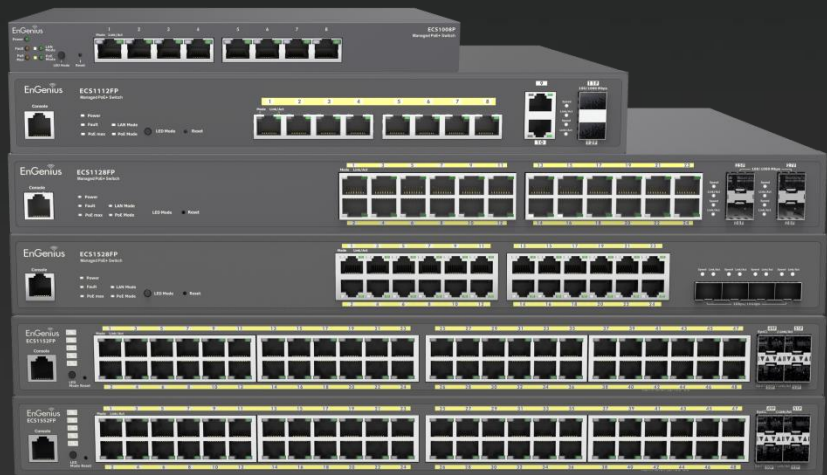


User Manual

Cloud Managed PoE Switch



ECS Switch Series

version 1.0

IMPORTANT

To install this device please refer to the Quick Installation Guide included in the product packaging.

Table of Contents

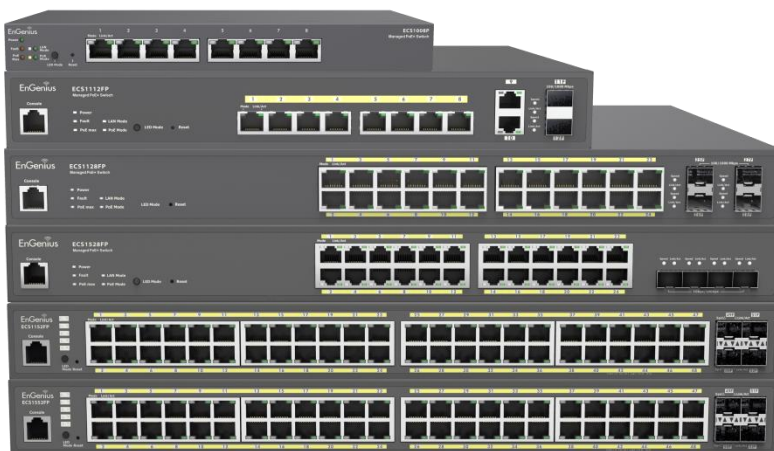
Product Overview	6
Introduction	7
Key Features	8
System Requirements	9
Package Contents	9
LED's behavior for ECS switch	10
Technical Specifications.....	15
Getting Started.....	19
Installing the Switch	20
Management Interface	20
Connecting the Switch to a Network	21
Software Features	23
Using the Switch.....	24
Ethernet Switch Features	24
System	24
Summary	24
IP Settings.....	25
ARP Settings	30
Static Route	32
Neighbor Table	33
System Time	34
Port Settings	37
DHCP Snooping	39
DHCP Relay.....	42
PoE	43
EEE.....	46
L2 Feature.....	47
Link Aggregation.....	47
Mirror Settings	52
STP.....	54
LBD	69
MAC Address Table	70

LLDP.....	73
IGMP Snooping	77
MLD Snooping.....	83
Multicast Filtering	87
Jumbo Frame.....	87
VLAN.....	89
802.1Q.....	90
PVID.....	91
Voice VLAN	93
Management.....	97
System Information	97
User Management	98
Dual Image	99
SNMP.....	100
ACL	111
MAC ACL.....	112
MAC ACE	113
IPv4 ACL.....	115
IPv4 ACE	116
IPv6 ACL.....	118
IPv6 ACE	119
ACL Binding	121
QoS.....	122
Global Settings	123
CoS Mapping	124
DSCP Mapping.....	125
Port Settings.....	126
Advanced mode	127
Bandwidth Control	128
Storm Control.....	129
Security	131
802.1x.....	131
RADIUS Server.....	135
Access.....	136

Port Security.....	138
Port Isolation.....	139
DoS.....	140
Monitoring.....	141
Port Statistics.....	141
RMON.....	142
Log.....	148
Diagnostics.....	153
Cable Diagnostics.....	153
Ping Test.....	154
IPv6 Ping Test.....	155
Trace Route.....	156
Maintenance.....	157
Configuration Manager.....	157
Firmware Upgrade.....	158
Appendix.....	159
Appendix A - Federal Communications Commission (FCC) EMC Statement.....	160
Appendix B - IC Interference Statement.....	160
Appendix C - EU Declaration of Conformity.....	161

Chapter 1

Product Overview



Introduction

ECS Cloud managed series switches can be managed by EnGenius Cloud and on-premises platform by ezMaster/Skykey or can be worked as standalone switches, providing enterprise-class features for simplifying network configuration and monitoring at prices affordable to small and mid-sized businesses. With advanced management, EnGenius Switches enhance network performance to allow companies to focus on growing their business.

Simple — With easy-to-deploy design, EnGenius Managed Gigabit PoE Switches are operational within minutes. Organizations with limited IT support and budgets can create a reliable, efficiently managed network in no time.

Flexible — Choose the port and physical configuration that meets your network and space requirements for optimal performance. Select the management method most effective for the network – locally manage, remotely and locally manage or Cloud manage.

Reliable — EnGenius Cloud’s reliable Gigabit access for networked devices reduces delays that interrupt communications

Secure — Keep your network safe with port and server-based security in addition to two factor authentication and encryption. By setting up event-based alerts, receive push notifications through the EnGenius Cloud app when potential issues arise.

Key Features

- > 100/1000/2500/5000/10000 Mbps Gigabit Ethernet Ports
- > Dedicated SFP / SFP+ slots for longer connectivity via fiber uplinks and for uplink redundancy and failover
- > IGMP and MLD snooping provides advanced multicast filtering
- > IEEE802.3ad Link Aggregation
- > STP/RSTP/MSTP
- > Access Control List/ Port Security
- > IEEE802.1X and RADIUS Authentication
- > RMON
- > SNMP v1/v2c/v3
- > Voice VLAN for fast and reliable deployment of VoIP
- > Energy Efficient Ethernet (IEEE802.3az) support for better energy saving when more EEE-compliant end devices are available in the market
- > Advanced QoS with IPv4/IPv6 ingress traffic filtering (ACLs) and prioritization
- > Easy to manage via Web-Based Management GUI for switch deployment
- > Standard-based technology, ensuring interoperability with any standard-based devices in the existing network
- > Dual firmware images, improving reliability and uptime for your network

System Requirements

The following are the minimum system requirements in order to configure the device:

- > Computer with an Ethernet interface or wireless network capability
- > Windows OS (XP, Vista, 7, 8, 10), Mac OS, or Linux-based operating systems
- > Web-Browsing Application (i.e. Internet Explorer, Firefox, Chrome, Safari, or another similar browser application)

Package Contents

The package contains the following items (all items must be in package to issue a refund):

[ECS1008P](#)

- > EnGenius Switch
- > Power Adapter / Power Cord
- > Rubber Footpads
- > Wall-mount Kit
- > Quick Installation Guide

[ECS1112FP/ECS1528/ECS1528FP/ECS1552/ECS1552FP](#)

[ECS2512FP/ECS2512/ECS5512FP/ECS5512](#)

- > EnGenius Switch
- > Power Cord
- > RJ-45 Console Cable
- > Rack-mount Kit
- > Quick Installation Guide

LED's behavior for ECS switch

ECS1008P				
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps
		Amber	Solid Light	Speed 100 Mbps
		Off	Light off	Speed 10 Mbps
	PoE Mode	Green	Solid Light	Power feeding
		Amber	Solid Light	Error Condition
		Off	Light off	No Power feeding
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
LED Per SFP Port	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

ECS1528FP/ ECS1552FP				
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps
		Amber	Solid Light	Speed 100 Mbps
		Off	Light off	Speed 10 Mbps
	PoE Mode	Green	Solid Light	Power feeding
		Amber	Solid Light	Error Condition
		Off	Light off	No Power feeding

	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
LED Per SFP Port	Speed	Green	Solid Light	Speed 10 Gbps
		Amber	Solid Light	Speed 1 Gbps
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

ECS1552/ ECS1528				
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 1000 Mbps
		Amber	Solid Light	Speed 100 Mbps
		Off	Light off	Speed 10 Mbps
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
LED Per SFP Port	Speed	Green	Solid Light	Speed 1000Mbps
			Light off	No Link
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

ECS2512				
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 2500 Mbps
		Amber	Solid Light	Speed 1000 Mbps/ 100 Mbps
		Off	Light off	No Link
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
LED Per SFP+ Port	Speed	Green	Solid Light	Speed 10000 Mbps
		Amber	Solid Light	Speed 1000 Mbps
		Off	Light off	No Link
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

ECS2512FP					
LED Per copper Port	LAN Mode	Green	Solid Light	Speed 2500 Mbps	
		Amber	Solid Light	Speed 1000 Mbps/ 100 Mbps	
		Off	Light off	No Link	
	PoE Mode	Green	Solid Light	Power feeding	
			Amber	Solid Light	Error Condition
			Off	Light off	No Power feeding
	Link/Act	Green	Solid Light	Link	
			Blinking	Transmit or receive on this port	
			Light off	No Link	
LED Per SFP+ Port	Speed	Green	Solid Light	Speed 10000 Mbps	

		Amber	Solid Light	Speed 1000 Mbps	
		Off	Light off	No Link	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
				Light off	No Link

ECS5512

LED Per copper Port	LAN Mode	Green	Solid Light	Speed 10G	
		Amber	Solid Light	Speed 5G/2.5G /1000 Mbps/ 100 Mbps	
		Off	Light off	No Link	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
				Light off	No Link

LED Per SFP+ Port	Speed	Green	Solid Light	Speed 10Gbps	
		Amber	Solid Light	Speed 1000 Mbps	
		Off	Light off	No Link	
	Link/Act	Green		Solid Light	Link
				Blinking	Transmit or receive on this port
				Light off	No Link

ECS5512FP

LED Per copper Port	LAN Mode	Green	Solid Light	Speed 10G	
		Amber	Solid Light	Speed 5G/2.5G /1000 Mbps/ 100 Mbps	
		Off	Light off	No Link	
	PoE Mode	Green		Solid Light	Power feeding
				Amber	Error Condition
				Off	No Power feeding

LED Per SFP+ Port	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link
	Speed	Green	Solid Light	Speed 10Gbps
			Amber	Speed 1000 Mbps
			Off	No Link
	Link/Act	Green	Solid Light	Link
			Blinking	Transmit or receive on this port
			Light off	No Link

Technical Specifications

	ECS1008P	ECS1112FP
10/100/1000Mbps Ports	8	10
SFP Slots	-	2
RJ45 Console Ports	-	1
PoE Standard	IEEE 802.3 af	
PoE Capable Ports	Port 1-8	Port 1-8
Total PoE Power Budget	55w	130W
Max PoE power	Up to 15W per port	
Switching Capacity	20Gbps	24Gbps
Packet Buffer Memory	512 KB	512 KB
Forwarding Rate	11.9Mpps	17,8Mpps
Mac Address Table Size	8K	8K
Jumbo Frame Size	9K	9K

	ECS1528	ECS1552	ECS1528FP	ECS1552FP
10/100/1000Mbps Ports	28	48	24	48
SFP+ Slots	4 (10G)	4 (10G)	4 (10G)	4 (10G)
RJ45 Console Ports	1	1	1	1
PoE Standard	NA	IEEE 802.3 af/at		
PoE Capable Ports	NA	Port 1-24		Port 1-48
Total PoE Power Budget	NA	410W		740W
Max PoE power	NA	Up to 30W per port		
Switching Capacity	128Gbps	176Gbps	128Gbps	176Gbps
Packet Buffer Memory	1.5MB	2MB	1.5MB	2MB
Forwarding Rate	95.23Mpps	130.95Mpps	95.23Mpps	130.95Mpps
Mac Address Table Size	16K	32K	16K	32K
Jumbo Frame Size	10K	10K	10K	10K

	ECS2512	ECS5512	ECS2512FP	ECS5512FP
MultiG RJ-45 Ports	8x2.5G	8x10G	8x2.5G	8x10G
SFP+ Slots	4	4	4	4
RJ45 Console Ports	1	1	1	1
PoE Standard		NA	IEEE 802.3 af/at / bt	IEEE 802.3 af/at / bt
PoE Capable Ports		NA	Port 1-8	Port 1-8
Total PoE Power Budget		NA	240W	420W
Max PoE power		NA	60W per port	60W per port
Switching Capacity	120Gbps	240Gbps	120Gbps	240Gbps
Packet Buffer Memory	1.5MB	1.5MB	1.5MB	1.5MB
Forwarding Rate	89.29Mpps	178.57Mpps	89.29Mpps	178.57Mpps
Mac Address Table Size	32K	32K	32K	32K
Jumbo Frame Size	10K	10K	10K	10K

Software Features

L3 Features

Multiple IP Interface

- 20 IPv6 address

ARP Table

- Maximum of 192 ARP entries
- Maximum of 192 Static ARP entries

Static Route

- Maximum 63 IPv4 Static Route entries
- Maximum 21 IPv6 Static Route entries

L2 Features

802.3ad Link Aggregation

- Maximum of 8 groups/8 ports per group

Port Mirroring

- One-to-One
- Many-to-One

Spanning Tree Protocol

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

MAC Address Table

- 8K entries (ECS1008P/ECS1112FP)
- 16K entries (ECS1528FP)
- 32K entries (ECS1552FP)

802.1ab Link Layer Discovery Protocol

IGMP Snooping

- IGMP v1/v2/v3 Snooping
- Supports 256 IGMP groups
- IGMP per VLAN

- IGMP Snooping Querier

- IGMP Snooping Fast Leave

MLD Snooping

- MDL Snooping v1/v2
- Supports 256 MLD groups
- IGMP per VLAN

Jumbo Frame

- Up to 9216 bytes

802.3x Flow Control

802.3az Energy Efficient Ethernet

VLAN

802.1Q support

VLAN Group

- Max 4094 static VLAN groups
- Voice VLAN

QoS

802.1p Quality of Service

- 8 queues per port

Queue Handling

- Strict
- Weighted Round Robin (WRR)

QoS based on:

- 802.1p Priority
- DSCP

Bandwidth Control

- Port-based (Ingress/Egress, 64 Kbps~1000 Mbps)

Broadcast/Unknown Multicast/ Unknown Unicast

Storm Control

Access Control List (ACL)

Layer 2/3

- Support maximum 32 entries (ACL)
- Support maximum 256 entries (ACE)

ACL based on:

- MAC address
- VLAN ID
- 802.1p priority
- Ethertype
- IP address
- Protocol type
- DSCP

Security

802.1X

- Guest VLAN

- Port-based Access Control

Supports RADIUS Authentication

Port Security

- up to 256 MAC Addresses per port

Port Isolation

DoS Attack Prevention

BPDU Attack Prevention

Monitoring

Port Statistics

System Log

RMON

Management

Web Graphical User Interface (GUI)

Command Line Interface (CLI)

BootP/DHCP Client/DHCPv6 Client

SSH Server

Telnet Server

TFTP Client

HTTPS

SNMP

- Supports v1/v2c/v3

SNMP Trap

SNTp

Configuration restore/backup

Dual Images

Diagnostic

Cable Diagnostic

Ping Test

Trace Route

MIB/RFC Standards

RFC1213

RFC1493

RFC1757

RFC2674

RFC2863

Environment Specifications

Operating Temperature

0 to 40°C (ECS1008P)

0 to 50°C (ECS1112FP, ECS1528, ECS1528FP,

ECS1552, ECS1552FP, ECS2512, ECS2512FP,

ECS5512, ECS5512FP)

Storage Temperature

-40°C to 70°C

Humidity (Non-condensing)

5% - 95%

Physical Specifications

Dimensions (W x D x H)

ECS1008P: 240x105x27mm

ECS1112FP: 330x230x44mm

ECS1528: 440x200x44mm

ECS1552: 440x260x44mm

ECS1528FP: 440x260x44mm

ECS1552FP: 440x310x44mm

ECS2512: 330x230x44mm

ECS2512FP: 330x230x44mm

ECS5512: 330x230x44mm

ECS5512FP: 330x230x44mm

Chapter 2

Getting Started

Installing the Switch

This section will guide you through the installation process.

Management Interface

The Switch features an embedded Web interface for the monitoring and management of your device.

Management Interface Default Values

IP Address: 192.168.0.239

Username: admin

Password: password

Connecting the Switch to a Network

Discovery in a Network with a DHCP server

Use the procedure below to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
5. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
6. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
7. Click **IP Settings** under the **System tab** and select IPv4 or IPv6.
8. Click **DHCP** under Auto-Configuration.
9. Click **Apply** to save the settings.
10. Connect the Switch to your network (DHCP enabled).
11. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

Discovery in a Network with a DHCP server

This section describes how to set up the Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based management interface.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000Mbps) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are **Green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connection**. Select **Internet Protocol Version 4 (TCP/IPv4)**.
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: **192.168.0.200** and the Subnet mask address as **255.255.255.0**).
6. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and press **Enter**.
7. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**. To make access to the web-based management interface more secure, it's highly recommended that you change the password to something more unique.
8. Click **IP Settings** under the **System menu** and select **Static IP** to configure the IP settings of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Chapter 3

Software Features

Using the Switch

The ECS Cloud managed Switch possesses functions of a full-featured Layer 2 Ethernet Switch.

Ethernet Switch Features

System

Summary

The Summary page shows general system information for the Switch including the device name, the software version, serial number, MAC address, IP Address, gateway address, and system uptime.



