

**C51-082-30-120**

**C51-164-30-250**

**C51-242-30-380**

PoE Managed Switches

## **User's Manual**

---

# About This Manual

## Copyright

Copyright © AETEK Inc. 2020 | All rights reserved.

The products and programs described in this User Guide are licensed products of AETEK Inc., This User Guide contains proprietary information protected by copyright, and this User Guide and all accompanying hardware, software and documentation are copyrighted. No parts of this User Guide may be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of AETEK Inc.

## Purpose

This GUI user guide gives specific information on how to operate and use the management functions of the C51 Series via HTTP web browser

## Audience

The Manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Hypertext Transfer Protocol (HTTP).

## CONVENTIONS

The following conventions are used throughout this manual to show information.

## WARRANTY

See the Customer Support/ Warranty booklet included with the product. A copy of the specific warranty terms applicable to your Manufacture products and replacement parts can be obtained from your Manufacture Sales and Service Office authorized dealer.

## Disclaimer

AETEK Inc. does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. Manufacture disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User Guide is subject to change without notice and does not represent a commitment on the part of Manufacture. Manufacture assumes no responsibility for any inaccuracies that may be contained in this User Guide. Manufacture makes no commitment to update or keep current the information in this User Guide, and reserves the right to make improvements to this User Guide and /or to the products described in this User Guide, at any time without notice.

# Table of Contents

<b>ABOUT THIS MANUAL</b> .....	<b>II</b>
<b>INTRODUCTION</b> .....	<b>1</b>
<b>CHAPTER 1 OPERATION OF WEB-BASED MANAGEMENT</b> .....	<b>2</b>
<b>CHAPTER 2 INTRODUCTION</b> .....	<b>3</b>
2-1 SYSTEM INFORMATION.....	3
2-2 SYSTEM TIME.....	5
2-3 IP ADDRESS SETTINGS .....	6
2-4 ACCOUNT / PASSWORD .....	7
2-5 SNMP SETTINGS.....	8
2-6 MAC ADDRESS TABLE.....	9
2-7 SysLOG.....	10
2-7.1 SysLOG CONFIGURATION .....	10
2-7.2 View Log.....	10
<b>CHAPTER 3 PORT</b> .....	<b>12</b>
3-1 PORT SETTING .....	12
3-2 LINK AGGREGATION .....	14
3-3 ENERGY EFFICIENT ETHERNET .....	15
3-4 JUMBO FRAME.....	16
3-5 PORT STATISTICS.....	16
<b>CHAPTER 4 POE MANAGEMENT</b> .....	<b>18</b>
4-1 PoE CONFIGURATION .....	18
4-2 PoE STATUS .....	19
4-3 PoE POWER DELAY .....	20
4-4 PoE AUTO CHECKING.....	21
4-5 PoE SCHEDULING PROFILE.....	22
<b>CHAPTER 5 VLAN</b> .....	<b>24</b>
5-1 VLAN CREATE.....	24
5-2 MEMBER .....	24
5-3 PVID .....	26
<b>CHAPTER 6 IGMP SNOOPING</b> .....	<b>27</b>
6-1 PROPERTY .....	27
6-2 GROUP ADDRESS.....	28
<b>CHAPTER 7 LLDP</b> .....	<b>29</b>
7-1 LLDP CONFIGURATION .....	29
7-2 LLDP INFORMATION.....	31
<b>CHAPTER 8 LOOP PREVENTION</b> .....	<b>33</b>
8-1 PROPERTY .....	33
8-2 STATUS.....	33
<b>CHAPTER 9 SECURITY</b> .....	<b>35</b>
9-1 IP FILTER.....	35
9-2 PORT ISOLATION.....	37
9-3 PORT SECURITY .....	38
9-4 STORM CONTROL .....	39
9-5 DOS ATTACK PREVENTION .....	40

<b>CHAPTER 10</b>	<b>QUALITY OF SERVICE.....</b>	<b>43</b>
10-1	PROPERTY .....	43
10-2	TCP/UDP BASED CoS .....	47
10-3	RATE LIMIT .....	47
<b>CHAPTER 11</b>	<b>SPANNING TREE.....</b>	<b>49</b>
11-1	STATE.....	49
11-2	REGION CONFIG.....	50
11-3	INSTANCE VIEW .....	51
<b>CHAPTER 12</b>	<b>DHCP.....</b>	<b>57</b>
12-1	DHCP SERVER .....	57
<b>CHAPTER 13</b>	<b>DIAGNOSTICS .....</b>	<b>58</b>
13-1	MIRRORING .....	58
13-2	PING.....	59
13-3	LAN CABLE DIAGNOSTICS .....	61
<b>CHAPTER 14</b>	<b>MAINTENANCE.....</b>	<b>63</b>
14-1	CONFIGURATION .....	63
14-1.1	IMPORT / EXPORT .....	63
14-2	RESTART DEVICE .....	64
14-3	RESET DEFAULT.....	64
14-4	FIRMWARE UPGRADE.....	64

## Overview

In this User Guide, it will not only tell you how to install and connect your network system but configure and monitor the C51 Series through the web by (RJ-45) serial interface and Ethernet ports step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface.

The C51 Series are web smart managed PoE switch from AETEK INC., is a portfolio of affordable managed switches that provides a reliable infrastructure for your business network. These switches deliver more intelligent features you need to improve the availability of your critical business applications, protect your sensitive information, and optimize your network bandwidth to deliver information and applications more effectively. It provides the ideal combination of affordability and capabilities for entry level networking includes small business or enterprise application and helps you create a more efficient, better-connected workforce.

C51 Series is Web Smart Managed Switch; the specification is highlighted as follows.

## Features

---

- **Layer 2 Switch**
  - 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP)
  - Loop protection
  - SNMP
  - QoS
  - VLAN
  - LACP
  - DHCP Server
- **PoE Management**
  - PoE Per Port On/OFF Control
  - PoE Status
  - PoE Power Delay
  - PoE Auto Checking
  - PoE Scheduling Profile

## Initial Configuration

This chapter instructs you how to configure and manage the C51 Series through the web user interface. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including, each port activity, Spanning tree status, port aggregation status, VLAN and priority status, and so on.

The default values of the C51 Series are listed in the table below:

<b>IP Address</b>	192.168.1.1
<b>Subnet Mask</b>	255.255.255.0
<b>Default Gateway</b>	192.168.1.254

After the C51 Series have been finished configuring the interface, you can browse it. For instance, type <http://192.168.1.1> in the address bar of a browser, it will show the following screen and ask you to input username and password in order to login and access authentication.

The first time login you need to create a new account. After the account has been created, please enter the new username and password and then click the <LOGIN> button. The login process is now completed.

In this login menu, you have to input the complete username and password respectively, the C51 Series will not give you a shortcut to username automatically. This looks inconvenient, but safer.

In the C51 Series, allowed two or more users using administrator's identity to manage this switch, which administrator to do the last setting, it will be an available configuration to effect the system.



---

**NOTE:**

To optimize the display effect, we recommend you to use Microsoft IE 6.0 above, Netscape V7.1 above or Firefox V1.00 above and have the resolution 1024x768. The switch supported neutral web browser interface

---

A registration form with three input fields and a button. The first field is labeled 'Username' with a person icon. The second field is labeled 'Password' with a key icon. The third field is labeled 'Confirm Password' with a key icon. Below the fields is a teal button labeled 'SIGN UP'.

**Figure 1-1: The first time login page**

A login form with two input fields and a button. The first field is labeled 'Username' with a person icon and contains the text 'admin'. The second field is labeled 'Password' with a key icon and contains the text '.....'. Below the fields is a teal button labeled 'LOGIN'.

**Figure 1-2: The login page**

AETEK PoE Managed switch software provides rich functionality for switches in your networks. This guide describes how to use Web-based management interface (Web UI) to configure AETEK managed switch software features.

The Web UI supports all frequently used web browsers listed below:



**Figure 2-0: Port Information**

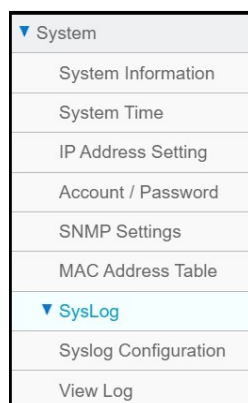
In the Web UI, the left column shows the configuration menu. The top row shows the switch's current linking status described below.

- Yellow color: The LAN port is powered on and is connected with 10/100M linking speed powered device.
- Green circles: The LAN port is powered on and is connected with 1000M linking speed powered device
- White circles: The LAN port is NOT connected with any device.

On the top-right part, it shows useful functions for users to save the system configuration, log out the system. The rest of the screen area displays the configuration settings.

## 2-1 System Information

You can identify the system by configuring system name, location and the contact of the switch. The switch system's contact information is provided here.



**Figure 2-1: System**



## Web interface

To configure System Information in the web interface:

1. Click System -> System Information.
2. Input System Name, Location and Contact information in this page.
3. Click Apply.

System Information	
Description	24xGbE PoE + 2xGbE R
Model Name	C51-242-30-380
MAC Address	68:8D:B6:00:02:55
IP Address	192.168.120.203
Subnet Mask	255.255.255.0
Default Gateway	192.168.120.1
Firmware Version	1.1.0.0
System Time	2020-3-9 11:17:25
Uptime	0 day, 0 hr, 1 min and 25

Figure 2-2: System Information

### Parameter Description:

#### ■ Description

Displays the system description.

#### ■ Model Name

Displays the factory defined model name for identification purpose.

#### ■ MAC Address

Base MAC address of the switch.

#### ■ IP Address

The IP Address of this switch.

#### ■ Subnet Mask

The Subnet Mask IP Address of this switch.

#### ■ Default Gateway

The Gateway IP Address of this switch.

#### ■ Firmware Version

The software version of this switch.

#### ■ System Time

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

#### ■ Uptime

The period of time the device has been operated.

■ **System name**

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 128.

■ **Location**

The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 1 to 32.

■ **Contact**

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 128, and the allowed content is the ASCII characters from 32 to 126.

## 2-2 System Time

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item.

### Web interface

To configure System Time in the web interface:

1. Click System -> System Time.
2. Specify the Time parameter.
3. Click Apply.

The screenshot shows a web interface titled "System Time". At the top, there are input fields for "System Time" with values: Yr 2000, Mon 1, Day 3, Hr 20, Mn. Below this is a "Copy Computer Time" button. There are two checkboxes: "Enable NTP client update" (unchecked) and "Enable Daylight Saving Time" (unchecked). The "Time Zone" is set to "(UTC+08:00)Taipei". Under "Start Time Settings", there are dropdown menus for Month (Jan), Day (1), and Hours (0). Under "End Time Settings", there are dropdown menus for Month (Jan) and Day (1).

Figure 2-3: System Time

### Parameter Description:

#### ■ **System Time**

You can input Year, Month, Day, Hour, Minute and Second manually, or by clicking "Copy Computer Time" button to get time through PC.

#### ■ **Enable NTP client update**

To enable/disable obtaining system time through the time server.

#### ■ **Time Zone**

Lists various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Apply to set.

#### ■ **Enable Daylight Saving Time**

To enable/disable daylight saving time function.

#### ■ **Start Time Settings**

Month - Select the starting month.

