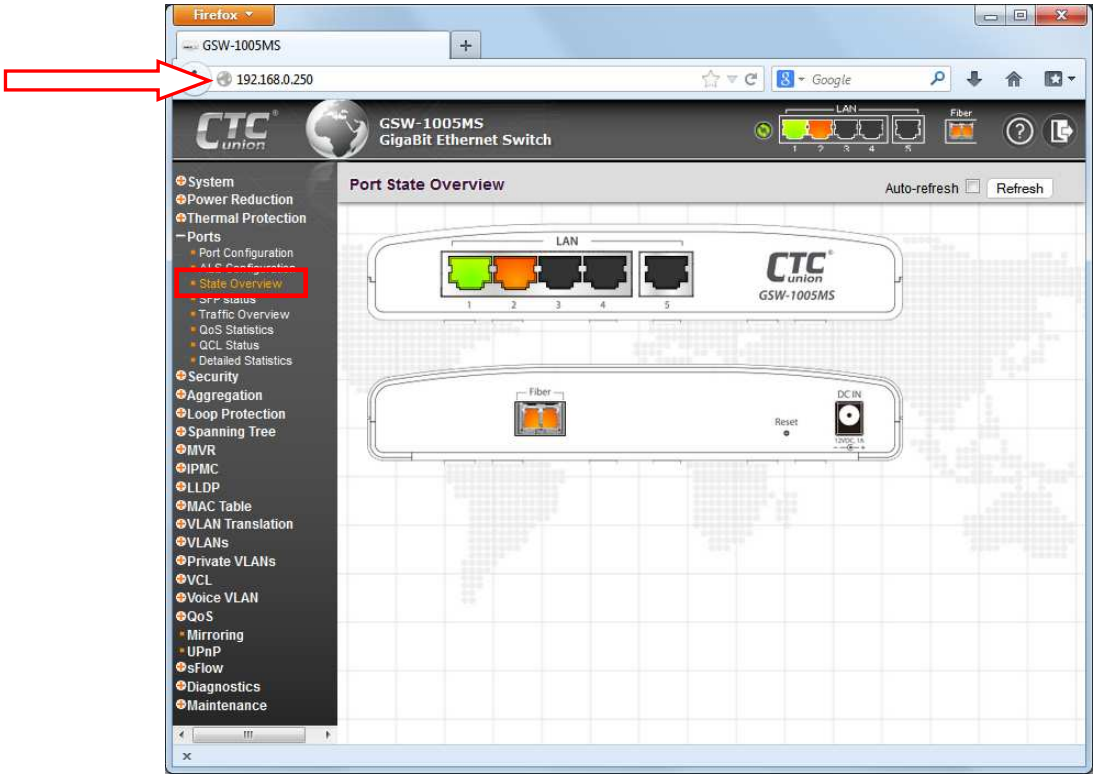
Using your favorite web browser, enter the IP address of the **GSW-1005MS** in the browser's location bar. The factory default address is 192.168.0.1.

3.3.1.1 Login

A standard login prompt will appear depending on the type of browser used. The example below is with Firefox browser.



The **GSW-1005MS** factory default is username 'admin' with no password.



Web Home Page

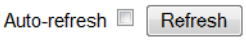
3.3.1.2 Port Status

The initial page, when logged in, displays a graphical overview of the port status for the electrical and optical ports. The "Green" port 1 LAN indicates a LAN connection with a speed of 100M. The "Amber" colored port 2 LAN and Fiber port 1 (6) indicate a connection speed of 1000M.

The status display can be reached by using the left side menu, and return to **Ports>State Overview**.

3.3.1.3 Refresh

To update the screen, click the "Refresh" button. For automatic updating of the screen, the "Auto-refresh" tick box may be ticked. The screen will be auto refreshed every 3 seconds.



Unless connected directly on a local LAN, we recommend not using the auto-refresh function as it does generate a bit of traffic.

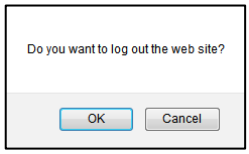
3.3.1.4 Help System

The **GSW-1005MS** has an online "help" system to aid the engineer when setting the parameters of the device. Each functional setting page is accompanied by a specific "help" for that functional page. The user can display this help "pop up" at any time by clicking the "help" icon.

3.3.1.5 Logout

After completing configuration, we recommend logging out of the web GUI. This is easily accomplished by clicking the logout icon.

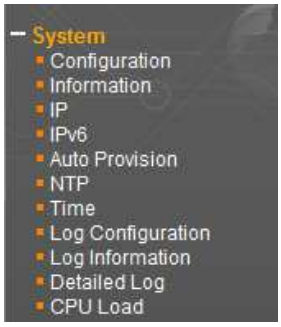
After clicking the logout icon, a confirmation screen will be displayed. Click "OK" to finish logging out or click "Cancel" to return to the web configuration GUI.



For the remainder of this section, each menu item will be explained one by one, in order as they descend down the menu screen, starting with the "System" menu.

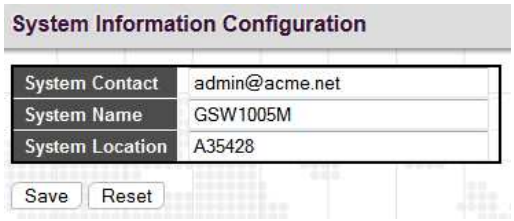
3.3.2 System

The configuration under the "System" menu includes device settings such as IP address, time server, etc.



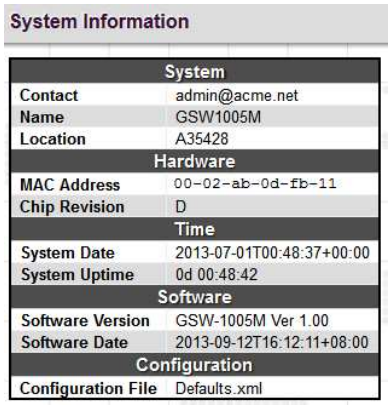
3.3.2.1 System Configuration

The configuration information entered here will be reported in the standard SNMP MIB2 for 'sysContact' (OID 1.3.6.1.2.1.1.4), 'sysName' (OID 1.3.6.1.2.1.1.5) and 'sysLocation' (OID 1.3.6.1.2.1.1.6). Remember to click the 'Save' button after entering the configuration information.