Device Name	Displays the model name of the device.
FW Version	Displays the installed firmware version of the device.
Serial Number	Displays the serial number of the device.
Base MAC Address	Displays the MAC address of the device.


Check Code	Check Codes are used for registering device to ezMaster
System Uptime	Displays the number of days, hours, and minutes since the last system restart. The System Uptime is displayed in the following format: days, hours, and minutes.

IP Settings

The IP Setting screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

To access the page, click **IP Settings** under the **System** menu.

IPv4 Management

You can see the current IPv4 IP setting in this page. Press  to edit the IPv4 address setting.

IPv4 Management			
VlanID	Address	Subnet Mask	Configuration
1	10.0.84.85	255.255.254.0	DHCP 

Select whether you wish to enable Static / DHCP / BOOTP for auto-configuration. If you would like to setup the Static IP address on your device, enter the information for the VLAN ID, IP address, and Subnet Mask.

IPv4 Management

VlanID	Address	Subnet Mask	Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="1"/>	<input type="text" value="192.168.0.239"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="Static"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Important:

If the device fails to retrieve an IP address through DHCP, the default IP address is **192.168.0.239** and the factory default subnet mask is **255.255.255.0**.

Dynamic IP Address (DHCP)	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway IP address, and a domain name server IP address automatically. Selecting this field disables the IP Address, Subnet Mask, and Gateway fields.
Static IP Address	Allows the entry of an IP address, subnet mask, and a default gateway for the Switch. Select this option if you don't have a DHCP server or if you wish to assign a static IP address to the Switch.
VlanID	Define the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: 192.168.0.239
Subnet Mask	A subnet mask separates the IP address into the network and host addresses. A bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: 255.255.255.0

Click to save settings.

IPv6 Management

IPv6 is an upgraded version to IPv4, providing more available IP addresses as well as other benefits. To access the switch over an IPv6 network you must first configure it with IPv6 information (IPv6 prefix, prefix length). To configure IPv6 for the Switch, select whether to you wish to enable **Stateful DHCPv6**, **Stateless DHCPv6**, or **Static**. Next, enter the information for the IP address, and Prefix Length.

IPv6 Management

DHCPv6

Static
 Stateless DHCPv6
 Stateful DHCPv6

VlanID	Address	Prefix Length	Address Type
1	fe80::8adc:96ff:fe78:4ea6	128	LinkLocal <input checked="" type="checkbox"/> <input type="checkbox"/>

DHCPv6	Select whether you wish to enable Static, Stateless DHCPv6, or Stateful DHCPv6.
Stateful DHCPv6	Stateful DHCPv6 is used to pass out addressing and service information in the same way that DHCP is used in IPv4. Use this option to set the IPv6 address for the IPv6 network interface in Auto Configuration. The Switch will automatically generate and use a globally-unique IPv6 address based on the network prefix and its Ethernet MAC address.
Stateless DHCPv6	Stateless DHCPv6 provides a host gains an address via an interface automatically "leasing" an address and does not require the establishment of an server to delve out address space. Stateless auto configuration allows a host to propose an address which will probably be unique (based on the network prefix and its Ethernet MAC address) and propose its use on the network. Because no server has to approve the use of the address, or pass it out, stateless auto configuration is simpler. Select this option if you do not have an IPv6 DHCP server that can assign the Switch an IPv6 address/prefix and a default gateway IP address.
Static	Allows the entry of an IPv6 address/prefix and a default gateway for the Switch. Select this option if you wish to assign static IPv6 address information to the Switch.
IPv6 Address	This field allows the entry of an IPv6 address/prefix to be assigned to this IP interface.
Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Goba Unicast IPv6 Address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.

Click  to save settings.

IPv4 Network

You can setup the multiple IPv4 address in this page. If you would like to setup the multiple Static IP address on your device, click **Add** button.

IPv4 Network

VlanID	Address	Subnet Mask	<input type="button" value="+ Add"/>
--------	---------	-------------	--------------------------------------

Enter the information for the VLAN ID, IP address, and Subnet Mask.

Pv4 Network

VlanID	Address	Subnet Mask	<input type="checkbox"/> <input type="button" value="✕"/>
2	192.168.1.200	255.255.255.0	

VlanID	Define the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: 192.168.0.239
Subnet Mask	A subnet mask separates the IP address into the network and host addresses. A bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: 255.255.255.0

IPv6 Network

You can setup the multiple IPv6 address in this page. If you would like to setup the multiple Static IP address on your device, click **Add** button.

IPv6

VlanID	Address	Prefix Length	Address Type
--------	---------	---------------	--------------

+ Add

Enter the information for the VLAN ID, IP address, Prefix Length and Choose the Address Type.

IPv6

VlanID	Address	Prefix Length	Address Type
		0 ~ 128	Unicast ▼







✓
✕

VlanID	Define the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
Address	This field allows the entry of an IPv6 address to be assigned to this IP interface.
Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Global Unicast IPv6 Address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.
Address Type	Unicast: Unicast IP address is standard globally unique unicast addresses (public IPv6 addresses) as in IPv6. LinkLocal: Link local address is a network address that is valid only for communications within the network segment or the broadcast domain that the host is connected to.

DNS Server

DNS (Domain Name System) is used for mapping a domain name to its corresponding IP addresses and vice versa. Enter a DNS IP address in order to be able to use a domain name to access the Switch instead of using an IP address.

DNS Servers

Name	Address	
DNS 1	2001:b000::1	 
DNS 2	2001:b000::8	 
DNS 3	n/a	
DNS 4	n/a	

ARP Settings

The Address Resolution Protocol (ARP) feature performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses.

ARP Global

You can setup the Address Resolution Protocol (ARP) in this page.

Address Resolution Protocol (ARP) Global

Settings

Max retries: (2-10)

Timeout: (30-86400)

Max retries	Setup the ARP max retries value. The default value is: 3. The range is from 2 to 10.
Timeout	Setup the timeout interval value. The default value is: 300. The range is from 30 to 86400.

ARP Table

You can setup the IP Address, MAC Address and interface in the ARP table.

Address Resolution Protocol (ARP) table

Address	MAC Address	Interface	Mapping
10.0.84.3	00:80:8e:8a:94:e6	vlan1	Dynamic
10.0.85.254	c0:ea:e4:af:79:f6	vlan1	Dynamic

<input type="text" value="xxx.xxx.xxx.xxx"/>	<input type="text" value="xx:xx:xx:xx:xx:xx"/>	<input type="text" value="vlan 1"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
--	--	-------------------------------------	--

Address	IP address for an ARP table entry.
MAC address	Hardware MAC address for the ARP table entry
Interface	The VLAN interface of the switch.

ARP Statistics

The ARP Statistics page displays a summary of ARP traffic statistics.

Address Resolution Protocol (ARP) Statistics






Total:	2781968
Bad type:	0
Bad length:	0
Base Address:	311542
Request Discards:	2455163
In Requests:	198
Received:	15065
Request Sent:	0
Drop:	0
Rreplied:	198

Static Route

IPv4 (IPv4 Route)

Use the IPv4 static route to view and configure the IPv4 static and default route settings. The Switch supports static routing for IPv4 formatted addressing. Users can create up to 63 static route entries for IPv4. For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP request will not be sent.

IPv4 Route

Destination IP	Subnet Mask	Gateway	Interface	Routing Protocol	 Add
0.0.0.0	0.0.0.0	10.0.85.254		Static	 
10.0.84.0	255.255.254.0	0.0.0.0	vlan1	Connected	 

IPv4 Route

Destination IP	Subnet Mask	Gateway	Interface	Routing Protocol
0.0.0.0	0.0.0.0	10.0.85.254		Static
10.0.84.0	255.255.254.0	0.0.0.0	vlan1	Connected
<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="checkbox"/> <input type="checkbox"/>

Destination IP	Enter the IPv4 address for this route here.
Subnet Mask	Enter the IPv4 network mask for this route here.
Gateway	Enter the gateway address for this route here.

IPv6 (IPv6 Route)

Use the IPv6 static route to view and configure the IPv6 static and default route settings. The Switch supports static routing for IPv6 formatted addressing. Users can create up to 21 static route entries for IPv6. For IPv6 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the Switch from that next hop, the route becomes enabled. However, if the ARP entry already exists, an ARP

request will not be sent.

IPv6 Route

Destination IP	Prefix Length	Gateway	Interface	Routing Protocol
<input type="text"/>	<input type="text" value="0 ~ 128"/>	<input type="text"/>		<input checked="" type="checkbox"/> <input type="checkbox"/>

Destination IP	Enter the IPv6 address for this route here.
Prefix Length	IPv6 Prefix Length is used to identify how many bits of a Global Unicast IPv6 Address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.
Gateway	Enter the gateway address for this route here.










Neighbor Table

Neighbor Discovery Protocol (NDP) is a function to detect whether IPv6 devices and addresses are duplicated. Use the following five packages:

- Neighbor Solicitation (NS): The request sent by the host to the link layer
- Neighbor Advertisement (NA): The response sent by the host to the link layer
- Router Request (RS): The request sent by the host to the router
- Router advertisement (RA): the response of the router to the host and the periodic multicast packet
- Redirection: Router

The Neighbor Discovery table function is similar with the ARP table function in IPv4.

Neighbor Discovery (ND) Table

IPv6 Address	Link-layer Addr	State	Interface	 Add
fe80::898b:693c:2be7:16a4	70:4d:7b:38:fd:e6	Stale	vlan1	 
fe80::b656:b9ff:fe10:78	b4:56:b9:f0:00:78	Stale	vlan1	 
fe80::f920:20d3:931e:1df9	34:97:f6:84:2d:45	Stale	vlan1	 
fe80::f9ac:d7d6:3a47:32a4	14:dd:a9:be:47:aa	Reachable	vlan1	 

The following is the content of the IPv6 Cache Table

IPv6 Address	IPv6 address of the neighbor
Link-layer Addr	Neighbor's MAC address
Stale	There are several types of Stale as below <ul style="list-style-type: none"> - Reachable (acceptable) - Stale (expired) - Delayed (response until stale) - Proble (wait for response) - Invalid, unknown, incomplete
Interface	Indicate the neighbor's VLAN interface

System Time

Use the System Time screen to view and adjust date and time settings.

The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This switch operates only as an SNTP client and cannot provide time services to other systems.

System Time

Settings

Current Time: 2015/Dec/09 15:48:41

Enable SNTP: Enabled Disabled

Time Zone: Set by time (GMT +8 : 0)

Daylight Savings Time: Disabled

SNTP/NTP Server Address: time.stdtime.gov.tw (x.x.x.x or Hostname)

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

Apply

Current time	Displays the current system time.
Enable SNTP	Select whether to enable or disable system time synchronization with an SNTP server.
Time Zone	Configure the time zone setting either by setting GMT difference or by country.
Daylight Savings Time	Select from Disabled, Recurring or Non-recurring.
Daylight Savings Time Offset	Enter the time of Daylight Savings Time Offset.
Recurring From	Select the Day, Week, Month, and Hour from the list.
Recurring To	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address	Enter the IP address or hostname of the SNTP/NTP server.
Server Port	Enter the server port of the SNTP/NTP server.

To configure date/time through SNMP:

1. Next to the Enable SNTP, select Enable.
2. In the Time Zone Offset list, select by country or by the GMT time zone in which the Switch is located.

3. Next select Disabled, Recurring, or Non-Recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
4. In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.
5. Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1–65535. The default is: 123.
6. Click Apply to update the system settings.

To configure date/time manually:

1. Next to the Enable SNTP, select Disable.
2. In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.
3. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.
4. Next select Disabled, Recurring or Non-recurring for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
5. Click Apply to update the system settings.

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings page allows you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports.

To access the page, click **Port Settings** under the **System** menu.

Port Settings				
	Port	Link Status	Mode	Flow Control
<input type="checkbox"/>			Auto <input type="button" value="v"/>	Disabled <input type="button" value="v"/>
<input type="checkbox"/>	1	Link Down	Auto	Disabled
<input type="checkbox"/>	2	Link Down	Auto	Disabled
<input type="checkbox"/>	3	Link Down	Auto	Disabled
<input type="checkbox"/>	4	Link Down	Auto	Disabled
<input type="checkbox"/>	5	Link Down	Auto	Disabled
<input type="checkbox"/>	6	Link Down	Auto	Disabled
<input type="checkbox"/>	7	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	8	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	9	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	10	Link Up	Auto-1000M/Full	Disabled
<input type="checkbox"/>	11	Link Down	Auto	Disabled
<input type="checkbox"/>	12	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk1	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk2	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk3	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk4	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk5	Link Down	Auto	Disabled
<input type="checkbox"/>	trunk6	Link Down	Auto	Disabled

Port	Displays the port number.
Link Status	Indicates whether the link is up or down.
Mode	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port

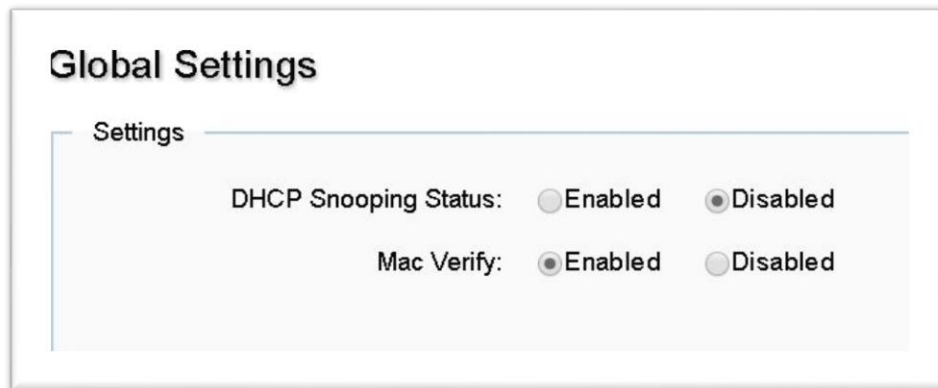
	uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	<p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.</p>

Click **Apply** to save settings.

DHCP Snooping

DHCP snooping is a layer 2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable. The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes. However, the most common DoS scenario is that of an end-user plugging in a consumer-grade router at their desk, ignorant that the device they plugged in is a DHCP server by default.


Global Setting



The screenshot shows a configuration window titled "Global Settings". Inside, there is a section labeled "Settings" which contains two radio button options. The first option is "DHCP Snooping Status", with "Enabled" selected (radio button is empty) and "Disabled" selected (radio button has a dot). The second option is "Mac Verify", with "Enabled" selected (radio button has a dot) and "Disabled" selected (radio button is empty).

DHCP Snooping Status	Setup the DHCP Snooping enable or disable.
Mac Verify	This feature verifies that the source MAC address and the client hardware address in the DHCP packets on untrusted ports match. Enable Mac Verify to enable this feature.

VLAN Setting

VLAN Settings		
VLAN ID	DHCP Snooping Status	
1	Enabled	
2	Disabled	

This setting is to configure the DHCP snooping function in other VLAN. You can configure DHCP snooping for switches and VLANs. When you enable DHCP snooping on a switch, the interface acts as a Layer 2 bridge, intercepting and safeguarding DHCP messages going to a Layer 2 VLAN. When you enable DHCP snooping on a VLAN, the switch acts as a Layer 2 bridge within a VLAN domain.

Trust Port Settings

Port Settings

<input type="checkbox"/>	Port	State
<input type="checkbox"/>		Untrusted ▾
<input type="checkbox"/>	1	Trusted
<input type="checkbox"/>	2	Trusted
<input type="checkbox"/>	3	Trusted
<input type="checkbox"/>	4	Trusted
<input type="checkbox"/>	5	Trusted
<input type="checkbox"/>	6	Trusted
<input type="checkbox"/>	7	Trusted
<input type="checkbox"/>	8	Trusted
<input type="checkbox"/>	trunk1	Trusted
<input type="checkbox"/>	trunk2	Trusted
<input type="checkbox"/>	trunk3	Trusted
<input type="checkbox"/>	trunk4	Trusted
<input type="checkbox"/>	trunk5	Trusted
<input type="checkbox"/>	trunk6	Trusted
<input type="checkbox"/>	trunk7	Trusted
<input type="checkbox"/>	trunk8	Trusted

A trusted port is a port that is connected to a DHCP server and is allowed to assign DHCP addresses. DHCP messages received on trusted ports are allowed to pass through the device. Packets from these ports are automatically forwarded. If DHCP Snooping is not enabled, all ports are trusted by default.

Port	Displays the port number.
State	Indicates whether the Port is Trusted or Untrusted.

Binding list

DHCP Snooping binding list			
VID	Port	MAC Address	IP Address

This table is to display the DHCP Snooping binding list table.

Vlan Statistics

Vlan Statistics												
Vlan	RXDiscovers	RXRequests	RXReleases	RXDeclines	RXInforms	TXOffers	TXAcks	TXNaks	MACDiscard	ServerDiscard	OptionDiscard	TotalDiscard
1	0	0	0	0	0	0	0	0	0	0	0	0

This table is to display the DHCP Snooping VLAN Statistics status.

DHCP Relay

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface.

Global Settings

Global Settings

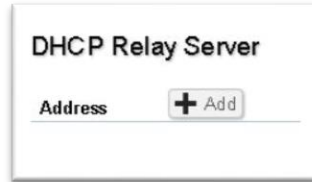
Settings

DHCP Relay Status: Enabled Disabled

Apply

Settings	Setup the DHCP Relay enable or disable.
-----------------	---

DHCP Relay Server



Address	Display the DHCP Relay Server address
Add	Add the DHCP Relay Server

PoE

The PoE Management screen contains system PoE information for monitoring the current power usage and assigns the total amount of power the Switch can provide to all of its PoE ports. To access the page, click PoE under the System menu.

Note: This feature is only available for PoE supported models listed below.

