. . . connecting your business

LANCOM ES-2126+
LANCOM ES-2126P+

LANCOM
Systems

LANCOM ES-2126+
LANCOM ES-2126P+

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Deutschland

www.lancom-systems.com

Wuerselen, August 2010

EN

Preface

Thank you for your confidence in us!

The LANCOM switch models LANCOM ES-2126+ and LANCOM ES-2126P+ are ideally suited to small, medium-sized and performance networks in business environments.

The LANCOM ES-2126+ switch features 24 Fast-Ethernet and two combo ports (TP/SFP), it integrates perfectly into LANCOM's Advanced Routing und Forwarding and it supports up to 256 active VLANs. It uses bandwidth control to prioritize the data traffic according to predefined criteria (e.g. voice data or certain ports).

Furthermore the LANCOM ES-2126P+ switch supports Power-over-Ethernet for connected network devices. The overall power output of 185 Watts from the PoE supply can be flexibly divided between the ports.

The LANCOM switch can be managed with the clearly structured Webconfig and is supported by the LANCOM Management Tools (LANconfig and LANmonitor).

Model variants

This documentation is intended for LANCOM switch users. The following models are available:

- The LANCOM ES-2126+ without PoE support.
- The LANCOM ES-2126P+ with PoE support.

Model restrictions

Passages applying only to certain models are identified either in the text itself or by a comment in the margin.

Otherwise the documentation refers to all models collectively as the LANCOM switch series.

This documentation was created by …

… several members of our staff from a variety of departments in order to ensure you the best possible support when using your LANCOM product.

Should you find any errors, or if you would like to suggest improvements, please do not hesitate to send an e-mail directly to:
info@lancom.de

Our online services www.lancom-systems.com are available to you around the clock if you have any questions on the content in this

manual, or if you require any further support. The area 'Support' will help you with many answers to frequently asked questions (FAQs). Furthermore, the knowledgebase offers you a large reserve of information. The latest drivers, firmware, utilities and documentation are constantly available for download.

In addition, LANCOM Support is available. For telephone numbers and contact addresses for LANCOM Support, please refer to the enclosed leaflet or the LANCOM Systems Web site.

EN

Information symbols	
	Very important instructions. Failure to observe these may result in damage.
	Important instruction that should be observed.
	Additional information that may be helpful but is not essential.

Contents

EN

EN

EN

EN

1 Introduction

The LANCOM switch models LANCOM ES-2126+ and LANCOM ES-2126P+ are managed layer-2 switches with 24 Fast Ethernet ports (for twisted pair cable – TP) and two Gigabit dual media ports with TP/SFP, which meets the IEEE 802.3/u/x/z Gigabit, Fast Ethernet and Ethernet specifications

The switch can be managed through RS-232 serial port via directly connection, or through Ethernet port using Telnet or WEBconfig. Additionally, the switches can be managed via SSH (Secure Shell) or WEBconfig with SSL-encryption. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity in a friendly way.

The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON and IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and office application.

Additionally, the switches support TACACS+, a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for certain authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions.

This LANCOM ES-2126P+ switch also complies with IEEE 802.3af, its advanced auto-sensing algorithm enables providing power devices (PD) discovery, classification, current limit, and other necessary functions. It also supports high safety with short circuit protection and power-out auto-detection to PD.

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

1.1 Key Features in the Device

- QoS:

  Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedule using Weighted Round

EN

Robin (WRR). User-defined weight classification of packet priority can be based on either VLAN tag on packets or user-defined port priority.

- Spanning Tree:

  Support IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

- VLAN:

  Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 256 active VLANs and VLAN ID 1~4094.

- Port Trunking:

  Support static port trunking and port trunking with IEEE 802.3ad LACP.

- Bandwidth Control:

  Support ingress and egress per port bandwidth control.

- Port Security:

  Support allowed, denied forwarding and port security with MAC address.

- SNMP/RMON:

  SNMP agent and RMON MIB. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

  RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

  The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643), Ethernet MIB (RFC 1643) and so on.

- TACACS+

  Tacacs+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for certain authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

- IGMP Snooping:

  Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the

member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

EN

1.2 Just what can your LANCOM switch do?

	LANCOM ES-2126+	LANCOM ES-2126P+
Hardware		
Supports 24-port 10/100M TP ports with Nway and auto MDIX function	✔	✔
2 Gigabit dual media ports(TP/SFP)	✔	✔
On-line pluggable fiber transceiver modules	✔	✔
256KB packet buffer and 128KB control memory	✔	✔
Maximal packet length can be up to 1536 bytes	✔	✔
Full-duplex flow control (IEEE802.3x) and half-duplex backpressure	✔	✔
Ssatus LEDs		
System: Power, CPURUN, ACT / FDX / SPD(LEDSET)	✔	✔
TP Port 1-24: LINK/ACT, FDX, SPD	✔	✔
SFP-Ports 25,26: LINK/ACT, FDX, SPD	✔	✔
PoE support		
PoE with 48VDC power through RJ-45 pin 1, 2, 3, 6.		✔
Powered Device(PD) auto detection and classification.		✔
PoE-PSE status and activity LED indicator.		✔
Management		
Concisely the status of port and easily port configuration	✔	✔
Per port traffic monitoring counters	✔	✔
Port mirror function	✔	✔
Static trunk function	✔	✔
802.1Q VLAN with 256 entries.	✔	✔
DHCP Broadcasting Suppression to avoid network suspended or crashed	✔	✔
Trap event while monitored events happened	✔	✔
Default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI	✔	✔

EN

	LANCOM ES-2126+	LANCOM ES-2126P+
5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority.	✔	✔
WEBconfig and CLI management over telnet	✔	✔
WEBconfig with optional SSL-encryption and CLI management over SSH	✔	✔
Rapid Spanning Tree (802.1w RSTP)	✔	✔
802.1x port security on a VLAN	✔	✔
SNMP access can be disabled and prevent from illegal SNMP access	✔	✔
Ingress, Non-unicast and Egress Bandwidth rating management	✔	✔
The trap event and alarm message can be transferred via e-mail and mobile phone short message	✔	✔
Diagnostics to let administrator knowing the hardware status	✔	✔
External loopback test to check if the link is ok	✔	✔
TFTP for firmware upgrade, system log upload and config file import/export	✔	✔
Remote boot the device through user interface and SNMP	✔	✔
Network time synchronization and daylight saving	✔	✔
TACACS+ for authorization, authentication and accounting (AAA)	✔	✔
120 event log records in the main memory and display on the local console	✔	✔
Options		
LANCOM SFP Transceiver: Item no. 61556 LANCOM SFP-SX-LC1 Item no. 61557 LANCOM SFP-LX-LC1	✔	✔

2 Installation

This chapter will assist you to quickly install hardware and software. First, check the package contents and system requirements. The device can be installed and configured quickly and easily if all prerequisites are fulfilled.

2.1 Package content

EN

Before beginning with the installation, please check that nothing is missing from your package. Along with the LANCOM switch the box should contain the following accessories:

	LANCOM ES-2126+	LANCOM ES-2126P+
Power cord	✔	✔
19'' adapter (2 pieces) and mounting materials	✔	✔
Serial configuration cable	✔	✔
LANCOM CD	✔	✔
Printed documentation	✔	✔

Should anything be missing, please take up immediate contact to your dealer or to the address on the delivery note supplied with your device.

2.2 System requirements

Computers that connect to a LANCOM must meet the following minimum requirements:

- Operating system with TCP/IP support, such as Windows, Linux, BSD Unix, Apple Mac OS, OS/2.
- Access to the LAN via the TCP/IP protocol.
- Browser for Web-based configuration.

The LANtools also require a Windows operating system. A web browser under any operating system provides access to WEBconfig.

2.3 Status displays and interfaces

Meanings of the LEDs

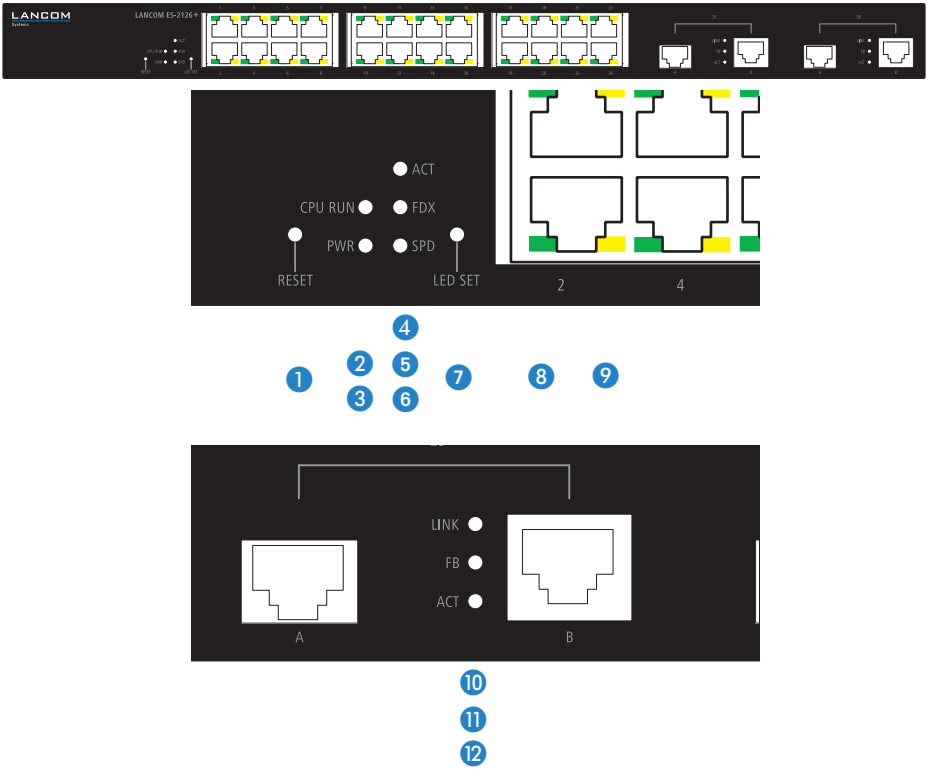
The following section describes the meaning of the LEDs.

Please be aware that LANmonitor shows far more information about the status of the LANCOM switch than the LEDs '→ Monitoring the LANCOM switch with LANmonitor'.

EN

2.3.1 LEDs and buttons on the LANCOM ES-2126+

Located on the front of the device are light-emitting diodes (LEDs) that provide information on device status, and also two buttons.



1 Reset — Button to re-start the system.

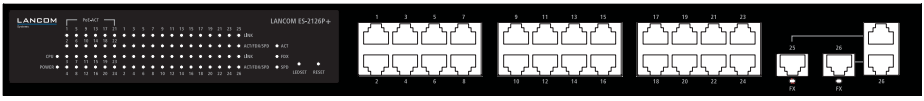
2 CPU RUN — Blinks green if the CPU is running without problem.

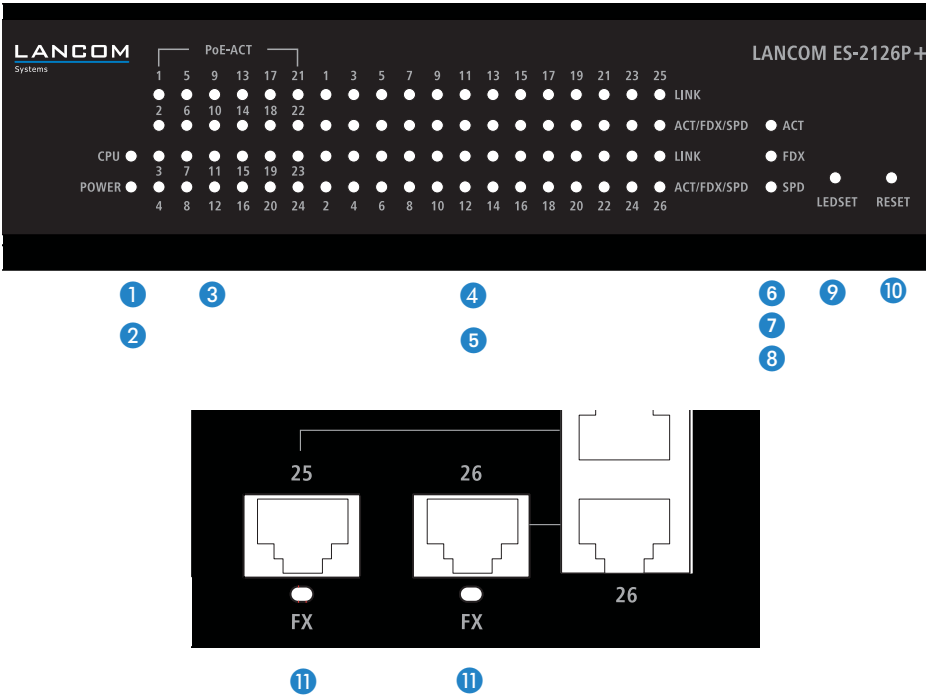
EN

3 PWR	Power LED: Constant green when power is supplied to the device.
4 ACT	Constant green when the LED mode is set to "Active".
5 FDX	Constant green when the LED mode is set to "Full-Duplex".
6 SPD	Constant green when the LED mode is set to "Speed".
7 LEDSET	Button to switch the LEDmode between -"Active", "Full-Duplex" and "Speed".
8 LINK Port 1 to 24	Constant green when the network connection is established to the connected device. Off if no network connection can be established to the connected device.
9 ACT/FDX/SPD Port 1 to 24	This LED displays the following information depending on the selected LED status: ■ LED mode "Active": Blinks yellow during data transfer. ■ LED mode "Full-Duplex": Constant green when full-duplex mode is active for this port; blinks yellow in case of collisions. ■ LED mode "Speed": Constant yellow when the 100 Mbps mode is active. Off when the 10 Mbps mode is active.
10 Link Port 25 and 26	Constant green when the network connection is established to the connected device. Off if no network connection can be established to the connected device.
11 FB Port 25 and 26	Constant green when the optical port is active. Off when the TP port is active
12 ACT Port 25 and 26	This LED displays the following information depending on the selected LED status: ■ LED mode "Active": Blinks yellow during data transfer. ■ LED mode "Full-Duplex": Constant green when full-duplex mode is active for this port; blinks yellow in case of collisions. ■ LED mode "Speed": Constant green when the Gbps mode is active. Off when the 10 Mbps or 100 Mbps mode is active.

2.3.2 LEDs and buttons on the LANCOM ES-2126P+

Located on the front of the device are light-emitting diodes (LEDs) that provide information on device status, and also two buttons.





EN

1	CPU RUN	Blinks green if the CPU is running without problem.
2	PWR	Power LED: Constant green when power is supplied to the device.
3	PoE-ACT	Constant green when the device connected to this port is powered via PoE.
4	LINK Port 1 to 24	Constant green when the network connection is established to the connected device. Off if no network connection can be established to the connected device.
5	ACT/FDX/SPD Port 1 to 24	This LED displays the following information depending on the selected LED status: ■ LED mode "Active": Blinks yellow during data transfer. ■ LED mode "Full-Duplex": Constant green when full-duplex mode is active for this port; blinks yellow in case of collisions. ■ LED mode "Speed": Constant yellow when the 100 Mbps mode is active. Off when the 10 Mbps mode is active.
6	ACT	Constant green when the LED mode is set to "Active".

7	FDX	Constant green when the LED mode is set to "Full-Duplex".
8	SPD	Constant green when the LED mode is set to "Speed".
9	LEDSET	Button to switch the LEDmode between -"Active", "Full-Duplex" and "Speed".
10	Reset	Button to re-start the system.
11	FX Port 25 and 26	Constant green when the optical port is active. Off when the TP port is active.

2.3.3 Connectors on the LANCOM ES-2126+ and LANCOM ES-2126P+

The following connectors are located on the rear of the device.

1 2

1. Connector for serial configuration cable for direct configuration.
2. Connector for IEC power cable for power supply.

2.4 Mounting and connecting up the LANCOM switch

Installating the LANCOM switch involves the following steps:

① **Mounting** – The device is designed for mounting in an available 19" unit in a server cabinet. If necessary fix the rubber pads to the underside of the device to prevent any scratching to other equipment.

Ensure that the device has sufficient ventilation to prevent damage from excessive heat build-up.

② **LAN connection** – Connect the network devices to the ports of the LANCOM switch by means of a suitable twisted-pair cable (TP cable). The connectors automatically detect the avalable data transfer speeds and the pin assignment (autosensing).

Use only standard TP cables of category CAT 5e or better with a maximum length of 100 m to ensure the best possible transfer of data. Cross-over cables can be used thanks to the auto-sensing function.

If optical connections are to be used, additional modules can be purchased as accessories.

③ **Configuration via serial ports** – In order to configure the LANCOM switch directly, connect the serial configuration cable (supplied) to the COM port of the device. Connect the other end of this cable to an available COM port (RS 232) on a PC. Instructions on carrying out a configuration via the serial interface and on enterning relevant parameters via a terminal program are available under →'Starting the Command Line Interface via serial connection' in the following chapter.

④ **Supply power and switch on** – Supply power to the device by means of the IEC power cable.

⑤ **Ready for operation?** – After a brief self-test, the power LED lights up continuously. Green LAN-LINK LEDs show which LAN connectors are being used for a connection.

2.5 Software installation

The following section describes the installation of the Windows-compatible system software LANtools, as supplied.

You may skip this section if you use your LANCOM switch exclusively with computers running operating systems other than Windows.

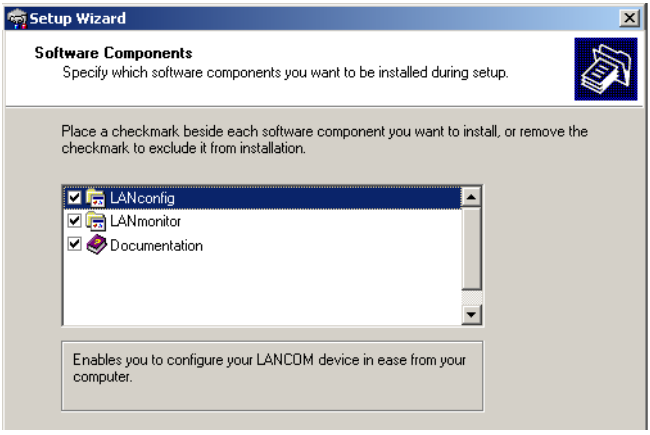
2.5.1 Starting the software setup

Place the product CD into your drive. The setup program will start automatically.

If the setup does not start automatically, run AUTORUN.EXE in the root directory of the LANCOM CD.

EN

In Setup, select **Install software**. The following selection menus will appear on screen:



2.5.2 Which software should I install?

- **LANconfig** is the Windows configuration program for all LANCOM devices. LANconfig searches for all LANCOM devices in your network. You can use this to start the Web-based configuration of a LANCOM switch.
- With **LANmonitor** you can use a Windows computer to monitor all of your LANCOM devices. This program displays all important status information for a LANCOM switch, such as link status or port PoE state.
- With **Documentation** you copy the documentation files onto your PC.

Select the appropriate software options and confirm your choice with **Next**. The software is installed automatically.

3 Configuring and monitoring the LANCOM switch

3.1 Configuration options

There are two different methods of configuring the device.

- By means of a graphical user interface or via a browser (WEBconfig). This option is only available if you have network access to the device's IP address from your computer. You can access WEBconfig via a encrypted connection over SSL as well.

  Instructions for configuring the device with WEBconfig are available in the chapter "Web-based configuration".

- Text-orientated configuration via a console (Command Line Interface – CLI): This method of configuration, which requires a program such as Telnet, SSH, Hyperterminal, or similar, can be conducted over a network connection or with a direct connection via serial interface (RS-232).

  Instructions for configuring the device with CLI are available in the chapter "Command line interface".

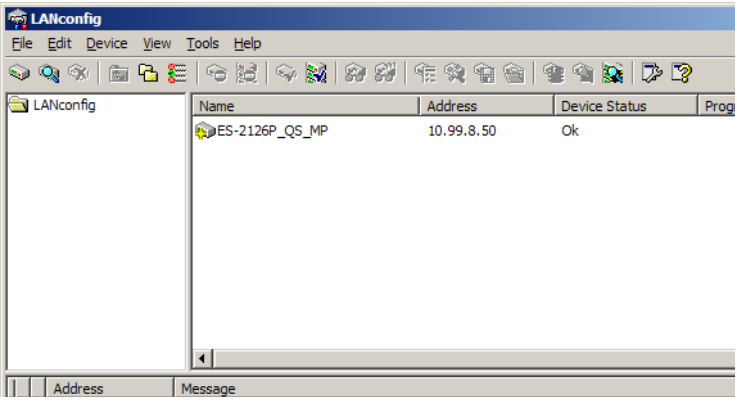
3.1.1 Starting WEBconfig

There are two ways of starting the configuration by browser:

- If you know the device's IP address, simply enter this into the address line in the browser. The factory settings for accessing the device are: User name "admin", password "admin".

EN

- If you do not have the device's IP number, LANconfig can be used to search for it. To start LANconfig click on **Start** ▶ **Programs** ▶ **LANCOM** ▶ **LANconfig**.



LANconfig automatically searches for all available devices in your network. Any available LANCOM devices will be displayed in the list, including the LANCOM switch. Double-click on this entry to start the browser automatically with the correct IP address.

What is the IP address of my LANCOM switch?

The current IP address of the LANCOM switch after being switched on depends on the network constellation.

Networks with DHCP server – In its factory settings, the LANCOM switch is set for auto DHCP mode, meaning that it searches for a DHCP server to assign it an IP address, subnet mask and gateway address. The assigned IP address can only be determined by using the appropriate tools or via the DHCP server. If the DHCP server is a LANCOM device, the IP address of the LANCOM switch can be read out from the DHCP table. If this is the case, the LANCOM switch can be accessed from any network computer that receives its IP address from the same DHCP server.

Network without a DHCP server – If no DHCP server is present in the network, the LANCOM switch automatically adopts the address "172.23.56.250".

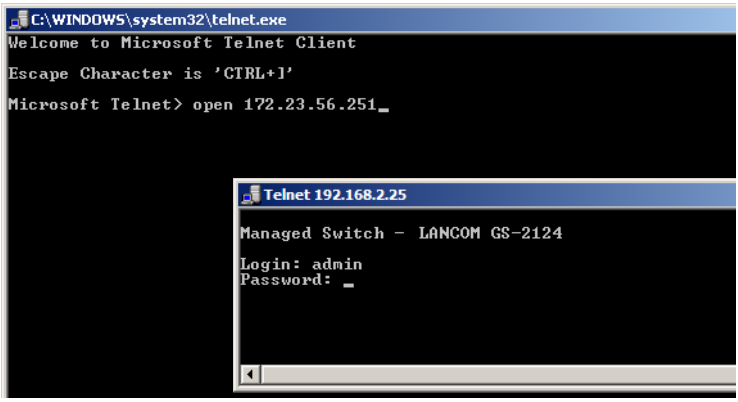
If this is the case, the LANCOM switch can be accessed from any network computer with its IP address set to the address range "172.23.56.x".

EN

3.1.2 Starting the Command Line Interface over the network

If you know the device's IP address (see section above) and the LANCOM switch is accessible from your computer via the network, the you can use the command line interface via the network.

1. To do this, start a console such as Telnet and enter the device's IP address as the target.
2. Log on with user name and password (default: admin, admin).



3.1.3 Starting the Command Line Interface over the serial connection

If you do not know the IP address of the device, you can use the command line interface via a serial connection.

1. Use the serial configuration cable to connect the LANCOM switch to the configuration computer (→"Mounting and connecting up the LANCOM Switch').
2. Start a terminal program on the configuration computer, such as Hyperterminal under Windows. Use the following parameters for the connection:
   - Baud rate: 115200
   - Stop bits: 1
   - Data bits: 8
   - Parity: N
   - Flow control: None

3. Log on with user name and password (default: admin, admin).

3.2 Which configuration does the device use?

The switch supports four different configurations: The start configuration, the current working configuration, the user configuration and the default configuration.

EN

1. Start configuration

   At the system start, the device takes the parameters from the start configuration and copies these to the working configuration. On shipping, the start configuration is the same as the default configuration.

To change the start configuration, the altered parameters have to be saved as the start configuration.

2. Working configuration:

   This is the currently active configuration in the device. It can be changed at any time. All changes to the configuration are saved here. Each time you make changes and press <Apply>, the changes are stored to the working configuration.

The changes to the working configuration are **not** automatically adopted for the start configuration. They have to be saved specifically as the start or user configuration. If you do not save the changes to your working configuration, they will be lost and the previous start configuration will be active when you start the system the next time.

3. User configuration:

   This configuration exists for specific requirements or for making backups. You can save any state of the working configuration as a user configuration and restore this state later or with the function "Restore user configuration".

If the start configuration is defective and the the device is not available via network, you use the serial configuration interface and the Command Line Interface to reload a functional start configuration.

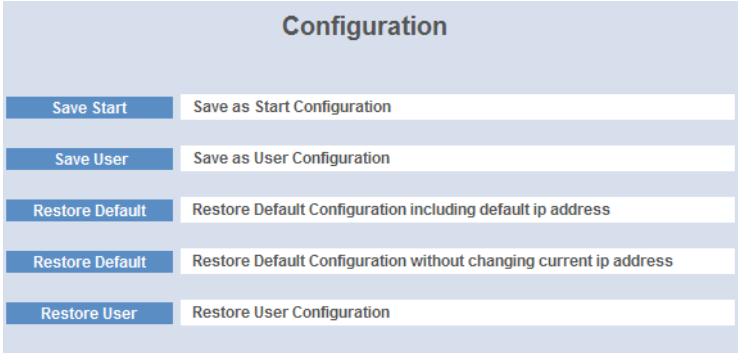
4. Default configuration

This is the default configuration and it cannot be altered. The web user interface has the following options to restore the switch to its default setting.

- With the function "restore default configuration included default IP address" you can reset the switch to the factory default settings (including the administrator´s password and the auto DHCP setting).
- With the function "restore default configuration without changing current IP address" you can reset the switch to the factory default settings, but without changing the IP address. You can access the switch at its last IP address.
- With the serial configuration interface you can reset the switch to the factory default setting, without knowing the current administrator´s password. To do this you have to set up a serial connection to the device as described in →'Start Command Line Interface via serial connection'. In the terminal program, before you enter the username press CTRL+Z, enter "RESET" as the username and the MAC address (without blank characters) as the password.

This action starts the reset process and all settings will be reset to the factory default state, including the administrator´s password and the auto DHCP setting.

3.2.1 Save/Restore



- Save as start configuration

  Here you can save your current configuration to the flash memory as a start configuration.
- Save as user configuration

Here you can save the current configuration to the flash memory as a user configuration.

- Restore default configuration (includes default IP address)

  Here you can reset the switch to its factory settings. The default configuration replaces the start configuration. The device is reset to Auto DHCP and it retrieves its IP address from a DHCP server in the network. If no DHCP server is available, the device takes the IP address "172.23.56.250".