Day - Select the starting day.

Hours - Select the starting hour.

#### ■ **End Time Settings**

Month - Select the ending month.

Day - Select the ending day.

Hours - Select the ending hour.

#### ■ **Offset**

The number of minutes to be added by Daylight Saving Time. (Range: 1 to 720 minutes)

#### ■ **NTP Server**

The time server to be synchronized.

## 2-3 IP Address Settings

The IPv4 address for the switch could be obtained via DHCP Server for VLAN 1. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

### Web Interface

To configure an IP Settings in the web interface:

1. Click System -> IP Address Settings.
2. Enable or Disable the IPv4 DHCP Client.
3. Specify the IPv4 Address, Subnet Mask and Gateway.
4. Input IPv4 DNS Server if desired.
5. Click Apply.

IP Address Setting	
<b>IPv4 Address</b>	
DHCP	<input type="checkbox"/> Er
IP Address	<input type="text" value="192"/>
Subnet Mask	<input type="text" value="255"/>
Default Gateway	<input type="text" value="192"/>
<b>IPv4 DNS Server</b>	
DNS Server	<input type="text"/>
<b>Operational Status</b>	

Figure 2-4: IP Address Setting

**Parameter Description:**

■ **DHCP Client Enable**

Enable the DHCP client by clicking this checkbox. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCP protocol. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.

■ **IPv4 Address**

The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field is not used. The field may also be left blank if IPv4 operation on the interface is not desired.

■ **Subnet Mask**

User IP subnet mask of the entry.

■ **Default Gateway**

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

■ **DNS Server**

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

2-4 Account / Password

This page provides an overview of the current users. Use this page to modify the user name and password.

**Web Interface**

To configure User Account in the web interface:

1. Click System -> Account/Password.
2. Specify the User Name.
3. Specify new password and confirm new password.
4. Click Apply.

Account / Password	
Username	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Figure 2-5: Account / Password

**Parameter Description:**

- **User Name**  
The name identifying the user. The field can be input 32 characters.
- **New Password**  
To type the new password. The field can be input 32 characters.
- **Confirm Password**  
To type the new password again. You must type the same password again in the field.

2-5 SNMP Settings

The page is used to configure SNMPv1/v2 Communities and Trap Host.

**Web Interface**

To configure the SNMP Communities in the web interface:

1. Click System -> SNMP Settings.
2. Specify Community parameters.
3. Specify Trap Host parameters.
4. Click Apply.

SNMP Settings	
<b>State</b>	
State	<input checked="" type="checkbox"/> Enable
<b>Community</b>	
Name	<input type="text" value="public"/> Access Mode
	<input type="text" value="private"/> Access Mode
<b>Trap Host</b>	
ID Address	<input type="text"/>

Figure 2-6: SNMP Settings

**Parameter Description:**

- **State**  
To enable/disable SNMP function.
- **Community Name**  
The SNMP community name. Its maximum length is 20 characters. There are two communities by

default: "public" and "private".

■ **Access Mode**

The access mode of SNMP Community String.(Read-Only and Read Write)

■ **Trap**

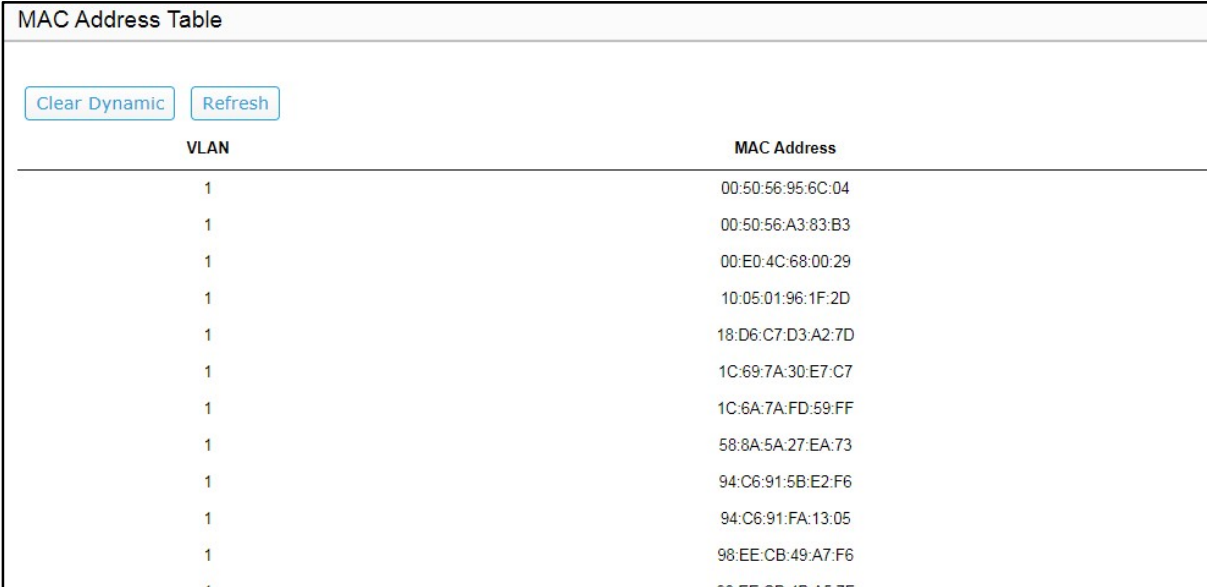
The SNMP Trap parameters. (IP Address, Version and Community)

## 2-6 MAC Address Table

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.

### Web Interface

To display MAC Address Table page, click System -> MAC Address Table



VLAN	MAC Address
1	00:50:56:95:6C:04
1	00:50:56:A3:83:B3
1	00:E0:4C:68:00:29
1	10:05:01:96:1F:2D
1	18:D6:C7:D3:A2:7D
1	1C:69:7A:30:E7:C7
1	1C:6A:7A:FD:59:FF
1	58:8A:5A:27:EA:73
1	94:C6:91:5B:E2:F6
1	94:C6:91:FA:13:05
1	98:EE:CB:49:A7:F6
1	98:EE:CB:49:A7:F6

Figure 2-7: MAC Address Table

#### Parameter Description:

■ **VLAN**

VLAN ID of the MAC address

■ **MAC Address**

MAC address

■ **Type**

Type of MAC address

- Management: DUT's base MAC address for management purpose
- SecureStatic: Manually configured by administrator for port security function.
- SecureDynamic: Dynamically learned by hardware associated with port security. It will be aged out.
- Dynamic: Dynamically learned by hardware, and it will be aged out.

■ **Port**

Type of Port

- CPU: DUT's CPU port for management purpose

· Other: Normal switch port

■ **Clear Dynamic[Button]**

To clear all dynamic entries.

■ **Refresh[Button]**

To retrieve latest MAC address entries shown on this page.

## 2-7 SysLog

### 2-7.1 Syslog Configuration

The Syslog Configuration is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

#### Web Interface

To configure the SysLog Settings in the web interface:

1. Click System -> Syslog Configuration.
2. Specify Mode and Server1(or Server2) parameters.
3. Click Apply.

System Log Configuration
Mode
Server 1
Server 2

Figure 2-8: Syslog Configuration

#### Parameter Description:

■ **Mode**

To enable/disable Syslog function.

■ **Server1(or Server2)**

SysLog Server. (IPv4 format)

### 2-7.2 View Log

To display Log, click System -> SysLog -> View Log

Log Information			
<input type="button" value="Refresh"/> <input type="button" value="Clear"/>			
Show <input type="text" value="10"/> entries			
ID	Level	Time	Message
1	notice	Jan 01 2000 00:05:49	SYSTEM-0: New http connection for user admin, source 192.168.120.26 ACCEPTED
2	notice	Jan 01 2000 00:01:25	SYSTEM-5: New http connection for user admin, source 192.168.120.163 ACCEPTED
3	notice	Jan 01 2000 00:00:57	PORT-5: Interface GigabitEthernet7 link up
4	notice	Jan 01 2000 00:00:35	SYSTEM-5: New console connection for user admin, source async ACCEPTED
5	notice	Jan 01 2000 00:00:15	PORT-5: Interface GigabitEthernet5 link up
6	notice	Jan 01 2000 00:00:15	PORT-5: Interface GigabitEthernet6 link up
7	notice	Jan 01 2000 00:00:13	SYSTEM-5: Cold startup

Showing 1 to 7 of 7 entries

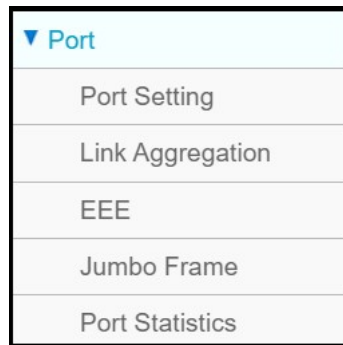
**Figure 2-9: View log**

**Parameter Description:**

- **Level**  
The log event category.
- **Time**  
The log event occurs time.
- **Message**  
The log event content.
- **Refresh[Button]**  
To reload log events.
- **Clear[Button]**  
To clear log events.



The section describes to configure the Port detail parameters of the switch. Others you could use the Port configure to enable or disable the Port of the switch. Monitor the ports content or status in the function



**Figure 3-0: Port Setting**

### 3-1 Port Setting

This page displays current port configuration. Ports can also be configured here.

#### **Web Interface**

To configure a Current Port Configuration in the web interface:

1. Click Port -> Port Setting.
2. Click the port number which you want to configure. (For example: Port 9)
3. Click Edit.
4. Specify the parameters you want to configure.
5. Click Apply.

Port Setting						
	Port	State	Link Status	Speed		
<input type="checkbox"/>	1	Enabled	Down	Auto		
<input type="checkbox"/>	2	Enabled	Down	Auto		
<input type="checkbox"/>	3	Enabled	Down	Auto		
<input type="checkbox"/>	4	Enabled	Down	Auto		
<input type="checkbox"/>	5	Enabled	Down	Auto		
<input type="checkbox"/>	6	Enabled	Down	Auto		
<input type="checkbox"/>	7	Enabled	Down	Auto		
<input type="checkbox"/>	8	Enabled	Down	Auto		
<input type="checkbox"/>	9	Enabled	Up	Auto (1000M)		
<input type="checkbox"/>	10	Enabled	Down	Auto		
<input type="checkbox"/>	11	Enabled	Down	Auto		
<input type="checkbox"/>	12	Enabled	Down	Auto		
<input type="checkbox"/>	13	Enabled	Down	Auto		
<input type="checkbox"/>	14	Enabled	Down	Auto		
<input type="checkbox"/>	15	Enabled	Down	Auto		
<input type="checkbox"/>	16	Enabled	Down	Auto		
<input type="checkbox"/>	17	Enabled	Down	Auto		
<input type="checkbox"/>	18	Enabled	Down	Auto		
<input checked="" type="checkbox"/>	19	Enabled	Down	Auto		

Figure 3-1.1: Port Setting

**Edit Port Setting**

---

Port

---

State

---

Speed

---

Duplex

Figure 3-1.2: Edit Port Setting

**Parameter Description:**

- **State**  
To enable/disable port link function.
- **Speed**  
Current port speed configuration and link speed status
- **Duplex**  
Current port duplex configuration and link duplex status
- **Flow Control**  
Current port flow control configuration and link flow control status