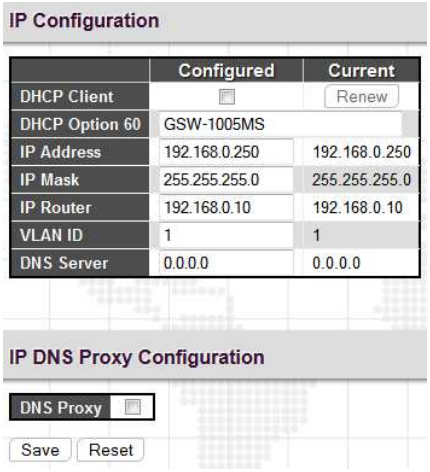
3.3.2.2 System Information

The system information screen will display the configuration information, the hardware MAC address and version, the system time, the system "uptime" and the software version and build date.



3.3.2.3 System IP

Setup the IP configuration, interface and routes



DHCP Client:

Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

DHCP Option 60:

Configure the DHCP option 60 vendor class ID. The allowed string length is 0 to 60, and the allowed content is the ASCII characters from 0x20 to 0x7E.

IP Address:

The IPv4 address of the interface is entered in dotted decimal notation. If DHCP is enabled, DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the IP address is configured, DHCP will stop and the configured IP settings will be used.

IP Mask:

The IPv4 network mask is entered by a number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.

IP Router:

This is the IP address of the gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

VLAN:

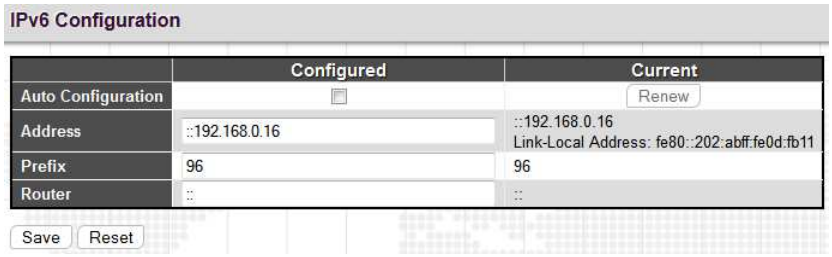
This is the VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface.

DNS Server:

This setting controls the DNS name resolution done by the switch.

3.3.2.4 System IPv6

Configure the switch-managed IPv6 information on this page. The Configured column is used to view or change the IPv6 configuration. The Current column is used to show the active IPv6 configuration.



Auto Configuration:

Enable IPv6 auto-configuration by checking this box. If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer.

Address:

Provides the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Prefix:

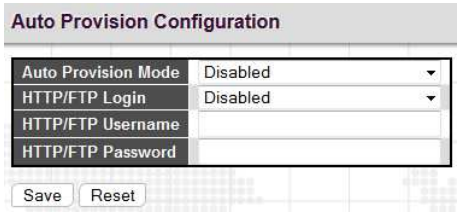
Provides the IPv6 Prefix of this switch. The allowed range is 1 to 128.

Router:

Provides the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.

3.3.2.5 System Auto Provision Configuration

Configure auto provision on this page.



Auto Provision Mode:

Indicates the auto provision operation mode. Possible modes are:

* Enabled: Enable auto provision mode operation. When auto provision mode operation is enabled, the device can download software and configuration automatically.
* Disabled: Disable auto provision mode operation.

HTTP/FTP Login:

Indicates the HTTP/FTP downloading mode operation. Possible modes are:

* Enabled: When HTTP/FTP Login is enabled, the device downloads software and configuration with username and password if given at below.
* Disabled: Downloads software and configuration without username and password.

HTTP/FTP Username:

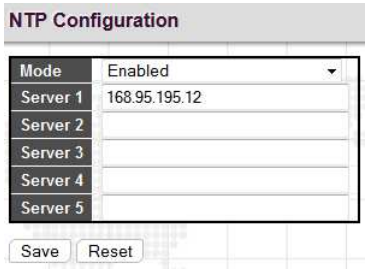
If both Auto Provision Mode and HTTP/FTP Login are enabled, this username is used as the ID when logging into HTTP or FTP server. The allowed string length is 0 to 20,

HTTP/FTP Password:

If both Auto Provision Mode and HTTP/FTP Login are enabled, this password is used as the secret when logging into HTTP or FTP server. The allowed string length is 0 to 20,

3.3.2.6 System NTP Configuration

Configure NTP (Network Time Protocol) on this page.

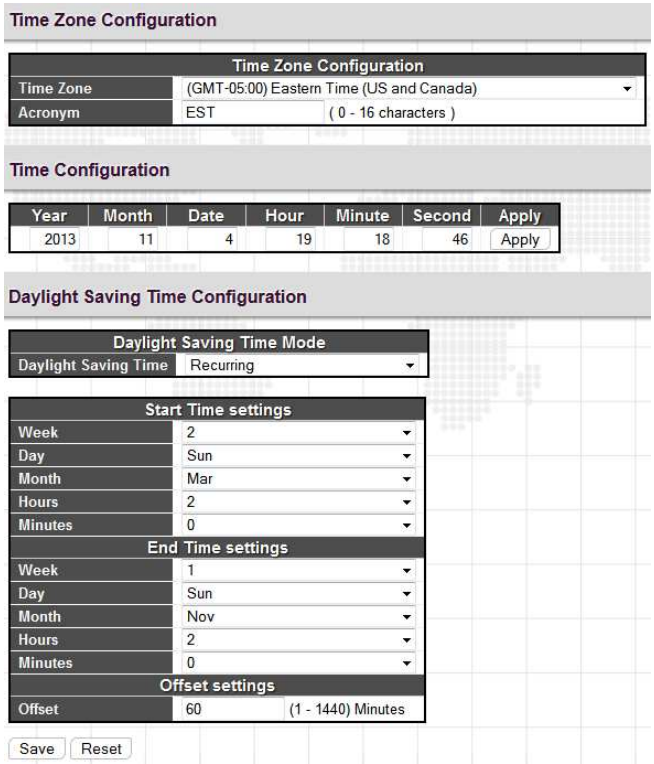


Mode:
Indicates the NTP mode operation. Possible modes are:
* Enabled: Enable NTP client mode operation.
* Disabled: Disable NTP client mode operation.

Server #:
Provides the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

3.3.2.7 System Time

Setup the device time.



The setting example above is for Eastern Standard Time in the United States. Daylight savings time starts on the second Sunday in March at 2:00AM. Daylight savings ends on the first Sunday in November at 2:00AM. The daylight savings time offset is 60 minutes (1 hour).

Time Zone: Lists various Time Zones worldwide
Select appropriate Time Zone from the drop down and click Save to set.
Acronym: Set the acronym of the time zone.
Daylight Saving Time: This page is used to setup Daylight Saving Time Configuration.