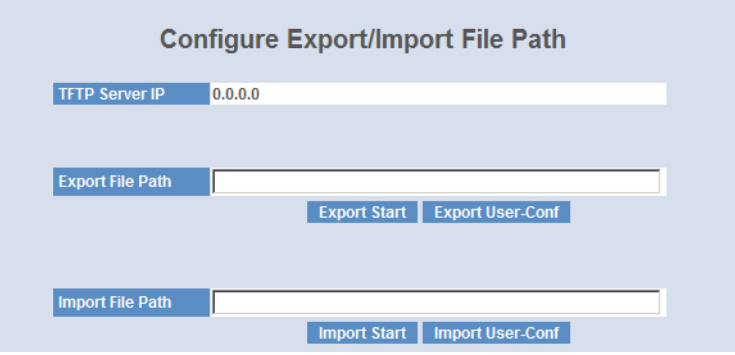
- Restore default configuration (excludes current IP address)

  Here you can reset the switch to its factory settings. The default configuration replaces the start configuration. However, the switch's current IP address as set up by the user is not changed and will NOT be restored to the default value.

- Restore user configuration

  Restore User Configuration function retrieves the previous confirmed working configuration from the flash memory to update the start configuration. After restoring the configuration, the system's start configuration is updated and activated after rebooting.

3.2.2 Config file



- Config file

  With this function you can backup or reload the start and user configuration via TFTP.

- Parameter

- Export file path:

  Export start: You can export the start configuration from the flash memory.

  Export user conf.: You can export the user configuration from the flash memory.

- Import file path:

  Import start: You can import the start configuration to the flash memory here.

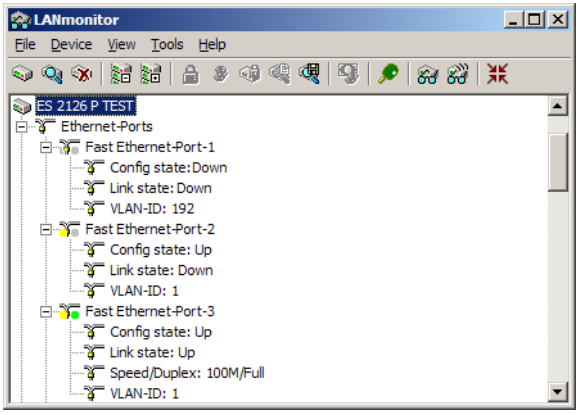
  Import user conf.: You can import the user configuration to the flash memory here.

3.3 Monitoring the LANCOM switch with LANmonitor

The current state of the device and all ports can be monitored using the LEDs on the front panel. With LANmonitor the devices can be observed from any workstation without being able to see the LEDs. Besides the status information provided by the LEDs the LANmonitor provides further important information on the ports.

3.3.1 Ethernet port status

LANmonitor displays the current status of all of the device's Ethernet ports. This includes monitoring of the state as configured by the admin (config state) and the actual state (link state) of the port. Each port is displayed with two colored symbols in LANmonitor:



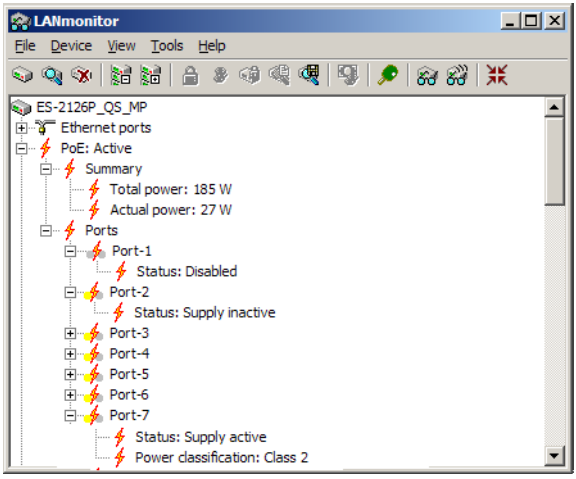
EN

- The left icon shows the config state:
  - Gray: The port is deactivated in the configuration
  - Yellow: The port is activated in the configuration
- The right-hand icon shows the link state:
  - Gray: No active network device is connected to the port
  - Green: A network device is connected to the port and active

Apart from the status, LANmonitor displays the VLAN ID for each port and the detected data rate at active ports connected to active network devices.

3.3.2 Port PoE status

LANmonitor displays the current PoE status of all of the device's ports. This includes the state configured by the admin (PoE enabled or disabled) and the current power feed to connected devices. Each port is displayed with two colored symbols in LANmonitor:



- The left icon shows the PoE configuration:
  - Gray: PoE feed for the port is deactivated in the configuration
  - Yellow: PoE feed for the port is activated in the configuration
- The right-hand icon shows the current power feed.
  - Gray: No PoE-powered device is connected to this port
  - Green: A PoE-powered device is connected to this port and is being fed with power

Along with PoE status, LANmonitor also shows the PoE class as detected for the powered devices. When a Powerded Device (PD) is connected, the Power Source Equipment (PSE) measures the power requirement of the device. Power requirements of the PDs are classified as follows:

PoE class	Use	Power range
0	default	0,44 W - 12.95 W
1	optional	0,44 W - 3.84 W
2	optional	3,84 W - 6.49 W
3	optional	6,49 W - 12.95 W
4	reserved	15,4 W

EN

4 Operation of Web-based Management

This chapter instructs you how to configure and manage the switch through the web user interface it supports, to access and manage the 24 10/100Mbps TP + 2 Gigabit dual media ports with TP/SFP Fiber management Ethernet switch. With this facility, you can easily access and monitor through any one port of the switch all the status of the switch, including MIBs status, each port activity, Spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the managed switch are listed in the table below:

	LANCOM ES-2126+	LANCOM ES-2126P+
IP Adress	172.23.56.250	172.23.56.250
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	172.23.56.254	172.23.56.254
Default DNS-Server	172.23.56.254	172.23.56.254
Username	admin	admin
Password	admin	admin

After the managed switch has been finished configuration in the CLI via the switch's serial interface, you can browse it. For instance, type http://192.168.1.1 in the address row in a browser, it will show the following screen and ask you inputting username and password in order to login and access authentication. The default username and password are both "admin". For the first time to use, please enter the default username and password, then click the <Login> button. The login process now is completed.

Alternatively you can login to the decive using an secure and encrypted connection via HTTPS and the Secure Sockets Layer SSL. The switch already contains the required certificate.

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

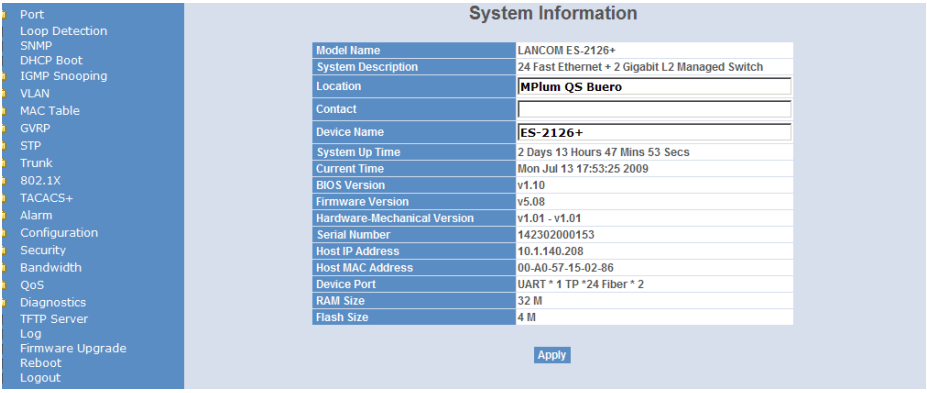
In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator's identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with adminis-

trator's identity, can only monitor the system. For those who have no administrator's identity, can only monitor the system. There are only a maximum of three users able to login simultaneously in the switch.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above or current FireFox and have the resolution 1024x768. The switch supported neutral web browser interface.

4.1 Web Management Home Overview

After you login, the switch shows you the system information. This page is default and tells you the basic information of the system, including "Model Name", "System Description", "Location", "Contact", "Device Name", "System Up Time", "Current Time", "BIOS Version", "Firmware Version", "Hardware-Mechanical Version", "Serial Number", "Host IP Address", "Host MAC Address", "Device Port", "RAM Size" and "Flash Size". With this information, you will know the software version used, MAC address, serial number, how many ports good and so on. This is helpful while malfunctioning.

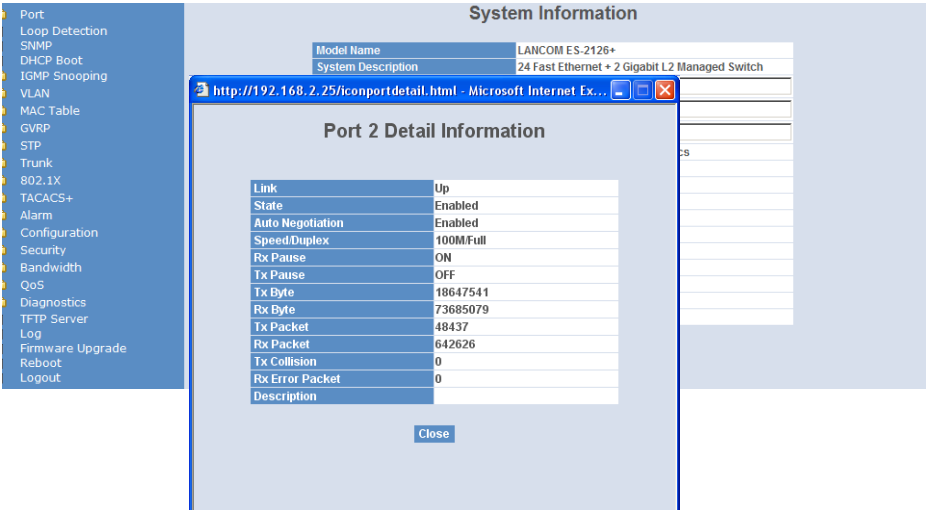


The Information of Page Layout

On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green.

EN

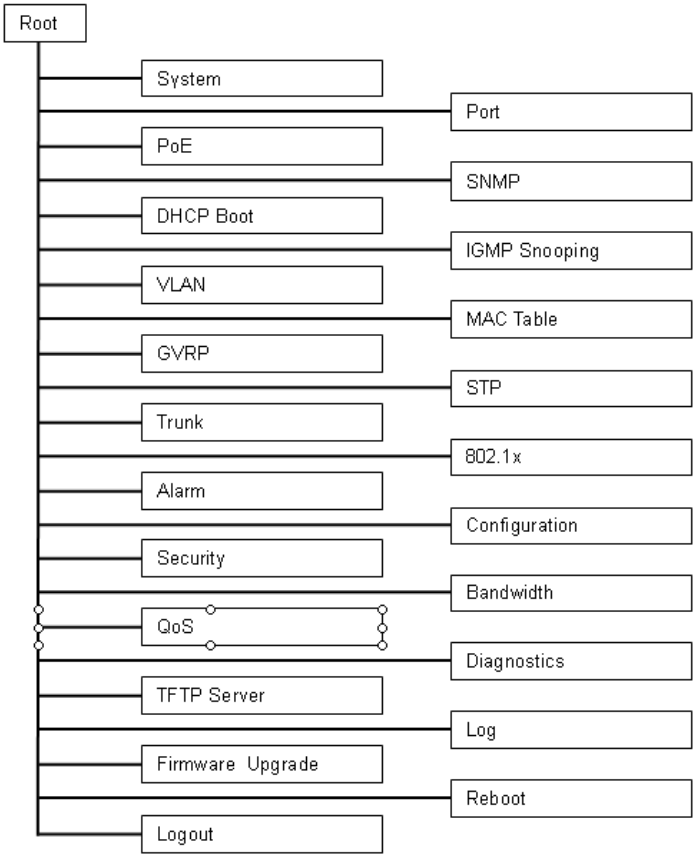
In this device, there are clicking functions on the panel provided for the information of the ports. These are very convenient functions for browsing the information of a single port. When clicking the port on the front panel, an information window for the port will be pop out.



The figure shows the basic information of the clicked port. With this, you'll see the information about the port status, traffic status and bandwidth rating for egress and ingress respectively.

On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON.

On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed. The following list is the full function tree for web user interface.



4.2 System

4.2.1 System Information

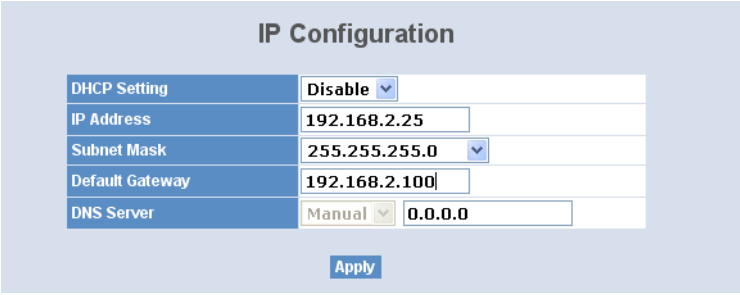
- Function name: System Information
- Function Description: Shows the basic system information.
- Parameter Description:
  - Model name: The model name of this device.

EN

- System Description: As it is, this tells what this device is. Here, it is "24-Port 10/100BaseT/TX Managed PoE Switch".
- Location: Basically, it is the location where this switch is put. User-defined.
- Contact: For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.
- Device name: The name of the switch. User-defined. Default is ES-2126+ respectively ES-2126P+.
- System up time: The time accumulated since this switch is powered up. Its format is day, hour, minute, second.
- Current time: Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, Tue Apr 20 23:25:58 2005
- BIOS version: The version of the BIOS in this switch.
- Firmware version: The firmware version in this switch.
- Hardware-Mechanical version: The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; the one after the hyphen is the version of mechanical.
- Serial number: The number is assigned by the manufacturer.
- Host IP address: The IP address of the switch.
- Host MAC address: It is the Ethernet MAC address of the management agent in this switch.
- Device Port: Show all types and numbers of the port in the switch.
- RAM size: The size of the DRAM in this switch.
- Flash size: The size of the flash memory in this switch.

4.2.2 IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.



- Function name: IP Configuration
- Function Description: Set IP address, subnet mask, default gateway and DNS for the switch.
- Parameter Description:
  - DHCP Setting: DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

    The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field "Disable", you'll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 "IP Address Assignment" in this manual.

    Default: Disable
  - IP address: Users can configure the IP settings and fill in new values if users set the DHCP function "Disable". Then, click <Apply> button to update. When DHCP is disabled, Default: 192.168.1.1 If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.
  - Subnet mask: Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices each other. But unfortunately, the network classes A, B, and C are all too large to fit for almost all

networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. This reduces the total IP number of a network able to support, by the amount of 2 power of Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches. For more information, please also see the Section 2-1-5 "IP Address Assignment" in this manual. Default: 255.255.255.0

- Default gateway: Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

  Default: 172.23.56.250

- DNS: It is Domain Name Server used to serve the translation between IP address and name address.

  The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

  There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

  Default: 0.0.0.0

4.2.3 Time Configuration

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. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC

1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

- Function name: Time
- Function Description: Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area's time adjustment.
- Parameter Description:
  - Current Time: Shows the current time of the system.
  - Manual: This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and press <Apply> button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are >=2000, 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and press <Apply> button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

    Default: Year = 2000, Month = 1, Day = 1, Hour = 0, Minute = 0, Second = 0
  - NTP: NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing <Apply> button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

    Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from –12 to +13 step 1 hour.

    Default Time zone: +8 Hrs.
  - Daylight Saving: Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the

EN

time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start :

This is used to set when to start performing the day light saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Day Light Saving End: This is used to set when to stop performing the daylight saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

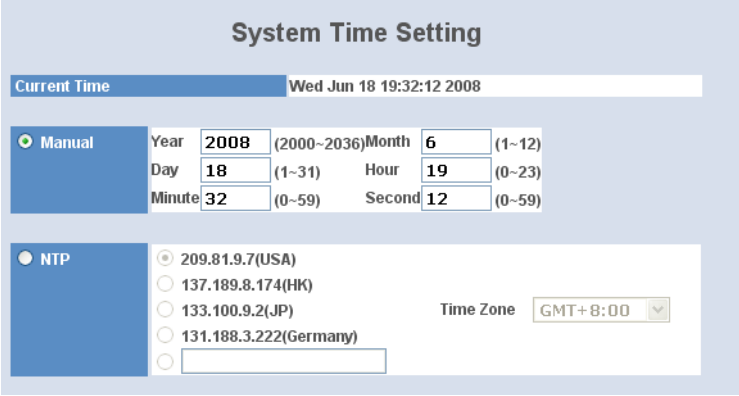
Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0



4.2.4 Account Configuration

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

The default setting for user account is:

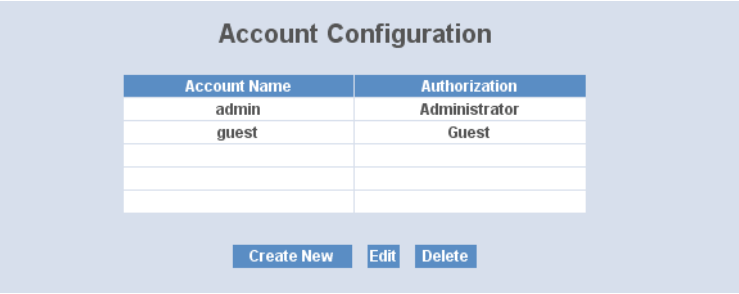
- Username: admin
- Password: admin

The default setting for guest user account is:

- Username: guest

EN

- Password: guest

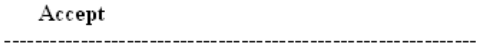


4.2.5 Management Security

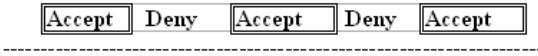
Through the management security configuration, the manager can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the manager to manage the switch:

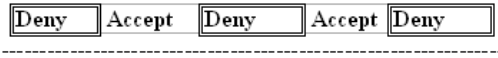
1. When no lists exists, then it will accept all connections.



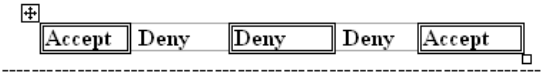
2. When only “accept lists” exist, then it will deny all connections, excluding the connection inside of the accepting range.



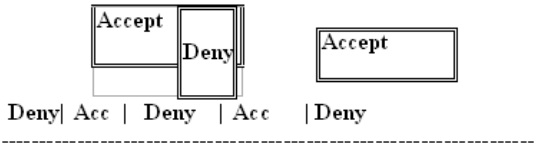
3. When only “deny lists” exist, then it will accept all connections, excluding the connection inside of the denying range.



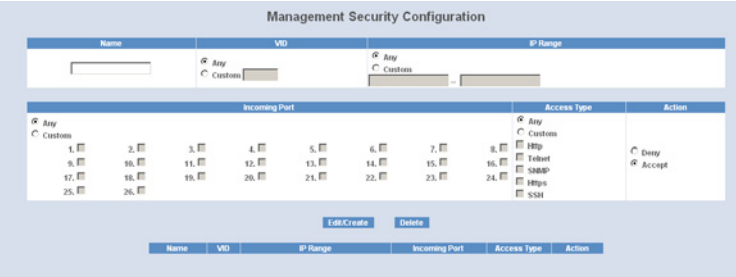
4 When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range.



5 When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.



- Function name: Management Security Configuration
- Function Description: The switch offers Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.



- Parameter Description:
  - Name: A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.
  - VID: The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.
  - IP Range: The switch supports two kinds of options for managed valid IP Range, including "Any" and "Custom". Default is "Any". In case that" Custom" had been chosen, you can assigned effective IP range. The valid range is 0.0.0.0~255.255.255.255.
  - Incoming Port: The switch supports two kinds of options for managed valid Port Range, including "Any" and "Custom". Default is "Any". You can select the ports that you would like them to be worked and restricted in the management security configuration if "Custom" had been chosen.
  - Access Type: The switch supports two kinds of options for managed valid Access Type, including "Any" and "Custom". Default is "Any". "Http", "Telnet", "SNMP", "ssh" and "HTTPS" are ways for the access and managing the switch in case that" Custom" had been chosen.
  - Action: The switch supports two kinds of options for managed valid Action Type, including "Deny" and "Accept". Default is "Deny". When you choose "Deny" action, you will be restricted and refused to manage the switch due to the "Access Type" you choose. However, while you select "Accept" action, you will have the authority to manage the switch.
  - Edit/Create: A new entry of Management Security Configuration can be created after the parameters as mentioned above had been setup

and then press <Edit/Create> button. Of course, the existed entry also can be modified by pressing this button.

- Delete: Remove the existed entry of Management Security Configuration from the management security table.

4.2.6 Virtual Stack

- Function name: Virtual Stack
- Function Description: Virtual Stack Management(VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switch, one switch will be a master machine, and the others in this group will become the slave devices.

  VSM offers a simple centralized management function. It is not necessary to remember the address of all devices, manager is capable of managing the network with knowing the address of the Master machine. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch become the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of these device.

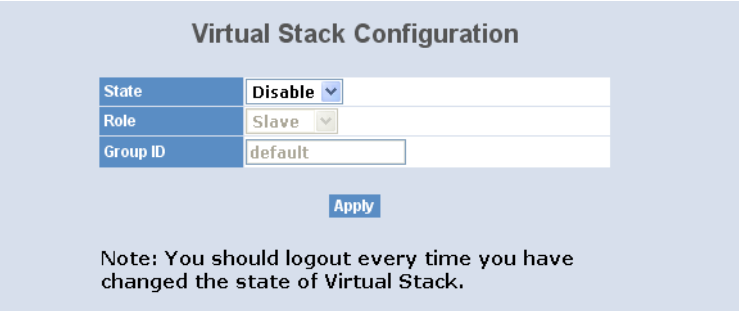
  The most top-left button is only for Master device. The background color of the button you press will be changed to represent that the device is under your management.

  Note: It will remove the grouping temporarily in case that you login the switch via the console.

  The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 196_ES-2126+), otherwise it will show " ---- " if no corresponding device exists.

  Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

  Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as Master device, however, the Master device with the smaller MAC value will be the Master one. All of these 16 devices can become Master device and back up with each other .



- Parameter Description:
  - State: It is used for the activation or de-activation of VSM. Default is Enable.
  - Role: The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Master.
  - Group ID: It is the group identifier (GID) which signs for VSM. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.

4.2.7 Login Protect

The login protect guards the device from repeated login errors caused by incorrect user data. Additionally, this function protects the device from brute force attacks, which spy out user data.

- Parameter.
  - Login-errors:

    Number of incorrect logins, after which the device blocks all logins.

    Possible Values:

    0 - 10, 0 disables login protect

    Default: 3

- Lock-Minutes:

  Time in Minutes, for which the device blocks all logins after the maximum number of login errors is achieved.

  Possible Values:

  0 - 10, 0 disables login protect

  Default: 3

EN

4.3 Port

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following section.

4.3.1 Status

The function Port Status gathers the information of all ports' current status and reports it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause and Tx Pause. An extra media type information for the module ports 25 and 26 is also offered.

Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause	Port Description
1	TP	Down	Enabled	Enabled	---/----	------	------	
2	TP	Up	Enabled	Enabled	100M/Full	On	Off	
3	TP	Down	Enabled	Enabled	---/----	------	------	
4	TP	Down	Enabled	Enabled	---/----	------	------	
5	TP	Down	Enabled	Enabled	---/----	------	------	
6	TP	Down	Enabled	Enabled	---/----	------	------	
7	TP	Down	Enabled	Enabled	---/----	------	------	
8	TP	Down	Enabled	Enabled	---/----	------	------	
9	TP	Down	Enabled	Enabled	---/----	------	------	
10	TP	Down	Enabled	Enabled	---/----	------	------	
11	TP	Down	Enabled	Enabled	---/----	------	------	
12	TP	Down	Enabled	Enabled	---/----	------	------	
13	TP	Down	Enabled	Enabled	---/----	------	------	
14	TP	Down	Enabled	Enabled	---/----	------	------	
15	TP	Down	Enabled	Enabled	---/----	------	------	

Port Status

Report the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it

will be automatically refreshed the port current status about every 5 seconds.

- Parameter:
  - Port No: Display the port number. The number is 1 – 26. Both port 25 and 26 are optional modules.
  - Media: Show the media type adopted in all ports. The Port 25 and Port 26 are optional modules, which support either fiber or UTP media with either Gigabit Ethernet (1000Mbps) or 10/100Mbps Fast Ethernet port. They may have different media types and speed. Especially, fiber port has comprehensive types of connector, distance, fiber mode and so on. The switch describes the module ports with the following page.
  - Link: Show that if the link on the port is active or not. If the link is connected to a working-well device, the Link will show the link "Up"; otherwise, it will show "Down". This is determined by the hardware on both devices of the connection.

    No default value.
  - State: Show that the communication function of the port is "Enabled" or "Disabled". When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

    Default: Enabled.
  - Auto Nego.: Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode "Enabled" and forced mode "Disabled". When in "Enabled" mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in "Disabled" mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is "Down".

    Default: Enabled
  - Speed / Duplex : Display the speed and duplex of all port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it is 1000Mbps supported only. The status of speed/duplex mode is determined by 1) the negotiation of both local

port and link partner in "Auto Speed" mode or 2) user setting in "Force" mode. The local port has to be preset its capability.

In port 1 – 24, they are supported Fast Ethernet with TP media only, so the result will show 100M/Full or 100M/Half, 10M/Full and 10M/Half duplex.

In port 25 and port 26, if the media is 1000Mbps with TP media, it will show the combinations of 10/100M and Full/Half duplex, 1000Mbps and Full duplex only. If the media is 1000Mbps with fiber media, it will show only 1000M/Full duplex.

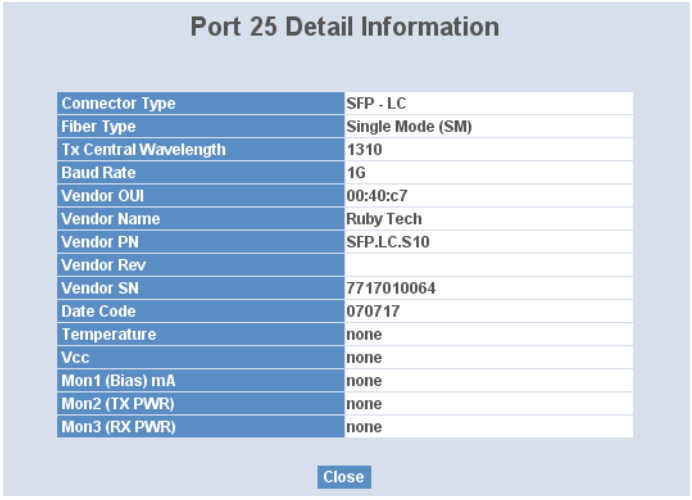
Default: None, depends on the result of the negotiation.

- Rx Pause: The way that the port adopts to process the PAUSE frame. If it shows "on", the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame.

  Default: None

- Tx Pause: It decides that whether the port transmits the PAUSE frame or not. If it shows "on", the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame.

  Default: None.



Details about SFP ports:

- Connector Type:

  Displays the connector type, for instance, UTP, SC, ST, LC and so on.