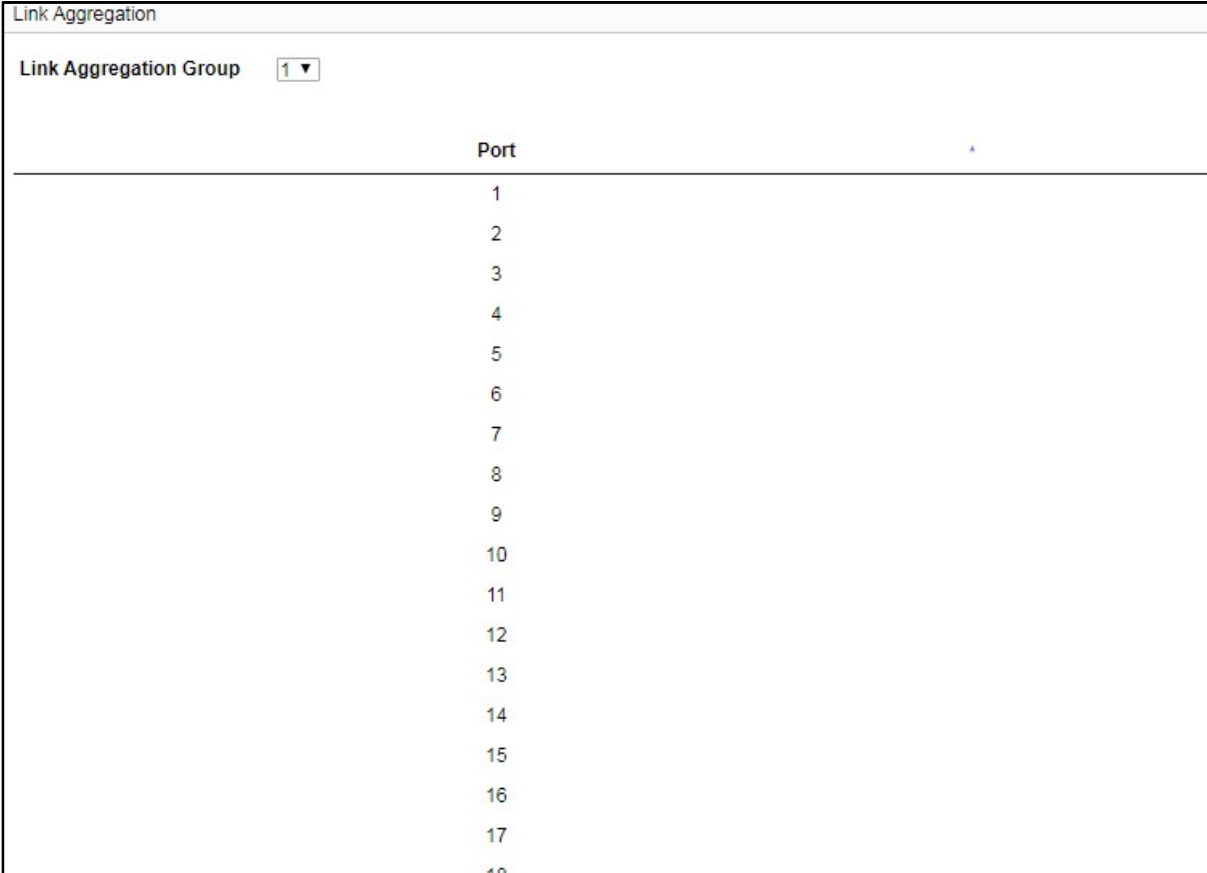
## 3-2 Link Aggregation

This page is used to configure port's LACP.

### Web Interface

To configure a Current Port's LACP in the web interface:

1. Click Port -> Link Aggregation.
2. Specify Link Aggregation Group and the port's LACP method you want to configure. (For example: Port 9)
3. Click Apply.



Port
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18

Figure 3-2: Link Aggregation

### Parameter Description:

#### ■ Link Aggregation Group

A link aggregation group (LAG) combines a number of physical ports together to make a single high-bandwidth data path, so as to implement the traffic load sharing among the member ports in the group and to enhance the connection reliability.

#### ■ Method

Current port's LACP method.(None/LACP)

### 3-3 Energy Efficient Ethernet

This page is used to set current ports' energy configuration.

#### Web Interface

To configure a Current Port EEE Configuration in the web interface:

1. Click Port -> EEE.
2. Specify the parameters you want to configure.
3. Click Apply.

Energy Efficient Ethernet	
Port	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	

Figure 3-3: Link Aggregation

#### Parameter Description:

##### ■ Setting

To enable/disable EEE function.

### 3-4 Jumbo Frame

This page is used to set jumbo frame function.

#### Web Interface

To configure jumbo frame function in the web interface:

1. Click Port -> Jumbo Frame.
2. Specify the parameters you want to configure.
3. Click Apply.

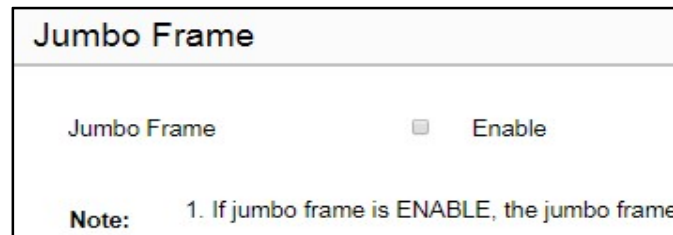


Figure 3-4: Jumbo Frame

#### Parameter Description:

##### ■ Enable

To enable/disable jumbo frame function.

### 3-5 Port Statistics

The Port Statistics page displays port summary and status information. This page displays standard counters on network traffic from the Interfaces. The port counters would be display in four groups individually.

#### Web Interface

To display Port Statistics in the web interface:

1. Click Port -> Port Statistics.
2. Click Rx/Tx, Collision , Dropped and CRC Error individually to view each port's statistics information.
3. Click "Clear" button will clear counter of current selected port.

Port Statistics		
Statistics	<input checked="" type="radio"/>	Rx / Tx
	<input type="radio"/>	Collision
	<input type="radio"/>	Dropped
	<input type="radio"/>	CRC Error
Port	Rx	
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	421	
10	0	
11	0	
12	0	
13	0	
14	0	
15	0	
16	0	

Figure 3-5: Port Statistics

**Parameter Description:**

■ **Statistics**

Select the different counter types to show different counters.

- Rx / Tx: Interface Rx and Tx packet counters.
- Collision: Interface Collision and Tx packet counters
- Dropped: Interface Dropped and Rx packet counters
- CRC Error: Interface CRC Error and Rx packet counters

■ **Clear[Button]**

To clear counter of current selected port.

This chapter describes the PoE management including PoE Configuration, PoE Status, PoE Power Delay, PoE Auto Check and PoE Scheduling Profile.

## 4-1 PoE Configuration

This page displays current PoE ports' power ON/OFF status and schedule profile. It can also be configured here.

### Web Interface

To configure a PoE port's power in the web interface:

1. Click PoE Management -> PoE Configuration.
2. Specify the parameters which you want to configure.
3. Click Apply.

PoE Configuration

Primary Power Supply [W] 370

PoE Port Configuration

Port	PoE Mode	PoE Schedule
1	Enabled ▼	Disabled ▼
2	Enabled ▼	Disabled ▼
3	Enabled ▼	Disabled ▼
4	Enabled ▼	Disabled ▼
5	Enabled ▼	Disabled ▼
6	Enabled ▼	Disabled ▼
7	Enabled ▼	Disabled ▼
8	Enabled ▼	Disabled ▼
9	Enabled ▼	Disabled ▼
10	Enabled ▼	Disabled ▼
11	Enabled ▼	Disabled ▼
12	Enabled ▼	Disabled ▼
13	Enabled ▼	Disabled ▼
14	Enabled ▼	Disabled ▼
15	Enabled ▼	Disabled ▼

Figure 4-1: PoE Configuration

### Parameter Description:

- **Primary Power Supply**  
The total power for all ports.
- **PoE Mode**  
To enable/disable port's power.
- **PoE Schedule**

To set port's schedule profile. (profile 1 to 10, disabled means no schedule profile)

- **Priority**

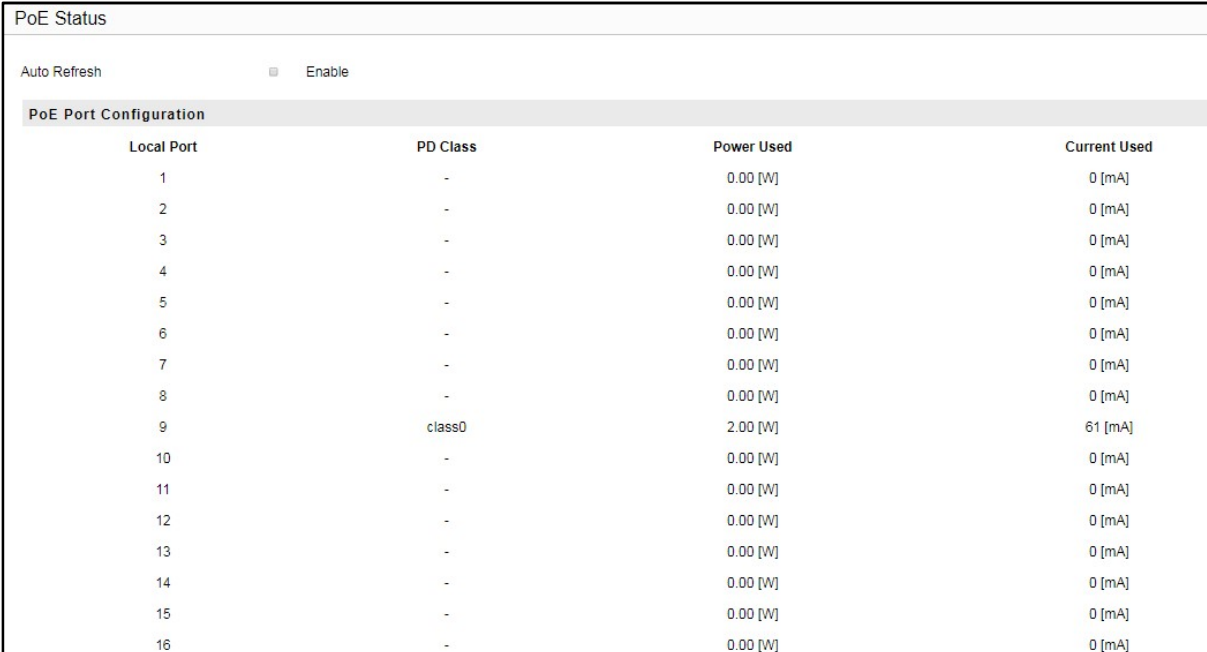
To set port's priority.

## 4-2 PoE Status

This page displays current ports' power status.

### Web Interface

To display PoE port's power information in the web interface, click PoE Management -> PoE Status.