Model	PoE Capable Ports	PoE Standard	PoE Power Budget
ECS1008P	8	IEEE 802.3af	55 Watts
ECS1112FP	8	IEEE 802.3af/at	130 Watts
ECS1528FP	24	IEEE 802.3af/at	410 Watts
ECS1552FP	48	IEEE 802.3af/at	740 Watts
ECS2512FP	8	IEEE 802.3af/at/bt	240 Watts
ECS5512FP	8	IEEE 802.3af/at/bt	420 Watts

Power Budget

Power Budget

Settings

Total Power Budget: Watts. (6~130 Watts.)

Consumed Power: Watts.

Total Power Budget	Enter the amount of power the Switch can provide to all ports.
Consumed Power	Displays the total amount of power (in watts) currently being delivered to all PoE ports.

PoE Port Settings

PoE Port Settings

Port	State	Priority	Power Limit Type	User Power Limit (W)	Status	Class	Output Voltage (V)	Output Current (mA)
<input type="checkbox"/>	Enabled	Low	Auto Class	31				
<input type="checkbox"/> 1	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 2	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 3	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 4	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 5	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 6	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 7	Enabled	Low	Auto Class		Searching			
<input type="checkbox"/> 8	Enabled	Low	Auto Class		Searching			

Port	Displays the specific port for which PoE parameters are defined. PoE parameters are assigned to the powered device that is connected to the selected port.
State	Displays the active participating members of the trunk group.

Member Port	<p>Enable: Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery protocol lets the device discover powered devices attached to device interfaces and learns their classification.</p> <p>Disable: Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.</p>
Priority	<p>Select the port priority if the power supply is low. The field default is Low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power.</p> <p>Low: Sets the PoE priority level as low.</p> <p>Medium: Sets the PoE priority level as medium.</p> <p>High: Sets the PoE priority level as high.</p> <p>Critical: Sets the PoE priority level as critical.</p>
Class (Auto)	<p>Shows the classification of the powered device. The class defines the maximum power that can be provided to the powered device. The possible field values are:</p> <p>Class 0: The maximum power level at the Power Sourcing Equipment is 15.4 Watts.</p> <p>Class 1: The maximum power level at the Power Sourcing Equipment is 4.0 Watts.</p> <p>Class 2: The maximum power level at the Power Sourcing Equipment is 7.0 Watts.</p> <p>Class 3: The maximum power level at the Power Sourcing Equipment is 15.4 Watts.</p> <p>Class 4: The maximum power level at the Power Sourcing Equipment is 30 Watts.</p>
Class (User Defined)	<p>Select this option to base the power limit on the value configured in the User Power Limit field.</p>
User Power Limit	<p>Set the maximum amount of power that can be delivered by a port.</p> <p>Note: The User Power Limit can only be implemented when the Class value is set to User-Defined.</p>
Status	<p>Shows the port's PoE status. The possible field values are:</p> <p>Delivering Power: The device is enabled to deliver power via the port.</p> <p>Disabled: The device is disabled for delivering power via the port.</p> <p>Test Fail: The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device.</p> <p>Testing: The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply.</p> <p>Searching: The device is currently searching for a powered device. Searching is the default PoE operational status.</p> <p>Fault: The device has detected a fault on the powered device when the port is forced on. For example, the power supply voltage is out of range, a short occurs, a communication or there is a communication error with PoE devices, or an unknown</p>

	error occurs.
--	---------------

Click **Apply** to save settings.

EEE

Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 Switch complies with the IEEE’s Energy-Efficient Ethernet (EEE) standard. The EEE compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet ideal time.

Use the **EEE** configuration page to configure Energy Efficient Ethernet.

Energy-Efficient Ethernet

	Port	EEE Status
<input type="checkbox"/>		Disabled <input type="button" value="v"/>
<input type="checkbox"/>	1	Disabled
<input type="checkbox"/>	2	Disabled
<input type="checkbox"/>	3	Disabled
<input type="checkbox"/>	4	Disabled
<input type="checkbox"/>	5	Disabled
<input type="checkbox"/>	6	Disabled
<input type="checkbox"/>	7	Disabled
<input type="checkbox"/>	8	Disabled
<input type="checkbox"/>	9	Disabled
<input type="checkbox"/>	10	Disabled

Port	Display the port for which the EEE setting is displayed.
EEE Status	Enable or disable EEE for the specified port.

Click **Apply** to save settings.

L2 Feature

The L2 Feature tab exhibits complete standard-based Layer 2 switching capabilities, including: Link Aggregation, 802.1D Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1s Multiple Spanning Tree Protocol, MAC Address Table, Internet Group Management Protocol (IGMP) Snooping, Port Mirroring, 802.1ab Link Layer Discovery Protocol (LLDP), and Multicast Listener Discovery (MLD) snooping. Utilize these features to configure the Switch to your preferences.

Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch. Link Aggregation is most commonly used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called Members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of the one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- > All ports within a LAG must be the same media/format type.
- > A VLAN is not configured on the port.
- > The port is not assigned to another LAG.
- > The Auto-negotiation mode is not configured on the port.
- > The port is in full-duplex mode.
- > All ports in the LAG have the same ingress filtering and tagged modes.

- > All ports in the LAG have the same back pressure and flow control modes.
- > All ports in the LAG have the same priority.
- > All ports in the LAG have the same transceiver type.
- > Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the participating Switches/devices that support the standard, to use it.









Port Trunking

Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger “pipe”.




Important:

You must enable Trunk Mode before you can add a port to a trunk group.

Group	Active Ports	Member Ports	Mode
1			Disabled 
2			Disabled 
3			Disabled 
4			Disabled 
5			Disabled 
6			Disabled 
7			Disabled 
8			Disabled 

Group	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups and each group consisting up to 8 ports on the Switch.
Active Ports	Displays the active participating members of the trunk group.
Member Port	Select the ports you wish to add into the trunk group. Up to eight ports per group can be assigned. Static: The Link Aggregation is configured manually for specified trunk group. LACP: The Link Aggregation is configured dynamically for specified trunk group.
Mode	LACP allows for the automatic detection of links in a port trunking group when connected to a LACP-compliant Switch. You will need to ensure that both the Switch and device connected to are in the same mode in order for them to function, otherwise they will not work. Static configuration is used when connecting to a Switch that does not support LACP.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

LACP Settings

Assign a system priority to run with Link Aggregation Control Protocol (LACP) and is become for a backup link if a link goes down. The lowest system priority is allowed to make decisions about which ports it is actively participating in in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is: **32768**.

LACP Settings

Settings

System Priority: (1~65535)

System Policy: ▼

System Priority	Enter the LACP priority value to the system. The default is 32768 and the range is from 1 to 65535.
System Policy	Src-mac: Source MAC address Dest-mac: Destination MAC address Src-dst-mac: Source or destination MAC address Src-ip: Source IP address Dest-ip: Destination IP address Src-dst-ip: Source or destination IP address Dest-l4-port/Src-l4-port: Destination & Source TCP/UDP port number - For a Layer 4 frame, it uses the source and destination MAC addresses, the source and destination IP addresses, and the source and destination port number.

Click **Apply** to save settings.

LACP Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between two members of aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is: **Long Timeout**.

Port	Timeout
<input type="checkbox"/>	Long Timeout
<input type="checkbox"/> 1	Long Timeout
<input type="checkbox"/> 2	Long Timeout
<input type="checkbox"/> 3	Long Timeout
<input type="checkbox"/> 4	Long Timeout
<input type="checkbox"/> 5	Long Timeout
<input type="checkbox"/> 6	Long Timeout
<input type="checkbox"/> 7	Long Timeout
<input type="checkbox"/> 8	Long Timeout
<input type="checkbox"/> 9	Long Timeout
<input type="checkbox"/> 10	Long Timeout
<input type="checkbox"/> 11	Long Timeout
<input type="checkbox"/> 12	Long Timeout

Apply

Timeout	Select the administrative LACP timeout. Long Timeout: The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds. Short Timeout: The LACP PDU will be sent every second. The timeout value is 3 seconds.
----------------	--

Click **Apply** to save settings.

Mirror Settings

Mirrors network traffic by forwarding copies of incoming and outgoing packets from specific ports to a monitoring port. The packet that is copied to the monitoring port will be the same format as the original packet.

Port mirroring is useful for network monitoring and can be used as a diagnostic tool. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring and predicting traffic patterns, and other correlating events. Port Mirroring is needed for traffic analysis on a Switch because a Switch normally sends packets only to the port to which the destination device is connected. The analyzer captures and evaluates the data without affecting the client on the original port. Port mirroring can consume significant CPU resources while active, so be cautious of such usage when configuring the Switch.



Mirror Settings						
Session ID	Destination Port	Source TX Port	Source RX Port	Ingress State	Session State	
1	N/A			Disabled	Disabled	
2	N/A			Disabled	Disabled	
3	N/A			Disabled	Disabled	

Session ID	A number identifying the mirror session. This Switch only supports up to 4 mirror sessions.
Destination Port	Select the port for traffic purposes from source ports mirrored to this port.
Source TX/RX Port	Sets the source port from which traffic will be mirrored. TX Port: Only frames transmitted from this port are mirrored to the destination port. RX Port: Only frames received on this port are mirrored to the destination port. Both: Frames received and transmitted on this port are mirrored to the specified destination port. None: Disables mirroring for this port.
Ingress State	Select whether to enable or disable ingress traffic forwarding.
Session State	Select whether to enable or disable port mirroring.



Note

You cannot mirror a faster port onto a slower port. For example, if you try to mirror the traffic from a 100Mbps port onto a 10Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

STP

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between Switches. This allows the Switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP provides a tree topology for the Switch. There are different types of Spanning tree versions, supported, including Spanning Tree Protocol (STP) IEEE 802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE 802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s. Please note that only one spanning tree can be active on the Switch at a time.

Global Settings

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on Switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDUs after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the Switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links is also accomplished automatically.

STP provides a tree topology and other Spanning tree versions supported include STP, Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP). Please note that only one spanning tree can be active on the Switch at a time. The default setting is: MSTP.

Global Settings

Settings

STP State: Enabled Disabled

Force Version:

Configuration Name: (char : 0 ~ 32)

Configuration Revision: (0-65535)

Priority: (4096*N)

Forward Delay: (4-30)

Maximum Age: (6-40)

TX Hold Count: (1-10)

Hello Time: (1-2)

MSTP:

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reduce the number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficient to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP	Select whether to enable or disable the spanning tree operation on the Switch.
Force Version	Select the Force Protocol Version parameter for the Switch.

	MSTP (Multiple Spanning Tree Protocol): IEEE 802.1s
Configuration Name	Sets the configuration name of the STP setting, the maximum number of character is 32.
Configuration Revision	Sets the MSTP revision level, the range of the level is from 0~65535. Default is 0.
Priority	Setup the priority to define the root bridge of the switch. The Priority number should be the multiple of the number 4096.
Forward Delay	It means the transfer delay time. The maximum time required for a frame to be transmitted from the beginning to the frame through all bridges, one cycle preset for 15 seconds
Maximum Age	It means the BPDU save time. It is used to detect any change in the topology. The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. This time is 20 sec by default, but you can tune the time to be between 6 and 40 sec.
Tx Hold Count	The Tx hold count controls the number of BPDUs that can be sent before pausing for 1 second. This time is 6 sec by default, but you can tune the time to be between 1 and 10 sec.
Hello Time	The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 2 sec.

RSTP:

The screenshot shows the 'Global Settings' interface for RSTP configuration. It includes a 'Settings' section with the following parameters:

- STP State: Enabled Disabled
- Force Version: RSTP (dropdown menu)
- Priority: 32768 (dropdown menu) (4096*N)
- Forward Delay: 15 (input field) (4-30)
- Maximum Age: 20 (input field) (6-40)
- TX Hold Count: 6 (input field) (1-10)
- Hello Time: 2 (input field) (1-2)

RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network. This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

STP	Select whether to enable or disable the spanning tree operation on the Switch.
Force Version	Select the Force Protocol Version parameter for the Switch. RSTP (Rapid Spanning Tree Protocol): IEEE 802.1w
Priority	Setup the priority to define the root bridge of the switch. The Priority number should be the multiple of the number 4096.
Forward Delay	It means the transfer delay time. The maximum time required for a frame to be transmitted from the beginning to the frame through all bridges, one cycle preset for 15 seconds
Maximum Age	It means the BPDU save time. It is used to detect any change in the topology. The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. This time is 20 sec by default, but you can tune the time to be between 6 and 40 sec.
Tx Hold Count	The Tx hold count controls the number of BPDUs that can be sent before pausing for 1 second. This time is 6 sec by default, but you can tune the time to be between 1 and 10 sec.
Hello Time	The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 2 sec.

Select whether to Enable or Disable the Spanning Tree function for the Switch. Next, select whether you wish to enable RSTP, or MSTP. Again, please note that only one Spanning tree function can be active at a time.

Click **Apply** to save settings.

Root Bridge:

The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops. From here, you can view all the information regarding the Root Bridge within the STP.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the “root” of the constructed “tree” within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge ID includes two parts; the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is: 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges “listen” for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

Root Bridge Information	
Bridge Address	88:dc:96:78:4e:67
Root Address:	00:00:FA:EB:6A:DD
Priority:	32768
Cost:	60000
Port:	1
Forward Delay:	15 (sec)
Maximum Age:	20 (sec)
Hello Time:	2 (sec)

Bridge Address	Display the MAC address of the bridged network.
Root Address	Displays the root bridge MAC address. Root in root bridge refers to the base of the spanning tree, which the Switch could be configured for.
Priority	Displays the priority for the bridge. When switches are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge.

Forward Delay	Displays the Switch Forward Delay Time. This is the time (in seconds) the root switch will wait before changing states (called listening to learning).
Maximum Age	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 2 seconds.

RSTP Port Setting

RSTP Port Settings												
Port	Priority	Path Cost	Designated Root Bridge	External Root Cost	Designated Bridge	Edge Port Conf / Oper	P2P MAC Conf / Oper	Port Role	Port State	Migration Start	Port Status	
<input type="checkbox"/>	128 ▼	0=Auto				Yes ▼	No ▼			<input type="checkbox"/>	Enabled ▼	
<input type="checkbox"/>	1	20000	32768 / 00:00:FA:EB:6A:DD	60000	32768 / 88:DC:96:78:4E:A6	No / No	Auto / Yes	Root	Forwarding	--	Enabled	
<input type="checkbox"/>	2	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	3	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	4	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	5	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	6	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	7	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	8	20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk1	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk2	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk3	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk4	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk5	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk6	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk7	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	
<input type="checkbox"/>	trunk8	200000000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / --	Auto / --	Disabled	Discarding	--	Enabled	

MST ID	Select the MST ID from the list.
Port	Port or trunked port identifier.
Priority	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a Switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When

	more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0 to 240, in steps of 16; and the default is: 128.
Path Cost	The Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Designated Root Bridge	Displays the root bridge ID for the root bridge. It is comprised using the bridge priority and the base MAC address of the bridge.
External Root Cost	Displays the root path cost from the switch to the root bridge.
Designated Bridge	This is the bridge identifier of the bridge of the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Edge Port Conf/Oper	Select Yes to set the port as an edge port. When the topology is changed, the edge port can transit its state from blocking to forwarding directly. For the quick generation of the spanning tree, it is recommended to set the ports that are connected to the end devices as edge ports.
P2P MAC Conf/Oper	Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. Three options are supported: Auto, Yes and No. By default, it is No. Auto: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. Yes: A port is set as the one that is connected to a P2P link. You should check the link first. No: A port is set as the one that is not connected to a P2P link. You should check the link first.
Port Role	Displays the role that the port plays in the spanning tree. Root Port: Indicates that the port is the root port in the spanning tree. It has the lowest path cost from the root bridge to this switch and is used to communicate with the root bridge. Designated Port: Indicates that the port is the designated port in the spanning tree. It has the lowest path cost from the root bridge to this physical network segment and is used to forward data for the corresponding network segment. Master Port: Indicates the port provides the lowest root path cost from the region to the root bridge in CIST. In CIST, each region is regarded as a switch, and the master port is the root port of the corresponding region.

	<p>Alternate Port: Indicates that the port is the alternate port in the spanning tree. It is the backup of the root port or master port.</p> <p>Backup Port: Indicates that the port is the backup port in the spanning tree. It is the backup of the designated port.</p> <p>Disabled: Indicates that the port is not participating in the spanning tree.</p>
Port State	<p>The forwarding state of this port.</p> <p>Forwarding: The port receives and sends BPDUs, and forwards user data.</p> <p>Learning: The port receives and sends BPDUs. It also receives user traffic, but doesn't forward the traffic.</p> <p>Disabled: The port only receives and sends BPDUs.</p> <p>Discarding: The port has the spanning tree function enabled but is not connected to any device.</p>

CIST Port Settings

Use the CIST Ports Settings page to configure and view STA attributes for interfaces when the spanning tree mode is set to STP or RSTP. You may use a different priority or path cost for ports of the same media type to indicate a preferred path or edge port to indicate if the attached device can support fast forwarding or link type to indicate a point-to-point connection or shared-media connection.