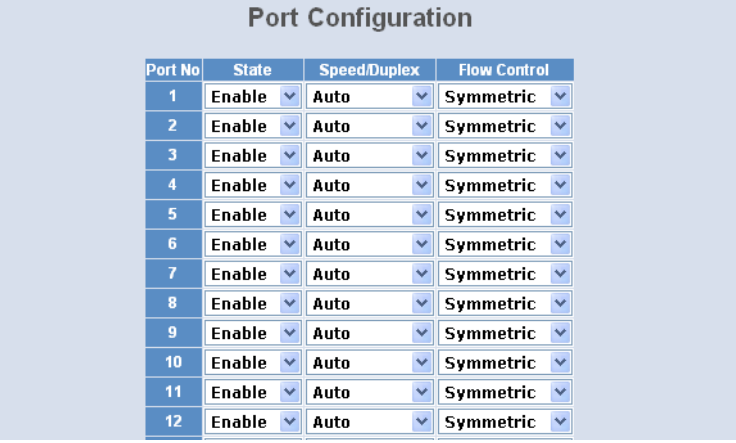
EN

- Fiber Type:
  Displays the fiber mode, for instance, Multi-Mode, Single-Mode.
- Tx Central Wavelength:
  Displays the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.
- Baud Rate:
  Displays the maximum baud rate of the fiber module supported, for instance, 10M, 100M, 1G and so on.
- Vendor OUI:
  Displays the Manufacturer's OUI code which is assigned by IEEE.
- Vendor Name:
  Displays the company name of the module manufacturer.
- Vendor P/N:
  Displays the product name of the naming by module manufacturer.
- Vendor Rev (Revision):
  Displays the module revision.
- Vendor SN (Serial Number):
  Shows the serial number assigned by the manufacturer.
- Date Code:
  Shows the date this module was made.
- Temperature:
  Shows the current temperature of module.
- Vcc:
  Shows the working DC voltage of module.
- Mon1(Bias) mA:
  Shows the Bias current of module.
- Mon2(TX PWR):
  Shows the transmit power of module.
- Mon3(RX PWR):
  Shows the receiver power of module.

EN

4.3.2 Port Configuration

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.



Port Configuration

It is used to set each port's operation mode. The switch supports 3 parameters for each port. They are State, Speed/Duplex and Flow Control.

- Parameter:
  - State: Set the communication capability of the port is Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states "Enable" and "Disable" able to choose. If you set a port's state "Disable", then that port is prohibited to pass any traffic, even it looks Link up.

    Default: Enable.
  - Speed/Duplex: Set the speed and duplex of the port. In speed, 10/100Mbps baud rate is available for Fast Ethernet, Gigabit module in port 25, 26. If the media is 1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

EN

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

- Flow Control: There are two modes to choose in flow control, including Symmetric and Asymmetric. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Asymmetric, this will let the receiving port care the PAUSE frame from transmitting device(s), but it doesn't send PAUSE frame. This is one-way flow control.

  Default: Symmetric.

4.3.3 Description

Here you can enter descriptions for the ports.

- Parameter:
  - Port:

    Number of the port.
  - Description:

    Field to enter a port's description.

    Possible Values: alpha numeric characters

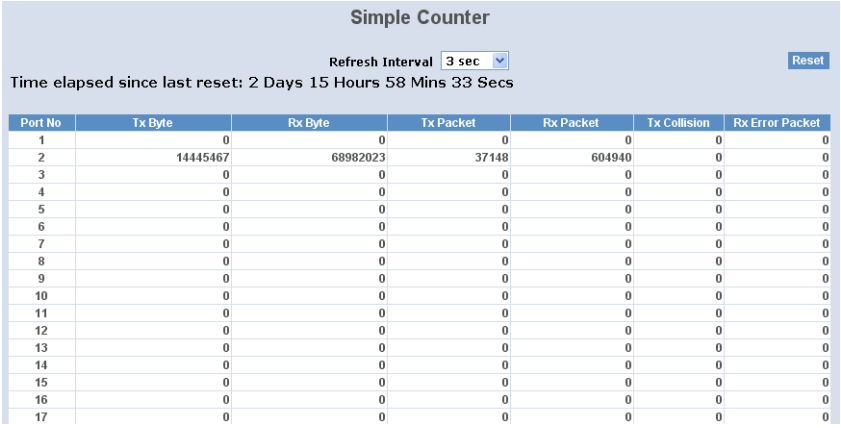
    Default: empty

EN

4.3.4 Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the following figure, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.



Port No	Tx Byte	Rx Byte	Tx Packet	Rx Packet	Tx Collision	Rx Error Packet
1	0	0	0	0	0	0
2	14445467	68982023	37148	604940	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0

Simple Counter

Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

- Parameter:
  - Tx Byte: Total transmitted bytes.

- Rx Byte: Total received bytes.
- Tx Packet: The counting number of the packet transmitted.
- Rx Packet: The counting number of the packet received.
- Tx Collision: Number of collisions transmitting frames experienced.
- Rx Error Packet: Number of bad packets received.

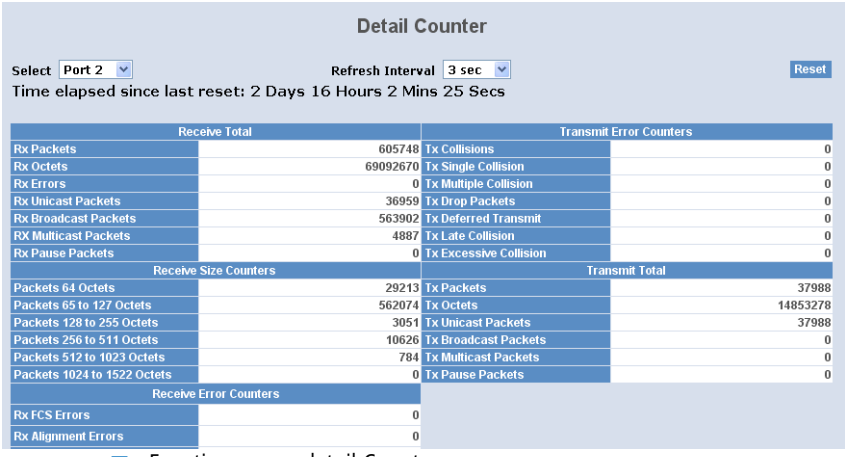
EN

4.3.5 Detail Counter

The function of Detail Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the following figure the window can show only one port counter information at the same time. To see another port's counter, you have to pull down the list of Select, then you will see the figures displayed about the port you had chosen.

Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.



- Function name: detail Counter
- Function Description: Display the detailed counting number of each port's traffic. The window can show all counter information of each port at one time.
- Parameter Description:
  - Rx Packets: The counting number of the packet received.

EN

- Rx Octets: Total received bytes.
- Rx Errors: Number of bad packets received.
- Rx Unicast Packets: Show the counting number of the received unicast packet.
- Rx Broadcast Packets: Show the counting number of the received broadcast packet.
- Rx Multicast Packets: Show the counting number of the received multicast packet.
- Rx Pause Packets: Show the counting number of the received pause packet.
- Tx Collisions: Number of collisions transmitting frames experienced.
- Tx Single Collision: Number of frames transmitted that experienced exactly one collision.
- Tx Multiple Collision: Number of frames transmitted that experienced more than one collision.
- Tx Drop Packets: Number of frames dropped due to excessive collision, late collision, or frame aging.
- Tx Deferred Transmit: Number of frames delayed to transmission due to the medium is busy.
- Tx Late Collision: Number of times that a collision is detected later than 512 bit-times into the transmission of a frame.
- Tx Excessive Collision: Number of frames that are not transmitted because the frame experienced 16 transmission attempts.
- Packets 64 Octets: Number of 64-byte frames in good and bad packets received.
- Packets 65-127 Octets: Number of 65 ~ 127-byte frames in good and bad packets received.
- Packets 128-255 Octets: Number of 128 ~ 255-byte frames in good and bad packets received.
- Packets 256-511 Octets: Number of 256 ~ 511-byte frames in good and bad packets received.
- Packets 512-1023 Octets: Number of 512 ~ 1023-byte frames in good and bad packets received.
- Packets 1024- 1522 Octets: Number of 1024-1522-byte frames in good and bad packets received.
- Tx Packets: The counting number of the packet transmitted.

EN

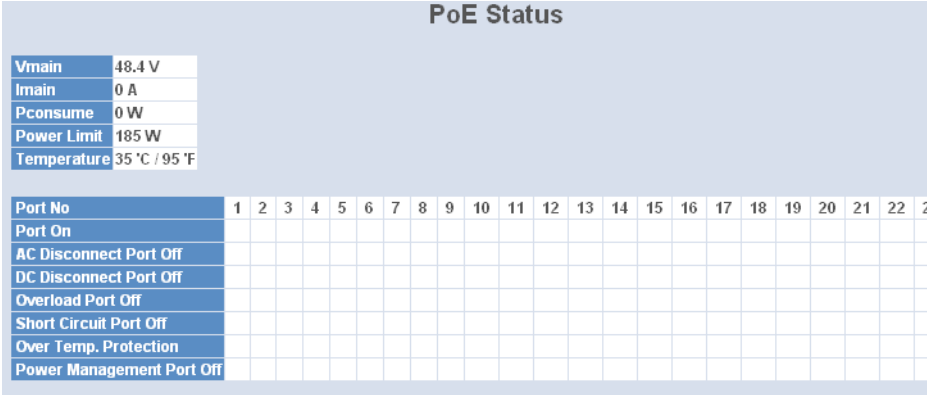
- TX Octets: Total transmitted bytes.
- Tx Unicast Packets: Show the counting number of the transmitted unicast packet.
- Tx Broadcast Packets: Show the counting number of the transmitted broadcast packet.
- Tx Multicast Packets: Show the counting number of the transmitted multicast packet.
- Tx Pause Packets: Show the counting number of the transmitted pause packet.
- Rx FCS Errors: Number of bad FSC packets received.
- Rx Alignment Errors: Number of Alignment errors packets received.
- Rx Fragments: Number of short frames (< 64 bytes) with invalid CRC.
- Rx Jabbers: Number of long frames(according tomax_length register) with invalid CRC.
- Rx Drop Packets: Frames dropped due to the lack of receiving buffer.
- Rx Undersize Packets: Number of short frames (<64 Bytes) with valid CRC.
- Rx Oversize Packets: Number of long frames(according to max_length register) with valid CRC.

4.3.6 PoE

LANCOM ES-2126P+ only

PoE Status

Display the information about the PoE status.



- Parameter:

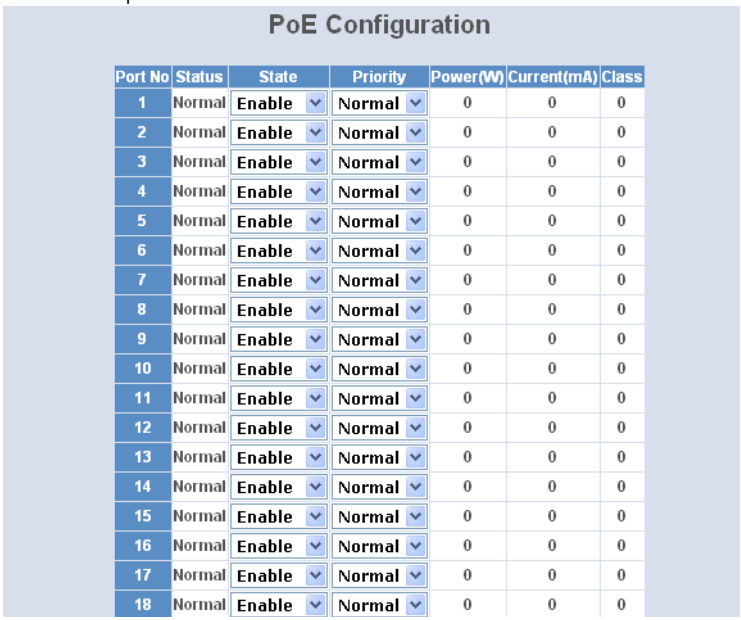
- Vmain: The volt is supplied by the PoE.
- Imain: The sum of the current that every port supplies.
- Pconsume: The sum of the power that every port supplies.
- Power Limit: The maximal power that the switch can supply (Read Only).
- Temperature: The temperature of the chip on PoE.
- Port No: Port number.
- Port On: Shows whether the port is supplying the power to the PD or not.
- AC Disconnect Port Off: Port is turned off due to the AC Disconnect function.
- DC Disconnect Port Off: Port is turned off due to the DC Disconnect function.
- Overload Port Off: The switch will stop supplying the power to the port due to the power required by the PD that is linked to the port on the switch excesses the Class setting of the PD.
- Short Circuit Port Off: The switch will stop supplying the power to the port if it detects that the PD linked to the port is short circuit.
- Over Temp. Protection: The port of the switch will be disabled due to fast transient rise in temperature to 240^{o}C or slow rise in temperature to 200^{o}C.
- Power Management Port Off: Due to total power required by all PDs linked to the switch excesses the power limit, so the switch stops supplying the power to this port after referring to the information of the priority.

PoE Configuration

In PoE Port Management function, user can configure the settings about PoE.

The switch complies with IEEE 802.3af protocol and be capable of detecting automatically that whether the device linked to the port on the switch is PD (Powered Device) or not. The switch also manage the power supplement based on the Class of the PD, and it will stop supplying the power

once the power required by the PD excesses the Class, Short Circuit or over temperature occurs.



- Parameter:
  - Status: Include “Normal” or “Active” two kinds of status. The former means the port is ready to link and supply the power to the PD at any time. The latter means the port is in the condition of supplying the power.
  - State: “Enable” means the manager allows the power supplied to the PD is legal while the port linked to the PD; “Disable” means the port does not own PoE function.
  - Priority: Three options are offered for the user to choose, including Normal, Low and High. Default is Normal. The switch will stop supplying the power to the port based on the order of the priority Low‡Normal‡High in case total power required by all PDs linked to the switch excesses the power limit. As the ports have the same priority, then the switch will cease the power supplement from the port with the highest port id (12‡1).
  - Power(W): The power is consumed by the port.
  - Current(mA): The current is supplied to the PD by the port.

- Class: The Class of the PD linked to the port of the switch.

4.4 Loop Detection

The loop detection is used to detect the presence of traffic. When switch receives packet's(looping detection frame) MAC address the same as oneself from port, show Loop detection happens. The port will be locked when it received the looping detection frames. If you want to resume the locked port, please find out the looping path and take off the looping path, then select the resume the locked port and click on "Resume" to turn on the locked ports

- Loop Detection

  Display whether switch open Loop detection.

- Parameter:
  - Port No:

    Display the port number. The number is 1 - 24.

  - Detection Port - Enable:

    When Port No is chosen, and enable port' s Loop detection, the port can detect loop happens. When Port-No is chosen, enable port' s Loop detection, and the port detects loop happen, port will be Locked. If Loop did not happen, port maintains Unlocked. The default is Disable.

  - Locked Port - Resume:

    When Port No is chosen, enable port' s Loop detection, and the port detects loop happen, the port will be Locked. When choosing Resume, port locked will be opened and turned into unlocked. If not choosing Resume, Port maintains locked.

4.5 SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

EN

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

- Function name: SNMP Configuration
- Function Description: This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names, then it can access the MIB information of the target device. So, both parties must have the same community name. Once completing the setting, click <Apply> button, the setting takes effect.
- Parameters Description:
  - SNMP: The term SNMP here is used for the activation or de-activation of SNMP.

    Default is Enable.
  - Get/Set/Trap Community: Community name is used as password for authenticating if the requesting network management unit belongs to the same community group. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit can not access the device with different community name via SNMP protocol; If they both have the same community name, they can talk each other.

    Community name is user-definable with a maximum length of 15 characters and is case sensitive. There is not allowed to put any blank in the community name string. Any printable character is allowable.

    The community name for each function works independently. Each function has its own community name. Say, the community name for GET only works for GET function and can't be applied to other function such as SET and Trap.

    Default SNMP function : Enable

    Default community name for GET: public

    Default community name for SET: private

    Default community name for Trap: public

    Default Set function : Enable

Default trap host IP address: 0.0.0.0

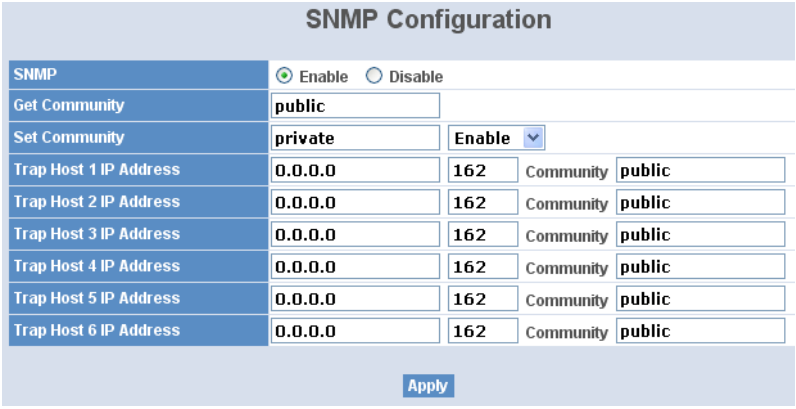
Default port number :162

- Trap:

  In the switch, there are 6 trap hosts supported. Each of them has its own community name and IP address; is user-definable. To set up a trap host means to create a trap manager by assigning an IP address to host the trap message. In other words, the trap host is a network management unit with SNMP manager receiving the trap message from the managed switch with SNMP agent issuing the trap message. 6 trap hosts can prevent the important trap message from losing.

  For each public trap, the switch supports the trap event Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Trap. They can be enabled or disabled individually. When enabled, the corresponded trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap message will be sent. As to the Enterprise (no. 6) trap is classified as private trap, which are listed in the Trap Alarm Configuration function folder.

  Default for all public traps: Enable.



4.6 DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the

power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

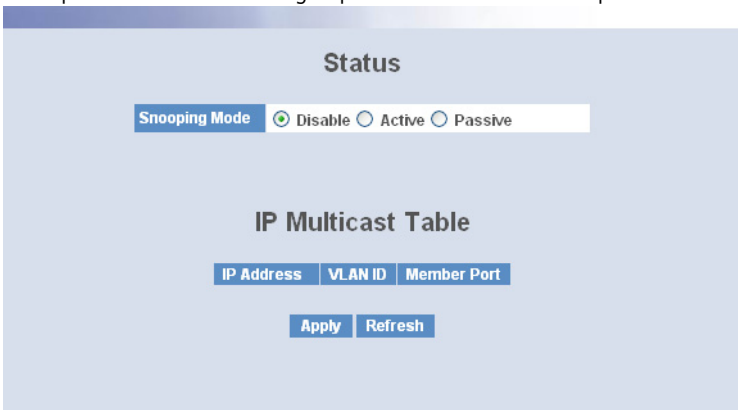
The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay time is 30 sec. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is “Disable”.

4.7 IGMP Snooping

The function, IGMP Snooping, 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 can not 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.



4.7.1 IGMP Snooping Status

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.

- Parameter:
  - IGMP snooping mode selection: The switch supports three kinds of IGMP Snooping status, including "Passive", "Active" and "Disable".
  - Disable: Set "Disable" mode to disable IGMP Snooping function.

    Default: Disable
  - Active: In Active mode, IGMP snooping switch will periodically issue the Membership Query message to all hosts attached to it and gather the Membership report message to update the database of the Multicast table. By the way, this also reduces the unnecessary multicast traffic.
  - Passive: In Passive Snooping mode, the IGMP snooping will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.
  - IP Address: how all multicast groups IP addresses that are registered on this device.

- VLAN ID: Shows VLAN ID for each multicast group.
- Member Port: Shows member ports that join each multicast group. Member port may be only or more than one.

4.7.2 Allowed Group

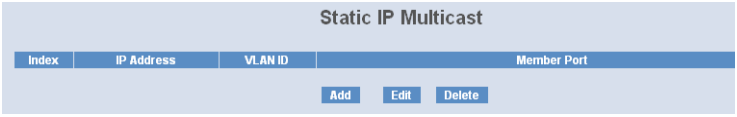
The Allowed Group function allows the IGMP Snooping to set up the IP multicast table based on user's specific conditions. IGMP report packets that meet the items you set up will be joined or formed the multicast group.

- Parameter:
  - IP Range: The switch supports two kinds of options for managed valid IP range, including "Any" and "Custom". Default is "Any". In case that" Custom" had been chosen, you can assigned effective IP range. The valid range is 224.0.0.0~239.255.255.255.
  - VID: The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.
  - Port: The switch supports two kinds of options for managed valid port range, including "Any" and "Custom". Default is "Any". You can select the ports that you would like them to be worked and restricted in the allowed group configuration if "Custom" had been chosen.
  - Add: A new entry of allowed group configuration can be created after the parameters as mentioned above had been setup and then press <Add> button.

- Edit: The existed entry also can be modified after pressing <Edit> button.
- Delete: Remove the existed entry of allowed group configuration from the allowed group.

4.7.3 Static IP Multicast

Here you can define mac table entries manually, which the device cannot learn automatically, for example.



- Parameter:
  - IP Adress:

    The ip address of the manually defined multicast group.
  - VLAN ID:

    VLAN, to which this ip address belongs. 0 to 4094.
  - Member Port:

    The device leads incoming packets with the defined ip multicast address to this ports.

4.7.4 Group Limit

The Group limit table is used to define the maximum number of IGMP groups to be given access to a port. Enter the maximum number of groups with access rights into the field "Group limit". If this limit is reached, further requests to the associated layer-2 interface are ignored and the associated data streams are dropped.

For LANCOM ES-2126+ only

- Parameter:
  - Port:

    For this port the group limit is activated.
  - Group Limit:

    Maximum number of groups which may use the port.

    Possible Values:

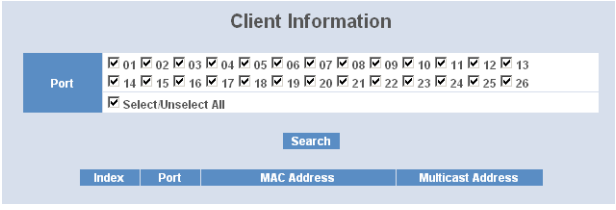
    0 to 256.

    Default: 256.

4.7.5 Client Information

This function displays information about the client connected to the device's port. Mark the port with the relevant client and click on 'Search'. With the selection box 'Select/Unselect all' you can activate or deactivate any or all of the ports.

For LANCOM ES-2126+ only



- Parameter:
  - Port:

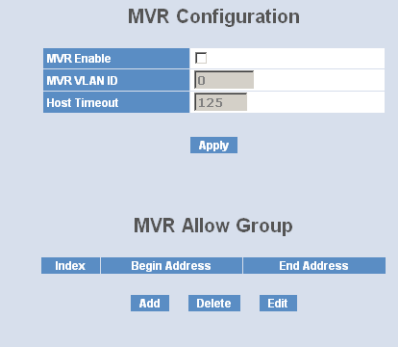
    Here you select the ports that are to be searched.

- Index:
  Shows the index of the client.
- Port:
  Shows the port, which is connected to the client.
- MAC Address:
  Shows the mac address of the client.
- Multicast Address:
  Shows the multicast address of the client.

4.7.6 MVR Configuration

Multicast VLAN Registration (MVR) enables multicast data streams to be transmitted between a sender VLAN and multiple receiver VLANs. MVR allows multicast streams to be transmitted continuously; the receiver VLANs are kept separate for security reasons.

For LANCOM ES-2126+ only



- Parameter:
  - MVR Enable:
    Enables or disables MVR.
  - MVR VLAN ID:
    VLAN ID of the sender network.
  - Host Timeout:
    Interval in seconds that the device waits for responses from the stations with information about their membership in multicast groups.
    0 to 125 seconds, default 125 seconds.

EN

- Apply:
  Applies the settings to the switch.
- Index:
  Index of the allowed group.
- Begin Address:
  Start address of the allowed group.
- End Address:
  End address of the allowed group.
- Add:
  Adds an entry to the allowed groups.
- Delete:
  Deletes an entry from the allowed groups.
- Edit:
  Edits an entry of the allowed groups.

4.7.7 MVR Group Status

Here you can look up the MVR group memberships.

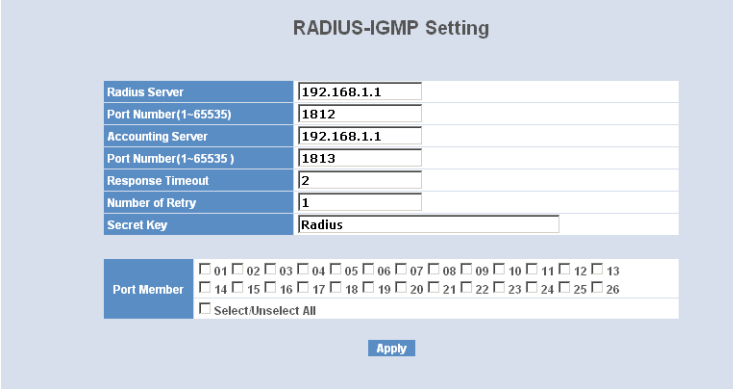
For LANCOM ES-2126+ only

- Parameter:
  - Available Groups Count:
    Displays the number of available groups.
  - Index:
    Displays the index of the group.
  - Group Address:
    Displays the ip address of the group.
  - Port Member:
    Displays the port, which is the group uses.

EN

4.7.8 RADIUS IGMP

Here you can configure the parameters for the igmp authentication via RADIUS server.



- Parameter:
  - Radius Server:

    Ip address of the RADIUS authentication server.

    Default: 192.168.1.1
  - Port-Number:

    Select the port, via which the device communicates with the authentication server.

    Possible values: numerical characters from 1 to 65535

    Default: 1812
  - Accounting-Server:

    Ip address of the accounting server.

    Default: 192.168.1.1
  - Response Timeout:

    Configurates the time out settings between the authenficator and the accounting server in seconds.

    Possible values: numerical characters from 1 to 65535

    Default: 2

EN

- Number of Retry:

  The maximum number of times that the authenticator forwards requests from the authentication server to the supplicant, before the authentication process is aborted.

  Possible values: numerical characters

  Default: 1

- Secret Key:

  The password which encrypts the communication between the authenticator and the authentication server.

  Possible values: 1 - 31 alpha numeric charachters (upper case letters, lower case letters, cyphers 0-9)

  Default: Radius

- Port Member:

  Selects the ports for the multicast group.

4.8 VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

4.8.1 VLAN Mode

VLAN Mode Setting

The VLAN Mode Selection function includes two modes: Port-based and Tag- based, you can choose one of them by pulling down list and pressing the <Downward> arrow key. Then, click <Apply> button, the settings will take effect immediately.

- Parameter Description:
  - VLAN Mode:

    Tag-based:

    This is the default setting.

    Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress

filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of 802.1q..

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 256 Tag VLAN groups.

Port-based:

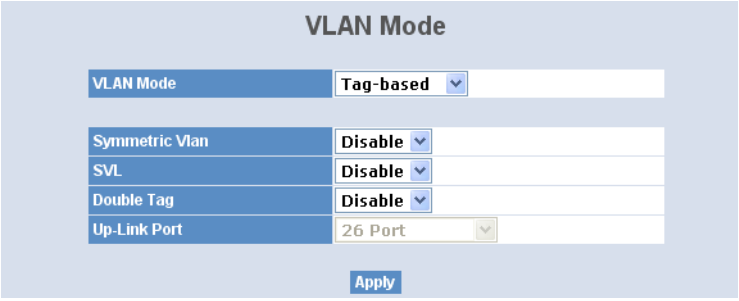
Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can support up to maximal 26 port-based VLAN groups.