The screenshot shows the 'PoE Status' web interface. At the top, there is a title 'PoE Status' and an 'Auto Refresh' section with a radio button labeled 'Enable'. Below this is a table titled 'PoE Port Configuration' with five columns: 'Local Port', 'PD Class', 'Power Used', and 'Current Used'. The table lists 16 ports. Port 9 is the only one with a 'class0' PD Class, showing 2.00 [W] Power Used and 61 [mA] Current Used. All other ports show 0.00 [W] Power Used and 0 [mA] Current Used.

Local Port	PD Class	Power Used	Current Used
1	-	0.00 [W]	0 [mA]
2	-	0.00 [W]	0 [mA]
3	-	0.00 [W]	0 [mA]
4	-	0.00 [W]	0 [mA]
5	-	0.00 [W]	0 [mA]
6	-	0.00 [W]	0 [mA]
7	-	0.00 [W]	0 [mA]
8	-	0.00 [W]	0 [mA]
9	class0	2.00 [W]	61 [mA]
10	-	0.00 [W]	0 [mA]
11	-	0.00 [W]	0 [mA]
12	-	0.00 [W]	0 [mA]
13	-	0.00 [W]	0 [mA]
14	-	0.00 [W]	0 [mA]
15	-	0.00 [W]	0 [mA]
16	-	0.00 [W]	0 [mA]

Figure 4-2: PoE Status

### Parameter Description:

- **Auto Refresh**

To refresh web page automatically every 10 seconds.

- **Local Port**

The logical port number.

- **PD Class**

The IEEE802.3af/at defined power classification.

Class0: 0.44~12.95 W

Class1: 0.44~3.84 W

Class2: 3.84W~6.49 W

Class3: 6.49~12.95 W

Class4: 12.95~25.5 W



- **Power Used**  
The port's PoE used power.
- **Current Used**  
The port's PoE used current.
- **Priority**  
The port's PoE priority.
- **Port Status**  
The port's PoE Status.

### 4-3 PoE Power Delay

This page displays current PoE ports' power delay function. It can also be configured here.

#### Web Interface

To configure a port power delay function in the web interface:

1. Click PoE Management -> PoE Power Delay.
2. Specify the parameters which you want to configure.
3. Click Apply.

PoE Power Delay	
Port	Delay Mode
1	Disabled ▼
2	Disabled ▼
3	Disabled ▼
4	Disabled ▼
5	Disabled ▼
6	Disabled ▼
7	Disabled ▼
8	Disabled ▼
9	Disabled ▼
10	Disabled ▼
11	Disabled ▼
12	Disabled ▼
13	Disabled ▼
14	Disabled ▼
15	Disabled ▼
16	Disabled ▼

Figure 4-3: PoE Power Delay

### Parameter Description:

- **Delay Mode**

To enable/disable power delay function

- **Delay Time**

To set port's power delay time. (0 ~ 300 seconds)

## 4-4 PoE Auto Checking

This page displays current PoE ports' power auto checking function. It can also be configured here.

### Web Interface

To configure a port power auto checking function in the web interface:

1. Click PoE Management -> PoE Auto Checking.
2. Specify the parameters which you want to configure.
3. Click Apply.

PoE Auto Checking Configuration

Ping Check  Enable  Disable

PoE Port Configuration

Port	Ping IP Address	Start Time	Interval Time	Retry Time
1	0.0.0.0	30	30	3
2	0.0.0.0	30	30	3
3	0.0.0.0	30	30	3
4	0.0.0.0	30	30	3
5	0.0.0.0	30	30	3
6	0.0.0.0	30	30	3
7	0.0.0.0	30	30	3
8	0.0.0.0	30	30	3
9	0.0.0.0	30	30	3
10	0.0.0.0	30	30	3
11	0.0.0.0	30	30	3
12	0.0.0.0	30	30	3
13	0.0.0.0	30	30	3
14	0.0.0.0	30	30	3
15	0.0.0.0	30	30	3

Figure 4-4: Power Auto Check

### Parameter Description:

- **Ping Check**

To enable/disable power auto check function.

- **Ping IP Address**

The PD's IP Address used to test its connectivity.

- **Start Time**

After Startup Time, PoE auto checking function will be started. Default: 30, range: 30-60 seconds.

- **Interval Time**

Device will send checking message to PD each interval time. Default: 30, range: 10-120 seconds.

■ **Retry Time**

When PoE port can't ping the PD, it will retry to send detection again. When reaching the retry time, it will trigger failure action. Default: 3, range: 1-5.

■ **Failure Log**

Failure loggings counter.

■ **Failure Action**

The action when reaching the retry time fail detection.

Nothing: Keep Ping the remote PD but does nothing further.

Reboot: Cut off the power of the PoE port, make PD rebooted.

■ **Reboot Time**

When PD has been rebooted, the PoE port restored power after the Reboot Time. Default: 15, range: 3-120 sec.

### 4-5 PoE Scheduling Profile

This page displays current PoE ports' power schedule profile function. It can also be configured here.

#### Web Interface

To configure power scheduling profile in the web interface:

1. Click PoE Management -> PoE Scheduling Profile.
2. Specify the parameters which you want to configure.
3. Click Apply.

The screenshot shows a web interface titled "Power Scheduling Profile". It contains several configuration fields:

- Profile:** A dropdown menu with "1" selected.
- Name:** A text input field containing "profile 1".
- Start Time:** A section with two columns: "HH" (Hours) and "MM" (Minutes). Each column has a "<>" dropdown menu for the first row and numeric dropdown menus for the subsequent rows.
- Week Day:** A section with rows for "Monday", "Tuesday", and "Wednesday". Each row has a numeric dropdown menu for the "HH" column and a "<>" dropdown menu for the "MM" column.

Figure 4-5: PoE Scheduling Profile

#### Parameter Description:

■ **Profile**

The profile number. (1-10)

■ **Name**

The profile name.

■ **Start Time <HH>**

The starting hour time.

- **Start Time <MM>**

The starting minute time.

- **End Time <HH>**

The ending hour time.

- **End Time <MM>**

The ending minute time.

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

### 5-1 VLAN Create

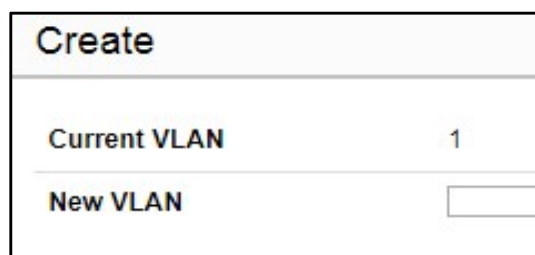
To create new VLANs for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. By default, the active management VLAN is VLAN 1, but you can designate any VLAN as the management VLAN and only one management VLAN can be active at a time.

When you specify a new management VLAN, your HTTP connection to the old management VLAN is lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN route

#### Web Interface

To create new VLANs the web interface:

1. Click VLAN -> Create.
2. Input new VLANs.
3. Click Apply.



Create	
Current VLAN	1
New VLAN	<input type="text"/>

Figure 5-1: VLAN Create

#### Parameter Description:

##### ■ New VLAN

The VLANs you want to create.

### 5-2 Member

This page provides an overview of membership status of VLANs. Users can set ports as untagged or tagged member of VLAN.

## Web Interface

To configure VLAN membership configuration in the web interface:

1. Click VLAN -> Member.
2. Select Tagged/Untagged/Not member for the port(s).
3. Click Apply.

Member	
VLAN ID	1 ▼
Port	▲
	1
	2
	3
	4
	5
	6
	7
	8
	9
	10
	11
	12
	13
	14
	15
	16
	17

Figure 5-2: VLAN Member

### Parameter Description:

- **VLAN ID**  
The VLAN ID list(s).
- **Setting**  
The VLAN membership type.

## 5-3 PVID

PVID is the VLAN ID that assign to untagged incoming packet of port.

### Web Interface

To assign PVID the web interface:

1. Click VLAN -> PVID.
2. Click the port number which you want to configure. (For example: Port 9)
3. Click Edit.
4. Select the PVID for this port.
5. Click Apply.

PVID	
	Port
<input type="checkbox"/>	1
<input type="checkbox"/>	2
<input type="checkbox"/>	3
<input type="checkbox"/>	4
<input type="checkbox"/>	5
<input type="checkbox"/>	6
<input type="checkbox"/>	7
<input type="checkbox"/>	8
<input type="checkbox"/>	9
<input type="checkbox"/>	10
<input type="checkbox"/>	11
<input type="checkbox"/>	12
<input type="checkbox"/>	13
<input type="checkbox"/>	14
<input type="checkbox"/>	15
<input type="checkbox"/>	16
<input type="checkbox"/>	17
<input type="checkbox"/>	18
<input type="checkbox"/>	19
<input type="checkbox"/>	20

Figure 5-3.1: VLAN PVID

Edit PVID	
	Port
	PVID

**Note:** 1. PVID is the VLAN ID that assign to untagged incoming packet of port

Figure 5-3.2: Edit VLAN PVID

### Parameter Description:

#### ■ PVID

The VLAN ID that assign to the port.

The function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping cannot tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance. IGMP mode enables the switch to issue IGMP function that you enable IGMP proxy or snooping on the switch, which connects to a router closer to the root of the tree. This interface is the upstream interface. The router on the upstream interface should be running IGMP.

## 6-1 Property

This page sets the property of IGMP Snooping, including State, Immediate Leave and Unknown Multicast.

### Web Interface

To configure the property of IGMP Snooping in the web interface:

1. Click IGMP Snooping -> Property.
2. Specify the parameters which you want to configure.
3. Click Apply.

Property	
State	<input type="checkbox"/> Enable
Immediate Leave	<input type="checkbox"/> Enable
Unknown Multicast	<input type="checkbox"/> Block

1. IGMP Snooping allows the switch to forward multicast traffic to interested receivers (without flooding)  
 2. With **Immediate Leave** enabled, the multicast traffic would

Figure 6-1: Property



### Parameter Description:

- **State**

To enable/disable IGMP Snooping function.

- **Immediate Leave**

If set enabled, the multicast traffic would be stopped as soon as an IGMP leave message received on a port

- **Unknown Multicast**

If set blocked, the unknown multicast received would be dropped; Otherwise, the packets would be flooded

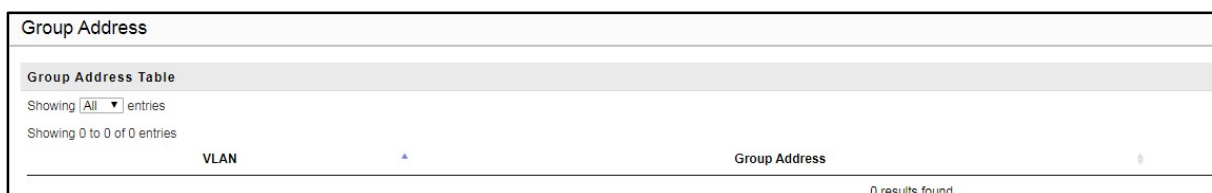
## 6-2 Group Address

This page displays the group address for all port members.

### Web Interface

To view the group address in the web interface:

1. Click IGMP Snooping -> Group Address.
2. Click "Clear" to delete the entries.
3. Click "Refresh" to reload the entries.



The screenshot shows a web interface titled "Group Address". Below the title is a "Group Address Table" section. It includes a dropdown menu set to "All" and the text "Showing 0 to 0 of 0 entries". The table has two columns: "VLAN" and "Group Address". The table is currently empty, and a status message at the bottom right indicates "0 results found."