CIST Port Settings															
	Port	Priority	Internal Path Cost Conf / Oper	External Path Cost Conf / Oper	Path Cost	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Edge Port Conf / Oper	P2P MAC Conf / Oper	Port Role	Port State	Migration Start
<input type="checkbox"/>		128			0=Aut						Yes	Yes			<input type="checkbox"/>
<input type="checkbox"/>	1	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	2	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	3	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	4	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	5	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	6	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	7	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	8	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	9	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	300000	28672 / 0 / 00:13:64:00:15:00	0	28672 / 0 / 00:13:64:00:15:00	Yes / Yes	Auto / Yes	Designated	Forwarding	--
<input type="checkbox"/>	10	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:85:65:52:65:65	280000	32768 / 0 / 88:DC:96:1D:9A:05	0	32768 / 0 / 88:DC:96:1D:9A:05	Yes / No	Auto / Yes	Root	Forwarding	--
<input type="checkbox"/>	11	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	12	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk1	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk2	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk3	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk4	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--
<input type="checkbox"/>	trunk5	128	0 / 20000	0 / 20000	20000	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	0	0 / 0 / 00:00:00:00:00:00	Yes / --	Auto / --	Disabled	Disabled	--

MST ID	Select the MST ID from the list.
Port	Port or trunked port identifier.
Priority	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a Switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0 to 240, in steps of 16; and the default is: 128.
Internal Path Cost Conf/Oper	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
External Path Cost Conf/Oper	The External Path Cost setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge.

Designated Root Bridge	Displays the root bridge for the CST. It is comprised using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	This is the cost to the CIST regional root in a region.
External Root Cost	External root cost is the cost to the CIST root.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	Enter the cost of the port.
Edge Port Conf/Oper	Displays the edge port state.
Designated Bridge	This is the bridge identifier of the bridge of the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Port Role	Each MST bridge port that is enabled is assigned a port role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State	The forwarding state of this port. The state parameters are: Discarding, Learning, Forwarding, or Disabled.
















Click **Apply** to update the system settings.

MST Instance Settings

Multiple Spanning Tree Protocol, or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications between STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support STP, RSTP, and MSTP protocols. Once you specify the VLANs you wish to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Click the Edit button to configure the MST settings. Next, enter information for the VLAN List and choose the priority you wish to use from the drop down list.

MST ID	VLAN List	Priority	Regional Root Bridge	Internal Root Cost	Designated Bridge	Root Port	
1		32768	--/--	0	--/--	--	
2		32768	--/--	0	--/--	--	
3		32768	--/--	0	--/--	--	
4		32768	--/--	0	--/--	--	
5		32768	--/--	0	--/--	--	
6		32768	--/--	0	--/--	--	
7		32768	--/--	0	--/--	--	
8		32768	--/--	0	--/--	--	
9		32768	--/--	0	--/--	--	
10		32768	--/--	0	--/--	--	
11		32768	--/--	0	--/--	--	
12		32768	--/--	0	--/--	--	
13		32768	--/--	0	--/--	--	
14		32768	--/--	0	--/--	--	
15		32768	--/--	0	--/--	--	

MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN List	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768. The range is from 0 to 61440. The bridge priority is a multiple of 4096.
Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the MST instance.
Designated Bridge	Displays the bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Root Port	Displays the port that accesses the designated root for MST instance.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MST Port Settings

This page displays the current MSTI configuration information for the Switch. From here you can update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.

MST Port Settings

	MST ID	Port	Priority	Internal Path Cost Conf / Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Port Role	Port State
<input type="checkbox"/>	1		128	0					
<input type="checkbox"/>	1	1	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	2	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	3	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	4	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	5	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	6	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	7	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	8	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	9	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	10	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	11	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	12	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk1	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk2	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk3	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk4	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk5	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk6	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk7	128	0 / 20000	--	--	--	--	--
<input type="checkbox"/>	1	trunk8	128	0 / 20000	--	--	--	--	--

Apply

MST ID	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
Port	Displays port or trunked port ID.
Priority	Select the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is: 32768. The valid range is from 0 to 61440.
Internal Path Cost Conf	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper	Displays the operation cost of the path from this bridge to the root bridge.

Regional Root Bridge	This is the bridge identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost	Displays the path cost to the designated root for the selected MST instance.
Designated Bridge	Displays the bridge identifier of the bridge for the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest optimal route automatically for an interface.
Port Role:	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
Port State	Displays the state of the selected port.
Edge Port Ope	Displays the operating edge port state.
P2P MAC Conf	Displays the P2P MAC state.
P2P MAC Oper	Displays the operating P2P MAC state.
Port Role	Displays the port role. Shows each MST bridge port that is assigned a port role for each spanning tree.
Port State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken regarding traffic. The possible port states are: Disabled: STP is disabled on the port. The port forwards traffic while learning MAC addresses. Blocking: The port is blocked and cannot be used to forward traffic or learn MAC addresses. Listening: The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. Learning: The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. Forwarding: The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state.

Click **Apply** to update the system settings.

STP Port Statistics

STP Port Statistics				
	Port	RX BPDU	TX BPDU	Invalid BPDU
<input type="checkbox"/>				
<input type="checkbox"/>	1	842	0	0
<input type="checkbox"/>	2	0	0	0
<input type="checkbox"/>	3	0	0	0
<input type="checkbox"/>	4	0	0	0
<input type="checkbox"/>	5	0	0	0
<input type="checkbox"/>	6	0	0	0
<input type="checkbox"/>	7	0	0	0
<input type="checkbox"/>	8	0	0	0
<input type="checkbox"/>	trunk1	0	0	0
<input type="checkbox"/>	trunk2	0	0	0
<input type="checkbox"/>	trunk3	0	0	0
<input type="checkbox"/>	trunk4	0	0	0
<input type="checkbox"/>	trunk5	0	0	0
<input type="checkbox"/>	trunk6	0	0	0
<input type="checkbox"/>	trunk7	0	0	0
<input type="checkbox"/>	trunk8	0	0	0

Port	Displays port or trunked port ID.
RX BPDU	Display the receive BPDU packet.
TX BPDU	Display the transmit BPDU packet.
Invalid BPDU	Display the Invalid BPDU packet.

LBD

Loopback Detection (LBD) is a feature on the switch that provides protection against loops by transmitting loop protocol packets out of ports where loop protection has been enabled. When the switch sends out a loop protocol packet and then receives the same packet, it shuts down the port that received the packet.

LBD operates independently of Spanning Tree Protocol (STP). After a loop is discovered, the port that received the loops is placed in the Shut Down state. A trap is sent and the event is logged. Network administrators can define a Detection Interval that sets the time interval between LBD packets.

LBD Global



Setting	Select whether to enable or disable the Loop back detection on the Switch.
----------------	--

LBD port Status

Port	state
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal

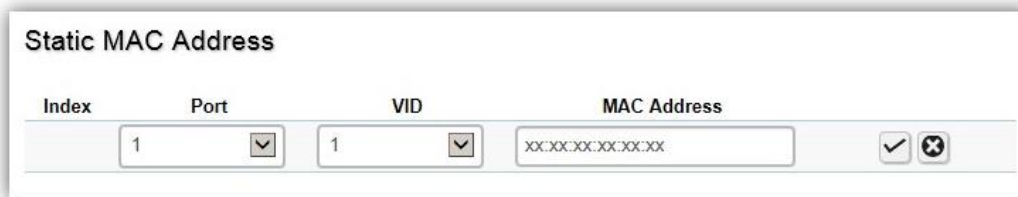
State	Display the Port status is normal or blocked by LBD function.
--------------	---

MAC Address Table


The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the dynamic address. A static address allows you to manually enter a MAC address to configure a specific port and VLAN.

Static MAC Address

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a static MAC address, you set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.



Index	Displays the index for the static MAC address table.
Port	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VID	Enter the VLAN ID on which the IGMP Snooping querier is administratively enabled and for which the VLAN exists in the VLAN database.
MAC Address	Enter a unicast MAC address for which the switch has forwarding or filtering information.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Dynamic MAC Address

The Switch will automatically learn the device's MAC address and store it to the dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The dynamic MAC address table shows the MAC addresses and their associated VLANs learned on the selected port.

Index	Port	VID	MAC Address	
1	1	1	00:00:00:00:00:00	
2	1	1	00:00:fa:eb:6a:dd	
3	1	1	00:02:6f:00:00:01	
4	1	1	00:02:6f:34:2f:c2	
5	1	1	00:02:6f:88:22:37	
6	1	1	00:0c:29:45:90:53	
7	1	1	00:0c:29:b0:ab:6c	
8	1	1	00:0c:29:f1:25:18	
9	1	1	00:13:57:01:8e:de	
10	1	1	00:13:57:01:bb:ae	

1 2 3 4 5 6 ... 12 Next >>

Index	Displays the index for the dynamic MAC address table.
Port	Select the port to which the entry refers.
VID	Displays the VLAN ID corresponding to the MAC address.
MAC Address	Displays the MAC addresses that the Switch learned from a specific port.

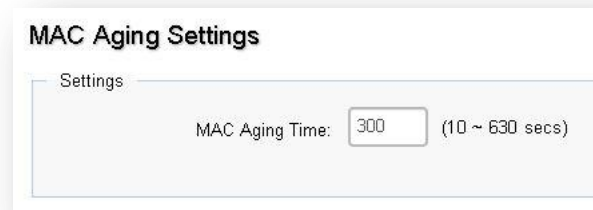
Search MAC Address

You can use this function to search the specific MAC address in the MAC address table. The MAC address format is xx:xx:xx:xx:xx:xx.



The screenshot shows a window titled "Search MAC Address". Inside the window, there is a section labeled "Searchings" which contains a text input field for "MAC Address".

MAC Aging Time



The screenshot shows a window titled "MAC Aging Settings". Inside the window, there is a section labeled "Settings" which contains a numeric input field for "MAC Aging Time" with the value "300" and a range "(10 ~ 630 secs)" to its right.

Setting	Sets the the aging time for entries in the MAC address table. This time is equal to 300 seconds (sec) by default, but you can tune the time to be between 10 and 630 sec.
----------------	---

LLDP

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to view the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction only; from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.

LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDPDU is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.

Global Settings

Global Settings

Settings

State: Enabled Disabled

Transmission Interval: (5-32767)

Holdtime Multiplier: (2-10)

Reinitialization Delay: (1-10)

Transmit Delay: (1-8191)

Apply

Select whether to enable or disable the LLDP feature on the Switch. Next, enter the Transmission Interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click Apply to update the system settings.

State	Select Enabled or Disabled to activate LLDP for the Switch.
Transmission Interval	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5 to 32768.
Holdtime Multiplier	Enter the amount of time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2 to 10.
Reinitialization Delay	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1 to 10.
Transmit Delay	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is from 1 to 8191 seconds.

Local Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the Switch.

Local Device

Information

Chassis ID Subtype:

Chassis ID:

System Name:

System Description:

Capabilities Supported:

Capabilities Enabled:

Port ID Subtype:

Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device transmitting the LLDP frame.

System Name	Displays the administratively assigned device name.
System Description	Describes the device.
Capabilities Supported	Describes the device functions.
Capabilities Enabled	Describes the device functions.
Port ID Subtype	Displays the port ID type.

Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can viewing detailed LLDP Information for the remote device.

Remote Device														
Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Remote ID	System Name	Time To Live	Auto-Negotiation Supported	Auto-Negotiation Enabled	Auto-Negotiation Advertised Capabilities	Operational MAU Type	802.3 Maximum Frame Size	802.3 Link Aggregation Capability	802.3 Link Aggregation Status	802.3 Link Aggregation Port ID
1	Mac Address	88:dc:96:53:c4:20	Interface Alias	Gi0/15	ECS1128FP	120	Supported	Enabled	1000base-T(FD), Asymmetric and Symmetric PAUSE(FD), 100base-TX(FD), 100base-TX(HD), 10base-T(FD), 10base-T(HD).	1000BASE-T full duplex mode	1522	Capable	Not In Aggregation	0
2	Mac Address	88:dc:96:78:4e:67	Interface Alias	Gi0/1	ECS1008P	120	Supported	Enabled	1000base-T(FD), Asymmetric and Symmetric PAUSE(FD), 100base-TX(FD), 100base-TX(HD), 10base-T(FD), 10base-T(HD).	1000BASE-T full duplex mode	1522	Capable	Not In Aggregation	0

Port	Displays the port.
Chassis ID Subtype	Displays the chassis ID type.
Chassis ID	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype	Displays the port ID type.
Remote ID	Displays the remote ID.
System Name	Displays the administratively assigned device name.
Time to Live	Displays the time to live.
Auto-Negotiation Supported	Displays state for the auto-negotiation supported.
Auto-Negotiation Enabled	Displays state for the auto-negotiation enabled.
Auto-Negotiation Advertised Capabilities	Displays the type of auto-negotiation advertised capabilities.
Operational MAU Type	Displays the type of MAU.

802.3 Maximum Frame Size	Displays the maximum size of 802.3 maximum frame.
802.3 Link Aggregation Capabilities	Displays the 802.3 Link Aggregation capabilities.
802.3 Link Aggregation Status	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID	Displays the port ID of 802.3 Link Aggregation.

IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast registers with their local multicast Switch.

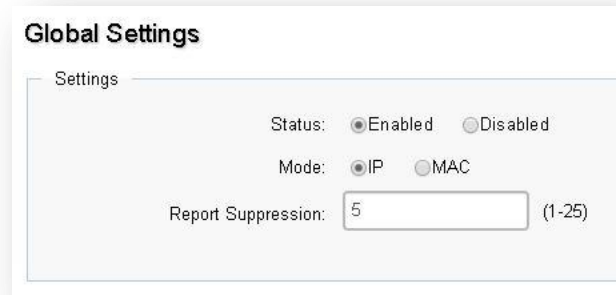
A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the Switch from the port.

A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures multicasting accordingly. Based on the IGMP query and report messages, the Switch forwards traffic only to the ports that request the multicast traffic. It enables the Switch to forward packets of multicast groups to those ports that have validated host nodes. The Switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your Switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a broadcast transmission, which forwards packets to all ports on the network.

IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group.

Global Settings

Click to enable or disable the IGMP Snooping feature for the Switch. Next, select whether you wish to use by IP or MAC address. Finally, setup the Report Suppression value for the Switch.



The screenshot shows a 'Global Settings' window with a 'Settings' section. It contains three controls: a 'Status' section with radio buttons for 'Enabled' (selected) and 'Disabled'; a 'Mode' section with radio buttons for 'IP' (selected) and 'MAC'; and a 'Report Suppression' section with a text input field containing the value '5' and a range indicator '(1-25)' to its right.

Status	Select to enable or disable IGMP Snooping on the Switch. The Switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled. The default setting is: Disabled.
Mode	Select the IGMP snooping mode you wish to use. IP: Use IP addresses to forward multicast traffic MAC: Use destination MAC addresses to forward multicast traffic.
Report Suppression	Setup the Report Suppression value. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers. The default value is 5. The range is from 1 to 25.

Click **Apply** to update the system settings.



VLAN Settings

Use the IGMP Snooping VLAN Settings to configure IGMP Snooping settings for VLANs on the system. The Switch performs IGMP Snooping on VLANs that send IGMP packets. You can specify the VLANs that IGMP Snooping should be performed on. Choose from the drop down box whether to enable or disable IGMP Snooping. Next, choose to enable or disable Fast Leave for the VLAN ID.



VLAN ID	IGMP Snooping Status	Version	Fast Leave
1	Disabled	v2	Disabled

VLAN ID	Displays the VLAN ID.
IGMP Snooping Status	Enables or disables the IGMP Snooping feature for the specified VLAN ID.
Version	Select the IGMP version is v1/v2 or v3.
Fast Leave	Enables or disables the IGMP Snooping Fast Leave for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an IGMP leave message without first sending out IGMPgroup-specific (GS) queries to the port.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

If Fast Leave is not used, a multicast querier will send a GS-query message when an IGMPv2/v3 group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one IGMP-enabled device.

Fast Leave is supported only with IGMPv2 or IGMPv3 Snooping when IGMP Snooping is enabled. Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.



Querier Settings

IGMP Snooping requires that one central Switch to periodically query all end devices on the network to announce their multicast memberships and this central device is the IGMP querier. The snooping Switch sends out periodic queries with a time interval equal to the configured querier query interval. The IGMP query keeps the Switch updated with the current multicast group membership information. If the Switch does not received the updated membership information, then it will stop forwarding multicasts to specified VLANs.

VLAN ID	Querier State	Querier Version	Querier Status	Interval	Max Response Interval	Startup Query Counter	Startup Query Interval
1	Disabled	v2	Non-Querier	125	12	2	15

VLAN ID	Displays the VLAN ID.
Querier State	Select whether to enable or disable the IGMP querier state for the specified VLAN ID. A querier can periodically ask their hosts if they wish to receive multicast traffic. The querier feature will check whether hosts wish to receive multicast traffic when enabled. An elected querier will assume the role of querying the LAN for group members, and then propagates the service requests on to any upstream multicast Switch to ensure that it will continue to receive the multicast service. This feature is only supported for IGMPv1 and v2 snooping.
Querier Version	Display the version of IGMP packet that will be sent by this port. If an IGMP packet received by the port has a version higher than the specified version, this packet will be dropped.
Querier Status	Display the IGMP Querier status.
Interval	Enter the amount of time in seconds between general query transmissions. The default is 125 seconds.
Max Response Interval	Enter the maximum response time used in the queries that are sent by the snooping querier. The default is 12 seconds.
Startup Query Counter	Enter the number of Query Counter values. Query count adjust the

	period between membership queries for a specified number of messages.
Startup Query Interval	Enter the time of Query interval values. The query interval is the period (seconds), between IGMP Membership Query message transmissions. The interval ranges from 5 to 3600 seconds.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Group List

The Group List displays VLAN ID, group IP address, and member port in the IGMP Snooping list.



Group List		
VLAN ID	Group IP Address	Member Ports

Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the Switch will be forwarded to the multicast router reachable from the port.

VLAN ID	Dynamic Port List	Static Port List	Forbidden Port List	
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

VLAN ID	Displays the VLAN ID.
Dynamic Port List	Displays router ports that have been dynamically configured.
Static Port list	Designates a range of ports as being connected to multicast-enabled routers. Ensures that all the packets will reach the multicast-enabled router.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time.