- Symmetric Vlan: This is a Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID".). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

  Note: If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

- SVL: While SVL is enable, all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. While SVL is disable, it means learning mode is IVL. In this mode, different VLAN uses different filtering database storing the membership information of the VLAN to learn or look up the information of a VLAN member.
- Double Tag: Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will

be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

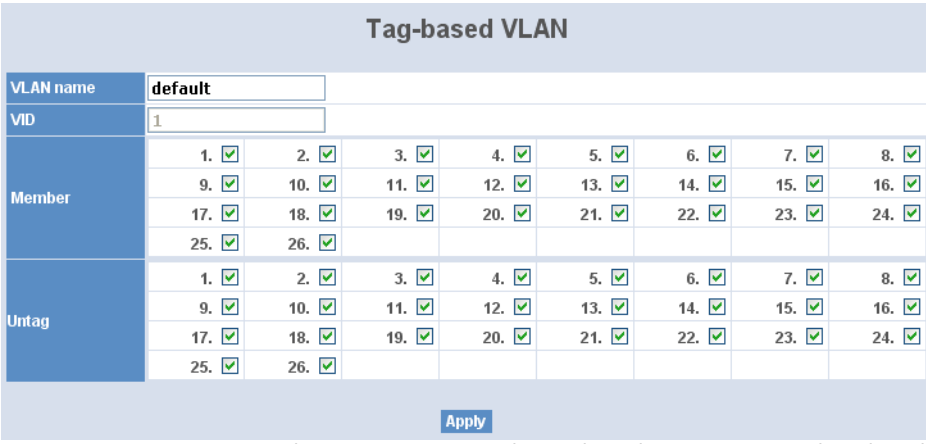


4.8.2 Tag-based Group

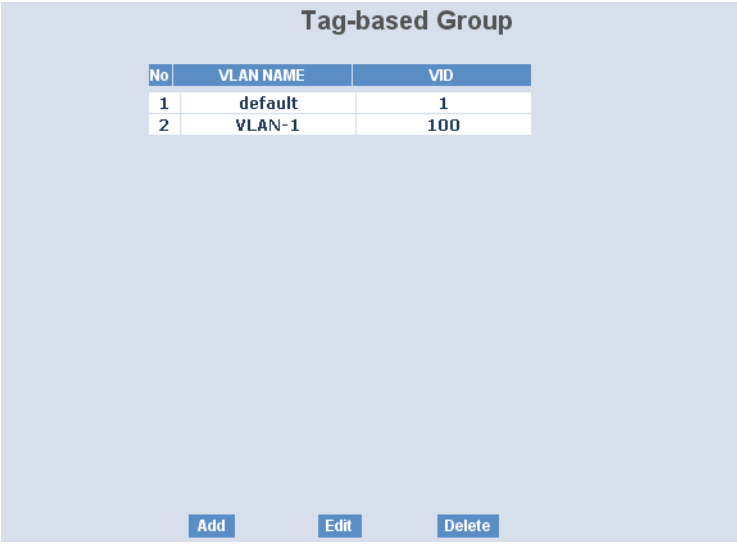
- Function name: Tag-based Group Configuration
- Function Description: It shows the information of existed Tag-based VLAN Groups. You can also easily create, edit and delete a Tag-based VLAN group by pressing <Add>, <Edit> and <Delete> function buttons. User can add a new VLAN group by inputting a new VLAN name and VLAN ID after pressing <Add> button.
- Parameter Description:
  - VLAN Name: The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.
  - VID: VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

- Member: This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box beside the port x to enable it.

Add Group: Input the VLAN name, VID and then choose the member by ticking the check box beside the port No. to create a new Tag-based VLAN. As to the parameter of Untag, it stands for an egress rule of the port. If you tick the check box beside the port No., packets with this VID outgoing from this port will be untagged. Finally, press the <Apply> button to have the setting taken effect.



- Delete Group: Just press the <Delete> button to remove the selected group entry from the Tag-based group table.



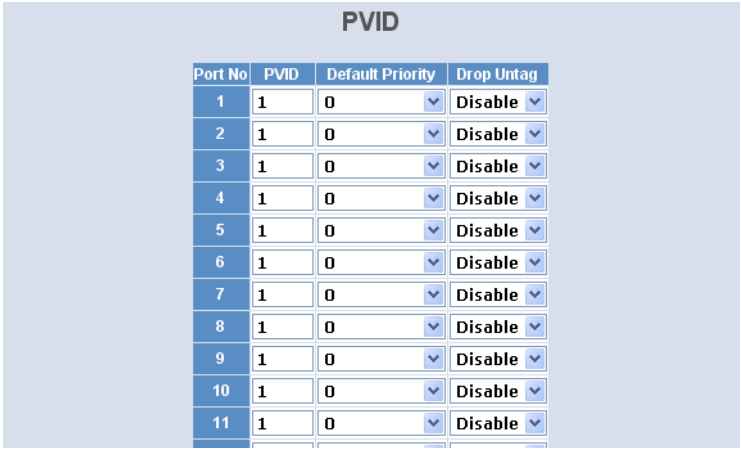
- Edit a group: ust select a group entry and press the <Edit> button, then you can modify a group's description, member and untag settings.

4.8.3 PVID

- Function name: PVID

EN

- Function Description: In PVID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rule (Rule 2) to each port. The Ingress Filtering Rule 2 is "drop untagged frame". While Rule 2 is enabled, the port will discard all Untagged-frames.

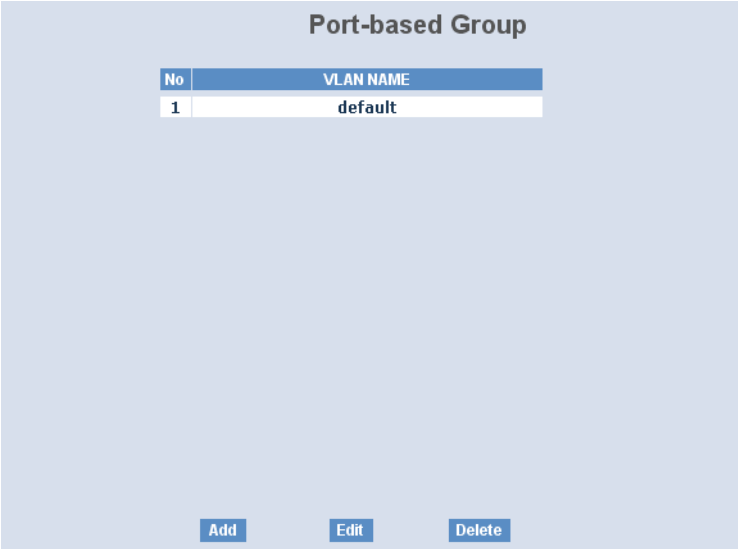


- Parameter Description:
  - Port 1-26: Port number.
  - PVID: This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.
  - Default Priority: It bases on 802.1p QoS and affects untagged packets. When the packets enter the switch, it would get the priority precedence according to your Default Priority setting and map to 802.1p priority setting in QoS function. For example, while you set Default Priority of port 2 with 2 and transmit untagged packets to port 2, these packets will own priority 2 precedence due to your default 802.1p Priority Mapping setting in QoS function and be put into Queue 1.
  - Drop Untag: Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged

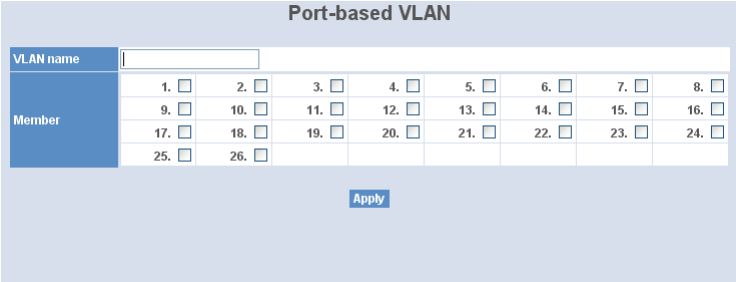
will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

4.8.4 Port-based Group

- Function name: Port-based Group Configuration
- Function Description: It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by pressing <Add>, <Edit> and <Delete> function buttons. User can add a new VLAN group by inputting a new VLAN name.
- Parameter Description:
  - VLAN Name: The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, " - " and "_" characters. The maximal length is 15 characters.
  - Member: This is used to enable or disable if a port is a member of the new added VLAN, "Enable" means it is a member of the VLAN. Just tick the check box beside the port x to enable it.



  - Add Group: Create a new Port-based VLAN. Input the VLAN name and choose the member by ticking the check box beside the port No., then, press the <Apply> button to have the setting taken effect.



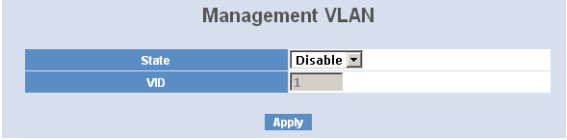
EN

- Delete Group: Just press the <Delete> button to remove the selected group entry from the Port-based group table.

- Edit a group: Just select a group entry and press the <Edit> button, then you can modify a group's description and member set.

4.8.5 Management VLAN

Here you can configure the settings for the port-based VLAN.



- Parameter:

- State:
  Enables or disables port-based VLAN.
- VID:
  VLAN identifier for the port-based VLAN.

4.9 MAC Table

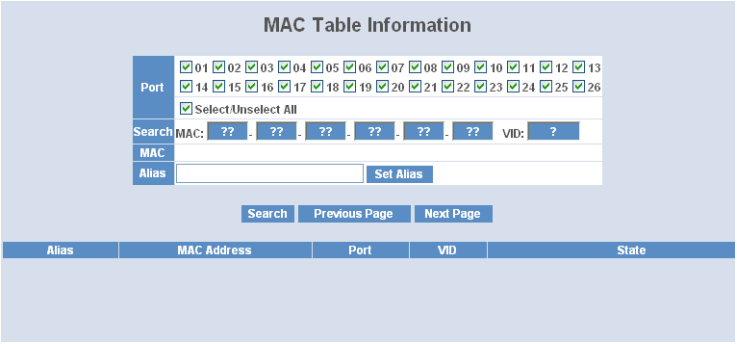
EN

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static and MAC Alias, which cannot be categorized to some function type. They are described below.

4.9.1 MAC Table Information

- Display the static or dynamic learning MAC entry and the state for the selected port.
- Parameter:
  - Port: Select the port you would like to inquire.
  - Search: Set up the MAC entry you would like to inquire.
    The default is ??-??-??-??-??-??
  - MAC: Display the MAC address of one entry you selected from the searched MAC entries table.
  - Alias: Set up the Alias for the selected MAC entry.
  - Set Alias: Save the Alias of MAC entry you set up.
  - Search: Find the entry that meets your setup.
  - Previous Page: Move to the previous page.
  - Next Page: Move to the next page.
  - Alias: The Alias of the searched entry.
  - MAC Address:The MAC address of the searched entry.
  - Port: The port that exists in the searched MAC Entry.
  - VID: VLAN Group that MAC Entry exists.

- State: Display the method that this MAC Entry is built. It may show "Dynamic MAC" or "Static MAC".



EN

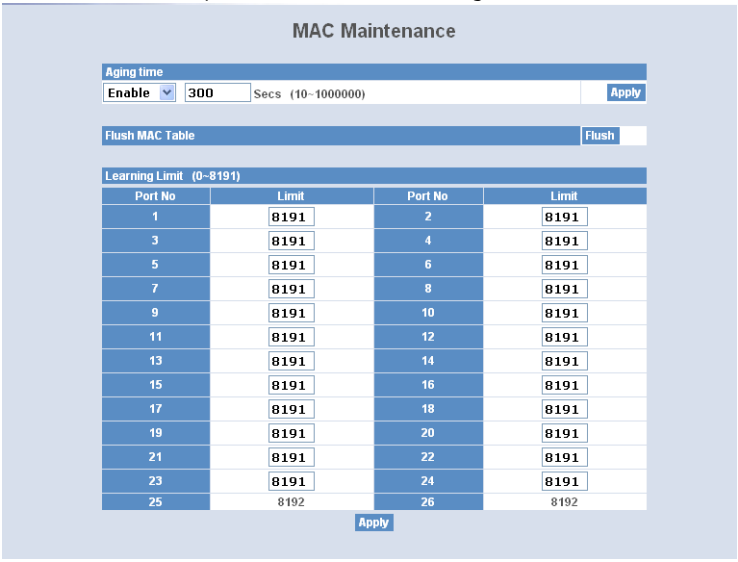
4.9.2 MAC Table Maintenance

- This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

  In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.

- Parameter:
  - Aging Time: Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds. The default Aging Time is 300 seconds.
  - Learning Limit: To set up the maximum amount of MAC that each port can learn. Valid value of learning limit for port 1~24 ranges from 0-

8191. As to port 25~port 26, only the fixed value "8192" is assigned to these two ports and user cannot configure this value.



4.9.3 Static Setting

- The function of Static is used to configure MAC's real manners inside of the switch. Three kinds of manners including static, static with destination drop and static with source drop are contained in this function .

  As "static" is chosen, assign a MAC address to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

  As "static with destination drop" is chosen, the packet will be dropped if its DA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

  As "static with source drop" is chosen, the packet will be dropped if its SA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

- Parameter:
  - MAC: It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,
  - 00 – 40 - C7 - D6 – 00 - 01
  - VID: VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.
  - Queue (Priority): Set up the priority(0~3) for the MAC.
  - Forwarding Rule(Drop Policy):

    Static: A MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

    Static with Destination Drop: While the DA of the incoming packets meets the value you set up, these packets will be dropped.

    Static with Source Drop: While the SA of the incoming packets meets the value you set up, these packets will be dropped.
  - Port : Select the port No. you would like to do setup in the switch. It is 1 ~26.

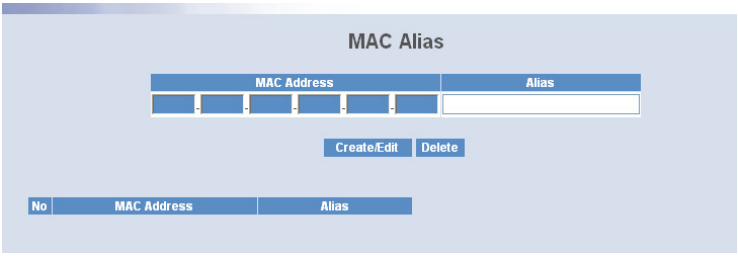
4.9.4 MAC Alias

- MAC Alias function is used to let you assign MAC address a plain English name. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

  There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click <Create/Edit> button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.
- Function name: MAC Alias Create/Edit or Delete
- Function Description: In the MAC Alias function, MAC Alias Add/Edit function is used to let you add or modify an association between MAC address and a plain English name. User can click <Create/Edit> button to add a new record with name.

EN

As to MAC Alias Delete function is used to let you remove an alias name to a MAC address. You can select an existed MAC address or alias name to remove.



- Parameter Description:
  - MAC Address:It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example,

    00 – 40 - C7 - D6 – 00 - 02
  - Alias: MAC alias name you assign.

    Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

4.9.5 Port Security

The port security function allows you to determine which MAC addresses can access a port. If this is activated by setting a mark in the corresponding check box, then only MAC addresses entered in the MAC table can access the port. Another MAC address attempting to communicate via this port will be blocked by port security. Furthermore, you can place a static limit on accesses to the port with the Port Static Mac function.

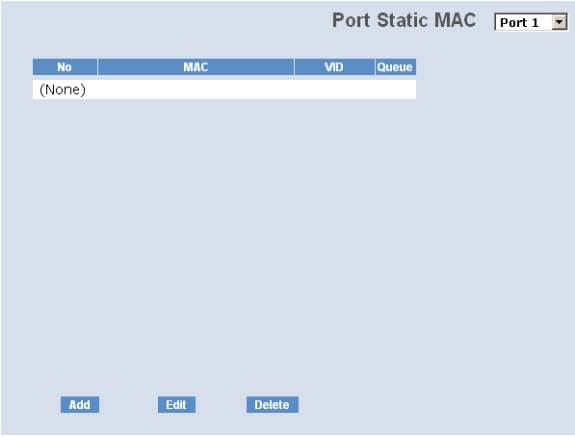
- Parameter:
  - Port:

    Enables port security for the port which you select.

4.9.6 Port Static MAC

The Port Static Mac function sets a static limitation on the MAC addresses able to access a port on the switch. All MAC addresses entered into the list for a

port are able to access this if Port Security is active. If there are no MAC addresses entered into the list for a port, then all addresses in the MAC table can access it.



- Parameter:
  - No:

    Number of the port, which the mac address may use.
  - MAC:

    Mac address, which may use a port.

    Possible values: 12 alpha numeric characters
  - VID:

    VLAN identifier, which is active if the device uses tagged VLAN.

    Possible values: 1 - 4094
  - Queue:

    Here you determine which queue is to be used for packets arriving at the port from a MAC address. Each port has four queues with different priorities. Choose 1 for the highest priority, 4 for the lowest.
  - Add:

    Adds a mac address to a port's list.
  - Edit:

    Edits a mac address entry in a port's list.

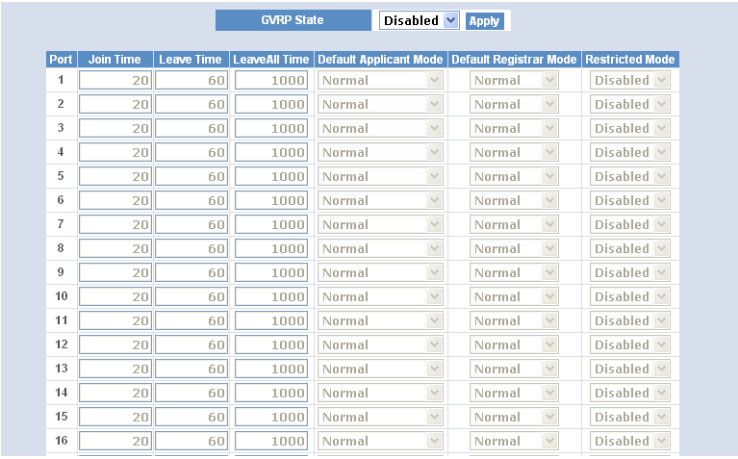
EN

- Delete:
  Deletes a mac address from a port's list.

4.9.7 GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.



EN

4.9.8 Config

GVRP Config

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

- Parameter Description:
  - GVRP State Setting: This function is simply to let you enable or disable GVRP function. You can pull down the list and click the <Downward> arrow key to choose "Enable" or "Disable". Then, click the <Apply> button, the system will take effect immediately.
  - Join Time:
  - Used to declare the Join Time in unit of centisecond. Valid time range: 20 –100 centisecond, Default: 20 centisecond.
  - Leave Time:
  - Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.
  - Leave All Time: A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.
  - Default Applicant Mode: The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice.
  - Normal: It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.
  - Non-Participant: It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.
  - Default Registrar Mode: The mode here means the type of Registrar. There are three types of parameters for registrar administrative control

value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice.

Normal:It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed: It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden: It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

- Restricted Mode: This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user's choice.

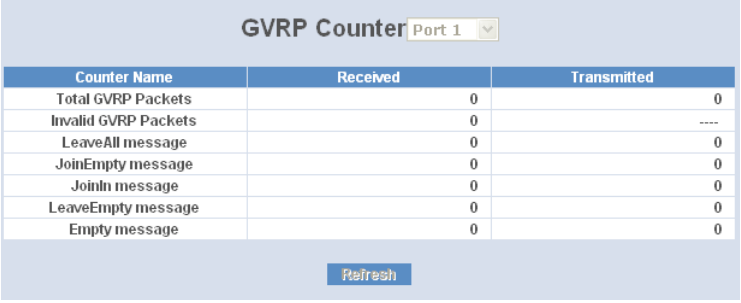
  Disabled: In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

  Enabled: In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

4.9.9 Counter

GVRP Counter

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.



- Parameter Description:

EN

- Received:

  Total GVRP Packets: Total GVRP BPDU is received by the GVRP application.

  Invalid GVRP Packets: Number of invalid GARP BPDU is received by the GARP application.

  LeaveAll Message Packets: Number of GARP BPDU with Leave All message is received by the GARP application.

  JoinEmpty Message Packets: Number of GARP BPDU with Join Empty message is received by the GARP application.

  JoinIn Message Packets: Number of GARP BPDU with Join In message is received by the GARP application.

  LeaveEmpty Message Packets:

  Number of GARP BPDU with Leave Empty message is received by the GARP application.

  Empty Message Packets:

  Number of GARP BPDU with Empty message is received by the GARP application.

- Transmitted:

  Total GVRP Packets: Total GARP BPDU is transmitted by the GVRP application.

  Invalid GVRP Packets: Number of invalid GARP BPDU is transmitted by the GVRP application.

  LeaveAll Message Packets: Number of GARP BPDU with Leave All message is transmitted by the GARP application.

  JoinEmpty Message Packets: Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

  JoinIn Message Packets: Number of GARP BPDU with Join In message is transmitted by the GARP application.

  LeaveEmpty Message Packets: Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

  Empty Message Packets: Number of GARP BPDU with Empty message is transmitted by the GARP application.

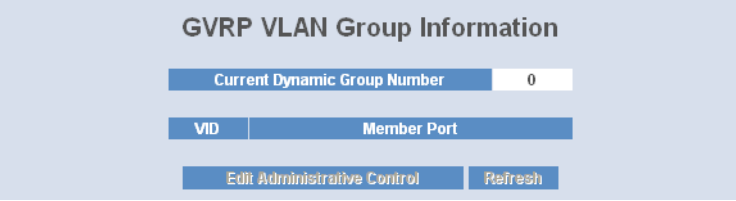
EN

4.9.10 Group

GVRP Group Information

To show the dynamic group member and their information.

- Parameter Description:
  - Current Dynamic Group Number: The number of GVRP group that are created currently.
  - VID: VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.
  - Member Port: Those are the members belonging to the same dynamic VLAN group.
  - Edit Administrative Control: When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.
  - Refresh: Refresh function can help you to see current GVRP group status.



4.10 STP

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

4.10.1 Status

- Function name: STP Status
- Function Description: In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' description is listed in the following table.

EN

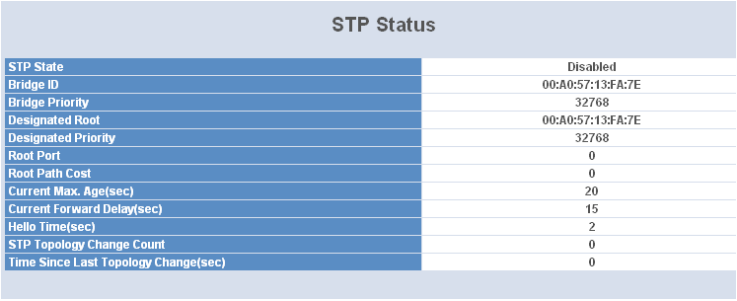
- Parameter Description:
  - STP State: Show the current STP Enabled / Disabled status. Default is "Disabled".
  - Bridge ID: Show switch's bridge ID which stands for the MAC address of this switch.
  - Bridge Priority: Show this switch's current bridge priority setting. Default is 32768.
  - Designated Root: Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.
  - Designated Priority: Show the current root bridge priority.
  - Root Port: Show port number connected to root bridge with the lowest path cost.
  - Root Path Cost: Show the path cost between the root port and the designated port of the root bridge.
  - Current Max. Age: Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

    All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.
  - Current Forward Delay: Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.
  - Hello Time: Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.
  - STP Topology Change Count: STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to

EN

0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.

- Time Since Last Topology Change: Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.



STP Status

STP State	Disabled
Bridge ID	00:A0:57:13:FA:7E
Bridge Priority	32768
Designated Root	00:A0:57:13:FA:7E
Designated Priority	32768
Root Port	0
Root Path Cost	0
Current Max. Age(sec)	20
Current Forward Delay(sec)	15
Hello Time(sec)	2
STP Topology Change Count	0
Time Since Last Topology Change(sec)	0

4.10.2 Configuration

The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for the user to configure as user's idea. Each parameter description is listed below.

- Function name: STP Configuration
- Function Description: User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is "Disable".
- Parameter Description:
  - Spanning Tree Protocol: Set 802.1W Rapid STP function Enable / Disable. Default is "Disable"
  - Bridge Priority: The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the switch as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.
  - Hello Time: Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the device is the root bridge of the LAN, for example, all

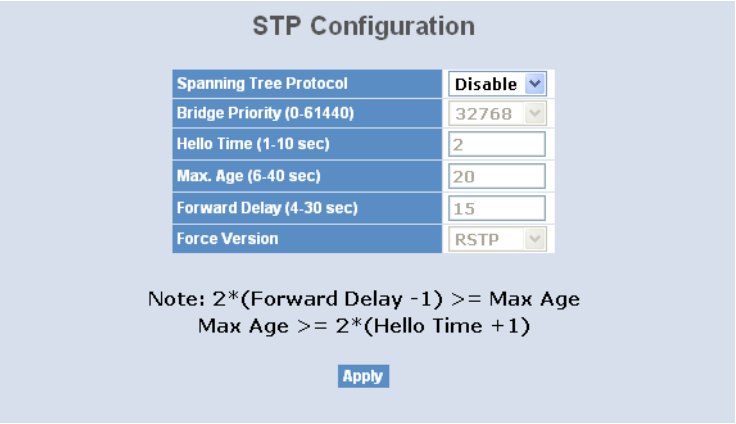
other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.

Default is 2 seconds.

- Max. Age: When the switch is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.
- Forward Delay: You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors.

  The valid value is 4 ~ 30 seconds, default is 15 seconds.
- Force Version: Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backward compatible with STP (802.1d).

EN



4.10.3 Port

- Function name: STP Port Setting
- Function Description: In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.
- Parameter Description:
  - Port Status: It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

    DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

    Notice: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

    LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets still.

    FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.
  - Path Cost Status: It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root

Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

- Configured Path Cost: The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

  802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

  10 Mbps : 2,000,000

  100 Mbps : 200,000

  1 Gbps : 20,000

  Default: 0

- Priority: Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

  Default is 128.

- Admin Edge Port: If user selects "Yes", this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

  Default: No

- Admin Point To Point: say a port is a point-to-point link, from RSTP's view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state.