Figure 6-2: Group Address

### Parameter Description:

- **VLAN**

VLAN.

- **Group Address**

Group Address of IGMP Snooping.

- **Member**

IGMP Snooping Members.

- **Clear[Button]**

To delete the entries.

- **Refresh[Button]**

To reload the entries.

The switch supports the LLDP. For current information on your switch model, The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices. The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Link Layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on a IEEE 802 local area network, principally wired Ethernet. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery specified in standards document IEEE 802.1AB.

## 7-1 LLDP Configuration

This page is used to configure LLDP settings. You can per port to do the LLDP configuration and the detail parameters, the settings will take effect immediately. This page allows the user to inspect and configure the current LLDP port settings.

### **Web Interface**

To configure the LLDP settings in the web interface:

1. Click LLDP -> LLDP Configuration.
2. Specify LLDP parameters you want to configure.
3. Click Apply.

LLDP Configuration	
<b>LLDP Global Settings</b>	
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
<b>LLDP Settings</b>	
Message TX Hold Multiplier	<input type="text" value="4"/> (2-10)
Message TX Interval	<input type="text" value="30"/> sec. (5-32768)
LLDP Reinit Delay	<input type="text" value="2"/> sec. (1-10)
LLDP TX Delay	<input type="text" value="2"/> sec. (1-8192)
Note : (LLDP TX Delay ) <= (0.25* (Message TX Interval)) and (Message TX Interval) * (Message TX Hold Multiplier) < 65535.	
<b>LLDP System Information</b>	
Chassis ID Subtype	macAddress
Chassis ID	68:8D:B6:00:02:55
System Name	C51-242-30-380
System Description	24xGbE PoE + 2xGbE RJ45 + 2xGbE SFP Managed Switch
<b>LLDP Port State Settings</b>	
	Port
	1
	2
	3
	4
	5

Figure 7-1: LLDP Configuration

**Parameter Description:**

■ **Status**

To enable/disable LLDP function.

■ **Message TX Hold Multiplier**

Specify the LLDP packet hold time interval as a multiple of the LLDP timer value. The range is 2 to 10, and the default value is 4.

■ **Message TX Interval**

Specify how often the software sends LLDP updates in seconds. The range is 5 to 32768 seconds. The default value is 30 seconds.

■ **LLDP Reinit Delay**

Specify the minimum time in seconds an LLDP port waits before reinitializing LLDP transmission. The range is from 1 to 10 and the default value is 2 seconds.

■ **LLDP TX Delay**

Specify the delay in seconds between successive LLDP frame transmissions initiated by value or status changes in the LLDP local systems MIB. The range is from 1 up to 8192 seconds and the default transmission delay is 2 seconds.

■ **Chassis ID Subtype**

Type of chassis ID (for example, MAC address).

■ **Chassis ID**

Identifier of the chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device is displayed.

- **System Name**

The Name of the device.

- **System Description**

The Description of the device.

- **LLDP Port Status:**

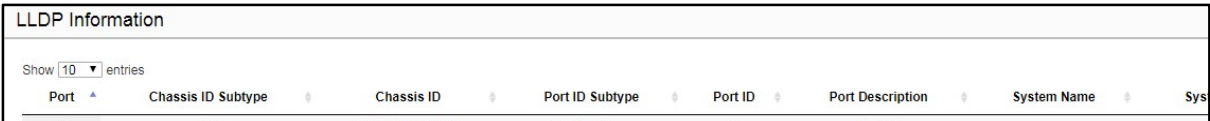
The LLDP State for the ports, including Disabled, RxTx, TxOnly and RxOnly.

## 7-2 LLDP Information

This page is to display LLDP neighborhood status.

### Web Interface

To display the LLDP neighborhood status in the web interface, click LLDP -> LLDP Information.



The screenshot shows the 'LLDP Information' page in a web interface. At the top, there is a header 'LLDP Information'. Below the header, there is a control 'Show 10 entries'. Below that is a table with the following columns: Port, Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, Port Description, System Name, and Sys. The table content is mostly obscured by a dark shadow.

Figure 7-2: LLDP Information

### Parameter Description:

- **Port**

The normal port of the device.

- **Chassis ID Subtype**

Type of chassis ID (for example, MAC address).

- **Chassis ID**

Identifier of the chassis. Where the chassis ID subtype is a MAC address, the MAC address of the device is displayed.

- **Port ID Subtype**

Type of the port identifier.

- **Port ID**

Port identifier.

- **Port Description**

The Description of the Port.

- **System Name**

The Name of the device.

- **System Capabilities**

Identifies the switch's primary capabilities (bridge, router).

- **System Description**

The Description of the device.

- **Management Address**

Specify the management address to be used in LLDP Management Address type, length, and value (TLV) messages. The Management Address TLV typically contains the IPv4 or IPv6 management addresses of the local system. Only out-of-band management addresses must be used for the management-address. Other remote managers can use this address to obtain information related to the local device.

The chapter describes how to prevent loop situation.

## 8-1 Property

This page is used to configure the loop prevention.

### Web Interface

To configure the loop prevention in the web interface:

1. Click Loop Prevention -> Property.
2. Specify the parameter you want to configure.
3. Click Apply.

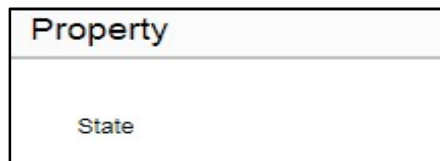


Figure 8-1: Property

### Parameter description:

- **State**  
To enable/disable loop prevention function.

## 8-2 Status

This page is used to display the loop status of ports.

### Web Interface

To view the loop status in the web interface, click Loop Prevention -> Status.

Status	
Port	▲
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	

Figure 8-2: Status

This section shows you to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

### 9-1 IP Filter

This page is used to configure the IP filter function.

#### Web Interface

To configure the IP filter function the web interface:

1. Click Security -> IP Filter.
2. Specify the parameter you want to configure.
3. Click Apply.



Figure 9-1.0: IP Filter

#### Add IP Filter

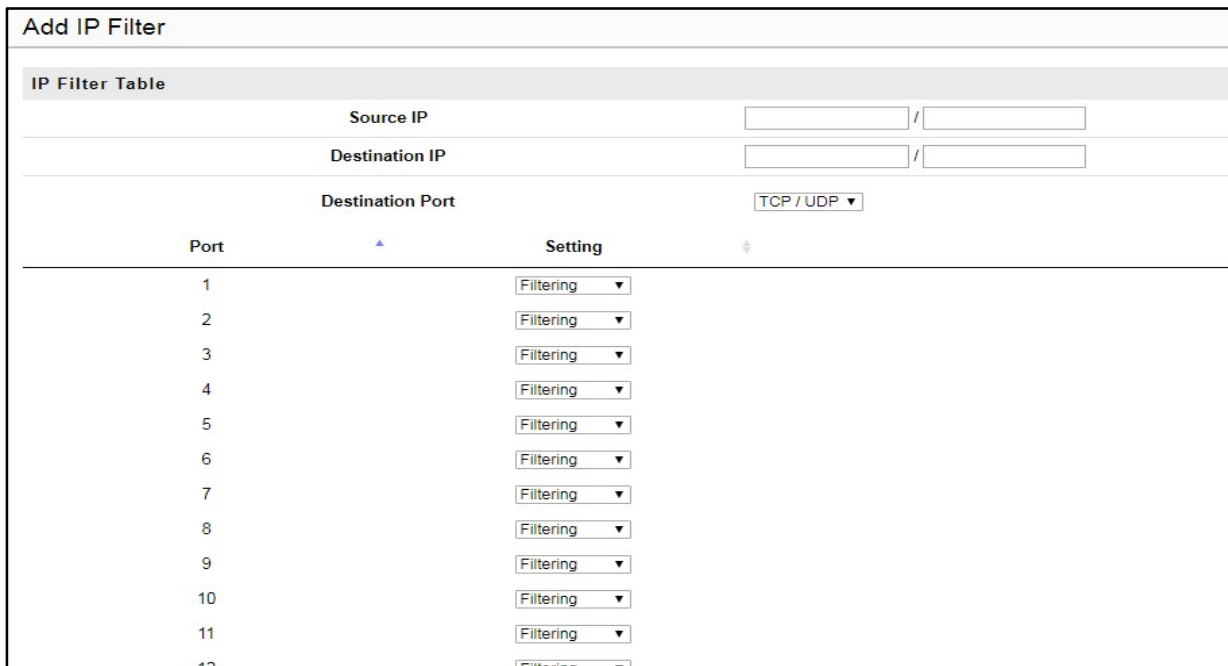


Figure 9-1.1: Add IP Filter



**Parameter Description:**

- **Source IP**  
The source IP address.
- **Destination IP**  
The destination IP address.
- **Destination Port**  
The destination Port.
- **Port**  
Range from 1 to 65535.
- **Setting**  
To filter or not filter.

**Edit IP Filter**

IP Filter

---

**IP Filter Table**  
Showing All entries  
Showing 1 to 1 of 1 entries

Source IP		Destination IP	
Address	Mask	Address	Mask
192.168.1.100	255.255.255.255	192.168.1.110	255.255.255.255

---

Edit IP Filter

**IP Filter Table**

Source IP:  /

Destination IP:  /

Destination Port:

Port	Setting
1	<input type="text" value="Filtering"/>
2	<input type="text" value="Filtering"/>
3	<input type="text" value="Filtering"/>
4	<input type="text" value="Filtering"/>
5	<input type="text" value="Filtering"/>
6	<input type="text" value="Filtering"/>
7	<input type="text" value="Filtering"/>
8	<input type="text" value="Filtering"/>
9	<input type="text" value="Filtering"/>
10	<input type="text" value="Filtering"/>
11	<input type="text" value="Filtering"/>
12	<input type="text" value="Filtering"/>
13	<input type="text" value="Filtering"/>
14	<input type="text" value="Filtering"/>
15	<input type="text" value="Filtering"/>
16	<input type="text" value="Filtering"/>
17	<input type="text" value="Filtering"/>

**Figure 9-13.: Edit IP Filter**

**Parameter Description:**

- **Source IP**  
The source IP address.
- **Destination IP**  
The destination IP address.

- **Destination Port**  
The destination Port.
- **Port**  
Range from 1 to 65535.
- **Setting**  
To filter or not filter.

## 9-2 Port Isolation

This page is used to configure the Port Isolation function.

### Web Interface

To configure the port isolation in the web interface:

1. Click Security -> Port Isolation.
2. Specify the parameter you want to configure.
3. Click Apply.

Port Isolation	
Group Index	1 ▼
Port	*
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	

Figure 9-2: Port Isolation

### Parameter Description:

- **Group Index**

Select which group belongs to.

- **Port**

The normal port of the device.

- **Setting**

Select to be member or not.