Global Settings

Global Settings

Settings

MLD Snooping Status: Enabled Disabled

MLD Snooping Mode: IP MAC

MLD Snooping Report Suppression: (1-25)

Apply

MLD Snooping Status	Select to enable or disable MLD Snooping on the Switch. The Switch snoops all MLD packets it receives to determine which segments should receive packets directed to the group address when enabled. The default setting is: Disabled.
MLD Snooping Mode	Select the MLD snooping mode you wish to use. IP: Use IP addresses to forward multicast traffic MAC: Use destination MAC addresses to forward multicast traffic.
MLD Snooping Report Suppression	Setup the Report Suppression value. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers. The default value is 5. The range is from 1 to 25.

Click **Apply** to update the system settings.

VLAN Settings

If the Fast Leave feature is not used, a multicast querier will send a GS-query message when an MLD group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one MLD-enabled device.





VLAN ID	MLD Snooping Status	Version	Fast Leave
1	Disabled	v2	Disabled

Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it. Fast Leave can improve bandwidth usage for a network which frequently experiences many MLD host add and leave requests.

VLAN ID	Displays the VLAN ID.
MLD Snooping Status	Select to enable or disable the MLD snooping feature for the specified VLAN ID.
Version	Select the MLD version is v1 or v2.
Fast Leave	Enables or disables the MLD snooping Fast Leave feature for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an MLD leave message without first sending out an MLD group-specific (GS) query to the port.

Select from the drop down list whether to enable or disable MLD Snooping. Next, select to enable or disable Fast Leave for the specified VLAN ID.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Querier Settings

Use the MLD snooping querier to support MLD snooping in a VLAN where PIM and MLD are not configured because the multicast traffic does not need to be routed.

In a network where IP multicast routing is configured, the IP multicast router acts as the MLD querier. If the IP-multicast traffic in a VLAN only needs to be Layer 2 switched, an IP-multicast router is not required, but without an IP-multicast router on the VLAN, you must configure another switch as the MLD querier so that it can send queries.

When enabled, the MLD snooping querier sends out periodic MLD queries that trigger MLD report messages from the switch that wants to receive IP multicast traffic. MLD snooping listens to these MLD reports to establish appropriate forwarding.

You can enable the MLD snooping querier on all the switches in the VLAN, but for each VLAN that is connected to switches that use MLD to report interest in IP multicast traffic, you must configure at least one switch as the MLD snooping querier.

You can configure a switch to generate MLD queries on a VLAN regardless of whether or not IP multicast routing is enabled.

VLAN ID	Querier State	Querier Status	Interval
1	Disabled	Non-Querier	125

VLAN ID	Displays the VLAN ID.
Querier State	Select whether to enable or disable the MLD querier state for the specified VLAN ID.
Querier Status	Display the MLD Querier status.
Interval	Enter the amount of time in seconds between general query transmissions. The default is 125 seconds.

Group List

The Group List displays the VLAN ID, Group IPv6 address, and member port in the MLD Snooping List.

Group List		
VLAN ID	Group IPv6 Address	Member Ports

Router Settings

The Router Settings feature shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the static and forbidden ports for the specified VLAN IDs that are utilizing MLD Snooping. All MLD packets snooped by the Switch will be forwarded to the multicast router reachable from the port.

Router Settings

VLAN ID	Dynamic Port List	Static Port List	Forbidden Port List	
1				<input checked="" type="checkbox"/> <input type="checkbox"/>

VLAN ID	Displays the VLAN ID.
Dynamic Port List	Displays router ports that have been dynamically configured.
Static Port List	Designates a range of ports as being connected to multicast-enabled routers. Ensure that all the packets will reach the multicast-enabled router.
Forbidden Port List	Designates a range of ports as being disconnected to multicast-enabled routers. Ensure that the forbidden router port will not propagate routing packets out.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Multicast Filtering

Multicast is a form of communication that allows multiple transmissions of multimedia and streaming data to specific recipients at the same time. Enabling the Multicast Filtering feature on your switch lets you sort out selective multiple transmissions for devices connected to the network.



Multicast Filtering

Setting

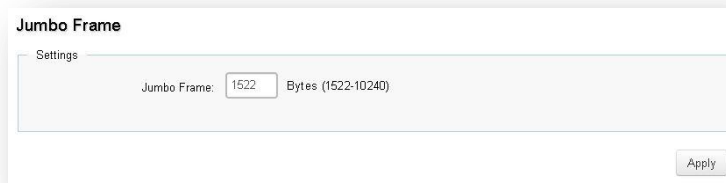
State : Enabled Disabled

State	Select whether to enable or disable the Multicast Filtering function.
--------------	---

Jumbo Frame

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 10000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The switch supports a jumbo frame size of up to **10240 bytes**. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum jumbo frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.



Jumbo Frame

Settings

Jumbo Frame: Bytes (1522-10240)

Apply

Jumbo Frame	Enter the size of jumbo frame. The range is from 1522 to 10240 bytes.
--------------------	--

Click **Apply** to update the system settings.

VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same Switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE 802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE 802.1Q to perform its functions is in its tags. 802.1Q-compliant Switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.

802.1Q

For the Controller to function properly, make sure that all ports (on all cascading switches as well) connected to APs on the switch are configured as the same VLAN ID as the Controller's Management VLAN ID.

VID	Name	Tagged Port	Untagged Port	
1	default		1-12,11-18	<input type="button" value="+ Add"/> <input type="button" value="✎"/>

Enabled	Enables 802.1Q VLANs. This feature is enabled by default.
VID	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1 to 4094.
Name	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port	Frames transmitted from this port are untagged.



NOTE

The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.

PVID

When an untagged packet enters a Switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address. If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet. Within the Switch, different PVIDs mean different VLANs, so VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1.

PVID

	Port	PVID	Accept Type	Ingress Filtering
<input type="checkbox"/>		<input type="text" value="1 ~ 4094"/>	<input type="text" value="ALL"/>	<input type="text" value="Enabled"/>
<input type="checkbox"/>	1	1	ALL	Disabled
<input type="checkbox"/>	2	1	ALL	Disabled
<input type="checkbox"/>	3	1	ALL	Disabled
<input type="checkbox"/>	4	1	ALL	Disabled
<input type="checkbox"/>	5	1	ALL	Disabled
<input type="checkbox"/>	6	1	ALL	Disabled
<input type="checkbox"/>	7	1	ALL	Disabled
<input type="checkbox"/>	8	1	ALL	Disabled
<input type="checkbox"/>	trunk1	1	ALL	Disabled
<input type="checkbox"/>	trunk2	1	ALL	Disabled
<input type="checkbox"/>	trunk3	1	ALL	Disabled

Port	Displays the VLAN ID to which the PVID tag is assigned. Configure the PVID to assign untagged or tagged frames received on the selected port.
PVID	Enter the PVID value. The range is from 1 to 4094.
Accept Type	Select Tagged Only and Untagged Only from the list. Tagged Only: The port discards any untagged frames it receives. The port only

	<p>accepts tagged frames.</p> <p>Untagged Only: Only untagged frames received on the port are accepted.</p> <p>All: The port accepts both tagged and untagged frames.</p>
Ingress Filtering	<p>Specify how you wish the port to handle tagged frames. Select Enabled or Disabled from the list.</p> <p>Enabled: Tagged frames are discarded if VID does not match the PVID of the port.</p> <p>Disabled: All frames are forwarded in accordance with the IEEE 802.1Q VLAN.</p>



NOTE

To enable PVID functionality, the following requirements must be met:

- > All ports must have a defined PVID.
- > If no other value is specified, the default VLAN PVID is used.
- > If you wish to change the port's default PVID, you must first create a VLAN that includes the port as a member.

Click **Apply** to update the system settings.

Voice VLAN

Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

Global Settings

Global Settings

Settings

Voice VLAN State:

Voice VLAN ID:

Vlan priority tag:

Dscp: (0~63)

802.1p Remark:

Remark CoS/802.1p:

Aging Time: (30~65535)min

Voice VLAN State	Select Enabled or Disabled for Voice VLAN on the Switch.
Voice VLAN ID	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the Switch.
VLAN Priority tag	Sets the Voice VLAN priority tag for the network.
DSCP	Sets the DSCP (Differentiated Services Code Point) value.
802.1p Remark	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p	Defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port. (Range: 0 to 7; Default: 6)
Aging Time	The aging time is used to remove a port from voice VLAN if the port is an

	automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 30 to 65535 minutes. The default is 1440 minutes.
--	---

Click **Apply** to update the system settings.



OUI Settings

The Switches determines whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a pre-configured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.

Index	OUI Address	Description	+ Add
1	00:E0:BB	3COM	
2	00:03:6B	Cisco	
3	00:E0:75	Veritel	
4	00:D0:1E	Pingtel	
5	00:01:E3	Siemens	
6	00:60:B9	NEC/Philips	
7	00:0F:E2	H3C	
8	00:09:6E	Avaya	

Index	Displays the VoIP sequence ID.
OUI Address	This is the globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description	Displays the ID of the VoIP equipment vendor.

To configure the OUI settings, click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specific entry and click the **Add** button to create a new OUI entry.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Port Settings

Enhance your VoIP service further by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.

Port Settings				
	Port	State	CoS Mode	Operate Status
<input type="checkbox"/>		Disabled	Src	
<input type="checkbox"/>	1	Disabled	Src	--
<input type="checkbox"/>	2	Disabled	Src	--
<input type="checkbox"/>	3	Disabled	Src	--
<input type="checkbox"/>	4	Disabled	Src	--
<input type="checkbox"/>	5	Disabled	Src	--
<input type="checkbox"/>	6	Disabled	Src	--
<input type="checkbox"/>	7	Disabled	Src	--
<input type="checkbox"/>	8	Disabled	Src	--
<input type="checkbox"/>	9	Disabled	Src	--
<input type="checkbox"/>	10	Disabled	Src	--
<input type="checkbox"/>	11	Disabled	Src	--
<input type="checkbox"/>	12	Disabled	Src	--
<input type="checkbox"/>	trunk1	Disabled	Src	--
<input type="checkbox"/>	trunk2	Disabled	Src	--
<input type="checkbox"/>	trunk3	Disabled	Src	--
<input type="checkbox"/>	trunk4	Disabled	Src	--

Port	Displays the port to which the Voice VLAN settings are applied.
State	Select Enabled to enhance VoIP quality on the selected port. The default is Disabled.
CoS Mode	Select Src or All from the list. Src: Src QoS attributes are applied to packets with OUIs in the source MAC address. All: All QoS attributes are applied to packets that are classified to the Voice VLAN.
Operate Status	Displays the operating status for the Voice VLAN on the selected port.

Click **Apply** to update the system settings.

Management

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

System Information

Information

System Name: (char : 1 ~ 255)

System Location: (char : 0 ~ 255)


System Contact: (char : 0 ~ 255)

System Name	Enter the name you wish to use to identify the Switch. You can use up to 255 alphanumeric characters.
System Location	Enter the location of the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.
System Contact	Enter the contact person for the Switch. You can use up to 255 alphanumeric characters. The factory default is: Default Location.

Click **Apply** to update the system settings.

User Management

Use the User Management page to control management access to the Switch based on manually configured user names and passwords. A User account can only view settings without the right to configure the Switch, and an Admin account can configure all the functions of the Switch. Click the Add button to add an account or the Edit button to edit an existing account.



User Name	Password	Password Retype	Privilege Type	
admin			Admin	

User Name	Enter a username. You can use up to 18 alphanumeric characters.
Password	Enter a new password for accessing the Switch.
Password Retype	Repeat the new password used to access the Switch.
Privilege Type	Select Admin or User from the list to regulate access rights.



Important:

Note that Admin users have full access rights to the Switch when determining the authority of the user account.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Dual Image

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.

Dual Image

Active	Flash Partition	Status	Image Name	Image Size(Byte)	Created Time
<input checked="" type="radio"/>	Partition 1	Active	IMG-2.01.045	10542191	2019/6/27_17:20
<input type="radio"/>	Partition 2	Backup	IMG-2.01.041	10464576	2019/5/27_12:00

Active	Selects the partition you wish to be active.
Flash Partition	Displays the number of the partition.
Status	Displays the partition which is currently active on the Switch.
Image Name	Displays the name/version number of the image
Image Size	Displays the size of the image file.
Created Time	Displays the time the image was created.

Click **Apply** to update the system settings.

SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as; servers, printers, hubs, Switches, and routers on an Internet Protocol (IP) network.

SNMP is used to exchange management information between a network management system (NMS) and a network device. A manager station can manage and monitor the Switch through their network via SNMPv1, v2c and v3. An SNMP managed network consists of two components; agents and a manager.

An agent translates the local management information from the managed Switch into a form that is compatible with SNMP. SNMP allows a manager and agents to communicate with each other for the purpose of accessing Management Information Bases (MIBs). SNMP uses an extensible design, where the available information is defined by MIBs. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

The manager is the console through which network administrators perform network management functions.

Several versions of SNMP are supported. They are v1, v2c, and v3. SNMPv1, which is defined in RFC 1157 "A Simple Network Management Protocol (SNMP)", is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it's required to support older hardware. SNMPv2c, which is defined in RFC 1901 "Introduction to Community-Based SNMPv2", RFC 1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", and RFC 1906 "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)". SNMPv2c updates protocol operations by introducing a GetBulk request and authentication based on community names. Version 2c adds several enhancements to the protocol, such as support for "Informs". Because of this, v2c has become the most widely used version. Unfortunately, a major weakness of v1 and v2c is security. To combat this, SNMP v3 adds a security features that overcome the weaknesses in v1 and v2c. If possible, it is recommended that you use v3 — especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex.

In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment. The SNMPv3 protocol uses different terminology

than SNMPv1 and SNMPv2c as well. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. In the SNMPv3 protocol, agents and managers are renamed to entities. With the SNMPv3 protocol, you create users and determine the protocol used for message authentication as well as if data transmitted between two SNMP entities is encrypted.

The SNMPv3 protocol supports two authentication protocols - HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password to provide even more security.

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. Users can assign viECS to Community Strings that specify which MIB objects can be accessed by a remote SNMP manager.

The default Community Strings for the Switch used for SNMPv1 and SNMPv2c management access for the Switch are public, which allows authorized management stations to retrieve MIB objects, and private, which allow authorized management stations to retrieve and modify MIB objects.

Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. The SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.

Global Settings

Settings

SNMP State: Enabled Disabled

Engine ID:

Default

(10~64 hex letters, the length of the Engine ID should be even.)

Apply


SNMP State	Enables or disables the SNMP function. The default SNMP global state is: Enabled.
Local Engine ID (10-64 hex characters)	Enter the Switch's Engine ID for the remote clients. A SNMPv3 engine is an independent SNMP agent that resides on the Switch. This engine protects against message replay, delay, and redirection issues. The engine ID is also used in combination with user passwords to generate security keys for authenticating and encrypting SNMPv3 packets. Normally, a local engine ID is automatically generated that is unique to the Switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all local SNMP users will be cleared and you will need to reconfigure all existing users.

Click **Apply** to update the system settings.

User List

Use the User List page to create SNMP users for authentication with managers using SNMP v3 to associate them to SNMP groups. Click **Add** to add a new user.

Privilege Mode	Select No Auth , Auth , or Priv security level from the list. No auth: Neither authentication nor the privacy security levels are assigned to the group. Auth: Authenticates and ensures that the origin of the SNMP message is authenticated. Priv: Encrypts SNMP messages.
Authentication Protocol	Select the method used to authenticate users. MD5: Using the HMAC-MD5 algorithm. SHA: Using the HMAC-SHA-96 authentication level. Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Authentication Password	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Encryption Protocol	Select the method used to authenticate users. None: No user authentication is used. DES: Using the Data Encryption Standard algorithm.
Encryption Key	Enter the Data Encryption Standard key.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Community List

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. It is important to note that the community name can limit access to the SNMP agent from the SNMP network management station, functioning as a password.

Click **Add** to add a community list to the Switch. Next, name the community and choose the level of access that will be granted to the specified list from the drop down boxes.



Community Name	Security Name	Transport Tag
NETMAN	none	
PUBLIC	none	

char : 1 ~ 20 none ▼ char : 1 ~ 20

Community Name	Enter the name of SNMP community string.
Security Name	Enter the security name of the group. The security name none, noAuthUser, templateMD5 and templateSHA are created, once the switch is started.
Transport Tag	This string specifies a set of target addresses from which the SNMP accepts SNMP requests and to which traps may be sent. The target addresses identified by this tag are defined in the "target address table". If this string is empty, addresses are not checked when an SNMP request is received or when a trap is sent. If this string is not empty, the transport tag must be contained in the value of the "tag list" of at least one entry in the "target address table."

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.



Group List

Configure SNMP Groups to control network access on the Switch by providing users in various groups with different management rights options.



The image shows a configuration dialog box titled "Group List". It contains three input fields: "Group Name" with the text "char : 1 ~ 30", "Security Mode" with a dropdown menu showing "v1", and "Security Name" with a dropdown menu showing "none". To the right of these fields are two buttons: a checkmark icon (Apply) and a close icon (Cancel).

Group Name	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Security Mode	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Name	Enter the security name of the group. The security name none, noAuthUser, templateMD5 and templateSHA are created, once the switch is started.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Access List

Configure SNMP Access List to allow SNMP access to the device. Access lists provide further protection when used in combination with other protective measures.

Group Name	Security Mode	Privilege Mode	Read View	Write View	Notify View
iso	v1	No Auth	iso	iso	iso
iso	v2c	No Auth	iso	iso	iso
noAuthUser	v3	No Auth	restricted	restricted	restricted
noAuthUser	v3	Auth	iso	iso	iso
noAuthUser	v3	Priv	iso	iso	iso

iso v1 No Auth char : 1 ~ 20 char : 1 ~ 20 char : 1 ~ 20

Group Name	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Security Mode	Selects the SNMP version (v1, v2c, v3) associated with the group.
Privilege Mode	Select No Auth , Auth , or Priv security level from the list. No auth: Neither authentication nor the privacy security levels are assigned to the group. Auth: Authenticates and ensures that the origin of the SNMP message is authenticated. Priv: Encrypts SNMP messages.
Read View	Management access is restricted to read-only.
Write View	Select a SNMP to allow SNMP write privileges to the Switch's SNMP agent.
Notify View	Select a SNMP group to receive SNMP trap messages generated by the Switch's SNMP agent.