  There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be

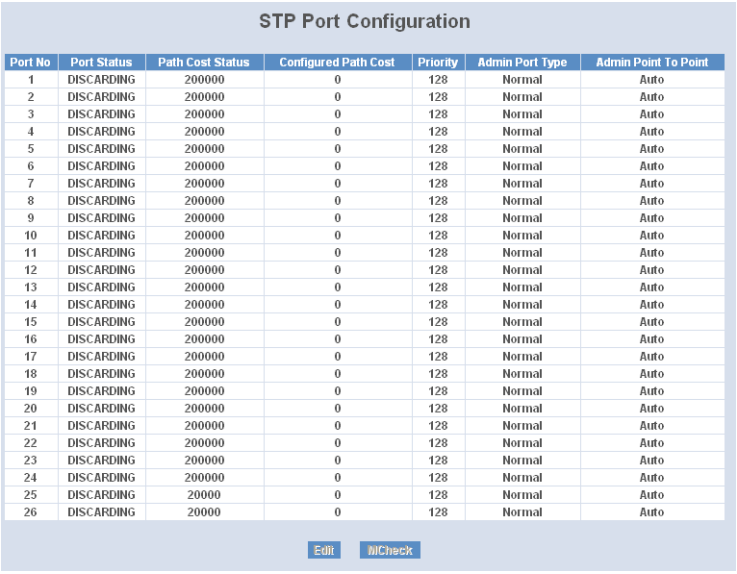
EN

Auto, it means RSTP will use the duplex mode resulted from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

Default: Auto

M Check:

Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click <M Check> button to send a RSTP BPDU from the port you specified.



Port No	Port Status	Path Cost Status	Configured Path Cost	Priority	Admin Port Type	Admin Point To Point
1	DISCARDING	200000	0	128	Normal	Auto
2	DISCARDING	200000	0	128	Normal	Auto
3	DISCARDING	200000	0	128	Normal	Auto
4	DISCARDING	200000	0	128	Normal	Auto
5	DISCARDING	200000	0	128	Normal	Auto
6	DISCARDING	200000	0	128	Normal	Auto
7	DISCARDING	200000	0	128	Normal	Auto
8	DISCARDING	200000	0	128	Normal	Auto
9	DISCARDING	200000	0	128	Normal	Auto
10	DISCARDING	200000	0	128	Normal	Auto
11	DISCARDING	200000	0	128	Normal	Auto
12	DISCARDING	200000	0	128	Normal	Auto
13	DISCARDING	200000	0	128	Normal	Auto
14	DISCARDING	200000	0	128	Normal	Auto
15	DISCARDING	200000	0	128	Normal	Auto
16	DISCARDING	200000	0	128	Normal	Auto
17	DISCARDING	200000	0	128	Normal	Auto
18	DISCARDING	200000	0	128	Normal	Auto
19	DISCARDING	200000	0	128	Normal	Auto
20	DISCARDING	200000	0	128	Normal	Auto
21	DISCARDING	200000	0	128	Normal	Auto
22	DISCARDING	200000	0	128	Normal	Auto
23	DISCARDING	200000	0	128	Normal	Auto
24	DISCARDING	200000	0	128	Normal	Auto
25	DISCARDING	20000	0	128	Normal	Auto
26	DISCARDING	20000	0	128	Normal	Auto

4.11 Trunk

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example,

if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

1. LACP:

   Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~3) to form a logic "trunked port". The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a "trunk group" (also called aggregator). LACP is safer than the other trunking method - static trunk.

   The switch LACP does not support the followings:

   - Link Aggregation across switches
   - Aggregation with non-IEEE 802.3 MAC link
   - Operating in half-duplex mode
   - Aggregate the ports with different data rates

2. Static Trunk:

   Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~3, this Static groupID can be the same with another LACP groupID) to form a logic "trunked port". The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a "logic trunked port". Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in "not ready" state when using static trunk to aggregate with high speed links.

   As to system restrictions about the port aggregation function on the switch, in the management point of view, the switch supports maximum 3 trunk groups for LACP and additional 3 trunk groups for Static Trunk. But in the system capability view, only 3 "real trunked" groups are supported. An LACP trunk group with more than one ready member-ports is a "real trunked" group. An LACP trunk group with only one or less than one ready member-ports is not a "real trunked" group. Any Static trunk group is a "real trunked" group.

EN

Per Trunking Group supports a maximum of 4 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports. Trunk Setting Rules are listed below:

Rule1:Maximum 3 groups are allowed

Rule 2: The members of each group cannot exceed more than 4 ports

Rule 3: Group 1 and 2 cannot exist member 25 and 26 port

Rule 4: Group 3 cannot exist member from 1 to 24 port

4.11.1 Port Setting/Status

Port setting/status is used to configure the trunk property of each and every port in the switch system.

- Parameter Description:
  - Method: This determines the method a port uses to aggregate with other ports.

    None: A port does not want to aggregate with any other port should choose this default setting.

    LACP: A port use LACP as its trunk method to get aggregated with other ports also using LACP.

    Static: A port use Static Trunk as its trunk method to get aggregated with other ports also using Static Trunk.
  - Group: Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 8) in order to declare that they wish to aggregate with each other.
  - Active LACP:

This field is only referenced when a port’s trunking method is LACP.

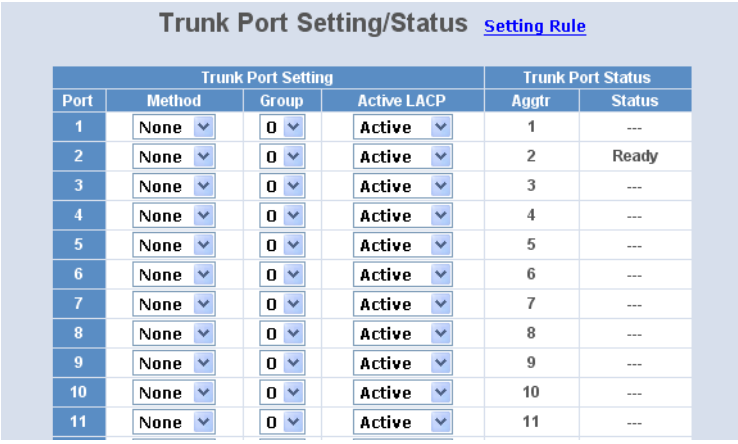
Active:

An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

- Aggtr: Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.
- Status: This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”



4.11.2 Aggregator View

To display the current port trunking information from the aggregator point of view.

- Parameter Description:
  - Aggregator: It shows the aggregator ID (from 1 to 26) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..
  - Method: Show the method a port uses to aggregate with other ports.
  - Member Ports: Show all member ports of an aggregator (port).

EN

- Ready Ports: Show only the ready member ports within an aggregator (port).

Aggregator View

Aggregator	Method	Member Ports	Ready Ports
1	None	1	
2	None	2	2
3	None	3	
4	None	4	
5	None	5	
6	None	6	
7	None	7	
8	None	8	
9	None	9	
10	None	10	
11	None	11	
12	None	12	
13	None	13	
14	None	14	
15	None	15	

4.11.3 LACP System Configuration

Show the detailed information of the LACP trunking group.

- Parameter Description:
  - Actor: The switch you are watching on.
  - Partner: The peer system from this aggregator's view.
  - System Priority: Show the System Priority part of a system ID.
  - MAC Address: Show the MAC Address part of a system ID.
  - Port: Show the port number part of an LACP port ID.
  - Key: Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.
  - Trunk Status: Show the trunk status of a single member port."---" means "not ready".

Zeigt Ihnen den Trunk-Status eines einzelnen Ports an. Dabei bedeutet "---" das der Port nicht bereit bzw. nicht aktiv ist.### Bild von einem Aggregator fehlt.

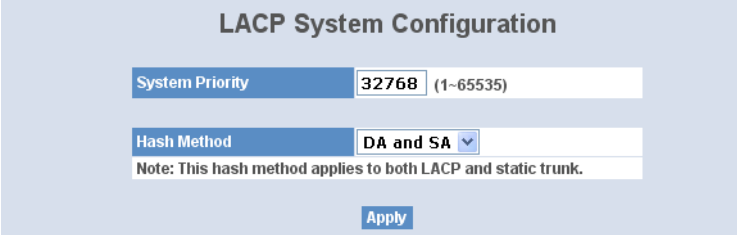
Aggregator 4 Information

Actor			Partner	
System Priority	MAC Address		System Priority	MAC Address
32768	00-a0-57-13-fa-7e		32768	00-00-00-00-00-00
Port	Key	Trunk Status	Port	Key
4	258	---	4	0

- Function name: LACP System Configuration

- Function Description: It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value.
- Parameter Description:
  - System Priority: The System Priority can be set by the user. Its range is from 1 to 65535. Default: 32768.
  - Hash Method: DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose.

    Default: DA and SA.



4.12 802.1x Configuration

802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through a 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from a 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server.

Supplicant:

EN

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

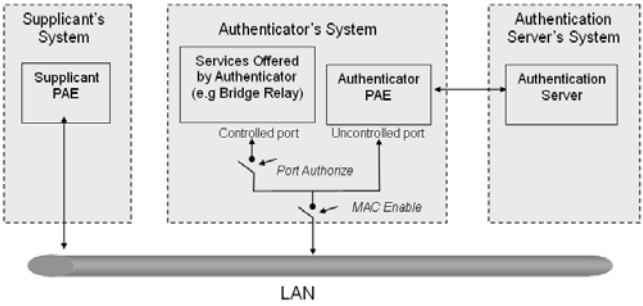
A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

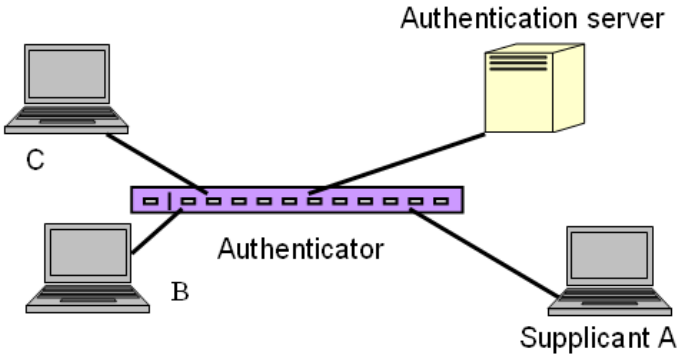
A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the following figure is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.



In this figure is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.



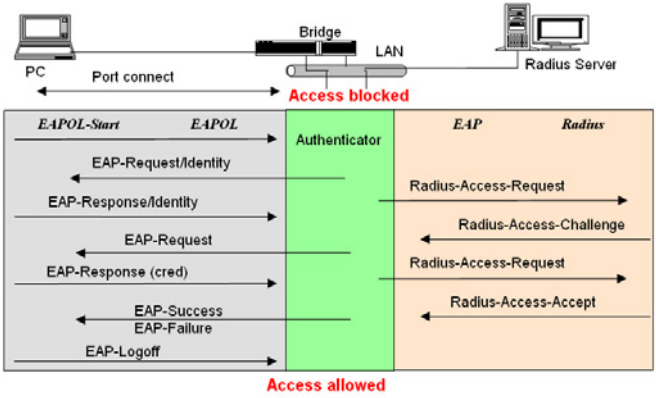
EN

The figure shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.
5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.
7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5 (Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm.
8. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.
9. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is

in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.

10 When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.



Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

EN

Port Mode	Port Control	Authentication	Port Status
Disable	Don't Care	Don't Care	Port Uncontrolled
Multihost	Auto	Successful	Port Authorized
Multihost	Auto	Failure	Port Unauthorized
Multihost	ForceUnauthorized	Don't Care	Port Unauthorized
Multihost	ForceAuthorized	Don't Care	Port Authorized

Table 3-3

802.1x State Setting

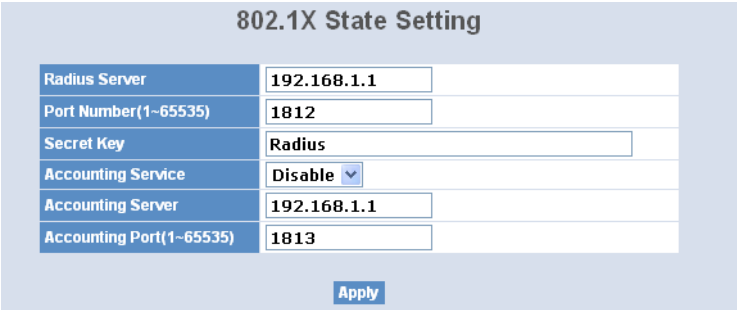
This function is used to configure the global parameters for RADIUS authentication in 802.1x port security application.

- Parameter Description:
  - Radius Server: RADIUS server IP address for authentication.

    Default: 192.168.1.1
  - Port Number: The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

    Default port number is 1812.
  - Secret Key: The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

    Default: Radius.



802.1x Mode Setting

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.

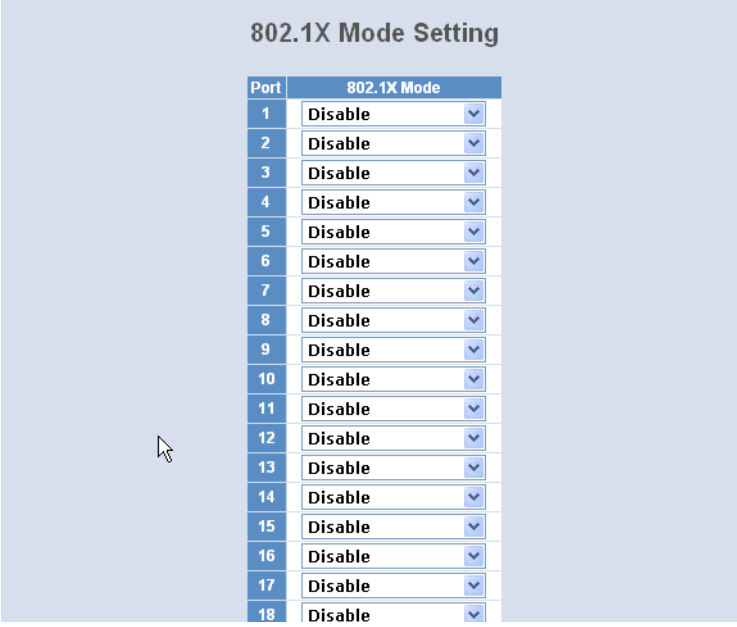
- Parameter Description:
  - Port Number: Indicate which port is selected to configure the 802.1x operation mode.
  - 802.1x Mode: 802.1x operation mode. There are two options, including Disable and Multi-host mode. Default is Disable.

    Disable:

    It will have the chosen port acting as a plain port, that is no 802.1x port access control works on the port.

    802.1x with Multi-host:

    In Multi-host mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.



EN

Port Security Management

Shows each port status. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

- Parameter Description:
  - Disable Mode: When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator. The Port Status will show the following screen.
  - Port Number:The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 26.
  - Port Status: The current 802.1X status of the port. In Disable mode, this field is Disabled.
  - 802.1x with Multihost mode: When selecting 802.1x with Multihost mode for a port in the function 802.1X Port Mode Configuration, Devices can access the network through this port once the authenticator is authorized. The Port Status will show the following screen. If

the port is granted to access the network, the port status is authorized, otherwise, unauthorized.

Param. Setting

- Function Description: This function is used to configure the parameters for each port in 802.1x port security application. Refer to the following parameters description for details.
- Parameter Description:
  - Port: It is the port number to be selected for configuring its associated 802.1x parameters which are Port control, reAuthMax, txPeriod, quietPeriod, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout, VlanAssignment, GuestVlan and AuthFailedVlan.

EN

- Port Control: This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

  ForceUnauthorized:

  The controlled port is forced to hold in the unauthorized state.

  ForceAuthorized:

  The controlled port is forced to hold in the authorized state.

  Auto:

  The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

  Default: Auto

- reAuthMax(1-10): The number of authentication attempt that is permitted before the port becomes unauthorized.

  Default: 2

- txPeriod(1-65535 s):A time period to transmitted EAPOL PDU between the authenticator and the supplicant.

  Default: 30

- Quiet Period(0-65535 s): A period of time during which we will not attempt to access the supplicant.

  Deafult: 60 seconds

- reAuthEnabled: Choose whether re-authentication will take place in this port.

  Default: ON

- reAuthPeriod(1-65535 s): A non-zero number seconds between the periodic re-authentication of the supplicant.

  Default: 3600

- max. Request(1-10): The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

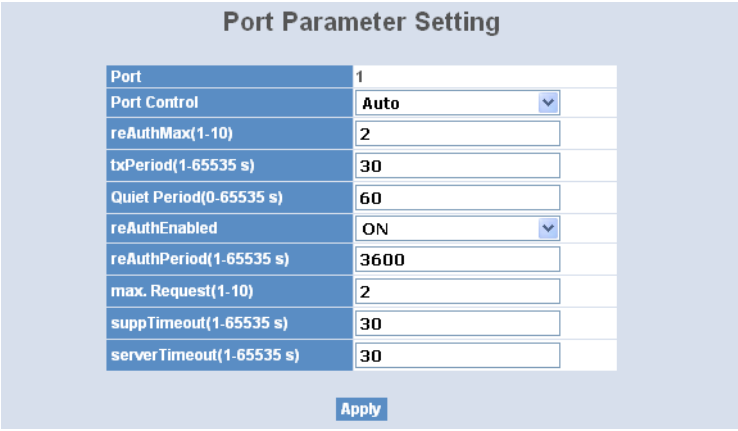
  Default: 2 times

- suppTimeout(1-65535 s): A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 – 65535.

Default: 30 seconds.

- serverTimeout(1-65535 s): A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

  Default: 30 seconds



4.13 TACACS+

4.13.1 Introduction

TACACS+ (Terminal Access Controller Access-Control System) is a protocol for authentication, authorization and accounting (AAA). It thus provides access to the network for authorized users only, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

TACACS+ is required in order to meet with PCI compliance (Payment Card Industry).

Modern networks with their numerous services and network components present a massive challenge in terms of controlling user access rights. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a

Network Access Server (NAS): It does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an accept or a reject.

EN

TACACS+ is configured with the following parameters:

4.13.2 State

Configures the TACACS+ server and sets the password for the encryption of data communications with the TACACS+ protocol.

- Server 1: Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

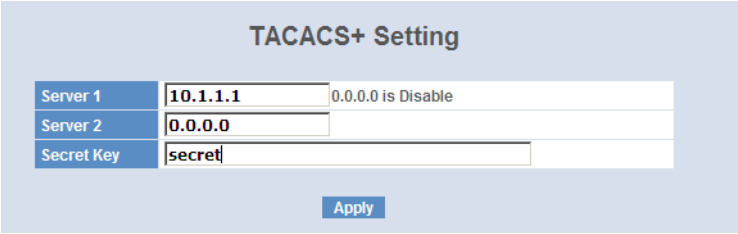
  The value 0.0.0.0 deactivates this entry.

- Server 2: You can optionally configure a second TACACS+ server address here. If the first TACACS+ server is not available and the maximum number of failed login attempts is reached, the device forwards its login requests to the alternative TACACS+ server. The maximum number of failed login attempts is set as the "Access retry" value under the "Access" menu item.

  The value 0.0.0.0 deactivates this entry.

- Secret key: The password for encrypting the communications between NAS and TACACS+ servers.

The password must be entered identically into the LANCOM and the TACACS+ server. We recommend that you do not operate TACACS+ without encryption.



You can choose the TACACS+ server manually. Enter your username, a colon and the number of the TACACS+ server in the login field to choose one of the two servers defined in the TACACs+ settings. For example, if your username is 'admin' and you want to fix TACACS+ server 2 for authentication, enter 'admin:2' in the login field.

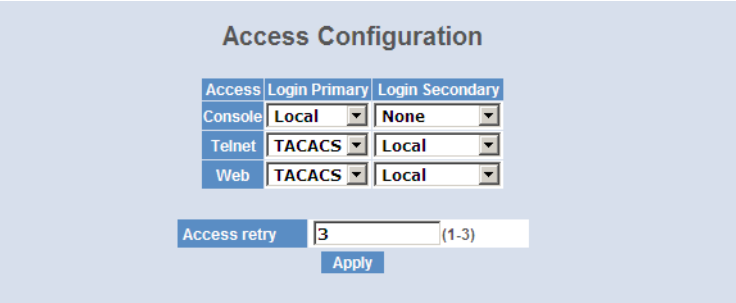
4.13.3 Authentication

The device for configuration can be accessed via the serial interface (console), via the LAN with Telnet or SSH, or with a browser. Access authentication for each of these three access methods can be individually set up either to refer to the user accounts in the device itself, or to the the user accounts on the TACACS+ server. A second login option can be defined in case access authentication fails several times for the selected user account.

- Login primary: "TACACS" for login via the TACACS+ server, "Local" for login using the local user accounts.
- Login secondary: "TACACS" and "Local", as above. The only value available here is the one not selected under 'Login primary". With the additional option "None", the secondary login can be deactivated.

The fallback to local user accounts presents a security risk if no root password is set. For this reason, TACACS+ authentication with fall-back to local user accounts can only be activated if a root password has been set.

- Access retry: Defines the number of login failures before switching to the secondary login option. If TACACS+ is set as the "Login primary", then the defined number of login failures are followed by an attempt to use the secondary TACACS+ server. Only in the event that the maximum number of login failures occurs for this server too, does the option set under "Login secondary" come into effect.



4.13.4 Authorization

- State: Activates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server. On the TACACS+ server, authorization can be defined separately for each of the configuration groups:

The authorization for the following commands can be defined separately in the TACACS+ server:

- 802.1X
- Account
- Alarm
- Autologout
- Bandwidth
- Config-file
- DHCP-boot
- Diagnostics
- Firmware
- GVRP
- Hostname
- IGMP-Snooping
- IP
- Log
- Loop detection
- MAC-table
- Management

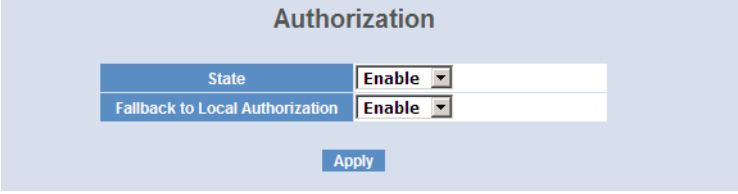
- Port
- QoS
- Reboot
- Security
- SNMP
- STP
- System
- TACACS+
- TFTP
- Time
- Trunk
- VLAN
- Virtual Stack.

The arguments “show” and “set” can be permitted or restricted separately for each command.

For the admin account all undefined commands must be permitted, e.g. using the "Permit Unmatched Commands" and "Permit Unmatched Args" options in the TACACS+ server configuration.

TACACS+ authorization will only activate if the defined TACACS+ server is available.
If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights must be defined in the TACACS+ server.
Here, rights are granted at the top menu level – this means, for example, that the complete configuration area "Account" can be allowed or blocked for a user.

- Fallback to local authorization: Activates the fallback to local authorization if the TACACS+ login should fail.

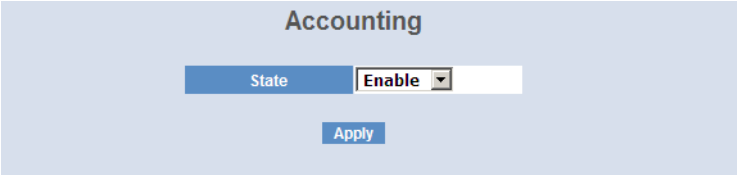


EN

4.13.5 Accounting

- State: Activates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server.

TACACS+ accounting will only activate if the defined TACACS+ server is available.



Please note that when using Telnet or the Web interface for the configuration, different entries may be found in the accounting for the same configuration. If, for example, the values for "Location", "Contact" and "Device name" are reset with Telnet, the accounting server lists three actions. With the Web interface, the three values are located on a single page, and changing these results in just one entry to the accounting.

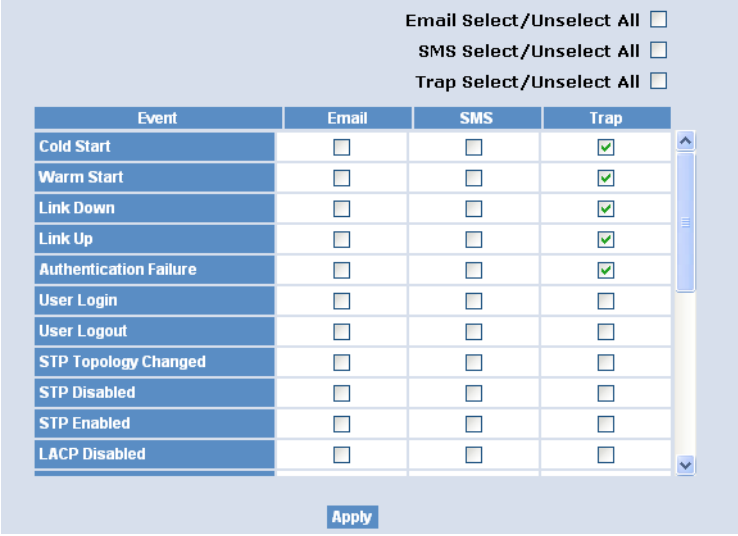
4.14 Alarm Configuration

4.14.1 Events

The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred. The switch offers 22 different trap events to users for switch management. The trap information can be sent out in three ways, including email, mobile phone SMS (short message system) and trap. The message will be sent while users tick (ž) the trap event individually on the web page shown as below.

- Parameter Description:
  - Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout
  - STP: STP Topology Changed, STP Disabled, STP Enabled
  - LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure
  - GVRP: GVRP Disabled, GVRP Enabled

- VLAN: Port-based VLAN Enabled, Tag-based VLAN Enabled
- Module Swap: Module Inserted, Module Removed, Dual Media Swapped
- PoE: PoE Failure



4.14.2 E-Mail

Alarm configuration is used to configure the persons who should receive the alarm message via email. It depends on your settings. An email address has to be set in the web page of alarm configuration. Then, user can read the trap information from the email. This function provides 6 email addresses at most. The 22 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses numbers. Then, please click <Apply> button to complete the alarm configuration. It will take effect in a few seconds.

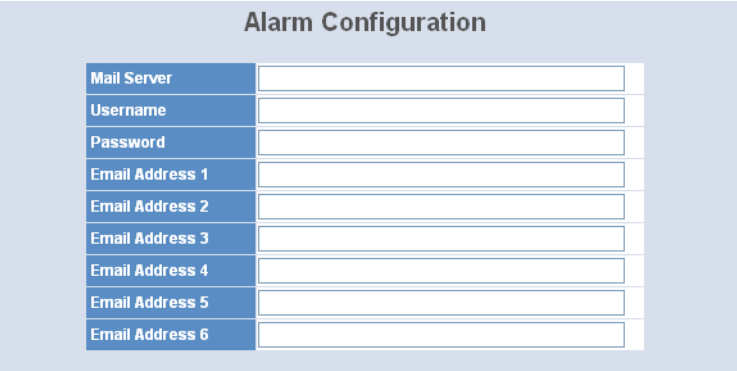
- Parameter Description:
  - Email:

    Mail Server: the IP address of the server transferring your email.

    Username: your username on the mail server.

    Password: your password on the mail server.

    Email Address 1 – 6: email address that would like to receive the alarm message.



EN

4.15 Configuration

4.15.1 Save/Restore

Here you can configure the settings for saving and restoring device configurations. For further information read the 'Save/Restore" section in the chapter 'Configuring and monitoring the LANCOM switch'.

4.15.2 Config file

Here you can save and restore backups of device configurations. For further information read the 'Config File' section in the chapter 'Configuring and monitoring the LANCOM switch'.