Daylight Saving Time Configuration

Daylight Saving Time:

This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default is Disabled)

Recurring Configurations:

Start time settings

Week - Select the starting week number.
Day - Select the starting day.
Month - Select the starting month.
Hours - Select the starting hour.
Minutes - Select the starting minute.

End time settings

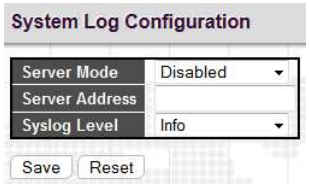
Week - Select the ending week number.
Day - Select the ending day.
Month - Select the ending month.
Hours - Select the ending hour.
Minutes - Select the ending minute.

Offset settings

Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

3.3.2.8 System Log Configuration

Configure System Log on this page.



Server Mode:

This sets the server mode operation. When the mode of operation is enabled, the syslog message will send out to syslog server (at the server address). The syslog protocol is based on UDP communication and received on UDP port 514. Syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out, even if the syslog server does not exist. When the mode of operation is disabled, no syslog packets are sent out.

Server Address:

This sets the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.

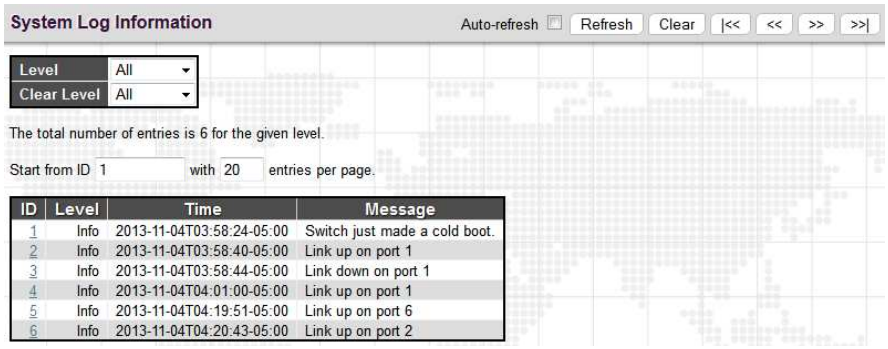
Syslog Level:

This sets what kind of messages will send to syslog server. Possible levels are:

* Info: Sends information, warnings and errors.
* Warning: Send warnings and errors.
* Error: Send errors only.

3.3.2.9 System Log Information

Displays the collected log information.



Level:
Use this pull down to display all messages or messages of type info, warning or error.
Clear Level:
Use this pull down to clear selected message types from the log.
Browsing buttons:
Use these buttons to quickly go to the beginning or end of the log or to page through the log.

3.3.2.10 System Detailed Log

Displays individual log records.

View each log, by ID number.

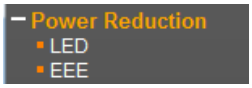
3.3.2.10 System CPU Load

This page displays the CPU load, using an SVG graph.

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Automatic refresh occurs every 3 seconds.

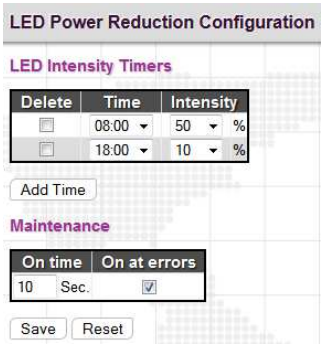
3.3.3 Power Reduction (Green Ethernet)

The configuration under the "Power Reduction" menu includes two power saving techniques.



3.3.3.1 Green Ethernet LED

Configure the LED light intensity to reduce power consumption.

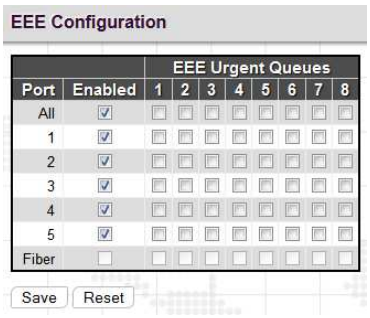


The LED light intensity may be adjusted in a percentage of intensity during programmable time periods. In the above setting example, the LED intensity has been adjusted to 50% during daylight hours and reduced to only 10% intensity during night hours.

The maintenance checkbox will bring LED intensity to 100% for 10 seconds in the event of any error (such as link down).

3.3.3.2 Green Ethernet Configuration

Configure EEE (Energy-Efficient Ethernet) Ethernet power savings.



Port Power Savings Configuration

Enables/disables the EEE function for this switch. The two options are:

* [checked] - The EEE function is enabled. This is the default setting.
* [not checked] - EEE is not enabled.

EEE (Energy-Efficient Ethernet)

EEE is a power saving option that reduces the power usage when there is low or no traffic utilization. EEE was developed through the IEEE802.3az task force of the Institute of Electrical and Electronic Engineers (IEEE).

EEE works by powering down circuits when there is no traffic. When a port gets data to be transmitted all circuits are powered up. The time it takes to power up the circuits is called wakeup time. The default wakeup time is 17 us for 1Gbit links and 30 us for other link speeds. EEE devices must agree upon the value of the wakeup time in order to make sure that both the receiving and transmitting device has all circuits powered up when traffic is transmitted. The devices can exchange wakeup time information using the LLDP (Link Layer Discovery Protocol) protocol.

EEE works for ports in auto-negotiation mode, where the port is negotiated to either 1G or 100 Mbit full duplex mode.

For ports that are not EEE-capable the corresponding EEE checkboxes are grayed out and thus impossible to enable EEE for.

When a port is powered down for saving power, outgoing traffic is stored in a buffer until the port is powered up again. Because there are some overhead in turning the port down and up, more power can be saved if the traffic can be buffered up until a large burst of traffic can be transmitted. Buffering traffic will give some latency in the traffic. For traffic that should not be held back, urgent queues may be assigned to reduce latency yet still result in overall power saving.

EEE Urgent Queues

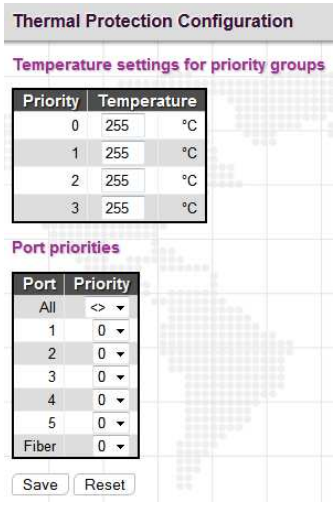
It is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

3.3.4 Thermal Protection

This page allows the user to inspect and configure the current setting for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different priorities. Each priority can be given a temperature at which the corresponding ports shall be turned off.