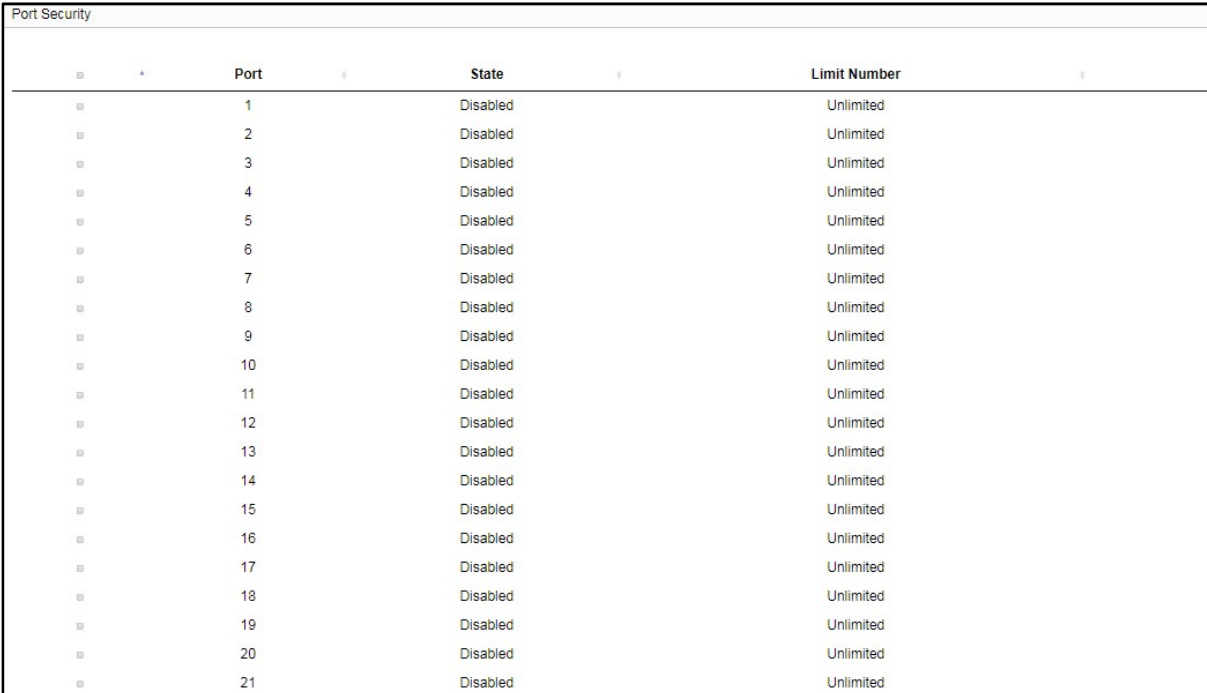
## 9-3 Port Security

This page is used to configure the Port Security function.

### Web Interface

To configure the port security in the web interface:

1. Click Security -> Port Security.
2. Specify the parameter you want to configure.
3. Click Apply.



Port	State	Limit Number
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited
9	Disabled	Unlimited
10	Disabled	Unlimited
11	Disabled	Unlimited
12	Disabled	Unlimited
13	Disabled	Unlimited
14	Disabled	Unlimited
15	Disabled	Unlimited
16	Disabled	Unlimited
17	Disabled	Unlimited
18	Disabled	Unlimited
19	Disabled	Unlimited
20	Disabled	Unlimited
21	Disabled	Unlimited

Figure 9-3.1: Port Security

### Parameter Description:

- **Port**

The normal port of the device.

- **State**

The state of the function.

- **Limit Number**

The limit number of MAC address.

- **Dynamic MAC**

Dynamic generated MAC address.

- **Static MAC**

Static set MAC address.

- **Edit[Button]**

Click if you want to edit the rule.

Edit Port Security	
Port	09
State	<input checked="" type="checkbox"/> Enable
Static MAC	<input type="text"/>
Limit Number	1

**Figure 9-3.2: Edit Port Security**

**Parameter Description:**

- **Port**

The normal port of the device.

- **State**

To enable/disable the function.

- **Static MAC**

Set static MAC.

- **VLAN**

Range from 1 to 4094.

- **Limit Number**

The number of MAC address to limit.

## 9-4 Storm Control

This page is used to configure the storm control function. A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic broadcast and multicast suppression (or storm control) feature prevents LAN ports from being disrupted by a broadcast, multicast and unicast traffic storm on physical interfaces.

### Web Interface

To configure the storm control function in the web interface:

1. Click Security -> Storm Control.
2. Specify the parameter you want to configure.
3. Click Apply.

Storm Control	
Rate	<input type="text" value="10000"/> Kbps (16 - 1000000, default 10000)
Port	*
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	

Figure 9-4: Storm Control

**Parameter description:**

- **Rate**  
The rate for controlling broadcast, multicast and unicast traffic storm on physical interfaces.
- **Setting**  
To enable/disable the function.

9-5 DoS Attack Prevention

This page is used to configure the DoS Attack Prevention function.

**Web Interface**

To configure the DoS Attack Prevention function in the web interface:

1. Click Security -> DoS Attack Prevention.
2. Specify the parameter you want to configure.
3. Click Apply.

DoS Attack Prevention		
POD	<input checked="" type="checkbox"/> Enable	Land
UDP Blat	<input checked="" type="checkbox"/> Enable	TCP Blat
DMAC = SMAC	<input checked="" type="checkbox"/> Enable	Null Scan Attack
X-Mas Scan Attack	<input checked="" type="checkbox"/> Enable	TCP SYN-FIN Atta
TCP SYN-RST Attack	<input checked="" type="checkbox"/> Enable	ICMP Fragment
TCP-SYN	<input checked="" type="checkbox"/> Enable	TCP Fragment
<input checked="" type="checkbox"/> Enable IPv4		

Figure 9-5.1: DoS Attack Prevention

Port
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Figure 9-5.2: DoS Attack Prevention(Detail)

**Parameter description:**

■ **Port**

The normal port of the device.

- **Setting**

To enable/disable the function.

Quality of Service refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. Quality of Service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Quality of Service is particularly important for the transport of traffic with special requirements. In particular, developers have introduced Voice over IP technology to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter network performance requirements.

## 10-1 Property

This page is used to configure the QoS mode, including FIFO, Port Based and 802.1p /DSCP.

### Web Interface

To configure the QoS mode in the web interface:

1. Click Quality of Service -> Property.
2. Specify the parameter you want to configure.
3. Click Apply.

### Parameter Description:

#### ■ FIFO

Ingress packets are First In First Out.

#### ■ Port Based

This is the default setting. It enables port-based QoS settings. You can then set the traffic priority for a particular port.

#### ■ 802.1p /DSCP

Differentiated Services Code Point (DSCP) is a priority level that prioritizes the network traffic based on the DSCP queue mapping on the DSCP Settings page.



## FIFO

Property
<p style="text-align: center;"><b>Mode</b></p> <ol style="list-style-type: none"><li>1. <b>FIFO:</b> Ingress packets are first in first out</li><li>2. <b>Port Based:</b> Ingress packet has different priority based on which port packet come from</li><li>3. <b>802.1p/DSCP:</b></li></ol>

Figure 10-1.1: FIFO

## Port Based(Strict Priority)

Property					
<p style="text-align: center;"><b>Mode</b></p>					
<p style="text-align: center;"><b>Scheduling</b></p> <ol style="list-style-type: none"><li>1. <b>FIFO:</b> Ingress packets are first in first out</li><li>2. <b>Port Based:</b> Ingress packet has different priority based on which port packet come from</li><li>3. <b>802.1p/DSCP:</b> If ingress packet has tag, use 802.1P priority field to assign priority</li></ol> <p><b>Note:</b> If ingress packet has no tag but DSCP field, use DSCP field to assign priority</p> <ol style="list-style-type: none"><li>4. <b>Strict Priority:</b> Low priority queue will not be served until all packets in high priority queue have been processed</li><li>5. <b>WRR:</b> Each queue will be served with round robin method, and served time is based on weight</li></ol>					
Port Priority					
<table border="1"><thead><tr><th>Port</th></tr></thead><tbody><tr><td>1</td></tr><tr><td>2</td></tr><tr><td>3</td></tr><tr><td>4</td></tr></tbody></table>	Port	1	2	3	4
Port					
1					
2					
3					
4					

Figure 10-1.2a: Port Based(Strict Priority)

### Parameter Description:

#### ■ Port

The user port of the switch.

#### ■ Priority

Egress traffic from the highest priority queue is transmitted first. The traffic from the lower queues is only processed after the traffic from the higher queue has been transmitted. The level includes

Low, Normal, Medium and High.

### Port Based(WRR)

Property	
<b>Mode</b>	<input type="radio"/> FIFO
	<input checked="" type="radio"/> Port Based
	<input type="radio"/> 802.1p / DSCP
<b>Scheduling</b>	<input type="radio"/> Strict Priority
	<input checked="" type="radio"/> WRR
<b>WRR Weight</b>	<input type="text" value="1"/>
	<input type="text" value="2"/>
	<input type="text" value="4"/>
	<input type="text" value="8"/>
<p>1. <b>FIFO:</b> Ingress packets are first in first out</p> <p>2. <b>Port Based:</b> Ingress packet has different priority based on which port packet come from</p> <p>3. <b>802.1p/DSCP:</b> If ingress packet has tag, use 802.1P priority field to assign priority</p> <p><b>Note:</b> If ingress packet has no tag but DSCP field, use DSCP field to assign priority</p> <p>4. <b>Strict Priority:</b> Low priority queue will not be served until all packets in high priority queue have been processed</p> <p>5. <b>WRR:</b> Each queue will be served with round robin method, and served time is based on weight</p>	
<b>Port Priority</b>	

Figure 10-1.2b: Port Based(WRR)

#### Parameter Description:

##### ■ WRR Weight

The number of packets sent is based on the weight value. The higher the value, the more frames sent. Queues are serviced until their quota has been met and then another queue is serviced.

## 802.1p/DSCP(Strict Priority)

Property
Mode
Scheduling
1. FIFO: Ingress packets are first in first out 2. Port Based: Ingress packet has different priority based on which port packet come from 3. 802.1p/DSCP: If ingress packet has tag, use 802.1P priority field to assign priority

Figure 10-1.3a: 802.1p / DSCP(Strict Priority)

### Parameter Description:

#### ■ Strict Priority

Low priority queue will not be served until all packets in high priority queue have been processed.

## 802.1p/DSCP(WRR)

Property
Mode
Scheduling
WRR Weight
1. FIFO: Ingress packets are first in first out 2. Port Based: Ingress packet has different priority based on which port packet

Figure 10-1.3b: 802.1p / DSCP(WRR)

### Parameter Description:

#### ■ WRR Weight

The number of packets sent is based on the weight value. The higher the value, the more frames sent. Queues are serviced until their quota has been met and then another queue is serviced.

## 10-2 TCP/UDP Based CoS

This page is used to configure the Class of Service (CoS) which prioritizes the network traffic based on the CoS queue mapping on the CoS Settings.

### Web Interface

To configure the TCP/UDP Based CoS in the web interface:

1. Click Quality of Service -> TCP/UDP Based CoS.
2. Specify the parameter you want to configure.
3. Click Apply.

Protocol	Priority	Protocol
DNS	FIFO	SMTP
FTP	FIFO	SNMP
HTTP	FIFO	SNTP
HTTPS	FIFO	SSH
IMAP	FIFO	TELNET
NetBIOS	FIFO	TFTP
NEWS	FIFO	
POP3	FIFO	

Custom Protocol

Figure 10-2: TCP/UDP Based CoS

### Parameter Description:

#### ■ Protocol

Including DNS, FTP, HTTP, HTTPS, IMAP, NetBIOS, NEWS, POP3, SMTP, SNMP, SNTP, SSH, TELNET and TFTP.