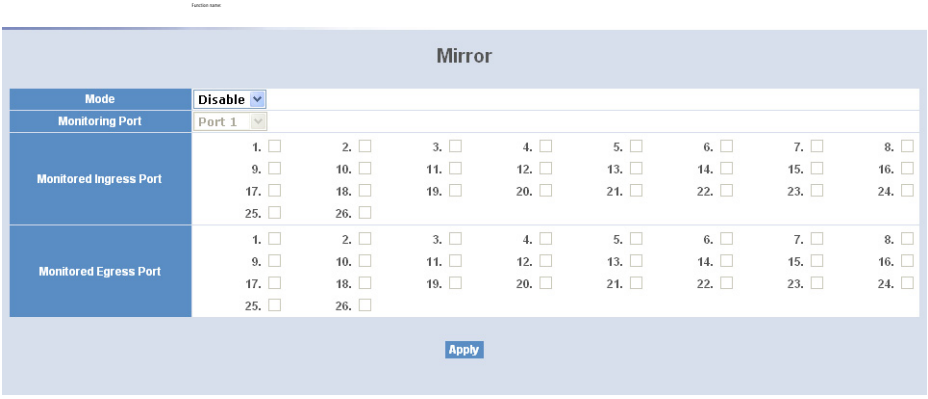
4.16 Security

4.16.1 Mirror Configuration

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.

- Parameter Description:
  - Mode: Used for the activation or de-activation of Port Mirror function. Default is disable.
  - Monitoring Port: Set up the port for monitoring. Valid port is Port 1~26 and default is Port 1.

- Monitored Ingress Port: Set up the port for being monitored. It only monitor the packets received by the port you set up. Just tick the check box (ž) beside the port x and valid port is Port 1~26.
- Monitored Egress Port: Set up the port for being monitored. It only monitor the packets transmitted by the port you set up. Just tick the check box (ž) beside the port x and valid port is Port 1~26.

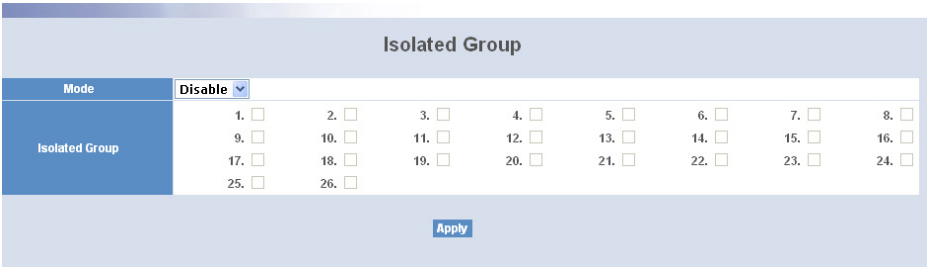


4.16.2 Isolated Group

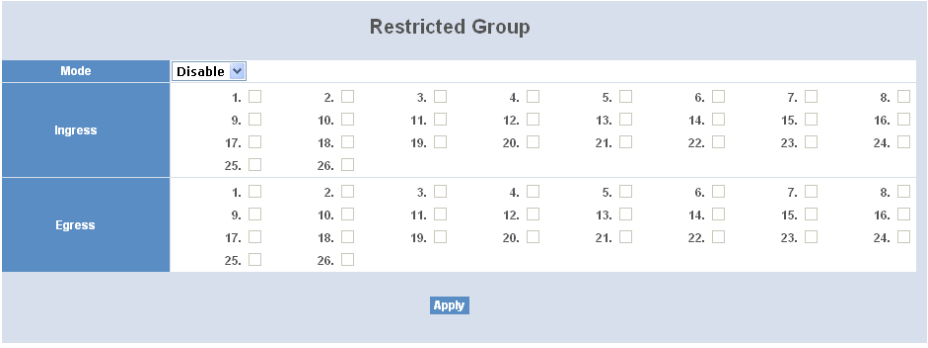
Isolated Group function can let the port be independent of other ports in the Isolated group, and the communication is also forbidden between these ports. But, the ports of the Isolated group are still able to communicate with the ports of the non-Isolated group. With this design, it will be helpful to the administrator to immediately find and solve the port that results in the occurrence of looping problems in the network.

- Parameter Description:
  - Mode: Used for the activation or de-activation of Isolated Group function. Default is disable
  - Isolated Group: User can choose any port to be the member of this group. Just tick the check box (ž) beside the port x and valid port is Port 1~26. In this group, all of these member ports cannot forward packets with each other. Thus, the switch will not be capable of for-

warding any packets in case its all ports become the members of the Isolated group.



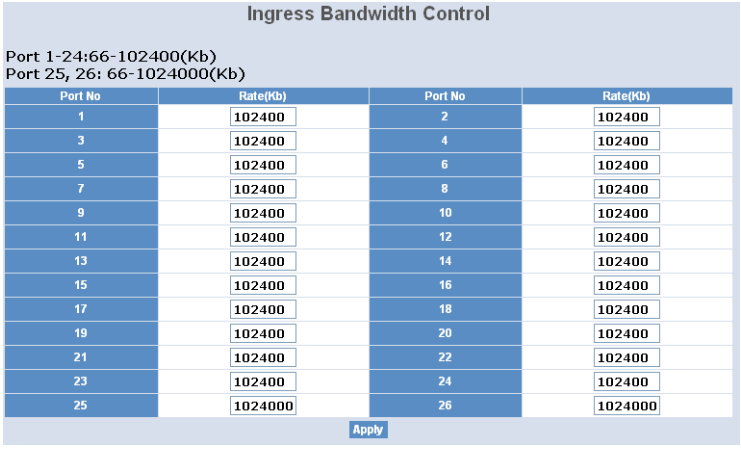
- Restricted Group
- Function Description: The function of the Restricted Group can decide the direction of transmitting packets for the specific port. The packets received by the port with the "Ingress" mode of Restricted Group will be sent to the ports with the "Egress" mode of Restricted Group.
- Parameter Description:
  - Mode: Used for the activation or de-activation of Restricted Group function. Default is disable.
  - Ingress: Select the ports that you would like their Restricted Group to set into "Ingress" mode. Just tick the check box beside the port x and valid port is Port 1~26.
  - Egress: Select the ports that you would like their Restricted Group to set into "Egress" mode. Just tick the check box beside the port x and valid port is Port 1~26.



4.17 Bandwidth Management

4.17.1 Ingress Bandwidth Setting

Ingress Bandwidth Setting function is used to set up the limit of Ingress bandwidth for each port.

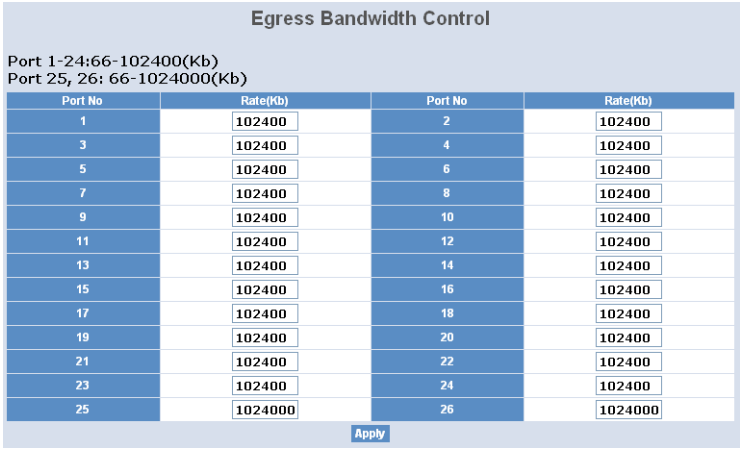


- Parameter Description:
  - Port No.: Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
  - Rate: Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

EN

4.17.2 Egress Bandwidth Setting

Egress Bandwidth Setting function is used to set up the limit of Egress bandwidth for each port.



- Parameter Description:
  - Port No.: Choose the port that you would like this function to work on it. Valid range of the port is 1~26.
  - Rate: Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~24 ranges from 66~102400, and Port 25~26 ranges from 66~1024000 with the minimum unit of 1. Default value of Port 1~24 is 102400 and Port 25~26 is 1024000.

4.17.3 Storm Setting

With the storm control one can set a common limit for the permitted percentage of the broadcast, multicast and unicast packets in comparison to the whole data traffic. If this limit is reached, the data packets of the corresponding type are discarded. The storm control can be activated separately for the different packet types.

- Parameter Description:
  - Storm Type:

    Disable: Disable the function of the bandwidth storm control.

    Broadcast Storm Control: Enable the function of bandwidth storm control for broadcast packets.

    Multicast Storm Control: Enable the function of bandwidth storm control for multicast packets.

    Unknown Unicast Storm Control: Enable the function of bandwidth storm control for unknown unicast packets. These packets are the MAC address that had not completed the learning process yet.

    Broadcast, Multicast, Unknown Unicast Storm Control: Enable the function of bandwidth storm control for all packets in transmission.

  - Storm Rate : Set up the limit of bandwidth for the storm control. With a storm rate of 15%, all data packets activated for storm control are discarded, if the percentage of broadcast, multicast or unicast packets exceeds 15% of the ports maximum bandwidth (e.g. 15 mbps on a 100 mbps port). Valid value of the storm rate ranges from 1-100 with the minimum unit of 1. And only integer is acceptable. Default is 100.

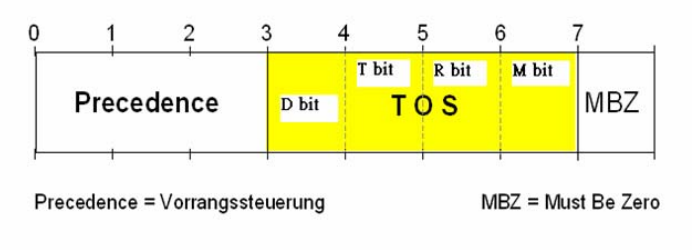
4.18 QoS (Quality of Service) Configuration

The switch supports 5 kinds of QoS, are as follows, MAC Priority, 802.1p Priority, IP TOS Priority, and DiffServ DSCP Priority. Port Based Priority has a special name called VIP Port in the switch. Any packets enter VIP Port will have highest transmitting priority. MAC Priority act on the destination address of MAC in packets. VLAN tagged Priority field is effected by 802.1p Priority setting. IP TOS Priority affects TOS fields of IP header, and you can find it has 8-

EN

bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED (1bit).

User can randomly control these fields to achieve some special QoS goals. When bits D, T, R, or M set, the D bit requests low delay, the T bit requests high throughput, the R bit requests high reliability, and the M bit requests low cost.



DiffServ DSCP Priority act on DSCP field of IP Header. In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

High Priority Packet streams will experience less delay into the switch. For handing different priority packets, each egress port has designed up to 4 queues. Each QoS is influenced by two scheduling, WRR (Weighted Round Robin) and Strict Priority as well. When you finish to set the priority mapping to the queue, WRR scheduling will distribute the bandwidth according to the weight you set for 4 queues (queue 0 to queue 3). Another scheduling is Strict Priority dedicated for the function named VIP Port of QoS. While we select some ports as the VIP Port, these ports will own the highest transmitting priority in egress queue of the switch.

The QoS functions as we mentioned above are able to enabled at the same time. But, the following precedence will decide whether these functions work or not.

1. enable both VIP and TOS

   Choose priorities of VIP and TOS.

2. enable both VIP and DSCP

   Choose priorities of VIP and DSCP.

3. enable both TOS and DSCP

   Choose "DSCP".

4. enable both VIP and DSCP

   Choose priorities of VIP and DSCP.

5. enable both 802.1p and TOS

   Choose "TOS".

6. enable both 802.1p and DSCP

   Choose "DSCP".

7. enable both 802.1p and DSCP and TOS

   Choose "DSCP".

8. enable both 802.1p and DSCP and TOS and VIP

   Choose priorities of VIP and DSCP.

   VIP/DSCP > TOS > 802.1p (Final result)

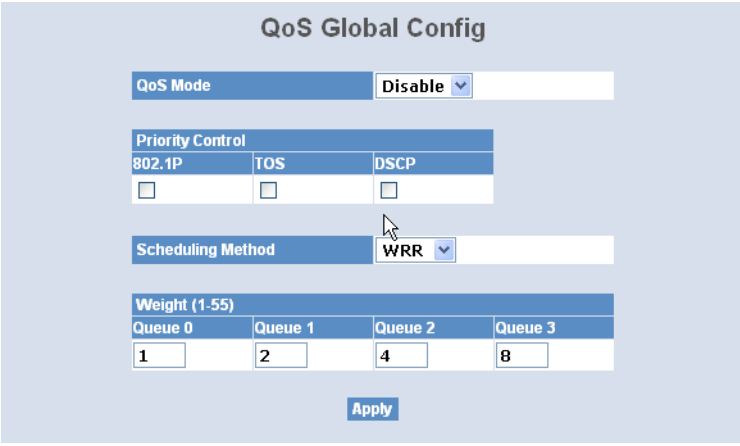
4.18.1 QoS Global Setting

When you want to use QoS function, please enable QoS Mode in advance. Then you can use MAC Priority, 802.1p Priority, IP TOS Priority, DiffServ DSCP Priority, or VIP Port functions and take effect. In this function, you can Enable QoS Mode. Choose any of Priority Control, such as 802.1p, TOS, DSCP. Moreover, you can select Scheduling Method of WRR (Weighted Round Robin) or Strict Priority. Next, you can arrange Weight values for queue 0 to queue 3.

- Parameter Description:
  - QoS Mode: You can Enable QoS Mode and let QoS function become effective. Default is Disable.
  - Priority Control:Just tick the check box (ž) of 802.1P, TOS, or DSCP Qos and click Apply button to be in operation.
  - Scheduling Method: There are two Scheduling Method, WRR and Strict Priority. Default is WRR. After you choose any of Scheduling Method, please click Apply button to be in operation.

EN

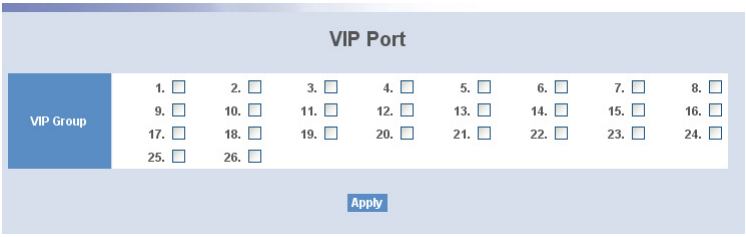
- Weight (1~55): Over here, you can make an arrangement to Weight values of Queue 0 to Queue 3. The range of Weight you can set is 1~55. In default, the weight of Queue 0 is 1, the weight of Queue 1 is 2, the weight of Queue 2 is 4, and the weight of Queue 3 is 8.



4.18.2 VIP Port Setting

When the port is set as VIP Port, the packets enter this port and will have highest transmitting priority. For example, as you choose port 2 is VIP Port, simultaneously transmit packets from port 2 and port 3 to port 1 at speed of 100MB and let congestion happen. The packets for port 3 will be dropped because the packets from port 2 owns highest precedence. For the sake of this function taking effect, you must choose Scheduling Method of Strict Priority ahead.

- Parameter Description:
  - VIP Port: Just tick the check box (ž) to select any port(port 1~26) as the VIP Port. Then, click the <Apply> button to have the setting taken effect.

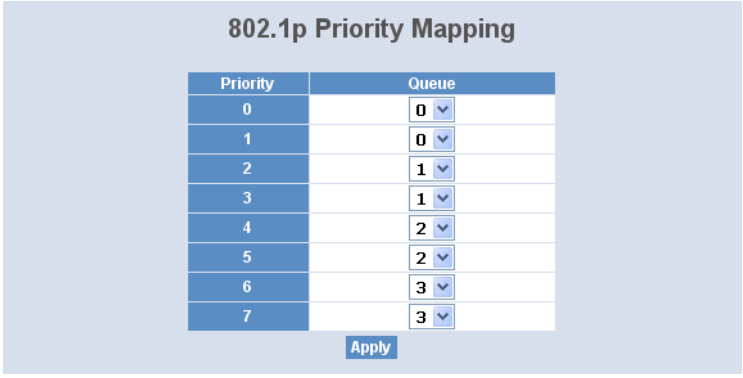


EN

4.18.3 802.1p Setting

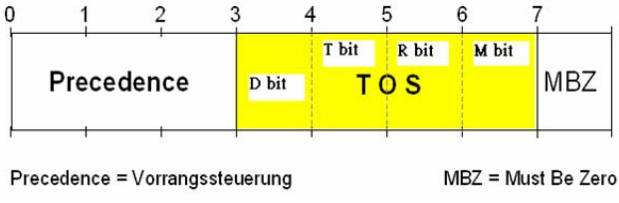
This function will affect the priority of VLAN tag. Based on priority of VLAN tag, it can arrange 0~8 priorities, priorities can map to 4 queues of the switch (queue 0~3) and possess different bandwidth distribution according to your weight setting.

- Parameter Description:
  - 802.1p Priority Mapping: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.



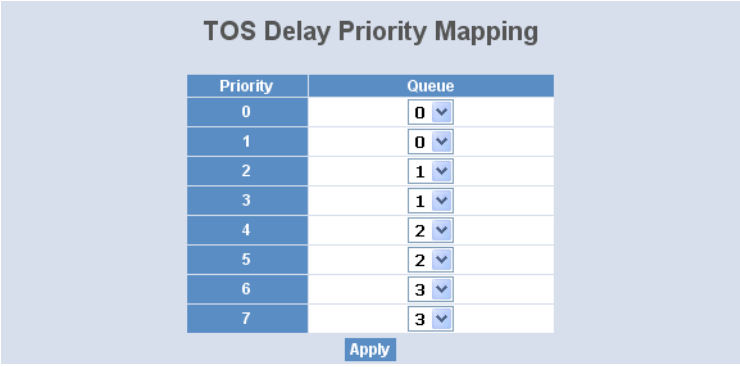
4.18.4 D-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Delay Priority Mapping works while D-TYPE in TOS field of IP header of the packets received by the switch is configured.



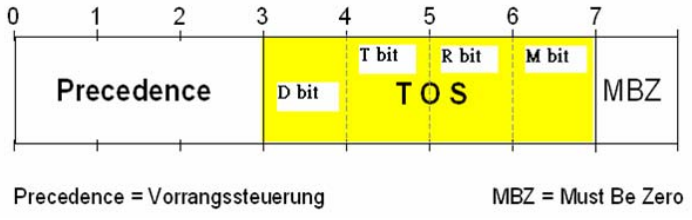
EN

- Parameter Description:
  - TOS Delay Priority Mapping: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.



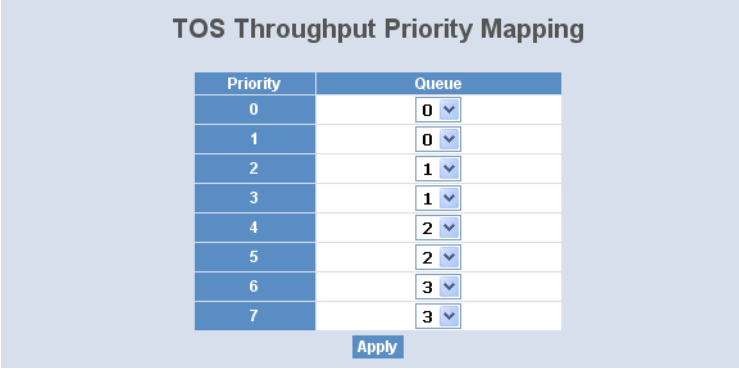
4.18.5 T-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Throughput Priority Mapping works while T-TYPE in TOS field of IP header of the packets received by the switch is configured.



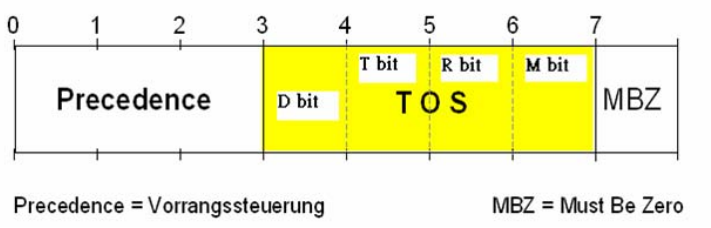
EN

- Parameter Description:
  - TOS Throughput Priority Mapping: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.



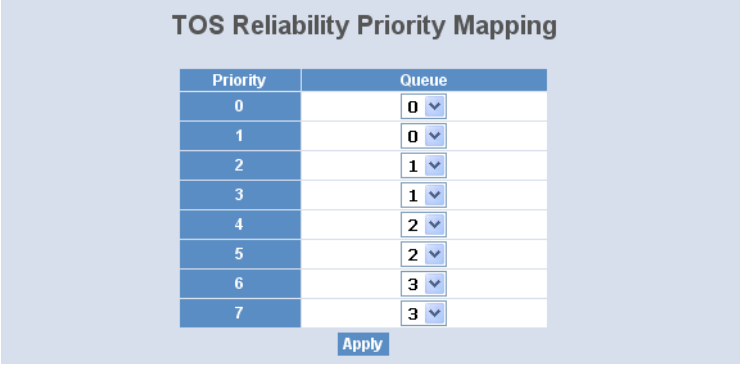
4.18.6 R-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Reliability Priority Mapping works while R-TYPE in TOS field of IP header of the packets received by the switch is configured.



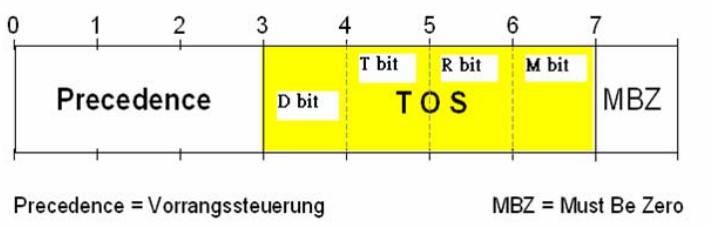
EN

- Parameter Description:
  - TOS Reliability Priority Mapping: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.



4.18.7 M-Type TOS

IP TOS Priority affect TOS fields of IP header, you can find it has 8-bit SERVICE TYPE field that specifies how the datagram should be handled. The field could be divided into six subfields as follows, PRECEDENCE (3 bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1bit), R-Type (Reliability Priority, 1bit), M-Type (Monetary Cost Priority, 1bit), and UNUSED. PRECEDENCE 3-bits can arrange 8 kinds of priorities corresponding to the 0~7 priority in the following priority diagram. TOS Monetary Cost Priority Mapping works while M-TYPE in TOS field of IP header of the packets received by the switch is configured.



EN

- Parameter Description:
  - TOS Monetary Cost Priority Mapping: Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 0 is mapping to Queue 3.

DSCP Priority Mapping

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

Apply

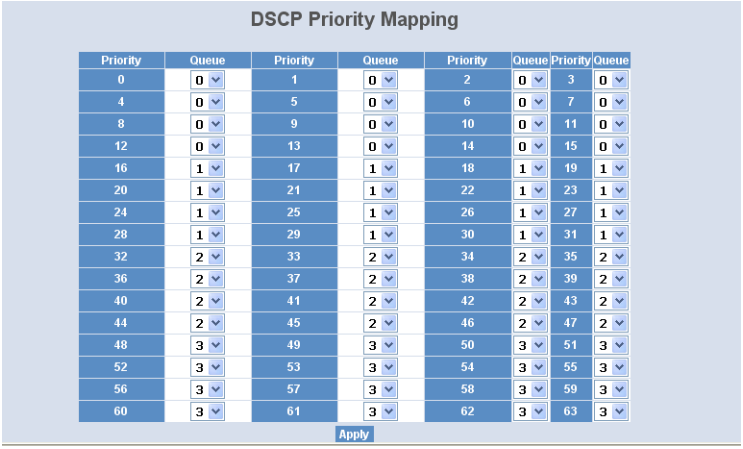
4.18.8 DSCP Setting

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue 0~3.

EN

- Parameter Description:
  - DSCP Priority Mapping: 64 kinds of priority traffic as mentioned above, user can set up any of Queue 0~3. In default, Priority 0~15 are mapping to Queue 0, Priority 16~31 are mapping to Queue 1, Priority 32~47 are mapping to Queue 0, Priority 48~63 are mapping to Queue 0.



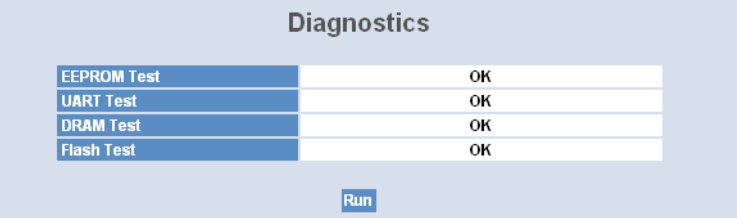
4.19 Diagnostics

Three functions, including Diagnostics, Loopback Test and Ping Test are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.

4.19.1 Diag

Diagnostics

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.



EN

4.19.2 Loopback

- Function name: Loopback Test

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.

Loopback Test

Port No	Internal Loopback	External Loopback
1	OK	Fail
2	OK	OK
3	OK	Fail
4	OK	Fail
5	OK	Fail
6	OK	Fail
7	OK	Fail
8	OK	Fail
9	OK	Fail
10	OK	Fail
11	OK	Fail
12	OK	Fail
13	OK	Fail
14	OK	Fail
15	OK	Fail
16	OK	Fail
17	OK	Fail
18	OK	Fail
19	OK	Fail
20	OK	Fail
21	OK	Fail
22	OK	Fail
23	OK	Fail
24	OK	Fail
25	OK	Fail
26	OK	Fail

Run Again

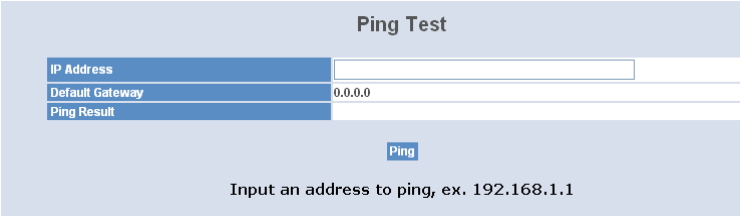
EN

4.19.3 Ping

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click <Ping> button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

- Parameter Description:
  - IP Address: An IP address with the version of v4, e.g. 192.168.1.1.
  - Default Gateway: IP address of the default gateway.

    For more details, please see the section of IP address in Chapter 2.



4.19.4 Watchdog

Watchdog function is a tool for detecting if the target device is alive or not through supports to ping one host IP address. It can be configured via web UI, CLI and SNMP. It supports continuing ping failed times counter setting.

If only one time Ping successful, then all Ping Failed Counter will reset to zero and re-account.

- Parameter
  - State:

    To enable or disable the watchdog function. Default is disable
  - Time Gap:

    To support the time gap for ping test.
  - Host

    To support to ping one host IP address. You need to configure one host IP address which you want to ping it.

- Reset the management CPU Interface:

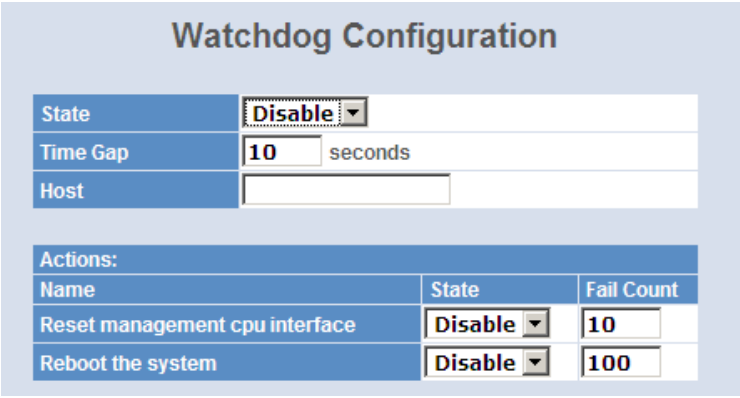
  When ping failure time reach configured value then switch will reset the managed switch's CPU interface. Default state is disable.