View List

SNMP uses an extensible design, where the available information is defined by Management Information Bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID) to organize themselves. Each OID identifies a variable that can be read or set via SNMP. The SNMP View List is created for the SNMP management station to manage MIB objects.

Click the **Add** button to create a new entry.

View List

View Name	Subtree OID	Subtree Mask	View Type
all	.1	all	Included

char : 1 ~ 30 max level : 20 char : 1 ~ 20 Included

* If user want to exclude some OID that the parent node included rule must be existed.

View Name	Enter the view name. The view name can contain up to 30 alphanumeric characters.
Subtree OID	Enter the Object Identifier (OID) Subtree. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using a period (.).
Subtree Mask	Select 0 or 1 for Subtree mask. The mask of the Subtree OID 1 means this object number "is concerned", and 0 means "do not concern".
View Type	Select whether the defined OID branch within MIB tree will be Included or Excluded from the selected SNMP view. Generally, if the view type of an entry is Excluded , another entry of view type Included should exist and its OID subtree should overlap the Excluded view entry.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Target Params

The target params table is used in conjunction with the target address table. It is required for all notification originators. It contains information about SNMP versions and security levels that is used when sending notifications to particular domains and addresses. This information is separate from the target address table to allow multiple rows in the target address table to correspond to a single row in the target paramstable. You can populate this table from information stored in non-volatile memory, or you can add entries as new targets are discovered.

Target Parameter Name	Message Processing Model	Security Mode	Security Name	Privilege Mode
internet	v2c	v2c	none	No Auth
test1	v2c	v1	none	No Auth

char : 1 ~ 30 v1 v1 none No Auth ✓ ✕

Target Parameter Name	Enter the parameter name into the field. The parameter name can contain up to 30 alphanumeric characters.
Message Processing Model	Selects the Message Processing Model version (v1, v2c, v3) associated with the group.
Security Mode	Selects the Security mode version (v1, v2c, v3) associated with the group.
Security Name	Enter the security name of the group. The security name none, noAuthUser, templateMD5 and templateSHA are created, once the switch is started.
Privilege Mode	Select No Auth , Auth , or Priv security level from the list. No auth: Neither authentication nor the privacy security levels are assigned to the group. Auth: Authenticates and ensures that the origin of the SNMP message is authenticated. Priv: Encrypts SNMP messages.

Target Address

The target address table is required for all notification originators. It contains domain and addressing information that allows applications, such as the notification originator, to determine where to send notifications. It also contains information about how often and how quickly packets should be retransmitted. You can populate this table from information stored in non-volatile memory, or you can add entries as new target addresses are discovered.

Target Address Name	IP Address	UDP port	Timeout	Retry	Tag Identifier	Target Parameter
char : 1 ~ 32	char : 1 ~ 63	162	15	3	char : 1 ~ 20	intern <input type="checkbox"/> <input type="checkbox"/>


Target Address Name	Enter the address name into the field. The address name can contain up to 32 alphanumeric characters.
IP address	Enter the target IP address into the field.
UDP	Enter the UDP port used to send notifications.
Timeout	Configurable only if the notify type is Informs . Enter the amount of time the device waits before re-sending. The default is 15 seconds.
Retry	Configurable only if the notify type is Informs . Enter the amount of time the device waits before re-sending an inform request. The default is 3 seconds.
Tag Identifier	Enter the Tag Identifier string into the field.
Target Parameter	Configure the SNMP parameter in different target parameters.

Notify List

The SNMP Notify List is a type of SNMP message. The Switch can send notifications to an SNMP manager when an event occurs. You can restrict user privileges by specifying which portions of the MIBs that a user can view. In this way, you restrict which MIBs a user can display and modify for better security. In addition, you can restrict the types of notifications users can send as well. You can do this by determining where messages are sent and what types of messages can be sent per user. The notifications indicating status changes can be issued by the Switch to the specified the notification by sending authentication failure messages and other notification messages.

Notify List

Notify Name	Tag Identifier	Notify Type		
<input type="text" value="char : 1 ~ 32"/>	<input type="text" value="char : 1 ~ 20"/>	<input type="text" value="Traps"/>	<input type="checkbox"/>	<input type="checkbox"/>

Notify Name	Enter the Notify name. The Notify name can contain up to 32 alphanumeric characters.
Tag Identifier	Enter the Tag Identifier string into the field.
Notify Type	Select the type of notification to be sent. Traps: Traps are sent. Informs: Informes are sent ONLY when v2c is enabled.  NOTE: The recipient of a trap message does not send a response to the Switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgment of receipt. Inform messages can be used to ensure that critical information is received by the host. However, please note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.




Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

ACL



An Access Control List (ACL) allows you to define classification rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized users to access specific areas or resources. ACLs can provide basic security for access to the network by controlling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols. Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is considered as a single rule, and up to 256 rules may be defined on each ACL, with up to 3000 rules globally. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

MAC ACL

This page displays the currently-defined MAC-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

MAC ACL		
Index	Name	 Add
1	acl1	
2	acl2	

Index	Profile identifier.
Name	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

MAC ACE

Use this page to view and add rules to MAC-based ACLs.

Mac-Based ACE

Mac-Based ACE

ACL Name

Sequence (Range: 1 - 2147483647, 1 is first processed)

Action

Destination MAC Address

Source MAC Address

VLAN ID (Range: 1 - 4094)

802.1p Value (Range: 0 - 7)

Ethertype Value (Hex) (Range: 0600~FFFF)

ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action taken if a packet matches the criteria. Permit: Forward packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Destination MAC Value	Enter the destination MAC address.
Destination MAC Wildcard Mask	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Source MAC Value	Enter the source MAC address.
Source MAC Wildcard Mask	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
VLAN ID	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1 to 4094 .

802.1p Value	Enter the 802.1p value. The range is from 0 to 7 .
Ethertype Value	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).

Click **Apply** to update the system settings.

IPv4 ACL

This page displays the currently-defined IPv4-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

IPv4 ACL

Index	Name
1	123

char : 1 ~ 32

Index	Displays the current number of ACLs.
Name	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv4 ACE

Use this page to view and add rules to IPv4-based ACLs.

The screenshot shows a configuration window titled "IPv4-Based ACE". Inside, there are several fields: "ACL Name" with a dropdown menu showing "123"; "Sequence" with an empty text box and a note "(Range: 1 - 2147483647, 1 is first processed)"; "Action" with a dropdown menu showing "Permit"; "Protocol" with a dropdown menu showing "Any"; "Source IP Address" with a dropdown menu showing "Any"; "Destination IP Address" with a dropdown menu showing "Any"; and "Type of Service" with a dropdown menu showing "Any". At the bottom left, there is an "Apply" button.

ACL Name	Select the ACL from the list for which a rule is being created.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action to take if a packet matches the criteria. Permit: Forwards packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Protocol	Select Any , Protocol ID , or Select from a List in the drop down menu. Any: Check Any to use any protocol. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Selects the protocol from the list in the provided field. <ul style="list-style-type: none"> • ICMP: Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host. • IPinIP: IP in IP encapsulates IP packets to create tunnels between two routers. This ensures that IP in IP tunnel appears as a single interface, rather than several separate interfaces. • TCP: Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent. EGP Exterior Gateway Protocol (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network. • IGP: Interior Gateway Protocol (IGP). Enables a routing information exchange between gateways within an autonomous network. • UDP: User Datagram Protocol (UDP). UDP is a communication protocol that

	<p>transmits packets but does not guarantee their delivery.</p> <ul style="list-style-type: none"> • HMP: The Host Mapping Protocol (HMP) collects network information from various networks hosts. HMP monitors hosts spread over the Internet as well as hosts in a single network. • RDP: Reliable Data Protocol (RDP). Provides a reliable data transport service for packet-based applications. • IPv6: Matches the packet to the IPV6 protocol. • IPv6: Rout: Routing Header for IPv6. • IPv6: Frag: Fragment Header for IPv6. • RVSP: Matches the packet to the ReSerVation Protocol(RSVP). • IPv6: ICMP: The Internet Control Message Protocol (ICMP) allows the gateway or destination host to communicate with the source host. • OSPF: The Open Shortest Path First (OSPF) protocol is a link-state hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocols. It is an extension to the PPP protocol • that enables ISPs to operate Virtual Private Networks (VPNs). • PIM: Matches the packet to Protocol Independent Multicast (PIM). • L2TP: Matches the packet to Internet Protocol (L2IP).
Source IP Address Value	Enter the source IP address.
Source IP Mask	Enter the mask of the new source IP address.
Destination IP Address Value	Enter the destination IP address.
Destination IP Mask	Enter the mask of the new source IP address.
Type of Service	Select Any or DSCP to match from drop down list. When DSCP to match is selected, enter the DSCP. The range is from 0 to 63.
ICMP Type	Select Any , Protocol ID , or Select from List from drop down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. The range is from 0 to 255. Select from List: Select the ICMP from the list in the provided field.
ICMP Code	Select Any or User Defined from drop down menu. When User Defined is selected, enter the ICMP code value. The range is from 0 to 255.

Click **Apply** to update the system settings.

IPv6 ACL

This page displays the currently-defined IPv6-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

IPv6 ACL

Index	Name
	<input type="text" value="char : 1 ~ 32"/> <input type="checkbox"/> <input type="checkbox"/>

Index	Displays the current number of ACLs.
Name	Enter the IPv6 based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv6 ACE

Allows IPv6 Based Access Control Entry (ACE) to be defined within a configured ACL.

The screenshot shows a configuration window titled "IPv6-Based ACE". Inside, there is a sub-section "IPv6-Based ACE" containing several fields:

- ACL Name:** A dropdown menu.
- Sequence:** A text input field with a note "(Range: 1 - 2147483647, 1 is first processed)".
- Action:** A dropdown menu currently set to "Permit".
- Protocol:** A dropdown menu currently set to "Any".
- Source IP Address:** A dropdown menu currently set to "Any".
- Destination IP Address:** A dropdown menu currently set to "Any".
- Type of Service:** A dropdown menu currently set to "Any".

 An "Apply" button is located at the bottom left of the configuration area.

ACL Name	Select the ACL from the list.
Sequence	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1 to 2147483647 , 1 being processed first.
Action	Select what action taken if a packet matches the criteria. Permit: Forward packets that meet the ACL criteria. Deny: Drops packets that meet the ACL criteria.
Protocol	Select the Any, Protocol ID, or Select from List from drop down menu. Protocol ID: Enter the protocol in the ACE to which the packet is matched. Select from List: Select the protocol from the list in the provided field.
Source IP Address Value	Enter the source IP address.
Source IP Prefix Length	Enter the prefix length of the new source IP address. The range is from 0 to 128.
Destination IP Address Value	Enter the destination IP address.
Destination IP Prefix Length	Enter the prefix length of the new source IP address. The range is from 0 to 128.
Source Port	Select Single or Range from the list. Enter the source port that is

	matched to packets. The range is from 0 to 65535.
Destination Port	Select Single or Range from the list. Enter the destination port that is matched to packets. The range is from 0 to 65535.
TCP Flags	Select whether to handle each six TCP control flags; URG (Urgent), ACK (Acknowledgment), PSH (Push), RST (Reset), SYN (Synchronize), and FIN (Fin) from drop down menu. Don't Care: The ACE do not treat the TCP control flag. Set: The packet with the TCP control flag being set matches the criteria. Unset: The packet with the TCP control flag being unset matches the criteria.
Type of Service	Select Any or DSCP to match from drop down list. When DSCP to match is selected, enter the DSCP. The range is from 0 to 63.

Click **Apply** to update the system settings.

ACL Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.

ACL Binding				
	Port	MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>		(none) ▼	(none) ▼	(none) ▼
<input type="checkbox"/>	1			
<input type="checkbox"/>	2			
<input type="checkbox"/>	3			
<input type="checkbox"/>	4			
<input type="checkbox"/>	5			

Port	Select the port for which the ACLs are bound to.
MAC ACL	Select the MAC ACL rule to apply to the port.
IPv4 ACL	Select the IPv4 ACL rule to apply to the port.
IPv6 ACL	Select the IPv6 ACL rule to apply to the port.

Click **Apply** to update the system settings.

QoS

Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS is a means of providing consistent and predictable data delivery to the Switch by distinguishing between packets that have stricter timing requirements from those that are more tolerant of delays. QoS enables traffic to be prioritized while avoiding excessive broadcast and multicast traffic. Traffic such as Voice and Video streaming which require minimal delays can be assigned to a high priority queue, while other traffic can be assigned to a lower priority queue, resulting in uninterrupted actions. Without QoS, all traffic data is as likely to be dropped when the network is congested. This can result in reductions in network performance and hinder the network in time-critical situations.

In a Switch, multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission within a port, the rate at which it is processed depends on how the queue is configured and the amount of traffic present within other queues on the port. If a delay is necessary, packets are held in the queue until they are authorized for transmission.

Global Settings

There are two options for applying QoS information onto packets: the 802.1p Class of Service (CoS) priority field within the VLAN tag of tagged Ethernet frames, and Differentiated Services (DiffServ) Code Point (DSCP). Each port on the Switch can be configured to trust one of the packet fields (802.1p, DSCP or DSCP+802.1p). Packets that enter the Switch's port may carry no QoS information as well. If so, the Switch places such information into the packets before transmitting them to the next node. Thus, QoS information is preserved between nodes within the network and the nodes know which label to give each packet. A trusted field must exist in the packet for the mapping table to be of any use. When a port is configured as untrusted, it does not trust any incoming packet priority designations and uses the port default priority value instead to process the packet.

Global Settings

Qos Global

State: Enabled Disabled

Scheduling Method: Strict Priority ▼

Trust Mode: 802.1p ▼

Apply

State	Select whether QoS is enabled or disabled on the switch.
Scheduling Method	Selects the Strict Priority or WRR to specify the traffic scheduling method. Strict Priority: Specifies traffic scheduling based strictly on the queue priority. WRR: Use the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.
Trust Mode	Select which packet fields to use for classifying packets entering the Switch. DSCP: Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. 802.1p: Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE 802.1p are from 1 to 8.

Click **Apply** to update the system settings.

CoS Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

	CoS	Queue
<input checked="" type="checkbox"/>		1
<input type="checkbox"/>	0	2
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	3
<input type="checkbox"/>	3	4
<input type="checkbox"/>	4	5
<input type="checkbox"/>	5	6
<input type="checkbox"/>	6	7
<input type="checkbox"/>	7	8

Apply

CoS	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to update the system settings.

DSCP Mapping

Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.

DSCP Mapping		
	DSCP	Queue
<input type="checkbox"/>		1
<input type="checkbox"/>	0	1
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	1
<input type="checkbox"/>	3	1
<input type="checkbox"/>	4	1
<input type="checkbox"/>	5	1
<input type="checkbox"/>	6	1
<input type="checkbox"/>	7	1
<input type="checkbox"/>	8	2
<input type="checkbox"/>	9	2
<input type="checkbox"/>	10	2
<input type="checkbox"/>	11	2
<input type="checkbox"/>	12	2

DSCP	Displays the packet's DSCP values, where 0 is the lowest and 10 is the highest.
Queue	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported and the field values are from 1 to 8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to update the system settings.

Port Settings

From here, you can configure the QoS port settings for the Switch. Select a port you wish to set and choose a CoS value from the drop down box. Next, Select to enable or disable the Trust setting to let any CoS packet be marked at ingress.

Port Settings			
<input type="checkbox"/>	Port	CoS Value	Trust
<input type="checkbox"/>		0	Enabled
<input type="checkbox"/>	1	1	Enabled
<input type="checkbox"/>	2	0	Enabled
<input type="checkbox"/>	3	0	Enabled
<input type="checkbox"/>	4	0	Enabled
<input type="checkbox"/>	5	0	Enabled
<input type="checkbox"/>	6	0	Enabled
<input type="checkbox"/>	7	0	Enabled
<input type="checkbox"/>	8	0	Enabled
<input type="checkbox"/>	9	0	Enabled
<input type="checkbox"/>	10	0	Enabled
<input type="checkbox"/>	11	0	Enabled
<input type="checkbox"/>	12	0	Enabled
<input type="checkbox"/>	trunk1	0	Enabled
<input type="checkbox"/>	trunk2	0	Enabled
<input type="checkbox"/>	trunk3	0	Enabled
<input type="checkbox"/>	trunk4	0	Enabled
<input type="checkbox"/>	trunk5	0	Enabled
<input type="checkbox"/>	trunk6	0	Enabled
<input type="checkbox"/>	trunk7	0	Enabled
<input type="checkbox"/>	trunk8	0	Enabled

Port	Displays the ports for which the CoS parameters are defined.
CoS Value	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust	Select Enabled to trust any CoS packet marking at ingress. Select Disabled to not trust any CoS packet marking at ingress.

Click **Apply** to update the system settings.

Advanced mode

Class Mapping

Policy Mapping

Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port's Ingress Rate Limit and Egress Rate.