Temperature settings for priority groups:

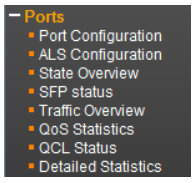
The temperature at which the ports with the corresponding priority will be turned off. Temperatures between 0 and 255 C are supported.

Port priorities:

The priority the port belongs to. There are 4 priority levels supported.

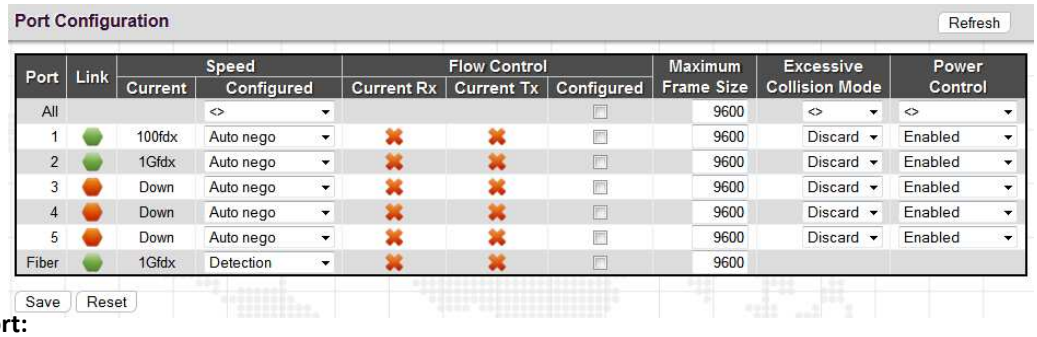
3.3.5 Ports

Configurations related to the fiber and electrical ports are performed under the Ports menu.



3.3.5.1 Ports Configuration

This page displays current port configurations and allows some configuration here.



Port:

GSW-1005MS are managed gigabit switches with 5 electrical LAN ports numbered 1~5 and 1 fiber optical port (for SFP module) numbered 6. Each logical port number is displayed in a row. The select all "*" port will apply actions on all ports.

Link:

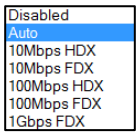
The current link state for each port is displayed graphically. Green indicates the link is up and red that it is down.

Current Speed:

This column provides the current link speed (10, 100, 1G) and duplex (fdx=Full Duplex, hdx=Half Duplex) of each port.

Configured Speed:

This pull down selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.



Options for **GSW-1005MS**

Possible copper port settings are:

* Disabled - Disables the switch port operation.
* Auto - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner and negotiating the duplex mode.
* 10Mbps HDX - Forces the port to 10Mbps half duplex mode.
* 10Mbps FDX - Forces the port to 10Mbps full duplex mode.
* 100Mbps HDX - Forces the port to 100Mbps half duplex mode.
* 100Mbps FDX - Forces the port to 100Mbps full duplex mode.
* 1Gbps FDX - Forces the port to 1Gbps full duplex

Possible fiber port settings are

* Disabled - Disables the switch port operation.
* Auto nego - Port auto negotiating speed with the link partner, selecting the highest speed that is compatible with the link partner.
* Detection - There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFP's speed might not be detectable.
* 100Mbps FDX - Forces the fiber port to 100Mbps full duplex mode.
* 1Gbps FDX - Forces the fiber port to 1Gbps full duplex mode.

Flow Control:

The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is also related to the setting for Configured Link Speed.

Maximum Frame Size:

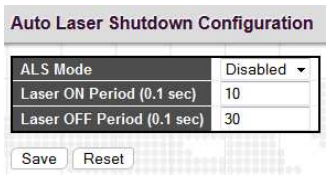
Enter the maximum frame size allowed for the switch port, including FCS. This switch supports up to 9600 byte packets.

Excessive Collision Mode:

This setting configures the port transmit collision behavior to either "Discard" (Discard frame after 16 collisions - default) or to "Restart" (Restart backoff algorithm after 16 collisions).

3.3.5.2 Ports Auto Laser Shutdown

This page allows the user to inspect and configure the current setting for transceiver module Tx power.



ALS mode:

Enable/Disable the laser power of transceiver module shutdown automatically.

Laser ON Period:

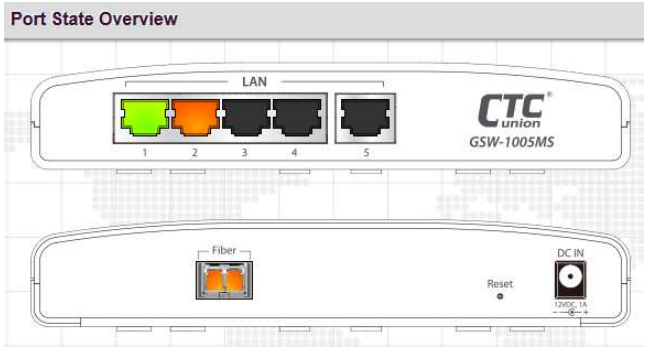
The period is Tx laser power turn ON. The allowed range is 2 to 30 in tenths of a second, default period is 10 in tenths of a second (1 second).

Laser OFF Period:

The period is Tx laser power turn OFF. The allowed range is 10 to 50 in tenths of a second, default period is 30 in tenths of a second (3 second).

3.3.5.3 Ports State

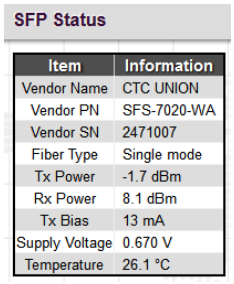
Display an overview graphic of the switch.



This is the same graphic overview shown when first logging into the switch for management. "Green" colored ports indicate a 100M linked state, while "Amber" colored ports indicate a 1G linked state. "Grey" ports have no link. The link status display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds.

3.3.5.4 Ports SFP

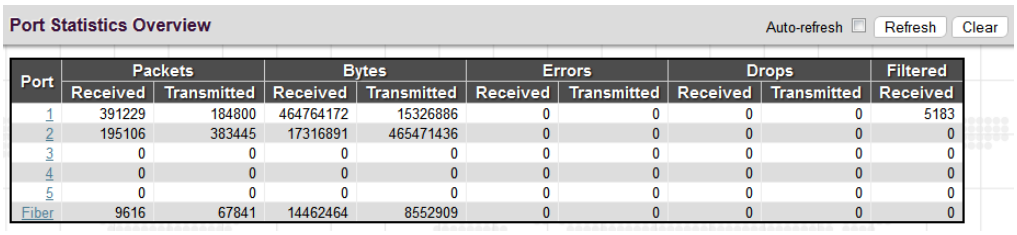
This page provides status of SFP.