#### ■ Priority

FIFO, Low, Normal, Medium and High.

#### ■ Custom Protocol

User-defined rule.

#### ■ Port

Range from 1 to 65535.

## 10-3 Rate Limit

This page is used to configure the rate control function.

### Web Interface

To configure the rate limit function in the web interface:

1. Click Quality of Service -> Rate Limit.
2. Select the port you want to configure.(For example: Port 9)
3. Click Edit.

4. Specify the parameters you want to configure.
5. Click Apply.
6. Click Close if you want to return to the previous page.

Rate Limit				
	Port	Ingress		
		State	Rate (Kbps)	State
<input type="checkbox"/>	1	Disabled		Disabled
<input type="checkbox"/>	2	Disabled		Disabled
<input type="checkbox"/>	3	Disabled		Disabled
<input type="checkbox"/>	4	Disabled		Disabled
<input type="checkbox"/>	5	Disabled		Disabled
<input type="checkbox"/>	6	Disabled		Disabled
<input type="checkbox"/>	7	Disabled		Disabled
<input type="checkbox"/>	8	Disabled		Disabled
<input type="checkbox"/>	9	Disabled		Disabled
<input type="checkbox"/>	10	Disabled		Disabled
<input type="checkbox"/>	11	Disabled		Disabled
<input type="checkbox"/>	12	Disabled		Disabled
<input type="checkbox"/>	13	Disabled		Disabled
<input type="checkbox"/>	14	Disabled		Disabled
<input type="checkbox"/>	15	Disabled		Disabled
<input type="checkbox"/>	16	Disabled		Disabled
<input type="checkbox"/>	17	Disabled		Disabled
<input type="checkbox"/>	18	Disabled		Disabled

**Figure 10-3.1: Rate Limit**

Edit Ingress / Egress Rate Control	
Port	09
Ingress	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/>
Egress	<input checked="" type="checkbox"/> Enable <input type="text" value="1000000"/>

**Figure 10-3.2: Edit Rate Limit**

**Parameter Description:**

■ **Ingress**

Ingress is traffic that enters the boundary of a network. Range 16 - 1000000 Kbps.

■ **Egress**

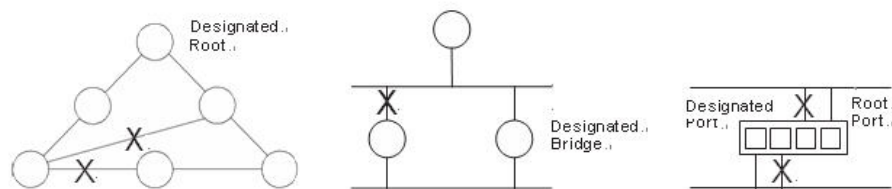
Egress is traffic that exits an entity or a network boundary. Range 16 - 1000000 Kbps.

■ **Enable**

To enable/disable Ingress or Egress function.

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) 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** - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it 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. 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, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



**Figure 11-0: The Spanning Tree Protocol**

Once a stable network topology has been established, 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 (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

## 11-1 State

The section describes that you can select enable spanning tree protocol or not, and you can select what protocol version you want.

### Web Interface

To configure the Spanning Tree Protocol version in the web interface:

1. Click Spanning Tree -> State.
2. To enable/disable the Spanning Tree Protocol.
3. Select the Spanning Tree Protocol version.
4. Click Apply.

Figure 11-1: State

**Parameter Description:**

■ **Multiple Spanning Tree Protocol**

To enable/disable spanning tree protocol.

■ **Force Version**

The Spanning Tree protocol version, including STP, RSTP and MSTP.

11-2 Region Config

The section describes how to configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

**Web Interface**

To configure the Region Config in the web interface:

1. Click Spanning Tree -> Region Config.
2. Specify the Region Name and Revision Level.
3. Click Apply.

Figure 11-2: Region Config

**Parameter Description:**

■ **Region Name**

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

■ **Revision Level**

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

## 11-3 Instance View

The section describes how to configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

The section providing an MST instance table which include information(vlan membership of a MSTI ) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.

### Web Interface

To configure the MSTP Instance in the web interface:

1. Click Spanning Tree -> Instance View.
2. Click Add VLAN.
3. Specify the Instance ID and Vlan Mapping.
4. Click Instance Config, Port Config, Instance Status and Port Status to see the detail.
5. If you want to cancel the setting, click Delete.

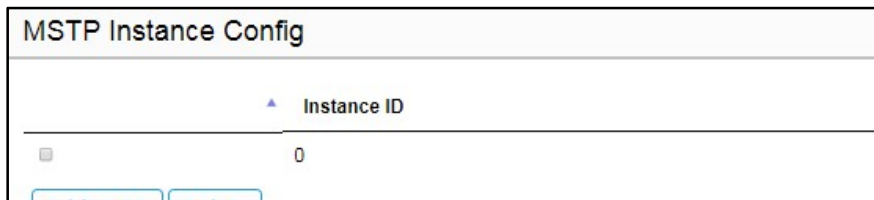


Figure 11-3.0: MSTP Instance Config

### Parameter Description:

#### ■ Instance ID

Every spanning tree instance need to have a unique instance ID within 1~15. Instance 0 (CIST) always exists and cannot be deleted. Additional spanning instances (MSTIs) can be added or deleted. At least one vlan must be provisioned for an MSTI to declare the need for the MSTI to be existent.

#### ■ Corresponding VLANs

1-4094.

Multiple vlans can belong to an MSTI. All vlans that are not provisioned through this will be automatically assigned to Instance 0(CIST).

#### ■ Add VLAN[Button]

To add an MSTI and provide its vlan members for a specific MSTI, you can add up to 15.

#### ■ Delete[Button]

To delete an MSTI.

#### ■ Instance Config[Button]

To provision spanning tree performance parameters per instance.

#### ■ Port Config[Button]

To provision spanning tree performance parameters per instance per port.

#### ■ Instance Status[Button]

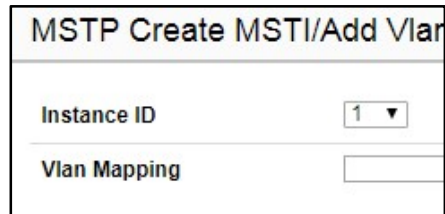
To show the status report of a particular spanning tree instance.



- **Port Status[Button]**

To show the status report of all ports regarding a specific spanning tree instance.

### Add VLAN



MSTP Create MSTI/Add Vlan	
Instance ID	1 ▼
Vlan Mapping	

Figure 11-3.1: Add VLAN

#### Parameter Description:

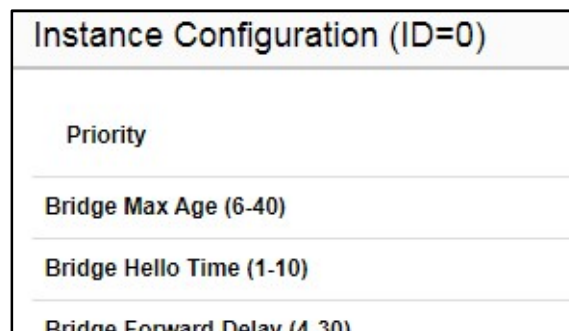
- **Instance ID**

The Range is 1-15

- **Vlan Mapping**

The list of VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx must be between 1 and 4094) VLAN, or a range (xx-yy), each of which must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: 2,5,20-40.

### Instance Config (ID=0)



Instance Configuration (ID=0)
Priority
Bridge Max Age (6-40)
Bridge Hello Time (1-10)
Bridge Forward Delay (4-30)

Figure 11-3.2: Instance Config (ID 0)

#### Parameter Description:

- **Priority**

The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 / 32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 / 61440

- **Bridge MAX. Age**

Range: 6-40 sec

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.

- **Bridge Hello Time**

Range: 1-10 sec

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 10 sec.

■ **Bridge Forward Delay**

Range: 4-30 sec

The same definition as in the RSTP protocol. The forward delay is the time that is spent in the listening and learning state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.

■ **MAX. Hops**

Range: 1-40 sec

It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decreased by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root)

**Port Config (ID=0)**

Port	STP Enable	Path Cost		Priority
1	<input checked="" type="checkbox"/>	Auto	0	128
2	<input checked="" type="checkbox"/>	Auto	0	128
3	<input checked="" type="checkbox"/>	Auto	0	128
4	<input checked="" type="checkbox"/>	Auto	0	128
5	<input checked="" type="checkbox"/>	Auto	0	128
6	<input checked="" type="checkbox"/>	Auto	0	128
7	<input checked="" type="checkbox"/>	Auto	0	128
8	<input checked="" type="checkbox"/>	Auto	0	128
9	<input checked="" type="checkbox"/>	Auto	0	128
10	<input checked="" type="checkbox"/>	Auto	0	128
11	<input checked="" type="checkbox"/>	Auto	0	128
12	<input checked="" type="checkbox"/>	Auto	0	128
13	<input checked="" type="checkbox"/>	Auto	0	128
14	<input checked="" type="checkbox"/>	Auto	0	128
15	<input checked="" type="checkbox"/>	Auto	0	128
16	<input checked="" type="checkbox"/>	Auto	0	128
17	<input checked="" type="checkbox"/>	Auto	0	128
18	<input checked="" type="checkbox"/>	Auto	0	128
19	<input checked="" type="checkbox"/>	Auto	0	128

Figure 11-3.3: Port Config (ID 0)

**Parameter Description:**

■ **Port**

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

■ **Path Cost**

Range: 0-200000000

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

■ **Priority**

0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

- **Admin Edge**  
Yes / No  
The same definition as in the RSTP specification for the CIST ports.
- **Admin P2P**  
Auto / True / False  
The same definition as in the RSTP specification for the CIST ports.
- **MCheck**  
The same definition as in the RSTP specification for the CIST ports.

### Instance Status (ID=0)

Instance Status (ID=0)
<div style="display: flex; gap: 10px;"> <span>Back</span> <span>Refresh</span> </div>
<b>MSTP State</b>
<b>Force Version</b>
<b>Bridge Max Age</b>
<b>Bridge Forward Delay</b>
<b>Bridge Max Hops</b>
<b>Instance Priority</b>
<b>Bridge Mac Address</b>
<b>CIST ROOT PRIORITY</b>
<b>CIST ROOT MAC</b>
<b>CIST EXTERNAL ROOT PATH COST</b>

Figure 11-3.4: Instance Status (ID 0)

#### Parameter Description:

- **MSTP State**  
MSTP protocol is Enable or Disable.
- **Force Version**  
It shows the current spanning tree protocol version configured.
- **Bridge Max Age**  
It shows the Max Age setting of the bridge itself.
- **Bridge Forward Delay**  
It shows the Forward Delay setting of the bridge itself.
- **Bridge Max Hops**  
It shows the Max Hops setting of the bridge itself.
- **Instance Priority**  
Spanning tree priority value for a specific tree instance(CIST or MSTI)

- **Bridge Mac Address**  
The Mac Address of the bridge itself.
- **CIST ROOT PRIORITY**  
Spanning tree priority value of the CIST root bridge
- **CIST ROOT MAC**  
Mac Address of the CIST root bridge
- **CIST EXTERNAL ROOT PATH COST**  
Root path cost value from the point of view of the bridge's MST region.
- **CIST ROOT PORT ID**  
The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.
- **CIST REGIONAL ROOT PRIORITY**  
Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST(Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST(Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.
- **CIST REGIONAL ROOT MAC**  
Mac Address of the CIST regional root bridge.
- **CIST INTERNAL ROOT PATH COST**  
Root path cost value from the point of view of the bridges inside the IST.
- **CIST CURRENT MAX AGE**  
Max Age of the CIST Root bridge.
- **CIST CURRENT FORWARD DELAY**  
Forward Delay of the CIST Root bridge.