  Fail Count: Default Ping Failed Count= 10, Range for Setting: 1~20

- Reboot the system:

  When ping failure time reach configured value then switch will reboot automatically. Default state is disable.

  Fail Count: Default Ping Failed Count= 100, Range for Setting: 1~1000



4.20 TFTP Server

The settings for the TFTP server are located here. The device features an internal TFTP server and it offers the option of connecting to an external TFTP server.

If you specify an external TFTP server, you can save log files from the device to it, backup and restore device configurations, and you can upload new firmware to the device from the external TFTP server. This is only possible if you are logged in to the device with a user name and password.

You can activate the internal TFTP server if you wish to use LANconfig to update your device firmware and save/restore device configurations.

LANconfig provides access to the internal TFTP server without requiring a user name and password, which actually present a security loophole. You can deactivate it in order to prevent unauthorized users

from using LANconfig to gain access to the configuration management and perform firmware updates.

Information about managing configurations and firmware is available in the sections 'Config File' and 'Save/Restore' in the chapter 'Configuring and monitoring the LANCOM switch'.

EN

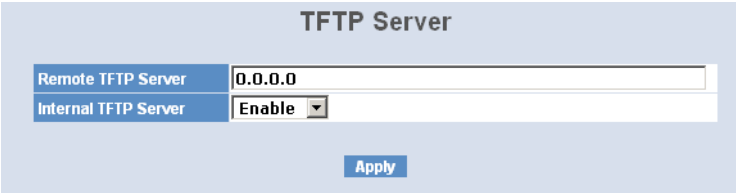
- Parameter:
  - Remote TFTP Server:

    Enter the IP address of the external TFTP server here.
  - Internal TFTP Server:

    Enable or disable the internal TFTP server here.

    Possible values: Enable, Disable

    Default: Enable



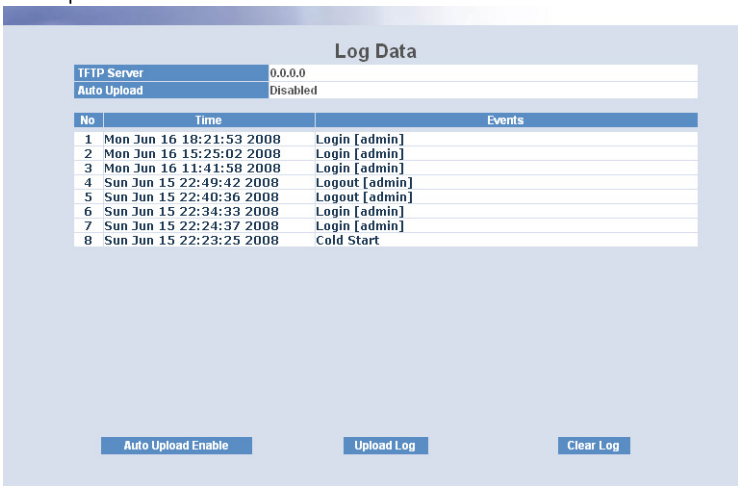
4.21 Log

This function shows the log data. The switch provides system log data for users. There are 17 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Trap/Alarm Configuration and SNMP Configuration.

Log Data

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In

the report table, No., Time and Events are three fields contained in each trap record.



- Parameter Description:
  - No.: Display the order number that the trap happened.
  - Time: Display the time that the trap happened.
  - Events:Display the trap event name.
  - Auto Upload Enable: Switch the enabled or disabled status of the auto upload function.
  - Upload Log: Upload log data through tftp.
  - Clear Log: Clear log data.

4.22 Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

Firmware Upgrade

- Function Description: The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

  1. Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in.

EN

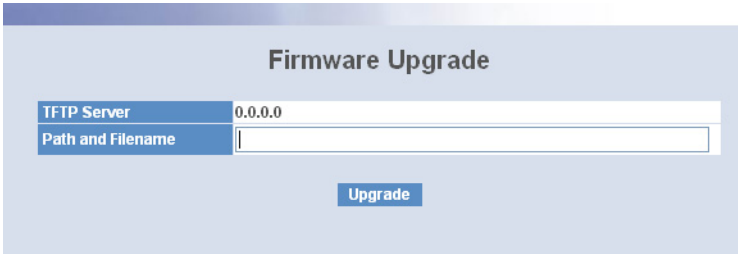
2. Specifying what the filename and where the file is. You must specify full path and filename.

Then, press <Upgrade> button if your download is not successful, the switch will also be back to "Software Upgrade", and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.

- Parameter Description:
  - TFTP Server: A TFTP server stored the image file you want to upgrade.
  - Path and Filename: File path and filename stored the image file you want to upgrade.



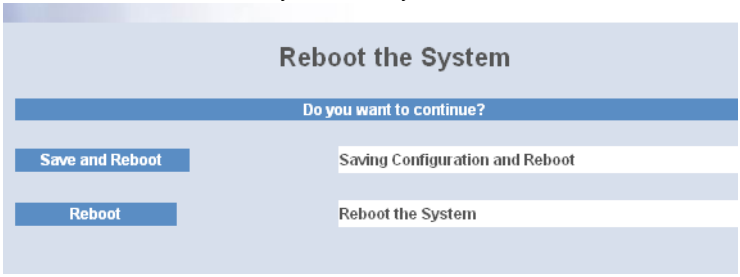
4.23 Reboot

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration taken effect. Here we are discussing is software reset for the "reboot" in the main menu.

Reboot

- Function Description: Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.
- Parameter Description:

- Save and Reboot:Save the current settings as start configuration before rebooting the switch.
- Reboot: Reboot the system directly.

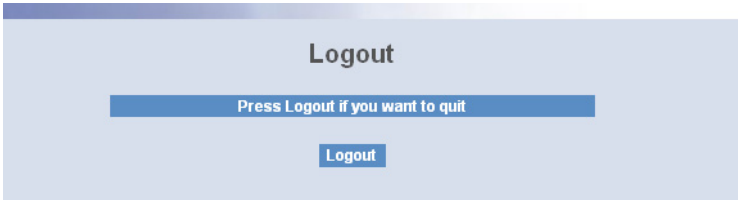


4.24 Logout

You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

Logout

- Function Description: The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the <Auto Logout> list at the left-top corner to explicitly ON/OFF this logout function.
- Parameter Description:
  - Auto Logout: Default is ON. If it is "ON", and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically.



5 Operation of CLI Management (englisch)

5.1 CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

-- Locate the correct DB-9 null modem cable with female DB-9 connector. Null modem cable comes with the management switch. Refer to the Appendix B for null modem cable configuration.

-- Attach the DB-9 female connector to the male DB-9 serial port connector on the Management board.

-- Attach the other end of the DB-9 cable to an ASCII terminal emulator or PC Com-1, 2 port. For example, PC runs Microsoft Windows HyperTerminal utility.

-- At "Com Port Properties" Menu, configure the parameters as below: (see the next section)

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

5.1.1 Login

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default values of the managed switch are listed below:

Username: admin

Password: admin

After you login successfully, the prompt will be shown as "**#**" if you are the first login person and your authorization is administrator; otherwise it may show "**$**". See the following two figures. The former means you behave as an administrator and have the access right of the system. As to the latter, it means you behave as a guest and are only allowed to view the system without the permission to do any setting for this switch.

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C#
```

Fig. 4-1

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C$
```

Fig. 4-2

5.2 Commands of CLI

```
Managed Switch - PSES-2126C

Login: admin
Password:

PSES-2126C# ?
  802.1X                Enter into 802.1X mode
  account               Enter into account mode
  alarm                 Enter into alarm mode
  autologout            Change autologout time
  bandwidth             Enter into bandwidth mode
  config-file           Enter into config file mode
  dhcp-boot             Enter into dhcp-boot mode
  diag                  Enter into diag mode
  firmware              Enter into firmware mode
  gvrp                  Enter into gvrp mode
  hostname              Change hostname
  igmp-snooping         Enter into igmp mode
  ip                    Enter into ip mode
  log                   Enter into log mode
  mac-table             Enter into mac table mode
  management            Enter into management mode
  poe                   Enter into PoE function
  port                  Enter into port mode
```

Fig. 4-3

5.2.1 Global Commands of CLI

- **end**
  - Syntax:

    end
  - Description:

    Back to the top mode.

    When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+# alarm
ES-2126+(alarm)# events
ES-2126+(alarm-events)# end
ES-2126+#
```

- **exit**
  - Syntax:

    exit
  - Description:

    Back to the previous mode.

    When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+# trunk
```

```
ES-2126+(trunk)# exit
ES-2126+#
```

- **help**
  - Syntax:

help

  - Description:

To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+# ip
ES-2126+(ip)# help
Commands available:
  ------------<< Local commands >>------------
  set ip                Set ip and gateway
  set dns               Set dns
  enable dhcp           Enable DHCP, and set dns auto or
manual
  disable dhcp          Disable DHCP
  show                  Show IP Configuration
  ------------<< Global commands >>------------
  exit                  Back to the previous mode
  end                   Back to the top mode
  help                  Show available commands
  history                 Show a list of previously run
commands
```

```
  logout                Logout the system
  save start            Save as start config
  save user             Save as user config
  restore default       Restore default config
  restore user          Restore user config
ES-2126+(ip)#
```

■ **history**

□ Syntax:

history [#]

□ Description:

To show a list of previous commands that you had ever run.

When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.

□ Argument:

[#]: show last number of history records. (optional)

□ Possible value:

[#]: 1, 2, 3, …., 256

□ Example:

```
ES-2126+(ip)# history
 Command history:
  0. ?
  1. trunk
  2. exit
  3. ES-2126+# trunk
  4. ES-2126+(trunk)# exit
  5. ES-2126+#
  6. trunk
  7. exit
  8. alarm
```

```
 9. events
10. end
11. ip
12. help
13. history
ES-2126+(ip)# history 3
 Command history:
12. help
13. history
14. history 3
ES-2126+(ip)#
```

- **logout**
  - Syntax:

    logout
  - Description:

    When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+# logout
    ```
- **restore default**
  - Syntax:

    restore default
  - Description:

    When you use this function in CLI, the system will show you the information "Do you want to restore the default IP address?(y/n)". If you choose Y or y, the IP address will restore to default "192.168.1.1". If you

choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.
```

- **restore user**
  - Syntax:

restore user

  - Description:

To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+# restore user
```

```
Restoring ...

Restore User Configuration Successfully

Press any key to reboot system.
```

- **save start**
  - Syntax:

save start

  - Description:

To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command 'save start'.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+# save start

Saving start...

Save Successfully

ES-2126+#
```

- **save user**
  - Syntax:

save user

  - Description:

To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+# save user
```

```
Saving user...
Save Successfully
ES-2126+#
```

5.2.2 Local Commands of CLI

DE

Please note: to use one of the local commands, you first have to change to the corresponding configuration area, e.g. `802.1x <Enter> set mode 1`.

802.1x

- **set max-request**
  - Syntax:

    set max-request <port-range> <times>
  - Description:

    The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.
  - Argument:

    <port range>: syntax 1,5-7, available from 1 to 26

    <times>: max-times, range 1-10
  - Possible value:

    <port range> : 1 to 26

    <times> : 1-10, default is 2
  - Example:

    `ES-2126+(802.1x)# set max-request 2 2`
- **set mode**
  - Syntax:

    set mode <port-range> <mode>
  - Description:

    To set up the 802.1X authentication mode of each port.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <mode> : set up 802.1x mode

    0:disable the 802.1x function

1:set 802.1x to Multi-host mode

- Possible value:

<port range> : 1 to 26

<mode>: 0 or 1

- Example:

```
ES-2126+(802.1x)# set mode 2 1
```

- **set port-control**
  - Syntax:

set port-control <port-range> <authorized>

  - Description:

To set up 802.1X status of each port.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<authorized> : set up the status of each port

0:ForceUnauthorized

1:ForceAuthorized

2:Auto

  - Possible value:

<port range> : 1 to 26

<authorized> : 0,1 or 2

  - Example:

```
ES-2126+(802.1x)# set port-control 2 2
```

- **set quiet-period**
  - Syntax:

set quiet-period <port-range> <sec>

  - Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

  - Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer, range 0-65535

  - Possible value:

<port range> : 1 to 26

<sec> : 0-65535, default is 60

- Example:

```
ES-2126+(802.1x)# set quiet-period 2 30
```

set reAuthEnabled

- Syntax:

set reAuthEnabled <port-range> <ebl>

- Description:

A constant that define whether regular reauthentication will take place on this port.

- Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<ebl> :

0:"OFF" to disable reauthentication

1:"ON" to enable reauthentication

- Possible value:

<port range> : 1 to 26

<ebl> : 0 or 1, default is 1

- Example:

```
ES-2126+(802.1x)# set reAuthEnabled 2 1
```

set reAuthMax

- Syntax:

set reAuthMax <port-range> <max>

- Description:

The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

- Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<max> : max. value , range 1-10

- Possible value:

<port range> : 1 to 26

<max> : 1-10, default is 2

- Example:

```
ES-2126+(802.1x)# set reAuthMax 2 2
```

- **set reAuthPeriod**
  - Syntax:

    set reAuthPeriod <port-range> <sec>
  - Description:

    A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 3600
  - Example:

```
ES-2126+(802.1x)# set reAuthPeriod 2 3600
```

- **set serverTimeout**
  - Syntax:

    set serverTimeout <port-range> <sec>
  - Description:

    A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 30
  - Example:

```
ES-2126+(802.1x)# set serverTimeout 2 30
```

DE

- **set state**
  - Syntax:

    set state <ip> <port-number> <secret-key>
  - Description:

    To configure the settings related with 802.1X Radius Server.
  - Argument:

    <ip> : the IP address of Radius Server, and the IP format is xxx.xxx.xxx.xxx

    <port-number> : the service port of Radius Server(Authorization port), range 1~65535

    <secret-key> : set up the value of secret-key, and the length of secret-key is from 1 to 31
  - Possible value:

    <port-number> : 1~65535, default 1812
  - Example:

```
ES-2126+(802.1x)# set state 192.168.1.115 1812
WinRadius
```

- **set suppTimeout**
  - Syntax:

    set suppTimeout <port-range> <sec>
  - Description:

    A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 30
  - Example:

```
ES-2126+(802.1x)# set suppTimeout 2 30
```

- **set txPeriod**
  - Syntax:

    set txPeriod <port-range> <sec>
  - Description:

    A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.
  - Argument:

    <port range> : syntax 1,5-7, available from 1 to 26

    <sec> : timer, range 1-65535
  - Possible value:

    <port range> : 1 to 26

    <sec> : 1-65535, default is 30
  - Example:

```
ES-2126+(802.1x)# set txPeriod 2 30
```

- **show mode**
  - Syntax:

    show mode
  - Description:

    To display the mode of each port.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(802.1x)# show mode
 Port       Mode
====== ============
   1      Disable
   2      Multi-host
   3      Disable
   4      Disable
   5      Disable
```

```
6       Disable
```

- **show parameter**
  - Syntax:

    show parameter
  - Description:

    To display the parameter settings of each port.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(802.1x)# show parameter
port  1) port control   : Auto
         reAuthMax      : 2
         txPeriod       : 30
         Quiet Period   : 60
         reAuthEnabled  : ON
         reAuthPeriod   : 3600
         max. Request   : 2
         suppTimeout    : 30
         serverTimeout  : 30
```

- **show security**
  - Syntax:

    show security
  - Description:

    To display the authentication status of each port.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(802.1x)# show security
 Port       Mode          Status
====== ============ ==============
   1      Disable
   2      Multi-host    Unauthorized
   3      Disable
   4      Disable
   5      Disable
   6      Disable
```

- **show state**
  - Syntax:

    show state
  - Description:

    To display the Radius server configuration.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(802.1x)# show state
Radius Server: 192.168.1.115
Port Number  : 1812
Secret Key   : WinRadius
```

account

- **add**
  - Syntax:

    add <name>
  - Description:

    To create a new guest user. When you create a new guest user, you must type in password and confirm password.
  - Argument:

<name> : new account name

- Possible value:

<name> : A string must be at least 5 character.

- Example:

```
ES-2126+(account)# add aaaaa
Password:
Confirm Password:
ES-2126+(account)#
```

- **del**
  - Syntax:

del <name>

  - Description:

To delete an existing account.

  - Argument:

<name> : existing user account

  - Possible value:

None.

  - Example:

```
ES-2126+(account)# del aaaaa
Account aaaaa deleted
```

- **modify**
  - Syntax:

modify <name>

  - Description:

To change the username and password of an existing account.

  - Argument:

<name> : existing user account

  - Possible value:

None.

  - Example:

```
ES-2126+(account)# modify aaaaa
username/password: the length is from 5 to 15.
```

```
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```


- **show**
  - Syntax:

  show
  - Description:

  To show system account, including account name and identity.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(account)# show
  Account Name       Identity
---------------- --------------
 admin              Administrator
 guest                  guest
 bbbbb                  guest
```

alarm

<<email>>

- **del mail-address**
  - Syntax:

  del mail-address <#>
  - Description:

  To remove the e-mail address.
  - Argument:

  <#>: email address number, range: 1 to 6
  - Possible value:

<#>: 1 to 6

- Example:

```
ES-2126+(alarm-email)# del mail-address 2
```

- **del server-user**
  - Syntax:

    del server-user
  - Description:

    To remove the server, user account and password.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(alarm-email)# del server-user
```

- **set mail-address**
  - Syntax:

    set mail-address <#> <mail address>
  - Description:

    To set up the email address.
  - Argument:

    <#> : email address number, range: 1 to 6

    <mail address> : email address
  - Possible value:

    <#>: 1 to 6
  - Example:

```
ES-2126+(alarm-email)# set mail-address 1
abc@mail.abc.com
```

- **set server**
  - Syntax:

    set server <ip>
  - Description:

    To set up the IP address of the email server.

- Argument:

<ip>:email server ip address or domain name

- Possible value:

None.

- Example:

```
ES-2126+(alarm-email)# set server 192.168.1.6
```

- **set user**
  - Syntax:

set user <username>

  - Description:

To set up the account of the email server.

  - Argument:

<username>: email server account

  - Possible value:

None.

  - Example:

```
ES-2126+(alarm-email)# set user admin
```

- **show**
  - **Syntax**:

show

  - Description:

To display the configuration of e-mail trap event.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(alarm-email)# show
Mail Server    : 192.168.1.6
Username       : admin
Password       : ****************
Email Address 1: abc@mail.abc.com
```

DE

```
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

<<events>>

- **del all**
  - **Syntax**:

    del all <range>
  - Description:

    To disable email, sms and trap of events.
  - Argument:

    <range>:del the range of email, sms and trap of events, syntax 1,5-7
  - Possible value:

    <range>: 1~22
  - Example:

```
ES-2126+(alarm-events)# del all 1-3
```

- **del email**
  - **Syntax**:

    del email <range>
  - Description:

    To disable the email of the events.
  - Argument:

    <range>:del the range of email, syntax 1,5-7
  - Possible value:

    <range>: 1~22
  - Example:

```
ES-2126+(alarm-events)# del email 1-3
```

- **del sms**
  - **Syntax**:

    del sms <range>
  - Description:

To disable the sms of the events.

- Argument:

<range>:del the range of sms, syntax 1,5-7

- Possible value:

<range>: 1~22

- Example:

```
ES-2126+(alarm-events)# del sms 1-3
```

- **del trap**
  - **Syntax**:

del trap <range>

  - Description:

To disable the trap of the events.

  - Argument:

<range>:del the range of trap, syntax 1,5-7

  - Possible value:

<range>: 1~22

  - Example:

```
ES-2126+(alarm-events)# del trap 1-3
```

- **set all**
  - **Syntax**:

set all <range>

  - Description:

To enable email, sms and trap of events.

  - Argument:

<range>:set the range of email, sms and trap of events, syntax 1,5-7

  - Possible value:

<range>: 1~22

  - Example:

```
ES-2126+(alarm-events)# set all 1-3
```

- **set email**
  - **Syntax**:

set email <range>

- Description:

  To enable the email of the events.

- Argument:

  <range>:set the range of email, syntax 1,5-7

- Possible value:

  <range>: 1~22

- Example:

```
ES-2126+(alarm-events)# set email 1-3
```

- **set sms**
  - Syntax:

    set sms <range>

  - Description:

    To enable the sms of the events.

  - Argument:

    <range>:set the range of sms, syntax 1,5-7

  - Possible value:

    <range>: 1~22

  - Example:

```
ES-2126+(alarm-events)# set sms 1-3
```

- **set trap**
  - Syntax:

    set trap <range>

  - Description:

    To enable the trap of the events.

  - Argument:

    <range>:set the range of trap, syntax 1,5-7

  - Possible value:

    <range>: 1~22

  - Example:

```
ES-2126+(alarm-events)# set trap 1-3
```

- **show**
  - Syntax:

show

- Description:

The Show here is used to display the configuration of alarm event.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(alarm-events)# show
   Events                    Email SMS Trap
-----------------------------------------
1  Cold Start                          v
2  Warm Start                          v
3  Link Down                           v
4  Link Up                             v
5  Authentication Failure              v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 Port-based Vlan Enabled
18 Tag-based Vlan Enabled
19 Module Inserted
```

DE

```
20 Module Removed
21 Moudle Media Swapped
22 PoE Failure
```

- **show (alarm)**
  - Syntax:

    show
  - Description:

    The Show for alarm here is used to display the configuration of Trap, SMS or E-mail.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(alarm)# show email
ES-2126+(alarm)# show events
ES-2126+(alarm)# show sms
<<sms>>
```

- **del phone-number**
  - Syntax:

    del phone-number <#>
  - Description:

    To delete sms phone number.
  - Argument:

    <#>: mobile phone number, range: 1 to 6
  - Possible value:

    <#>: 1 to 6
  - Example:

```
ES-2126+(alarm-sms)# del phone-number 3
```

- **del server-user**
  - Syntax:

    del server-user

- Description:

To delete sms server, user account and password.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(alarm-sms)# del server-user
```

set phone-number

- Syntax:

set phone-number <#> <phone-number>

- Description:

To add sms phone number.

- Argument:

<#>: mobile phone number, range: 1 to 6

<phone-number>: phone number

- Possible value:

<#>: 1 to 6

- Example:

```
ES-2126+(alarm-sms)# set phone-number 1 0968777777
```

set server

- Syntax:

set server <ip>

- Description:

To set up the IP address of sms server.

- Argument:

<ip>: SMS server ip address or domain name

- Possible value:

None.

- Example:

```
ES-2126+(alarm-sms)# set server 192.168.1.7
```

DE

- **set user**
  - **Syntax**:

    set user <username>
  - Description:

    To set up user account and password of sms server.
  - Argument:

    <username>: SMS server account
  - Possible value:

    None.
  - Example:

```
ES-2126+(alarm-sms)# set user ABC
```

- **show**
  - **Syntax**:

    show
  - Description:

    To display the configuration of SMS trap event.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(alarm-sms)# show
SMS Server     : 192.168.1.7
Username       : ABC
Password       : ****************
Mobile Phone  1: 0968777777
Mobile Phone  2:
Mobile Phone  3:
Mobile Phone  4:
Mobile Phone  5:
Mobile Phone  6:
```

autologout

- **autologout**
  - Syntax:

    autologout <time>
  - Description:

    To set up the timer of autologout.
  - Argument:

    <time>: range 1 to 3600 seconds, 0 for autologout off, current setting is 180 seconds.
  - Possible value:

    <time >: 0,1-3600
  - Example:

```
ES-2126+# autologout 3600
Set autologout time to 3600 seconds
```

bandwidth

- **set egress-rate**
  - Syntax:

    set egress-rate <range> <data_rate>
  - Description:

    To set up the egress-rate of the ports.
  - Argument:

    <range>:syntax 1,5-7, available from 1 to 26

    <data_rate>: 66-1024000(Kb).

    port 1-24: 66-102400(Kb); port 25-26: 66-1024000(Kb)
  - Possible value:

    <range>: 1 to 26

    <data_rate>: 66-102400(Kb) for port 1-24; 66-1024000(Kb) for port 25-26
  - Example:

```
ES-2126+(bandwidth)# set egress-rate 1-16 299
```

- **set ingress-rate**
  - Syntax:

set ingress-rate <range> <data_rate>

- Description:

To set up the ingress-rate of the ports.

- Argument:

<range>:syntax 1,5-7, available from 1 to 26

<data_rate>: 66-1024000(Kb).

port 1-24: 66-102400(Kb); port 25-26: 66-1024000(Kb)

- Possible value:

<range>: 1 to 26

<data_rate>: 66-102400(Kb) for port 1-24; 66-1024000(Kb) for port 25-26

- Example:

```
ES-2126+(bandwidth)# set ingress-rate 1-16 100
```

set storm-rate

- Syntax:
- Description:

To set up the storm-rate of the ports.

- Argument:
- <range>:syntax: 1,3-5, available from 1 to 5

1: Disable 2: Broadcast Storm Control

3: Multicast Storm Control

4: Unknown Unicast Storm Control

5: Broadcast, Multicast, Unknown Unicast Storm Control

<data_rate>: 1-100. The value must be the integer.

The value 100 disables broadcast storm control.

- Possible value:

<range>: 1 to 5

<data_rate>: 1-100.

- Example:

```
ES-2126+(bandwidth)# set storm-rate 2 99
```

show

- Syntax:

- Description:

To display all current settings of the bandwidth.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(bandwidth)# show
 Port   Ingress Rate(Kb)    Egress Rate(Kb)
====== ================== =================
    1      102400               102400
    2      102400               102400
    3      102400               102400
              :
             :
   23      102400               102400
   24      102400               102400
   25     1024000              1024000
   26     1024000              1024000

   Broadcast Storm Control
=========================================================
==
Type: Disable
Rate: 100 %
```

config-file

- **export start**

- Syntax:

export start

- Description:

To run the export start function.

DE

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(config-file)# export start

Export successful.
```

export user-conf

- Syntax:
- Description:

To run the export user-conf function.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(config-file)# export user-conf

Export successful.
```

import start

- Syntax:
- Description:

To run the import start function.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(config-file)# import start

Import successful.
```

import user-conf

- Syntax:
- Description:

To run the import user-conf function.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(config-file)# import user-conf
Import successful.
```

- **set export-path**
  - Syntax:
  - Description:

To set up the file path and filename that user would like to export.

- Argument:

<filepath>:filepath and filename

- Possible value:

<filepath>:filepath and filename

- Example:

```
ES-2126+(config-file)# set export-path log/21511.txt
```

- **set import-path**
  - Syntax:
  - Description:

To set up the filepath and filename that user would like to import.

- Argument:

<filepath>:filepath and filename

- Possible value:

<filepath>:filepath and filename

- Example:

```
ES-2126+(config-file)# set import-path log/21511.txt
```

- **show**
  - Syntax:
  - Description:

To display the information of the config file.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: log/21511.txt
Import Path and Filename: log/21511.txt
```

dhcp-boot

- **set dhcp-boot**
  - Syntax:
  - Description:

To set up the delay time for DHCP Boot.