Vendor Part number: The part number provided by SFP vendor.
Vendor Serial number: The serial number provided by SFP vendor.
Type: The type of fiber channel transmission media (multi-mode or single mode).
Tx power: The TX output power in dBm.
Rx power: The RX received optical power in dBm.
Tx bias: The TX bias current in mA.
Supply voltage: The transceiver supply voltage in mV.
Temperature: The transceiver temperature in degree C.

3.3.5.5 Ports Traffic Overview

Displays a comprehensive overview of traffic on all ports.



Port Statistics Overview

Auto-refresh | Refresh | Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	391229	184800	464764172	15326886	0	0	0	0	5183
2	195106	383445	17316891	465471436	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
Fiber	9616	67841	14462464	8552909	0	0	0	0	0

The displayed counters are:

Port

* The logical port (1~6) for the data contained in the same row.

Packets

* The number of received and transmitted packets per port.

Bytes

* The number of received and transmitted bytes per port.

Errors

* The number of frames received in error and the number of incomplete transmissions per port.

Drops

* The number of frames discarded due to ingress or egress congestion.

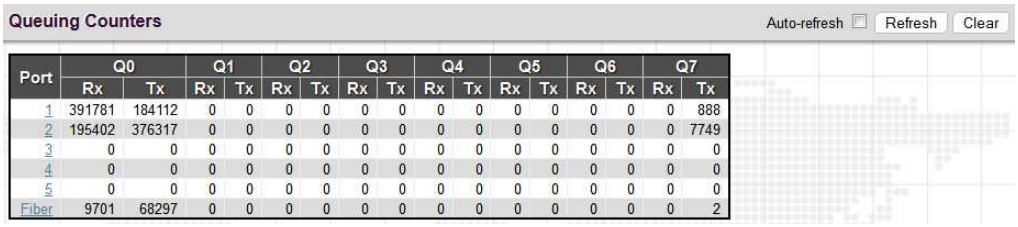
Filtered

* The number of received frames filtered by the forwarding process.

The counter display can be updated by clicking the "Refresh" button. When "Auto-refresh" is checked, the display will be updated every 3 seconds. Clicking the "Clear" button will zero all counters and start counting again.

3.3.5.6 Ports QoS Statistics

This page provides statistics for the different queues for all switch ports.



Queuing Counters

Auto-refresh | Refresh | Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	391781	184112	0	0	0	0	0	0	0	0	0	0	0	0	0	888
2	195402	376317	0	0	0	0	0	0	0	0	0	0	0	0	0	7749
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Fiber	9701	68297	0	0	0	0	0	0	0	0	0	0	0	0	0	2

The displayed counters are:

Port

* The logical port for the settings contained in the same row.

Qn

* There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

* The number of received and transmitted packets per queue.

3.3.5.7 Ports QCL Status

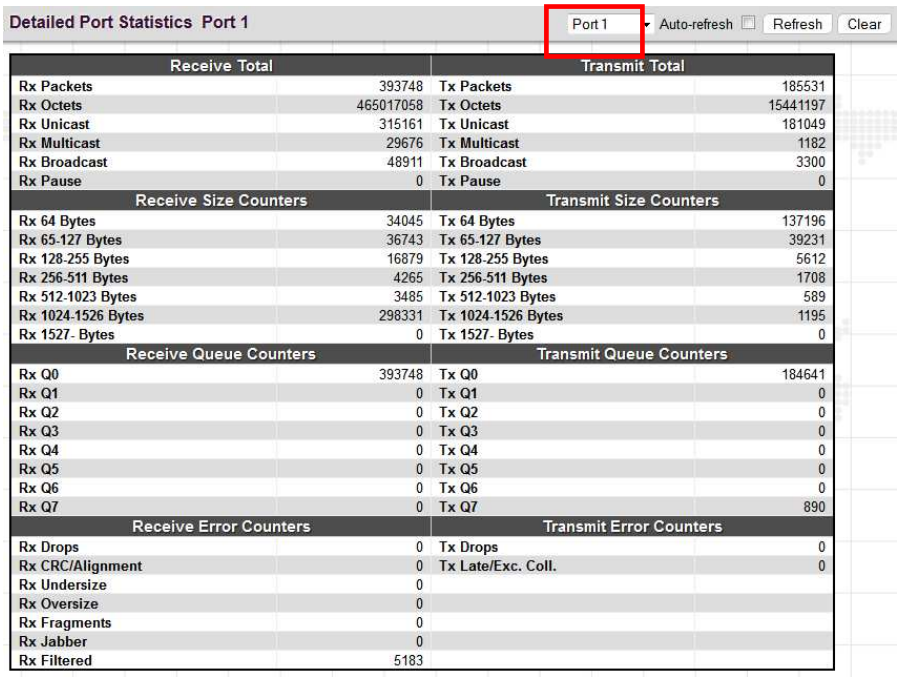
This page shows the QCL status by different QCL users.

Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

User
* Indicates the QCL user.
QCE#
* Indicates the index of QCE.
Frame Type
Indicates the type of frame to look for incoming frames. Possible frame types are:
* Any: The QCE will match all frame type.
* Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.
* LLC: Only (LLC) frames are allowed.
* SNAP: Only (SNAP) frames are allowed.
* IPv4: The QCE will match only IPV4 frames.
* IPv6: The QCE will match only IPV6 frames.
Port
* Indicates the list of ports configured with the QCE.
Action
* Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.
There are three action fields: Class, DPL and DSCP.
* Class: Classified QoS class; if a frame matches the QCE it will be put in the queue.
* DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.
* DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.
Conflict
* Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications, it may happen that resources required to add a QCE may not be available. In that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

3.3.5.8 Ports Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. Use the port select pull down to select which switch port details to display.



Receive Total		Transmit Total	
Rx Packets	393748	Tx Packets	185531
Rx Octets	465017058	Tx Octets	15441197
Rx Unicast	315161	Tx Unicast	181049
Rx Multicast	29676	Tx Multicast	1182
Rx Broadcast	48911	Tx Broadcast	3300
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	34045	Tx 64 Bytes	137196
Rx 65-127 Bytes	36743	Tx 65-127 Bytes	39231
Rx 128-255 Bytes	16879	Tx 128-255 Bytes	5612
Rx 256-511 Bytes	4265	Tx 256-511 Bytes	1708
Rx 512-1023 Bytes	3485	Tx 512-1023 Bytes	589
Rx 1024-1526 Bytes	298331	Tx 1024-1526 Bytes	1195
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	393748	Tx Q0	184641
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	890
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	5183		

Receive Total and Transmit Total:

Rx and Tx Packets

* The number of received and transmitted (good and bad) packets.