## Port Status (ID=0)

Port Status (ID=0)				
<input type="button" value="Back"/> <input type="button" value="Refresh"/>				
Port No	Status	Role	Path Cost	Priority
1	Disabled	Disabled	20000	128
2	Disabled	Disabled	20000	128
3	Disabled	Disabled	20000	128
4	Disabled	Disabled	20000	128
5	Disabled	Disabled	20000	128
6	Disabled	Disabled	20000	128
7	Disabled	Disabled	20000	128
8	Disabled	Disabled	20000	128
9	Disabled	Disabled	20000	128
10	Disabled	Disabled	20000	128
11	Disabled	Disabled	20000	128
12	Disabled	Disabled	20000	128
13	Disabled	Disabled	20000	128
14	Disabled	Disabled	20000	128
15	Disabled	Disabled	20000	128
16	Disabled	Disabled	20000	128
17	Disabled	Disabled	20000	128

Figure 11-3.5: Port Status (ID 0)

### Parameter Description:

#### ■ Port No

The port number to which the configuration applies.

#### ■ Status

The forwarding status. Same definition as of the RSTP specification.

Possible values are "FORWARDING" , "LEARNING" , "DISCARDING"

#### ■ Role

The role that a port plays in the spanning tree topology.

Possible values are "disable"(disable port) , "alternate"(alternate port) , "backup"(backup port) , "ROOT"(root port) , "DSGN"(designated port) , "MSTR"(master port). The last 3 are possible port roles for a port to transit to FORWARDING state

#### ■ Path Cost

Display currently resolved port path cost value for each port in a particular spanning tree instance.

#### ■ Priority

Display port priority value for each port in a particular spanning tree instance.

#### ■ Hello

Per port Hello Time display. It takes the following form:

Current Hello Time/Hello Time Setting

#### ■ Oper. Edge

Whether or not a port is an Edge Port in reality.

#### ■ Oper. P2P

Whether or not a port is a Point-to-Point Port in reality.

The section describes how to configure and display the DHCP Snooping parameters of the switch. The DHCP Snooping can prevent attackers from adding their own DHCP servers to the network.

## 12-1 DHCP Server

This page is used to configure the DHCP Server, including State, Start IP/End IP addresses and Client Lease Time. DHCP Server will allocate these IP addresses to DHCP clients. And deliver configuration parameters to DHCP clients.

### Web Interface

To configure the DHCP Server in the web interface:

1. Click DHCP -> DHCP Server.
2. Specify the parameter you want to configure.
3. Click Apply.

DHCP Server Settings	
<b>DHCP Server Settings</b>	
State	Disable
Start IP Address	192.168.1
End IP Address	192.168.1

Figure 12-1: DHCP Server

### Parameter description:

#### ■ State

To enable/disable DHCP Server function.

#### ■ Start IP Address and End IP Address

Define the IP range. The Start IP Address must be smaller than or equal to the End IP Address.

#### ■ Client Lease Time

Range: 1 - 14400000, 0: infinite

Display the lease time of the pool.

This chapter provides a set of basic system diagnosis, including Mirroring, Ping and LAN Cable Diagnostics.

### 13-1 Mirroring

This page is used to configure the ports' mirror function. You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

#### **Web Interface**

To configure port mirroring in the web interface:

1. Click Diagnostics -> Mirroring.
2. Click the Enable checkbox.
3. Select Monitor Destination Port. (Mirror Port)
4. Specify the state of Monitor Source Port.
5. Click Apply.

Mirroring

---

**State**  Enable

---

**Monitor Destination Port**  ▼

---

**Monitor Source Port Configuration**

	Port
	1
	2
	3
	4
	5
	6
	7
	8
	9
	10
	11
	12
	13
	14
	15
	16
	17
	18

Figure 13-1: Mirroring

**Parameter Description:**

- **State**  
To enable/disable port mirroring function.
- **Monitor Destination Port**  
Port to output the mirrored traffic. Also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port.
- **Monitor Source Port State**  
To enable/disable source port mirroring function.
  - Disabled : neither frames transmitted nor frames received are mirrored.
  - Enabled : Frames received and frames transmitted are mirrored on the mirror port.

13-2 Ping

This section allows you to issue ICMP Echo packets to troubleshoot Ipv4 connectivity issues.

**Web Interface**

To configure a PING in the web interface:

1. Click Diagnostics -> Ping.



2. Specify IP Address and Ping Count..
3. Click Ping to start.
4. Click Stop to stop.

### Ping

---

IP Address

---

Count

### Ping Result

Packet Status	
Status	N/A
Transmit Packet	0
Receive Packet	0
Packet Lost	0%

Figure 13-2: Ping

**Parameter Description:**

■ **IP Address**

To specify the target IP Address of the Ping.

■ **Count**

Specify the numbers of each ICMP ping request. Values range from 1 to 65535 times.

■ **Status**

Ping status

- Ping in progress: Ping does not reach the count values and be in progress.
- Ping failed (timeout): Ping failed due to timeout.
- Ping failed (unknown host): Ping failed due to unknown host.
- Ping aborted: Press the Stop button before ping is done.
- Success: Ping success.

■ **Transmit Packet**

Numbers ICMP ping requests have been sent.

■ **Receive Packet**

Numbers ICMP ping replies have been received.

■ **Packet Lost**

Numbers of percentage ICMP ping have been lost.

■ **Min**

Minimum time of the round trip time.

■ **Max**

Maximum time of the round trip time.

■ **Average**

Average time of the round trip time.

## 13-3 LAN Cable Diagnostics

This section shows how to run LAN Cable Diagnostics for copper ports.

### Web Interface

To configure a LAN Cable Diagnostics Configuration in the web interface:

1. Click Diagnostics -> LAN Cable Diagnostics.
2. Specify Port which you want to check.
3. Click Cable Test.

**LAN Cable Test**

**Note:**

1. **Cable Testing** could be executed on the port which is administratively enabled
2. On the link-up port, **Cable Testing** might have the slight effects against the network performance

[Cable Test](#)

**Cable Test Result**

Cable Status

Figure 13-3: LAN Cable Diagnostics

### **Parameter Description:**

#### ■ **Port**

The port where you are requesting Cable Diagnostics.

#### ■ **Result**

The status of copper test. It include:

- OK: Correctly terminated pair
- Short Cable: A short circuit was detected on the twisted pair.
- Open Cable: Opening pair. One scenario is the cable doesn't plug to the link partner.
- Impedance Mismatch : The normal impedance should be 100Ω, impedance mismatch is detected if the impedance measured is not in the range 70Ω~130Ω.
- Line Drive: The high impedance is detected. One scenario is the cable plug to a power down link partner.

#### ■ **Length**

Distance in meter from the port to the location on the cable where the fault was discovered.

This chapter provides the maintenance of the system. These includes Configuration Import/Export, Restart Device, Reset to default and Firmware Upgrade.

## 14-1 Configuration

### 14-1.1 Import / Export

This section describes how to import or export the Switch Configuration for maintenance needs. Any current configuration files will be exported as text format, and the configuration files on the switch can be backed up and saved on the station running the web browser.

It is possible to transfer any of the files on the switch to the web browser. Select the configuration file for uploading, as the file must be backup before uploading.

#### Web Interface

To import or export the current device's configuration in the web interface:

1. Click Maintenance -> Configuration -> Import / Export.
2. For upload configuration, select the file you want to upload and click Upload.
3. For backup, click Backup to save the configuration file.

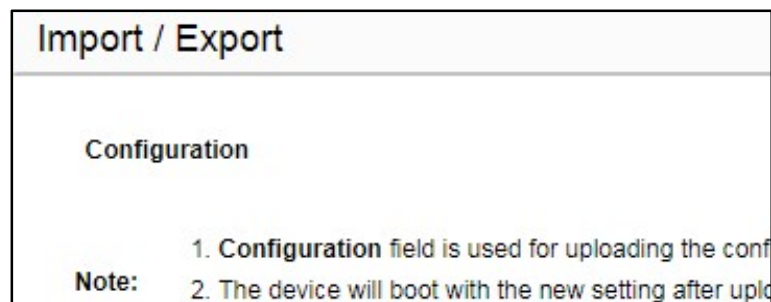


Figure 14-1.1: Import / Export

#### Parameter Description:

- **Upload[Button]**  
Set port enable/disable.
- **Backup[Button]**  
Set port enable/disable.

## 14-2 Restart Device

This section describes how to restart the device for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

### Web Interface

To Restart Device in the web interface:

1. Click Maintenance -> Restart Device.
2. Click Restart Device.



Figure 14-2: Restart Device

### Parameter Description:

#### ■ Restart Device[Button]

To restart device.

## 14-3 Reset Default

This section describes how to restore the Switch configuration to factory default value.

### Web Interface

To restore to factory default value in the web interface:

1. Click Maintenance -> Reset Default.
2. Click Reset.



Figure 14-3: Reset Default

### Parameter Description:

#### ■ Reset[Button]

To reset the device to factory default value.

## 14-4 Firmware Upgrade

To display firmware upgrade page, click Maintenance > Firmware Upgrade. This page allows user to upgrade firmware image through HTTP.

## Web Interface

To update firmware of the device in the web interface:

1. Click Maintenance -> Firmware Upgrade.
2. Choose the firmware you want to upgrade.
3. Click Upgrade.

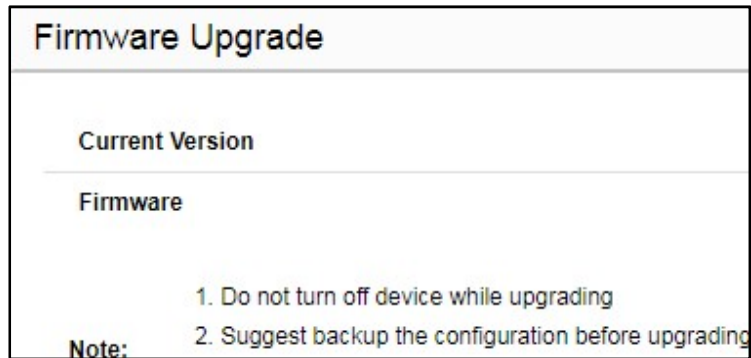


Figure 14-4: Firmware Upgrade

### Parameter Description:

- **Current Version**  
The firmware version which currently runs on this device.
- **Upgrade[Button]**  
Click to perform firmware upgrading.  
Don't turn off the device during the firmware upgrading.