Bandwidth Control

<input type="checkbox"/>	Port	Ingress	Ingress Rate (kbps)	Egress	Egress Rate (kbps)
<input type="checkbox"/>		Disabled	1000000	Disabled	1000000
<input type="checkbox"/>	1	Disabled	Off	Disabled	Off
<input type="checkbox"/>	2	Disabled	Off	Disabled	Off
<input type="checkbox"/>	3	Disabled	Off	Disabled	Off
<input type="checkbox"/>	4	Disabled	Off	Disabled	Off
<input type="checkbox"/>	5	Disabled	Off	Disabled	Off
<input type="checkbox"/>	6	Disabled	Off	Disabled	Off
<input type="checkbox"/>	7	Disabled	Off	Disabled	Off
<input type="checkbox"/>	8	Disabled	Off	Disabled	Off
<input type="checkbox"/>	9	Disabled	Off	Disabled	Off
<input type="checkbox"/>	10	Disabled	Off	Disabled	Off
<input type="checkbox"/>	11	Disabled	Off	Disabled	Off
<input type="checkbox"/>	12	Disabled	Off	Disabled	Off

Port	Displays the ports for which the bandwidth settings are displayed.
Ingres	Select enable or disable ingress on the interface.
Ingress Rate	Enter the ingress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress	Select from the drop down box to Enable or Disable egress on the interface.
Egress Rate	Enter the egress rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.

Click **Apply** to update the system settings.

Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The Switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.

Storm Control

	Port	Status	Broadcast (kbps)	Unknown Multicast (kbps)	Unknown Unicast (kbps)
<input type="checkbox"/>		Disabled <input type="button" value="v"/>	<input type="checkbox"/> 16~1000000,Enter 16'	<input type="checkbox"/> 16~1000000,Enter 16'	<input type="checkbox"/> 16~1000000,Enter 16'
<input type="checkbox"/>	1	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	2	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	3	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	4	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	5	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	6	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	7	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	8	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	9	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	10	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	11	Disabled	Off (10000)	Off (10000)	Off (10000)
<input type="checkbox"/>	12	Disabled	Off (10000)	Off (10000)	Off (10000)

Port	Displays the ports for which the Storm Control information is displayed.
Status	Select whether Storm Control is Enabled or Disabled ingress on the interface.
Broadcast	Enter the broadcast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

Unknown Multicast	Enter the Unknown Multicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast	Enter the Unknown Unicast rate in kilobits per second. The gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

Click **Apply** to update the system settings.

Security

802.1x

The IEEE 802.1X standard authentication uses the RADIUS (Remote Authentication Dial In User Service) protocol to validate users and provide a security standard for network access control. The user that wishes to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. The mediating device, such as a Switch, is called the authenticator. Clients connected to a port on the Switch must be authenticated by the Authentication server (RADIUS) before accessing any services offered by the Switch on the LAN. Use a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the client and server. This establishes the requirements needed for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

Global Settings

When a supplicant is connected to a Switch port, the port issues an 802.1X authentication request to the attached the 802.1X supplicant. The supplicant replies with the given username and password and an authentication request is then passed to a configured RADIUS server. The authentication server's user database supports Extended Authentication Protocol (EAP), which allows particular guest VLAN memberships to be defined based on each individual user. After authorization, the port connected to the authenticated supplicant then becomes a member of the specified guest VLAN. When the supplicant is successfully authenticated, traffic is automatically assigned to the guest VLAN. The EAP authentication methods supported by the Switch are: EAP-MD5, EAP-TLS, EAP-TTLS, and EAP-PEAP.

Global Settings

802.1x Global

State: Enabled Disabled

Guest VLAN:

Guest VLAN ID:

State	Select whether authentication is Enabled or Disabled on the Switch.
Guest VLAN	Select whether Guest VLAN is Enabled or Disabled on the Switch. The default is Disabled.
Guest VLAN ID	Select the guest VLAN ID from the list of currently defined VLANs.

Click **Apply** to update the system settings.

Port Settings

The IEEE 802.1X port-based authentication provides a security standard for network access control with RADIUS servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides the required credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification to the guest VLAN. If the authentication server determines the credentials are valid, the supplicant is allowed to access resources located on the protected side of the network.

From here, you can configure the port settings as they relate to 802.1X. First, select the mode from you wish to utilize from the drop down box. Next, choose whether to enable or disable re-authentication for the port. Enter the time span that you wish to elapse for the re-authentication Period, Quiet Period, and Supplicant Period. After this, enter the max number of times you wish for the Switch to retransmit the EAP request. Finally, choose whether you wish to enable or disable the VLAN ID.

Port Settings

Port	Mode	Reauthentication	Reauthentication Period	Quiet Period	Supplicant Period	Authorized Status	Guest VLAN	RADIUS VLAN Assign
<input type="checkbox"/>	Auto	Enabled	3600	60	30		Disabled	Disabled
<input type="checkbox"/> 1	Force_Authorized	Disabled	3600	60	30	AUTH_FORCEAUTH	Disabled	Enabled
<input type="checkbox"/> 2	Force_Authorized	Disabled	3600	60	30	AUTH_FORCEAUTH	Disabled	Enabled
<input type="checkbox"/> 3	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled
<input type="checkbox"/> 4	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled
<input type="checkbox"/> 5	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled
<input type="checkbox"/> 6	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled
<input type="checkbox"/> 7	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled
<input type="checkbox"/> 8	Force_Authorized	Disabled	3600	60	30	AUTH_INITIALIZE	Disabled	Enabled

Port	Displays the ports for which the 802.1X information is displayed.
Mode	Select Auto or Force_UnAuthorized or Force_Authorized mode from the list.
Re-Authentication	Select whether port re-authentication is Enabled or Disabled.
Re-authentication period	Enter the time span in which the selected port is re-authenticated. The default is 3600 seconds.
Quiet Period	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.
Supplicant Period	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Authorized Status	Displays the port authorized status
Guest VLAN ID	Select whether guest VLAN ID is Enabled or Disabled.
Radius VLAN assign	Select whether Radius VLAN assign is Enabled or Disabled.

Click **Apply** to update the system settings.

Authenticated Host

The Authenticated Host section displays the Authenticated User Name, Port, Session Time, Authenticated Method, and Mac Address.

Authenticated Host						
User Name	Port	Session Time	Authenticate Method	MAC Address	Dynamic VLAN Cause	Dynamic VLAN ID

Statistics

The Statistics displays the 802.1X authentication and statistics on specified ports

Statistics													
	Port	TxReqId	TxReq	TxTotal	RxStart	RxLogoff	RxRespId	RxResp	RxInvalid	RxLenErr	RxTotal	RxVersion	LastRxSrcMac
<input type="checkbox"/>													
<input type="checkbox"/>	1	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	2	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	6	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	7	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00
<input type="checkbox"/>	8	0	0	0	0	0	0	0	0	0	0	0	00:00:00:00:00:00

Click **Clear** to clear authenticator statistics counters.

RADIUS Server

RADIUS proxy servers are used for centralized administration. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service for greater convenience. RADIUS is a server protocol that runs in the application layer, using UDP as transport. The Network Switch with port-based authentication and all have a RADIUS client component that communicates with the RADIUS server. Clients connected to a port on the Switch must be authenticated by the Authentication server before accessing services offered by the Switch on the LAN. Use a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the client and server. The RADIUS server maintains a user database, which contains authentication information. The Switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network.

Index	Server IP	Authorized Port	Key String	Timeout Reply	Retry	
	<input type="text" value="x.x.x.x"/>	<input type="text" value="1812"/>	<input type="text" value="char : 0 ~ 46"/>	<input type="text" value="3"/>	<input type="text" value="3"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Index	Displays the index for which RADIUS server is displayed.
Server IP	Enter the RADIUS server IP address.
Authorized Port	Enter the authorized port number. The default port is 1812.
Accounting Port	Enter the name you wish to use to identify this Switch.
Key String	Enter the key string used for encrypting all RADIUS communication between the device and the RADIUS server.
Timeout Reply	Enter the amount of time the device waits for an answer from the RADIUS server before switching to the next server. The default value is 3.
Retry	Enter the number of transmitted requests sent to the RADIUS server before a failure occurs. The default is 3.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Access

Access Settings

Access Settings

Web

Session Timeout: 0~10000 minutes (0 : no limit)

HTTP Service: Enabled Disabled

HTTPS Service: Enabled Disabled

CLI

Session Timeout: 0~10000 minutes (0 : no limit)

Telnet Service: Enabled Disabled

SSH Service: Enabled Disabled

Apply

Web Settings:

The EnGenius Switch provides a built-in browser interface that enables you to configure and manage the Switch via Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) requests selectively to help prevent security breaches on the network. You can manage your HTTP and HTTPS settings for the Switch further by choosing the length of session timeouts for HTTP and HTTPS requests. Select whether to enable or disable the HTTP service and enter the HTTP Timeout session. Next, select whether to enable or disable the HTTPS service and enter the HTTPS timeout session for the Switch.

Session Timeout	Enter the amount of time that elapses before HTTP/HTTPS service is timed out. The default is 5 minutes. The range is from 0 to 10000 minutes.
HTTP Service	Select whether HTTP service for the Switch is Enabled or Disabled. This is enabled by default.
HTTPS Service	Select whether the HTTPS service is Enabled or Disabled. This is enabled by default.

CLI Settings:

From here, you can configure and manage the Switch's Telnet protocol settings. The Telnet protocol is a standard Internet protocol which enables terminals and applications to interface over the Internet with remote hosts by providing Command Line Interface (CLI) communication using a virtual terminal connection. This protocol provides the basic rules for making it possible to link a client to a command interpreter. The Telnet service for the Switch is enabled by default. Please note that for secure communication, it is better to use SSH over Telnet. To enable and configure SSH Settings, please refer to SSH Settings on the next page.

Session Timeout	Enter the amount of time that elapses before telnet/SSH service is timed out. The default is 30 minutes. The range is from 0 to 10000 minutes.
Telnet Service	Select whether telnet service for the Switch is Enabled or Disabled. This is enabled by default.
SSH Service	Select whether the SSH service is Enabled or Disabled. This is enabled by default.

Click **Apply** to update the system settings.

Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.

Port Security

<input type="checkbox"/>	Port	State	Max MAC Address
<input type="checkbox"/>		Disabled <input type="button" value="v"/>	<input type="text" value="256"/>
<input type="checkbox"/>	1	Disabled	256
<input type="checkbox"/>	2	Disabled	256
<input type="checkbox"/>	3	Disabled	256
<input type="checkbox"/>	4	Disabled	256
<input type="checkbox"/>	5	Disabled	256
<input type="checkbox"/>	6	Disabled	256
<input type="checkbox"/>	7	Disabled	256
<input type="checkbox"/>	8	Disabled	256
<input type="checkbox"/>	9	Disabled	256
<input type="checkbox"/>	10	Disabled	256
<input type="checkbox"/>	11	Disabled	256
<input type="checkbox"/>	12	Disabled	256

Max MAC Address	Enter the maximum number of MAC addresses that can be learned on the port. The range is from 1 to 256.
Port	Displays the port for which the port security is defined.
State	Select Enabled or Disabled for the port security feature for the selected port.

Click **Apply** to update the system settings.

Port Isolation

Port Isolation feature provides L2 isolation between ports within the same broadcast domain. When enabled, **Isolated ports** can forward traffic to **Not Isolated ports**, but not to other **Isolated ports**. **Not Isolated ports** can send traffic to any port; whether **Isolated** or **Not Isolated**. The default setting is **Not Isolated**.

Port Isolation		
	Port	Status
<input type="checkbox"/>		Not Isolated <input type="button" value="v"/>
<input type="checkbox"/>	1	Not Isolated
<input type="checkbox"/>	2	Not Isolated
<input type="checkbox"/>	3	Not Isolated
<input type="checkbox"/>	4	Not Isolated
<input type="checkbox"/>	5	Not Isolated
<input type="checkbox"/>	6	Not Isolated
<input type="checkbox"/>	7	Not Isolated
<input type="checkbox"/>	8	Not Isolated
<input type="checkbox"/>	9	Not Isolated
<input type="checkbox"/>	10	Not Isolated

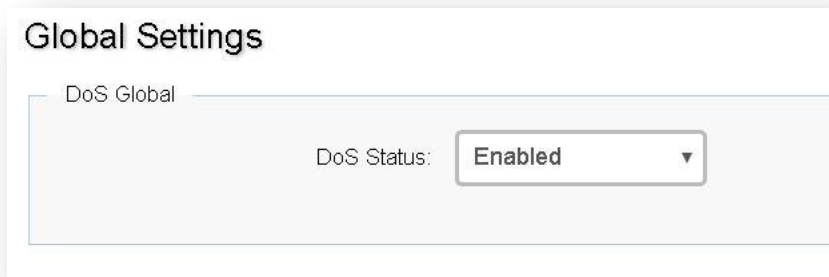
Click **Apply** to update the system settings.

DoS

DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the Switch to monitor and block different types of attacks.

Global Settings

On this page, the user can enable or disable the prevention of different types of DoS attacks. When enabled, the switch will drop the packets matching the types of DoS attack detected.



The screenshot shows a web interface titled "Global Settings". Below the title, there is a section labeled "DoS Global". Inside this section, the text "DoS Status:" is followed by a dropdown menu. The dropdown menu is currently set to "Enabled" and has a small downward-pointing triangle on its right side.

Click **Apply** to update the system settings.

Monitoring

Port Statistics

The Port Statistics page displays a summary of all port traffic statistics.

Port Statistics													
	Port	RXByte	RXUcast	RXNUcast	RXDiscard	TXByte	TXUcast	TXNUcast	TXDiscard	RXMcast	RXBcast	TXMcast	TXBcast
<input type="checkbox"/>													
<input type="checkbox"/>	1	68425444	256869	39943	0	1608175557	384133	11968890	0	32978	6965	3299502	8669388
<input type="checkbox"/>	2	1183982561	4423669	591931	0	1202944962	6789468	64236755	0	218709	373222	17637471	46599284
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	14543	0	113	0	652787142	740821	4367228	10	51	62	1022949	3344279
<input type="checkbox"/>	7	1422341998	5321905	17279	0	3721828038	5893463	82980852	0	4190	13089	21025720	61955132
<input type="checkbox"/>	8	1258800280	5333578	69426	0	1916129700	6792252	82929143	0	63296	6130	20966739	61962404
<input type="checkbox"/>	9	395175380	5716714	237502	0	355120309	5674469	82760755	0	111212	126290	20918692	61842063
<input type="checkbox"/>	10	1579406332	28707090	82155864	0	769244081	26430416	963478	0	20738436	61417428	412219	551259

Port	Displays the port for which statistics are displayed.
RXByte	Displays the number of all packets received on the port.
RXUcast	Displays the number of unicast packets received on the port.
RXNUcast	Displays the number of unicast packets received on the port.
RXDiscard	Displays the number of received packets discarded on the port.
TXByte	Displays the number of all packets transmitted on the port.
TXUcast	Displays the number of unicast packets transmitted on port.
TXNUcast	Displays the number of unicast packets transmitted on the port.
TXDiscard	Displays the number of transmitted packets discarded on the port.
RXMcast	Displays the number of multicast packets received on the port.
RXBcast	Displays the number of broadcast packets received on the port.
TXMcast	Displays the number of multicast packets transmitted on the port.
TXBcast	Displays the number of broadcast packets transmitted on the port.
TXError	Displays the number of error packets transmitted on the port.
HCOutCount	Displays the number of outcount packets transmitted on the port.

RMON

Remote Network Monitoring, or RMON is used for support monitoring and protocol analysis of LANs by enabling various network monitors and console systems to exchange network monitoring data through the Switch.

Stat List

The Status List defines RMON status on the switch.

Stat List

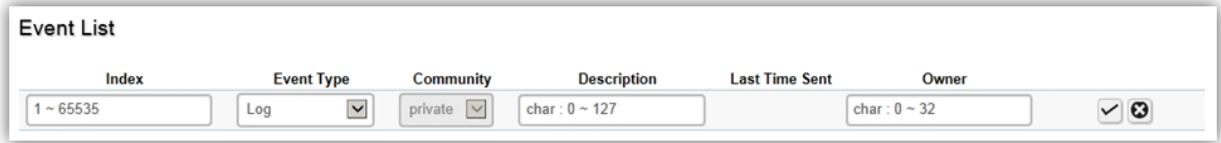
Index	Data Source	Owner	
1 ~ 65535	1	char : 0 ~ 127	<input checked="" type="checkbox"/> <input type="checkbox"/>

Index	Enter the entry number for event.
Data Source	Select the data source from the port.
Owner	Enter the switch that defined the event.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Event List

The Event List defines RMON events on the Switch.

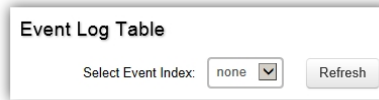


Index	Enter the entry number for event.
Event Type	Select the event type. Log: The event is a log entry. SNMP Trap: The event is a trap. Log & Trap: The event is both a log entry and a trap.
Community	Enter the community to which the event belongs.
Description	Displays the number of good broadcast packets received on the interface.
Last Time Sent	Displays the time that event occurred.
Owner	Enter the switch that defined the event.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Event Log Table

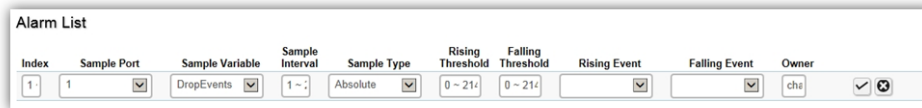
From here, you can view specific event logs for the Switch. Choose an event log you wish to view from the drop down list.



The dialog box titled "Event Log Table" contains a label "Select Event Index:" followed by a dropdown menu currently set to "none" and a "Refresh" button.


Alarm List

You can configure network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop down boxes.



The "Alarm List" dialog box shows a configuration table with the following fields: Index (1), Sample Port (1), Sample Variable (DropEvents), Sample Interval (1), Sample Type (Absolute), Rising Threshold (0-21), Falling Threshold (0-21), Rising Event (empty), Falling Event (empty), and Owner (che). There are checkmarks in the Sample Port, Sample Variable, and Owner fields.