Rx and Tx Octets

* The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast

* The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast

* The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast

* The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause

* A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE.

Receive and Transmit Size Counters:

Displays the number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters:

Displays the number of received and transmitted packets per input and output queue.

Receive Error Counters:

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short [1] frames received with valid CRC.

Rx Oversize

The number of long [2] frames received with valid CRC.

Rx Fragments

The number of short [1] frames received with invalid CRC.

Rx Jabber

The number of long [2] frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

[1] Short frames are frames that are smaller than 64 bytes.

[2] Long frames are frames that are longer than the configured maximum frame length for this port.

Transmit Error Counters:

Tx Drops

The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.

The number of frames dropped due to excessive or late collisions.

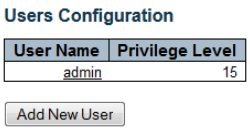
3.3.6 Security

Under the security heading are three major icons, switch, network and RADIUS.

edit here

3.3.6.1 Users

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to close and reopen the browser.



By default, there is only one user, 'admin', assigned the highest privilege level of 15.

The displayed values for each user are:

User Name

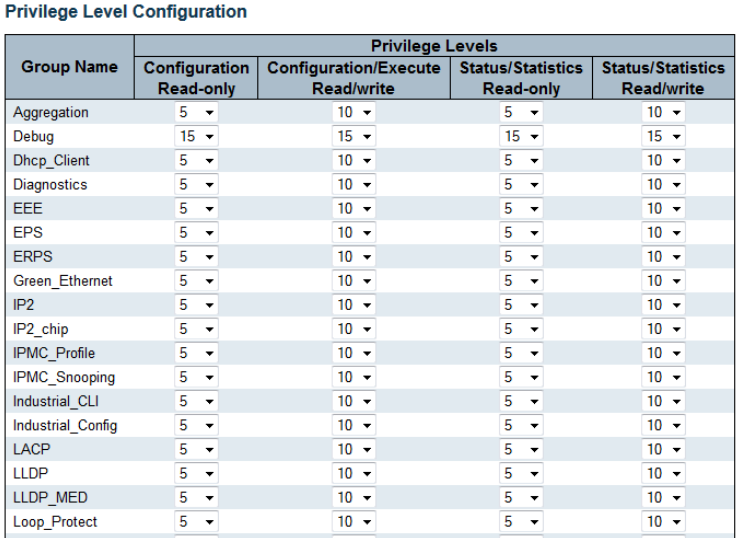
* The name identifying the user. This is also a link to Add/Edit User.

Privilege Level

* The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

3.3.5.2 Privilege Levels

This page provides an overview of the privilege levels.



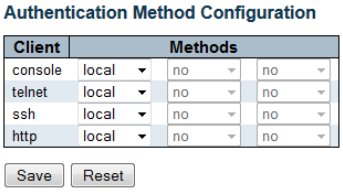
Group Name:
* This name identifies the privilege group. In most cases, a privilege level group consists of a single module (e.g. LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:
* System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
* Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
* IP: Everything except 'ping'.
* Port: Everything except 'VeriPHY'.
* Diagnostics: 'ping' and 'VeriPHY'.
* Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
* Debug: Only present in CLI.

Privilege Levels:
* Every group has an authorization Privilege level for the following sub groups:
  configuration read-only
  configuration/execute read-write
  status/statistics read-only
  status/statistics read-write (e.g. for clearing of statistics)

User Privilege should be the same or greater than the authorization Privilege level to have access to that group.

3.3.5.3 Auth Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.



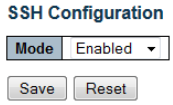
Client:
* The management client for which the configuration below applies.

Methods:
* Method can be set to one of the following values:
  no: Authentication is disabled and login is not possible.
  local: Use the local user database on the switch for authentication.
  radius: Use remote RADIUS server(s) for authentication.
  tacacs+: Use remote TACACS+ server(s) for authentication.

note:
Methods that involve remote servers will time out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.

3.3.5.4 SSH

Configure SSH on this page.

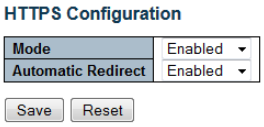


Mode: Indicates the SSH mode operation. Possible modes are:
* Enabled: Enable SSH mode operation. (default)
* Disabled: Disable SSH mode operation.

note:
SSH is preferred to Telnet, unless the management network is trusted. Telnet passes authentication credentials in plain text, making those credentials susceptible to packet capture and analysis. SSH provides a secure authentication method. The SSH in **IFS/IGS803** uses version 2 of SSH protocol.

3.3.5.5 HTTPS

Configure HTTPS on this page.

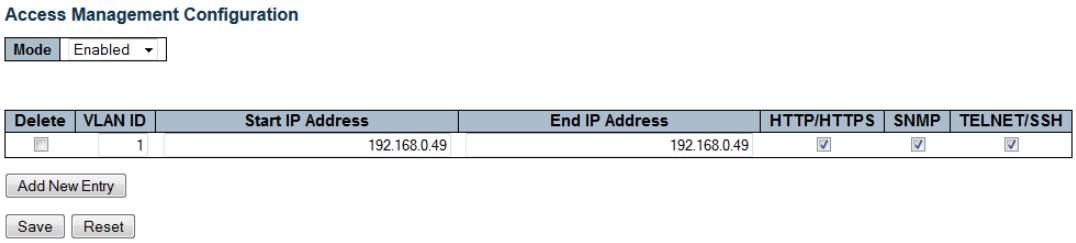


Mode: Indicates the HTTPS operation mode. When the current connection is HTTPS and HTTPS mode operation is disabled, web browser will automatically redirect to an HTTP connection. Possible modes are:
* Enabled: Enable HTTPS mode operation.
* Disabled: Disable HTTPS mode operation.

Automatic Redirect: Indicates the HTTPS redirect mode operation. It applies only if HTTPS mode "Enabled" is selected. Automatically redirects HTTP of web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled. Possible modes are:
Enabled: Enable HTTPS redirect mode operation.
Disabled: Disable HTTPS redirect mode operation.

3.3.5.6 Access Management Configuration

Configure the access management table on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will be allowed access to the switch.

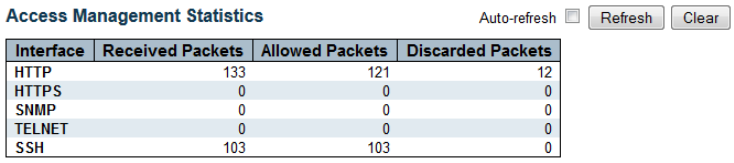


Mode: Indicates the access management mode operation. Possible modes are:
* Enabled: Enable access management mode operation.
* Disabled: Disable access management mode operation.

Delete: Check to delete the entry. It will be deleted during the next save.
VLAN ID: Indicates the VLAN ID for the access management entry.
Start IP address: Indicates the start IP address for the access management entry.
End IP address: Indicates the end IP address for the access management entry.
HTTP/HTTPS: Checked indicates that the matched host can access the switch from HTTP/HTTPS interface.
SNMP: Checked indicates that the matched host can access the switch from SNMP.
TELNET/SSH: Indicates that the matched host can access the switch from TELNET/SSH interface.

3.3.5.7 Access Management Statistics

This page provides statistics for access management.

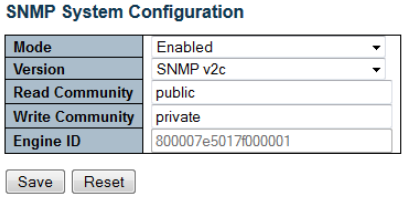


Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	133	121	12
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	103	103	0

Interface: The interface type through which any remote host can access the switch.
Received Packets: The number of received packets from the interface when access management mode is enabled.
Allowed Packets: The number of allowed packets from the interface when access management mode is enabled.
Discarded Packets: The number of discarded packets from the interface when access management mode is enabled.

3.3.5.8 SNMP System Configuration

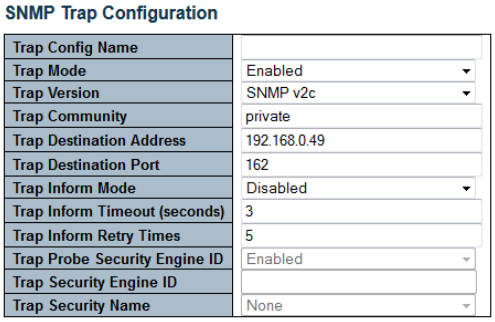
Configure SNMP on this page.



Mode: Indicates the SNMP mode operation. Possible modes are:
* Enabled: Enable SNMP mode operation.
* Disabled: Disable SNMP mode operation.
Version: Indicates the SNMP supported version. Possible versions are:
* SNMP v1: Set SNMP supported version 1.
* SNMP v2c: Set SNMP supported version 2c.
* SNMP v3: Set SNMP supported version 3.
Read Community: Indicates the community read access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.
Write Community: Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 0x21 to 0x7E.
These two fields are applicable only for SNMP version v1 or v2c. If SNMP version is v3, the community string will be associated with SNMPv3 communities table. SNMPv3 provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Engine ID: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Changes to the Engine ID will clear all original local users.

3.3.5.9 SNMP Trap Configuration

Configure SNMP trap on this page.

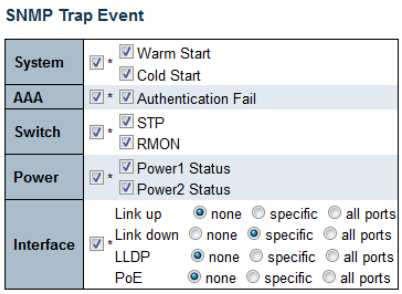


Trap Mode: Indicates the SNMP trap mode operation. Possible modes are:
* Enabled: Enable SNMP trap mode operation.
* Disabled: Disable SNMP trap mode operation.

Trap Version: Indicates the SNMP trap supported version. Possible versions are:
* SNMP v1: Set SNMP trap supported version 1.
* SNMP v2c: Set SNMP trap supported version 2c.
* SNMP v3: Set SNMP trap supported version 3.
Trap Community: Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 0x21 to 0x7E.
Trap Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). Also allowed is a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.) and dash (-). Spaces are not allowed. The first character must be an alpha character, and the first and last characters cannot be a dot or a dash.
Trap Destination port: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535. The default SNMP trap port is 162.
Trap Inform Mode: Indicates the SNMP trap inform mode operation. Possible modes are:
* Enabled: Enable SNMP trap inform mode operation.
* Disabled: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds): Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times: Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID: Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:
* Enabled: Enable SNMP trap probe security engine ID mode of operation.
* Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID: Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs use USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name: Indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

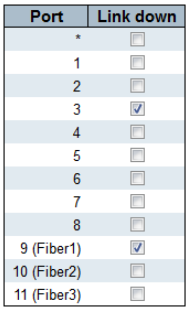
3.3.5.10 SNMP Trap Event

Setup what events will be sent as trap messages.



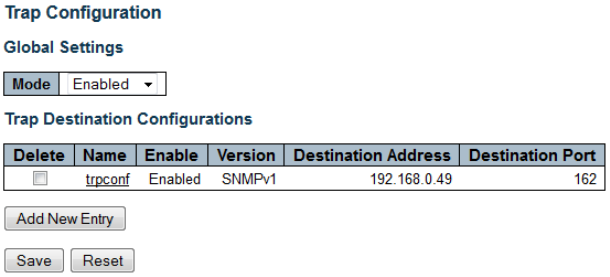
System: The system trap events include the following.
* Warm Start: The switch has been rebooted from an already powered on state.
* Cold Start: The switch has booted from a powered off or due to power cycling (power failure).
AAA: Authentication, Authorization and Accounting; A trap will be issued at any authentication failure.
Switch: Indicates that the Switch group's traps. Possible traps are:
* STP: Enable/disable STP trap.
* RMON: Enable/disable RMON trap.
Power: Indicates the Power group's traps. Possible trap event are:
* Power 1 Status: Enable/disable Power 1 status trap.
* Power 2 Status: Enable/disable Power 2 status trap.
Interface: Indicates the Interface group's traps. Possible traps are:
* Link Up: none/specific/all ports Link up trap.
* Link Down: none/specific/all ports Link down trap.
* LLDP: none/specific/all ports LLDP (Link Layer Discovery Protocol) trap.
* PoE: none/specific/all ports PoE status trap.

When the "specific" radio button is selected, a popup graphic with port check boxes allows selection specific ports.



Port	Link down
*	☐
1	☐
2	☐
3	☑
4	☐
5	☐
6	☐
7	☐
8	☐
9 (Fiber1)	☑
10 (Fiber2)	☐
11 (Fiber3)	☐

After completing all the trap settings, click the "Save" button.



Trap Configuration

Global Settings

Mode: Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
☐	trpconf	Enabled	SNMPv1	192.168.0.49	162

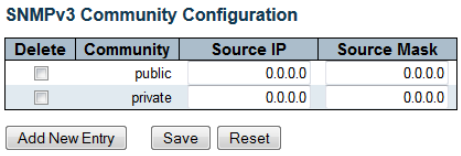
Add New Entry

Save Reset

Additional trap configurations can be created. To delete a configuration, click the delete checkbox and then click the save button.