Index	Enter the entry number for the Alarm List.
Sample Port	Select the port from which the alarm samples were taken.
Sample Variable	Select the variable of samples for the specified alarm sample.
Sample Interval	Enter the alarm interval time.
Sample Type	Select the sampling method for the selected variable and comparing the value against the thresholds. Absolute: Compares the values with the thresholds at the end of the sampling interval. Delta: Subtracts the last sampled value from the current value.
Rising Threshold	Enter the rising number that triggers the rising threshold alarm.
Falling Threshold	Enter the falling number that triggers the falling threshold alarm.
Rising Event	Enter the event number by the falling alarm are reported.
Falling Event	Enter the event number by the falling alarms are reported.
Owner	Enter the Switch that defined the alarm.

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

History List

History List

Index	Sample Port	Bucket Requested	Interval	Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
1 ~ 65535	1	1 ~ 50	1 ~ 3600	char : 0 ~ 32		

Index	Enter the entry number for the History List.
Sample Port	Select the port from which the history samples were taken.
Bucket Requested	Enter the number of samples to be saved. The range is from 1 to 50.
Interval	Enter the time that samples are taken from the ports. The field range is from 1 to 3600.
Owner	Enter the RMON user that requested the RMON information. The range is from 0 to 32 characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

History Log Table

From here, you can view the History Index for history logs on the Switch. Select a history index to view from the drop down box.

History Log Table

Select History Index: none ▼ Refresh

Statistics

From here, you can view all the RMON statistics of the Switch.

Statistics																		
	Port	Drop Events	Octets	Pkts	Broadcast Pkts	Multicast Pkts	CRC Align Errors	Under Size Pkts	Over Size Pkts	Fragments	Jabbers	Collisions	Pkts 64 Octets	Pkts 65 to 127 Octets	Pkts 128 to 255 Octets	Pkts 256 to 511 Octets	Pkts 512 to 1023 Octets	Pkts 1024 to 1518 Octets
<input type="checkbox"/>																		
<input type="checkbox"/>	1	0	68425444	296812	6965	32978	0	0	0	0	0	0	119763	82197	32811	13992	40047	8002
<input type="checkbox"/>	2	0	1183991729	5015632	373236	218717	0	0	0	0	0	0	457631	3352136	389564	147102	303989	365210
<input type="checkbox"/>	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	6	0	14543	113	62	51	0	199	0	0	0	195	20	60	28	5	0	0
<input type="checkbox"/>	7	0	1422354322	5339283	13089	4190	42	4	0	0	5	0	1546901	2153386	412948	577706	86773	561560
<input type="checkbox"/>	8	0	1258810916	5403047	6130	63299	0	0	0	0	0	0	1630174	2170577	344589	454008	486857	316842
<input type="checkbox"/>	9	0	395187668	5954372	126364	111212	0	0	0	0	0	0	355586	2207222	259740	116842	75385	2939597
<input type="checkbox"/>	10	0	1579921264	110866964	61419749	20739682	0	0	0	0	0	0	34970962	47545335	14504915	5037080	1427176	7381496
<input type="checkbox"/>	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
<input type="checkbox"/>	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Port	Indicates the specific port for which RMON statistics are displayed.
Drop Events	Displays the number of dropped events that have occurred on the port.
Octets	Displays the number of octets received on the port.

Pkts	Displays the number of packets received on the port.
Broadcast Pkts	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts	Displays the number of good Multicast packets received on the port.
CRC & Align Errors	Displays the number of CRC and Align errors that have occurred on the port.
Undersize Pkts	Displays the number of undersized packets (less than 64 octets) received on the port.
Oversize Pkts	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments	Displays the number of fragments received on the port.
Jabbers	Displays the total number of received packets that were longer than 1518 octets.
Collisions	Displays the number of collisions received on the port.
Pkts of 64 Octets	Displays the number of 64-byte frames received on the port.
Pkts of 65 to 127 Octets	Displays the number of 65 to 127 byte packets received on the port.
Pkts of 128 to 255 Octets	Displays the number of 128 to 255 byte packets received on the port.
Pkts of 256 to 511 Octets	Displays the number of 256 to 511 byte packets received on the port.
Pkts of 512 to 1023 Octets	Displays the number of 512 to 1023 byte packets received on the port.
Pkts of 1024 to 1518 Octets	Displays the number of 1024 to 1518 byte packets received on port.

Log

The Syslog protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operation and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.

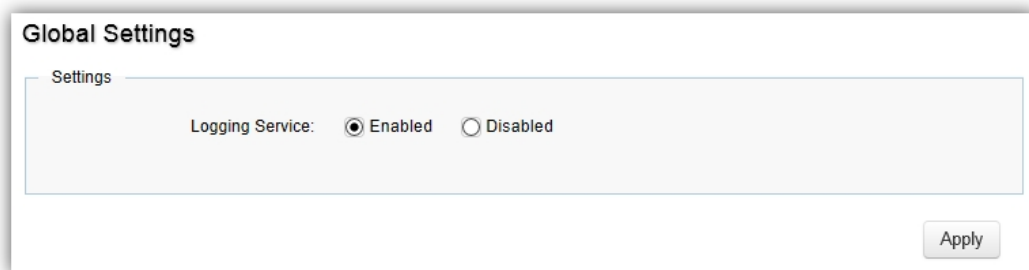
Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details. The following table describes the Syslog severity levels.

Code	Severity	Description	General Description
0	EMERG	System is unusable.	A "panic" condition usually affecting multiple apps/servers/sites. At this level it would usually notify all tech staff on call.
1	ALERT	Action must be taken immediately.	Should be corrected immediately, therefore notify staff who can fix the problem. An example would be the loss of a primary ISP connection.
2	CRIT	Critical conditions.	Should be corrected immediately, but indicates failure in a secondary system, an example is a loss of a backup ISP connection.
3	ERROR	Error conditions.	Non-urgent failures, these should be relayed to developers or admins; each item must be resolved within a given time.
4	WARNING	Warning conditions.	Warning messages, not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Normal but significant condition.	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.

6	INFO	Informational messages	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
---	------	------------------------	--

Global Settings

From here, you can Enable or Disable the log settings for the Switch.





The image shows a 'Global Settings' dialog box. It has a title bar 'Global Settings' and a sub-section 'Settings'. Inside the 'Settings' section, there is a label 'Logging Service:' followed by two radio buttons: 'Enabled' (which is selected) and 'Disabled'. At the bottom right of the dialog box, there is an 'Apply' button.

Click **Apply** to update the system settings.

Local Logging

The System Log is designed to monitor the operation of the Switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

The Switch supports log output to two directions: Flash and RAM. The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's Flash will be kept effective even if the Switch is rebooted or powered off. The log has a fixed capacity; at a certain level, the ECS Switch will start deleting the oldest entries to make room for the newest.

Target	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG	
RAM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Flash	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Click the **Apply** button  to accept the changes or the **Cancel** button  to discard them.

Remote Logging

The internal log of the ECS Switch has a fixed capacity; at a certain level, the ECS Switch will start deleting the oldest entries to make room for the newest. If you want a permanent record of all logging activities, you can set up your syslog server to receive log contents from the ECS Switch. Use this page to direct all logging to the syslog server. Click the Add button, define your syslog server, and select the severity level of events you wish to log.

IP/Hostname	Server Port	EMERG	ALERT	CRIT	ERROR	WARNING	NOTICE	INFO	DEBUG	Facility	
char: 1 ~ 63	514	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	No <input type="checkbox"/>	local0 <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Log table

This page displays the most recent records in the Switch's internal log. Log entries are listed in reverse chronological order (with the latest logs at the top of the list). Click a column header to sort the contents by that category.

Event Logs

Display logs in: **RAM**

Q

Time	Category	Severity	Message
2019 Sep 10 07:38:57	WEB	info	WEBNM: Successfully logged as User - admin
2019 Sep 10 03:03:44	SNTP	info	Old Time : Mon Sep 09 2019 15:03:46 (UTC +00:00), New Time : Tue Sep 10 2019 03:03:44 (UTC +00:00), ServerIpAddress : 183.177.72.202
2019 Sep 9 16:20:12	WEB	info	WEBNM: Successfully logged as User - admin
2019 Sep 9 15:03:46	SNTP	info	Old Time : Mon Sep 09 2019 03:03:43 (UTC +00:00), New Time : Mon Sep 09 2019 15:03:46 (UTC +00:00), ServerIpAddress : 183.177.72.202
2019 Sep 9 10:17:19	WEB	info	WEBNM: Successfully logged as User - admin
2019 Sep 9 09:57:45	WEB	info	WEBNM: Successfully logged as User - admin
2019 Sep 9 07:25:28	WEB	info	WEBNM: Successfully logged as User - admin
2019 Sep 9 03:03:43	SNTP	info	Old Time : Sun Sep 08 2019 15:03:47 (UTC +00:00), New Time : Mon Sep 09 2019 03:03:43 (UTC +00:00), ServerIpAddress : 183.177.72.202
2019 Sep 8 15:03:47	SNTP	info	Old Time : Sun Sep 08 2019 03:03:44 (UTC +00:00), New Time : Sun Sep 08 2019 15:03:47 (UTC +00:00), ServerIpAddress : 183.177.72.202
2019 Sep 8 03:03:44	SNTP	info	Old Time : Sat Sep 07 2019 15:03:45 (UTC +00:00), New Time : Sun Sep 08 2019 03:03:44 (UTC +00:00), ServerIpAddress : 183.177.72.202

10 1 to 10 of 50 event(s) Previous Next

Export Clear

Display logs in

- **RAM:** The information stored in the system's RAM log will be lost after the Switch is rebooted or powered off
- **Flash:** The information stored in the system's Flash will be kept effective even if the Switch is rebooted or powered off.

Export: Click Export button to export the current buffered log to a .txt file.

Clear: Click Clear button to clear the buffered log in the system's memory.

Diagnostics

Cable Diagnostics

Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.

Cable Diagnostics

Note: Cable length is only for reference and may be inaccurate when 'OK' is indicated.

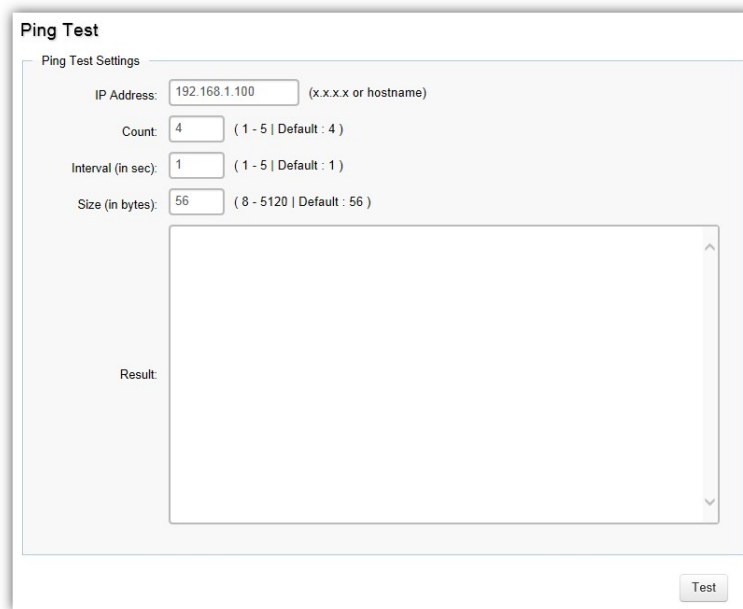
Port	Pair A	Cable Length A (meter)	Pair B	Cable Length B (meter)	Pair C	Cable Length C (meter)	Pair D	Cable Length D (meter)
Port 2 <input type="checkbox"/>	OK	8	OK	8	OK	8	OK	8

To verify accuracy of the test, it is recommended that you run multiple tests in case of test fault or user error.

Click **Test** to perform the cable tests for the selected port.

Ping Test

The Packet Internet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss. Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.



You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IP address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the Switch can communicate with a particular network host before testing.

IPv6 Ping Test

Ping Test Settings

IP Address: (xxxx:xx:xx)

Count: (1 - 5 | Default : 4)

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

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

Result:

You can vary the test parameters by entering the data in the appropriate boxes. To verify accuracy of the test, it is recommended that you run multiple tests in case of a test fault or user error.

IP Address	Enter the IPv6 address or the host name of the station you want the Switch to ping to.
Count	Enter the number of ping to send. The range is from 1 to 5 and the default is 4.
Interval	Enter the number of seconds between pings sent. The range is from 1 to 5 and the default is 1.
Size	Enter the size of ping packet to send. The range is from 8 to 5120 and the default is 56.
Result	Displays the ping test results.

Click **Test** to perform the ping test.

Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

Trace Route

Trace Route Settings

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

Max Hop: (2 - 255 | Default : 30)

Result:

```

traceroute to google.com (64.233.187.101), 30 hops max, 40 byte packets
 1 118.163.20.254 (118.163.20.254) 48 bytes to 10.0.85.245  20 ms  20 ms  10 ms
 2 168.95.228.42 (168.95.228.42) 36 bytes to 10.0.85.245  20 ms  30 ms  20 ms
 3 220.128.2.158 (220.128.2.158) 148 bytes to 10.0.85.245  20 ms  220.128.3.102
(220.128.3.102) 148 bytes to 10.0.85.245  20 ms  220.128.1.70 (220.128.1.70) 148 bytes to
10.0.85.245  20 ms
 4 220.128.9.81 (220.128.9.81) 148 bytes to 10.0.85.245  20 ms  20 ms  220.128.8.81
(220.128.8.81) 148 bytes to 10.0.85.245  20 ms
 5 220.128.9.173 (220.128.9.173) 36 bytes to 10.0.85.245  20 ms  220.128.8.173
(220.128.8.173) 36 bytes to 10.0.85.245  20 ms  220.128.9.173 (220.128.9.173) 36 bytes to
10.0.85.245  20 ms
 6 72.14.196.3 (72.14.196.3) 36 bytes to 10.0.85.245  20 ms  74.125.49.158 (74.125.49.158)
36 bytes to 10.0.85.245  20 ms  20 ms
 7 209.85.243.30 (209.85.243.30) 36 bytes to 10.0.85.245  30 ms  30 ms  20 ms
 8 216.239.46.223 (216.239.46.223) 148 bytes to 10.0.85.245  30 ms  209.85.250.229
(209.85.250.229) 148 bytes to 10.0.85.245  20 ms  209.85.252.213 (209.85.252.213) 148
bytes to 10.0.85.245  30 ms
 9 216.239.43.101 (216.239.43.101) 36 bytes to 10.0.85.245  20 ms  66.249.94.131
(66.249.94.131) 36 bytes to 10.0.85.245  20 ms  216.239.50.45 (216.239.50.45) 36 bytes to
10.0.85.245  30 ms

```

IP Address	Enter the IP address or the host name of the station you wish the Switch to ping to.
Max Hop	Enter the maximum number of hops. The range is from 2 to 255 and the default is 30.
Result	Displays the trace route results.

Click **Test** to initiate the trace route.

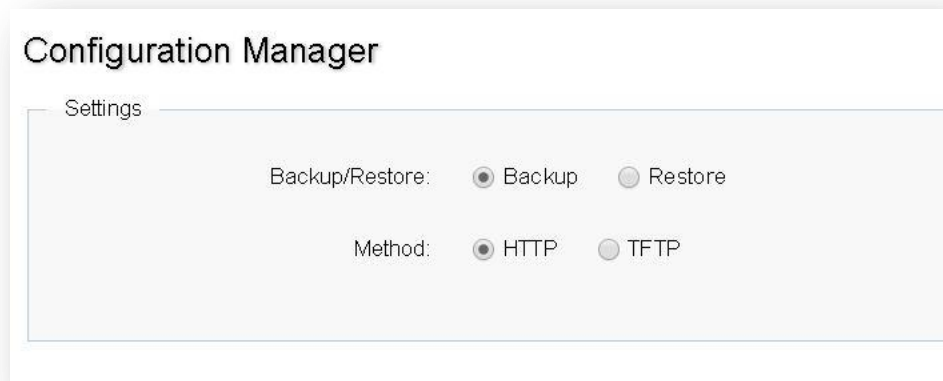
Maintenance

Maintenance functions are available from the maintenance bar located on the upper right corner of the user interface. Maintenance functions include: saving configuration settings, upgrading firmware, resetting the configuration to factory default standards, rebooting the device, and logging out of the interface. The following represents the Maintenance menu bar.



Configuration Manager

The File Management feature is used for saving your current configuration to a file on your computer or a TFTP server, or to restore previously saved configuration settings to the Switch using a configuration file from your local drive or TFTP server.



Click **Apply** to download configuration settings to your computer or a TFTP server, or to upload previously saved configuration file to the system.

Firmware Upgrade

Firmware Upgrade

Settings

Upgrade Method:

Partition:

File: 瀏覽...

Apply



WARNING

Backup your configuration before upgrading to prevent loss of settings information.



NOTE: The upgrade process may require a few minutes to complete. It is advised to clear your browser cache after upgrading your firmware.

Appendix

Appendix A - Federal Communications Commission (FCC)

EMC Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operations.



WARNING!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

Appendix B - IC Interference Statement

The following information applies if you use the product within Canada area.

Industry Canada ICES Statement

CAN ICES-003 (Issue 6)

Appendix C - EU Declaration of Conformity

The following information applies if you use the product within European Union.

CE EMC statement

This device complies with the essential requirements and other relevant provisions of the directives 2004/108 / EC (EMC); 2014 / 30 / EU (EMC); 2006/95 / EC (LVD); 2014/35 / EU (LVD). The following test methods have been applied in order to prove presumption of conformity with the essential requirements:

EN 55032:2015+AC: 2016 (Class A)

EN 55024:2010+A1:2015

EN 60950-1:2005+A1:2009+A2:2013

EN 62368-1: 2014

NOTICE:

Operation of this equipment in a residential environment may cause radio interference.

AVISO:

la operación de este equipo en un entorno residencial puede causar interferencias de radio.