3.3.5.11 SNMPv3 Community Configuration

Configure SNMPv3 community table on this page. The entry index key is Community.



SNMPv3 Community Configuration

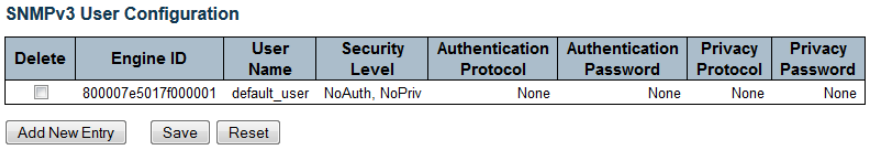
Delete	Community	Source IP	Source Mask
☐	public	0.0.0.0	0.0.0.0
☐	private	0.0.0.0	0.0.0.0

Add New Entry Save Reset

Delete: Check to delete the entry. It will be deleted during the next save.
Community: Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string. This string is case sensitive.
Source IP: Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
Source Mask: Indicates the SNMP access source address mask.

3.3.5.12 SNMPv3 User Configuration

Configure SNMPv3 user table on this page. The entry index keys are Engine ID and User Name.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

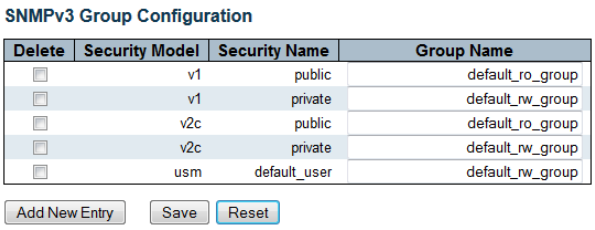
Add New Entry Save Reset

Delete: Check to delete the entry. It will be deleted during the next save.
Engine ID: An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it is a remote user.

User Name: A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.
Security Level: Indicates the security model that this entry should belong to. Possible security models are:
* NoAuth, NoPriv: No authentication and no privacy.
* Auth, NoPriv: Authentication and no privacy.
* Auth, Priv: Authentication and privacy.
The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
Authentication Protocol: Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:
* None: No authentication protocol.
* MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
* SHA: An optional flag to indicate that this user uses SHA authentication protocol.
The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.
Authentication Password: A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32 characters. For SHA authentication protocol, the allowed string length is 8 to 40 characters. The allowed content is ASCII characters from 0x21 to 0x7E.
Privacy Protocol: Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:
* None: No privacy protocol.
* DES: An optional flag to indicate that this user uses DES authentication protocol.
* AES: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

3.3.5.13 SNMPv3 Group Configuration

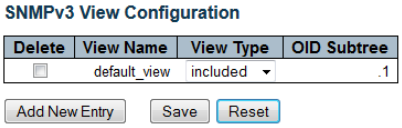
Configure SNMPv3 group table on this page. The entry index keys are Security Model and Security Name.



Delete: Check to delete the entry. It will be deleted during the next save.
Security Model: Indicates the security model that this entry should belong to. Possible security models are:
* v1: Reserved for SNMPv1.
* v2c: Reserved for SNMPv2c.
* usm: User-based Security Model (USM) for SNMPv3.
Security Name: A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.
Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

3.3.5.14 SNMPv3 View Configuration

Configure SNMPv3 view table on this page. The entry index keys are View Name and OID Subtree.

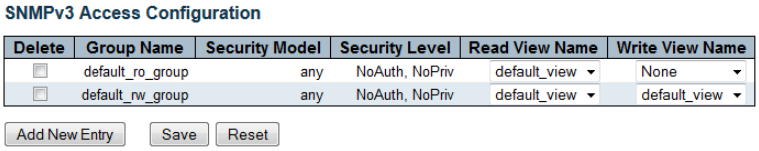


Delete: Check to delete the entry. It will be deleted during the next save.
View Name: A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

View Type: Indicates the view type that this entry should belong to. Possible view types are:
* included: An optional flag to indicate that this view subtree should be included.
* excluded: An optional flag to indicate that this view subtree should be excluded.
In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.
OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or an asterisk(*).

3.3.5.15 SNMPv3 Access Configuration

Configure SNMPv3 access table on this page. The entry index keys are Group Name, Security Model and Security Level.



Delete: Check to delete the entry. It will be deleted during the next save.
Group Name: A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.
Security Model: Indicates the security model that this entry should belong to. Possible security models are:
* any: Any security model accepted(v1|v2c|usm).
* v1: Reserved for SNMPv1.
* v2c: Reserved for SNMPv2c.
* usm: User-based Security Model (USM) for SNMPv3.
Security Level: Indicates the security model that this entry should belong to. Possible security models are:
* NoAuth, NoPriv: No authentication and no privacy.
* Auth, NoPriv: Authentication and no privacy.
* Auth, Priv: Authentication and privacy.
Read View Name: The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.
Write View Name: The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 0x21 to 0x7E.

3.3.5.16 RMON Statistics Configuration

Configure RMON Statistics table on this page. The entry index key is ID.

Delete: Check to delete the entry. It will be deleted during the next save.
ID: Indicates the index of the entry. The range is from 1 to 65535.
Data Source: Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2005

edit here

Chapter 4. Maintenance and Troubleshooting

Acronyms

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID. There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights. ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the preferred media.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logins. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is no longer considered an adequate degree of encryption for commercial exchange.

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server. IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server. The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast. IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile

IPMC Profile is an acronym for IP MultiCast Profile. IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximum response time used to calculate the Maximum Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier

A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

OAM

OAM is an acronym for Operation Administration and Maintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implements the Ethernet physical layer (IEEE-802.3).

PING

Ping (Packet InterNet Grouper) is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

Ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet. Power over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN Access Points (AP), IP cameras and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCI

QCI is an acronym for QoS Class Identifier. This is a special identifier defining the quality of packet communication provided by LTE (Long Term Evolution, marketed as 4G LTE).

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

Querier Election

Querier election is used to dedicate the Querier, the only one router sends Query messages, on a particular link. Querier election rule defines that IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

SAMBA

Samba is a program running under UNIX-like operating systems (not the Brazilian dance) that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.

Additional information can be found at http://sflow.org.

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

Switch ID

Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame. The 3-bits provide 8 priority levels (0~7).

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, and are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

CTC union®

www.ctcu.com

T +886-2 2659-1021 **F** +886-2 2659-0237 **E** sales@ctcu.com