  - Argument:
  - <sec>:range syntax: 0, 1-30. The value "0" is to disable dhcp-boot delay
  - Possible value:

<sec>:0-30

  - Example:

```
ES-2126+(dhcp-boot)# set 30
```

- **show**
  - Syntax:
  - Description:

To display the status of DHCP Boot.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(dhcp-boot)# show
DHCP Boot : Enable
```

```
Second        : 30
ES-2126+(dhcp-boot)#
```

diag

diag

- Syntax:

diag

- Description:

Diag is used to test whether EEPROM, UART, DRAM and Flash is normal or not.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(diag)# diag
EEPROM Test  : OK
UART Test    : OK
DRAM Test    : OK
Flash Test   : OK
```

Loopback

- Syntax:

loopback

- Description:

For Internal/External Loopback Test.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(diag)# loopback
Internal Loopback Test : OK
```

```
External Loopback Test : Port 1 2 3 4 5 6 7 8 9 10 11
12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 Fail
```

- **ping**
  - Syntax:

    ping <ip>
  - Description:

    To confirm that whether the remote end-station or switch itself is alive or not.
  - Argument:

    <ip> : IP address or domain name
  - Possible value:

    IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com
  - Example:

```
ES-2126+(diag)# ping 192.168.1.115
Gateway       : 192.168.1.253
192.168.1.115 is alive.
```

firmware

- **set upgrade-path**
  - Syntax:
  - Description:

    To set up the image file that will be upgraded.
  - Argument:

    <filepath>: upgrade file path and name
  - Possible value:

    <filepath>: upgrade file path and name
  - Example:

```
ES-2126+(firmware)#          set          upgrade-path
FEL2SW26_ES2126_v2.05.img
```

- **show**
  - Syntax:
  - Description:

    To display the information of tftp server and upgrade-path and file name.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(firmware)# show
TFTP Server IP Address: 192.168.3.111
Path and Filename     : FEL2SW26_ES2126_v2.05.img
```

- **upgrade**
  - Syntax:
  - Description:

To run the software upgrade function.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(firmware)# upgrade
```

Upgrading firmware ...

gvrp

- **disable**
  - Syntax:

disable

  - Description:

To disable the gvrp function

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(gvrp)# disable
```

DE

- **enable**
  - Syntax:

    enable
  - Description:

    To enable the gvrp function.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(gvrp)# enable
```

- **group**
  - Syntax:

    group <group number>
  - Description:

    To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.
  - **Argument:**

    <group number>: enter which gvrp group you had created, using value is vid. Available range: 1 to 4094
  - Possible value:

    <group number>: 1~4094
  - Example:

```
ES-2126+(gvrp)# show group
GVRP group information
Current Dynamic Group Number: 1
VID  Member Port
---- ------------------------------------------------
-
2    5
ES-2126+(gvrp)# group 2
```

    ES-2126+(gvrp-group-2)# set applicant 1-6 non-participant

```
ES-2126+(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Normal
2    Non-Participant Normal
3    Non-Participant Normal
4    Non-Participant Normal
5    Non-Participant Normal
6    Non-Participant Normal
7    Normal          Normal
8    Normal          Normal
12   Normal          Normal
13   Normal          Normal
            :
            :
23   Normal          Normal
24   Normal          Normal
25   Normal          Normal
26   Normal          Normal
ES-2126+(gvrp-group-2)# set registrar 1-10 fixed

ES-2126+(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant       Registrar
---- --------------- ---------
1    Non-Participant Fixed
2    Non-Participant Fixed
3    Non-Participant Fixed
4    Non-Participant Fixed
```

DE

```
5     Non-Participant Fixed
6     Non-Participant Fixed
7     Normal          Fixed
8     Normal          Fixed
9     Normal          Fixed
10    Normal          Fixed
17    Normal          Normal
             :
              :
23    Normal          Normal
24    Normal          Normal
25    Normal          Normal
26    Normal          Normal
```

- **set applicant**
  - Syntax:

    set applicant <range> <normal|non-participant>
  - Description:

    To set default applicant mode for each port.
  - Argument:

    <range>: port range, syntax 1,5-7, available from 1 to 26

    <normal>: set applicant as normal mode

    <non-participant>: set applicant as non-participant mode
  - **Possible value:**

    <range>: 1 to 26

    <normal|non-participant>: normal or non-participant
  - Example:

    `ES-2126+(gvrp)# set applicant 1-10 non-participant`
- **set registrar**
  - Syntax:

    set registrar <range> <normal|fixed|forbidden>
  - Description:

To set default registrar mode for each port.

- Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

<normal>: set registrar as normal mode

<fixed>: set registrar as fixed mode

<forbidden>: set registrar as forbidden mode

- Possible value:

<range>: 1 to 26

<normal|fixed|forbidden>: normal or fixed or forbidden

- Example:

```
ES-2126+(gvrp)# set registrar 1-5 fixed
```

- **set restricted**
  - Syntax:

set restricted <range> <enable|disable>

- Description:

To set the restricted mode for each port.

- Argument:

<range>: port range, syntax 1,5-7, available from 1 to 26

<enable>: set restricted as enabled

<disable>: set restricted as disabled

- Possible value:

<range>: 1 to 26

<enable|disable>: enable or disable

- Example:

```
ES-2126+(gvrp)# set restricted 1-10 enable

ES-2126+ES-2126+(gvrp)# show config

GVRP state: Enable

Port Join Time Leave Time LeaveAll Time     Applicant
Registrar Restricted

---- --------- ---------- ------------- --------------
- --------- ----------
```

DE

```
  1      20        60         1000      Normal          Normal
Enable
  2      20        60         1000      Normal          Normal
Enable
  3      20        60         1000      Normal          Normal
Enable
  4      20        60         1000      Normal          Normal
Enable
  5      20        60         1000      Normal          Normal
Enable
  6      20        60         1000      Normal          Normal
Enable
  7      20        60         1000      Normal          Normal
Enable
  8      20        60         1000      Normal          Normal
Enable
  9      20        60         1000      Normal          Normal
Enable
 10      20        60         1000      Normal          Normal
Enable
                                                  :
                                              :
                                              :
 22      20        60         1000      Normal          Normal
Disable
 23      20        60         1000      Normal          Normal
Disable
 24      20        60         1000      Normal          Normal
Disable
 25      20        60         1000      Normal          Normal
Disable
 26      20        60         1000      Normal          Normal
Disable
```

- **set timer**
  - Syntax:

    set timer <range> <join> <leave> <leaveall>
  - Description:

    To set gvrp join time, leave time, and leaveall time for each port.
  - Argument:

    <range> : port range, syntax 1,5-7, available from 1 to 26

    <join>: join timer, available from 20 to 100

    <leave>: leave timer, available from 60 to 300

    <leaveall>: leaveall timer, available from 1000 to 5000

    Leave Time must equal double Join Time at least.
  - Possible value:

    <range> : 1 to 26

    <join>: 20 to 100

    <leave>: 60 to 300

    <leaveall>: 1000 to 5000
  - Example:

    ```
    ES-2126+(gvrp)# set timer 2-8 25 80 2000
    ```
- **show config**
  - Syntax:

    show config
  - Description:

    To display the gvrp configuration.
  - **Argument:**

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+(gvrp)# show config

    GVRP state: Disable

    Port  Join  Time  Leave  Time  LeaveAll  Time  Applicant
    Registrar Restricted
    ```

DE

```
---- --------- ---------- ------------ --------------
- --------- ----------
  1     20       60        1000     Normal         Normal
Disable
  2     20       60        1000     Normal         Normal
Disable
  3     20       60        1000     Normal         Normal
Disable
  4     20       60        1000     Normal         Normal
Disable
                                  :
                                  :
                                  :
 23     20       60        1000     Normal         Normal
Disable
 24     20       60        1000     Normal         Normal
Disable
 25     20       60        1000     Normal         Normal
Disable
 26     20       60        1000     Normal         Normal
Disable
```

- **show counter**
  - Syntax:

    show counter <port>
  - Description:

    To show counter of the port.
  - Argument:

    <port>: port number, available from 1 to 26
  - Possible value:

    <port>: 1 to 26
  - Example:

```
ES-2126+(gvrp)# show counter 2
GVRP Counter port: 2
```

```
Counter Name            Received Transmitted
--------------------    -------- -----------
Total GVRP Packets             0           0
Invalid GVRP Packets           0        ----
LeaveAll message               0           0
JoinEmpty message              0           0
JoinIn message                 0           0
LeaveEmpty message             0           0
Empty message                  0           0
```

- **show group**
  - Syntax:

  show group
  - Description:

  To show the gvrp group.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(gvrp)# show group

GVRP group information
Current Dynamic Group Number: 0
VID  Member Port
---- ------------------------------------------------
-
```

hostname

- **hostname**
  - Syntax:
  - Description:

  To set up the hostname of the switch.

DE

- Argument:

<name>: hostname, max. 40 characters.

- Possible value:

<name>: hostname, max. 40 characters.

- Example:

```
ES-2126+# hostname Company
Company#
```

igmp-snooping

- **add allowed-group**
  - Syntax:

  add allowed-group <ip-multicast> <vid> <port-range>

  - Description:

  To add the entry of allowed IP multicast group.

  - Argument:

  <ip-multicast>: the range of IP multicast.

  <vid>: VLAN ID. 1-4094 or any.

  <port-range>: syntax 1,5-7, available from 1 to 26

  - Possible value:

  <ip-multicast>: ex: 224.1.1.1-225.2.3.3 or any

  <vid>: 1-4094 or any

  <port-range>: 1 to 26

  - Example:

```
ES-2126+(igmp-snooping)# add allowed-group 224.1.1.1-
225.2.3.3 100 1-10
```

- **add mvr-allow-group**
  - Syntax:

  add mvr-allow-group <begin address> <end address>

  - Description:

  To add an entry to the MVR allowed group entries. The MVR group table may contain 10 entries.

  - Argument:

  <begin address> : first multicast address of the group.

<end address> : last multicast address of the group.

- Possible value:

<begin address> : 224.0.1.0 - 239.255.255.255

<end address> : 224.0.1.0. - 239.255.255.255

- Example:

```
ES-2126+(igmp-snooping)# add mvr-allow-group 224.0.1.0
224.0.2.0
```

add static-multicast

- Syntax:

add static-multicast <ip-multicast> <vid> <port-range>

- Description:

To add ab entry to static ip-multicast.

- Argument:

<ip-multicast>: the range of IP multicast.

<vid>: VLAN ID. 0-4094, 0 means tag-based vlan is disabled

<port-range>: syntax 1,5-7, available from 1 to 26

- Possible value:

<ip-multicast>: ex: 224.1.1.1-225.2.3.3 or any

<vid>: 0-4094 or any

<port-range>: 1 to 26

- Example:

```
ES-2126+(igmp-snooping)# add static-multicast 224.1.1.1
100 5
```

del allowed-group

- Syntax:

del allowed-group <index>

- Description:

To remove the entry of allowed IP multicast group

- Argument:

<index>: the index of the allowed-group.

- Possible value:

<index>: the index of the allowed-group.

- Example:

```
ES-2126+(igmp-snooping)# del allowed-group 1
```

- **del mvr-allow-group**
  - Syntax:

    del mvr-allow-group <index>
  - Description:

    To delete an entry of the MVR allowed group entries.
  - Argument:

    <index> : index of the MVR allowed group entry.
  - Possible value:

    <index> : 1 - 10
  - Example:

```
ES-2126+(igmp-snooping)# del mvr-allow-group 2
```

- **del static-multicast**
  - Syntax:

    del static-multicast <index>
  - Description:

    To remove an static-ip multicast entry .
  - Argument:

    <index>: the index of the static-ip mutlicast entry.
  - Possible value:

    <index>: the index of the static-ip multicast entry.
  - Example:

```
ES-2126+(igmp-snooping)# del static-multicast 1
```

- **modify mvr-allow-group**
  - Syntax:

    modify mvr-allow-group <index> <begin address> <end address>
  - Description:

    To edit an entry of the MVR group.
  - Argument:

    <index> : index of the MVR allowed group entry.

    <begin address> : first multicast address of the group.

<end address> : last multicast address of the group.

- Possible value:

<index>: 1 - 10

<begin address> : 224.0.1.0 - 239.255.255.255

<end address> : 224.0.1.0. - 239.255.255.255

- Example:

```
ES-2126+(igmp-snooping)#  modify  mvr-allow-group  2
224.0.2.0 225.0.0.4
```

- **modify static-multicast**
  - Syntax:

del static-multicast <port-range>

  - Description:

To modify an static-ip multicast entry .

  - Argument:

<port-range>: syntax 1, 5-7, available from 1 to 26.

  - Possible value:

<port-range> : 1 - 26

  - Example:

```
ES-2126+(igmp-snooping)# modify static-multicast 1
```

- **set grp-limit**
  - Syntax:

set grp-limit <range> <limit>

  - Description:

To set up the limit of possible group members.

  - Argument:

<range> : syntax: 1, 5-7, available from 1 to 26

<limit> : number of possible group members

  - Possible value:

<range> : 1 - 26

<limit> : 0 - 256

  - Example:

```
ES-2126+(igmp-snooping)# set grp-limit 2 25
```

DE

- **set mode**
  - Syntax:

    set mode <status>
  - Description:

    To set up the mode of IGMP Snooping.
  - Argument:

    <status>: 0:disable, 1:active, 2:passive
  - Possible value:

    <status>: 0,1or 2
  - Example:

    ```
    ES-2126+(igmp-snooping)# set mode 2
    ```
- **set mvr-host-timeout**
  - Syntax:

    set mvr-host-timeout <time>
  - Description:

    To set up MVR Host Timeout.
  - Argument:

    <time> : timeout in seconds
  - Possible value:

    <time> : 12 - 255
  - Example:

    ```
    ES-2126+(igmp-snooping)# set mvr-host-timeout 26
    ```
- **set mvr-state**
  - Syntax:

    set mvr-state <mode> [<mvid>]
  - Description:

    To enable or disable MVR.
  - Argument:

    <mode> : disable (0) or enable (1)

    <mvid> : MVR Vlan ID
  - Possible value:

    <mode> : 0 - 1

<mvid> : 1 - 4094

- Example:

```
ES-2126+(igmp-snooping)# set mvr-state 1 22
```

- **set mvr-vid**
  - Syntax:

    set mvr-vid <vid>
  - Description:

    To set MVR Vlan ID.
  - Argument:

    <vid> : MVR Vlan ID
  - Possible value:

    <vid> : 1 - 4094
  - Example:

```
ES-2126+(igmp-snooping)# set mvr-vid 22
```

- **set rad-igmp-port**
  - Syntax:

    set rad-igmp-port <port-range> <mode>
  - Description:

    To set up radius-igmp enabled ports.
  - Argument:

    <port-range> : 1, 5-7, available from 1 to 26

    <mode> : set enable (1) or disable (0)
  - Possible value:

    <port-range>: 1 - 26

    <mode> : 0 - 1
  - Example:

```
ES-2126+(igmp-snooping)# set rad-igmp-port 22 1
```

- **set rad-igmp-retry**
  - Syntax:

    set rad-igmp-retry <value>
  - Description:

    To set up radius-igmp numbers of retries.

- Argument:

<value> : 0 to 10 times

- Possible value:

<value> : 0 - 10

- Example:

```
ES-2126+(igmp-snooping)# set rad-igmp-retry 5
```

- **set rad-igmp-state**
  - Syntax:

set rad-igmp-state <ip> <port-number> <secret-key> <Accounting Server> <Accounting Port>

  - Description:

To set up radius-igmp state.

  - Argument:

<ip> : ip address

<port-number> : 1 to 65535

<secret-key> : the secret key for the accounting server

<Accounting Server> : ip address of the accounting server

<Accounting Port> : 1 to 65535

  - Possible value:

<ip> : example 244.111.111.111 or any

<port-number> : 1 - 65535

<secret-key> : 1 - 31 alpha numeric characters

<Accounting Server> : example 244.111.111.111 or any

<Accounting Port> : 1 - 65535

  - Example:

```
ES-2126+(igmp-snooping)# set rad-igmp-state 123.4.5.6 2
secretkey 234.564.8.9 56
```

- **set rad-igmp-timeout**
  - Syntax:

set rad-igmp-timeout <value>

  - Description:

To set up radius-igmp timeout.

- Argument:

<value> : 0 to 60 seconds

- Possible value:

<value> : 0 - 60

- Example:

```
ES-2126+(igmp-snooping)# set rad-igmp-timeout 5
```

- **show client-info**
  - Syntax:

show client-info <range>

  - Description:

To display information about the clients connected to a port.

  - Argument:

<range> : syntax: 1, 5-7, available from 1 to 26

  - Possible value:

<range> : 1 - 26

  - Example:

```
ES-2126+(igmp-snooping)# show client-info 22

Port     MAC Address     Multicast Address
----  -----------------  -----------------

total 0 entries
```

- **show grp-limit**
  - Syntax:
  - Description:

To display each port's group limit.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(igmp-snooping)# show grp-limit
```

DE

```
Port  Limit  Port  Limit  Port  Limit
----  -----  ----  -----  ----  -----
  1     22    10    256    19    256
  2    256    11    256    20    256
  3    256    12    256    21    256
  4    256    13    256    22    256
  5    256    14    256    23    256
  6    256    15    256    24    256
  7    256    16    256    25    256
  8    256    17    256    26    256
  9    256    18    256
```

- **show igmp-snooping**
  - Syntax:
  - Description:

  To display IGMP snooping mode and allowed IP multicast entry.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(igmp-snooping)# show igmp-snooping
Snoop Mode: Active
IP Multicast:
 1)  IP Address    : 224.1.1.1
     VLAN ID       : 0
     Member Port : 22
```

- **show multicast**
  - Syntax:
  - Description:

  To display IP multicast table.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(igmp-snooping)# show multicast
IP Multicast: None
```

show mvr-config

- Syntax:
- Description:

To display the MVR configuration.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(igmp-snooping)# show mvr-config
MVR State        : enable
MVR VLan ID      : 22
MVR Host Timeout : 125
MVR Allow Groups : 1

Index      begin address      end address
----------------------------------------
  1            224.0.1.0        224.0.2.0
```

show mvr-group-membership

- Syntax:
- Description:

To display the MVR group membership.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+# igmp-snooping
ES-2126+(igmp-snooping)# show mvr-group-membership
  1) Group Address: 224.0.1.76
     Port Member  : 5
  2) Group Address: 224.0.1.24
     Port Member  : 5
  3) Group Address: 224.0.1.41
     Port Member  : 5

There are 125 group entries available
```

- **show query**
  - Syntax:
  - Description:

To display the query interval.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(igmp-snooping)# show query

Query Interval: 25 second
```

- **show rad-igmp**
  - Syntax:
  - Description:

To display Radius IGMP Snooping configuration.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(igmp-snooping)# show rad-igmp


Radius Server: 192.168.1.1
```


- **show static-multicast**
  - Syntax:
  - Description:

To display static-ip multicast entry.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126P+(igmp-snooping)# show static-multicast


 1)  IP Address : 244.1.1.1
     VLAN ID    : 26
     Member Port: 5IP
```

- **disable dhcp**
  - Syntax:

disable dhcp

- Description:

To disable the DHCP function of the system.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(ip)# disable dhcp
DHCP is already stopped.
```

DE

- **enable dhcp**
  - Syntax:

    enable dhcp <manual|auto>
  - Description:

    To enable the system DHCP function and set DNS server via manual or auto mode.
  - Argument:

    <manual|auto> : set DNS by using manual or auto mode.
  - Possible value:

    <manual|auto> : manual or auto
  - Example:

    ```
    ES-2126+(ip)# enable dhcp manual
    ```
- **set dns**
  - Syntax:

    set dns <ip>
  - Description:

    To set the IP address of DNS server.
  - Argument:

    <ip> : dns ip address
  - Possible value:

    <ip> : 168.95.1.1
  - Example:

    ```
    ES-2126+(ip)# set dns 168.95.1.1
    ```
- **set ip**
  - Syntax:

    set ip <ip> <mask> <gateway>
  - Description:

    To set the system IP address, subnet mask and gateway.
  - Argument:

    <ip> : ip address

    <mask> : subnet mask

    <gateway> : default gateway

- Possible value:

<ip> : 192.168.1.1 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

- Example:

```
ES-2126+(ip)#  set  ip  192.168.1.2  255.255.255.0
192.168.1.253
```

- **show**
  - Syntax:

show

  - Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(ip)# show
DHCP               : Disable
IP Address         : 192.168.1.1
Current IP Address : 192.168.1.1
Subnet mask        : 255.255.255.0
Gateway            : 192.168.1.253
DNS Setting        : Manual
DNS Server         : 192.95.1.1
```

log

- **clear**
  - Syntax:

clear

  - Description:

To clear the log data.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(log)# clear
```

- **disable auto-upload**
  - Syntax:

disable auto-upload

  - Description:

To disable the auto-upload function.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(log)# disable auto-upload
```

- **enable auto-upload**
  - Syntax:

enable auto-upload

  - Description:

To enable the auto-upload function.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(log)# enable auto-upload
```

- **show**
  - Syntax:

show

- Description:

To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(log)# show

Tftp Server : 0.0.0.0
Auto Upload : Disable

1)  Wed Apr 13 12:13:27 2005  Link Up [Port 1]
2)  Wed Apr 13 12:13:26 2005  Link Down [Port 1]
3)  Wed Apr 13 11:58:31 2005  Login [admin]
4)  Wed Apr 13 11:19:45 2005  Login [admin]
5)  Wed Apr 13 11:19:37 2005  Logout [admin]
```

upload

- Syntax:

Upload

- Description:

To upload log data through tftp.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(log)# upload
```

DE

login-protect

- **set Lock-Minutes**
  - Syntax:

    set Lock-Minutes <min>
  - Description:

    To set login lock time.
  - Argument:

    <min> : time in minutes
  - Possible value:

    <min> : numeric characters from 1 to 10
  - Example:

    ```
    ES-2126P+(login-protect)# set Lock-Minutes 4
    ```
- **set Login-errors**
  - Syntax:

    set Login-errors <count>
  - Description:

    To set login error count.
  - Argument:

    <count> : login error count
  - Possible value:

    <count> : 1 to 10, set 0 as disabled
  - Example:

    ```
    ES-2126+(Login-protect)# set Login-errors 10
    ```
- **show**
  - Syntax:

    show
  - Description:

    To show login protect config.
  - Argument:

    None.
  - Possible value:

    None.

- Example:

```
ES-2126+(login-protect)# show
```

mac-table

<<alias>>

- **del**
  - Syntax:

    del <mac>
  - Description:

    To delete the mac alias entry.
  - Argument:

    <mac> : mac address, format: 00-02-03-04-05-06
  - Possible value:

    <mac> : mac address
  - Example:

```
ES-2126+(mac-table-alias)# del 00-44-33-44-55-44
```

- **set**
  - Syntax:

    set <mac> <alias>
  - Description:

    To set up the mac alias entry.
  - Argument:

    <mac> : mac address, format: 00-02-03-04-05-06

    <alias> : mac alias name, max. 15 characters
  - Possible value:

    <mac> : mac address

    <alias> : max. 15 characters
  - Example:

```
ES-2126+(mac-table-alias)# set 00-44-33-44-55-44 www
```

- **show**
  - Syntax:

    show

DE

- Description:

To display the mac alias entry.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(mac-table-alias)# show

MAC Alias List

      MAC Address       Alias

----- ----------------- ----------------

1)    00-02-03-04-05-06 aaa

2)    00-33-03-04-05-06 ccc
```

<<information>>

search

- Syntax:

search <port> <mac> <vid>

- Description:

To look for the relative mac information in mac table.

- Argument:

<port> : set up the range of the ports to search for,
syntax 1,5-7, available form 1 to 26

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : VLAN id, from 1 to 4094; '?' as don't care, 0 as untagged

- Possible value:

<port> : 1 to 26

<vid> : 0, 1 ~4094

- Example:

```
ES-2126+(mac-table-information)# search 1-26 ??-??-??-
??-??-?? ?

MAC Table List

Alias            MAC Address       Port VID  State
```

```
---------------- ----------------- ---- ---- ---------
--------
                  00-40-c7-88-00-06    1    0  Dynamic
ES-2126+(mac-table-information)#
```

- **show**
  - Syntax:

    show
  - Description:

    To display all mac table information.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(mac-table-information)# show
MAC Table List
Alias            MAC Address       Port VID  State
---------------  ----------------------  ----   ----
-----------------
ABC              00-40-c7-d6-00-01     1     2    Static
Forwarding
ABC123     00-40-c7-d6-00-02    1    3   Static Filtering
<<maintain>>
```

- **set aging**
  - Syntax:

    set aging <time>
  - Description:

    To set up the age out time of dynamic learning mac.
  - Argument:

    <time> : Mac table ageout time between 10 and 1000000 seconds. The value “0”
    means to disable age out time

DE

- Possible value:

<time> : 10-1000000 seconds or 0

- Example:

```
ES-2126+(mac-table-maintain)# set aging 300
```

set learning

- Syntax:

set learning <port> <num>

- Description:

To set up the maximum amount of MAC that each port can learn.

- Argument:

<port> : port range, syntax 1,5-7, available form 1 to 24

<num>: MAC address numbers which can be dynamically learned

num range: between 0 to 8191; 0 for learning disabled

- Possible value:

<port> : 1 to 24

<num>: 0 to 8191

- Example:

```
ES-2126+(mac-table-maintain)# set learning 5 100
```

show

- Syntax:

show

- Description:

To display the settings of MAC table ageout time and the learning limit of each port.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(mac-table-maintain)# show
Mac table ageout time: 300 seconds
 Port    Dynamically learn limit
```

```
------ ------------------------
   1     8191
   2     8191
   3     8191
   4     8191
   5     8191
          :
          :
          :
  21     8191
  22     8191
  23     8191
  24     8191
  25     8192
  26     8192
```

<<port-security>>

- **disable**
  - Syntax:

    disable <range>
  - Description:

    To disable port security for a port.
  - Argument:

    <range> : Number of port that you want to disable.
  - Possible value:

    <range> : 1 - 26
  - Example:

    `ES-2126+(mac-table-port-security)# disable 2`
- **enable**
  - Syntax:

    enable <range>
  - Description:

To enable port security for a port.

- Argument:

<range> : number of port that you want to enable.

- Possible value:

<range> : 1 - 26

- Example:

```
ES-2126+(mac-table-port-security)# enable 2
```

- **show**
  - Syntax:

show

  - Description:

To display enabled and disabled port security per port.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(mac-table-port-security)# show
Port Security:
----------------------
 Port   State
  1     Disable
  2     Enable
  3     Disable
  4     Disable
  5     Disable
  6     Disable
  7     Disable
  8     Disable
  9     Disable
 10     Disable
```

```
 11      Disable
 12      Disable
 13      Disable
 14      Disable
 15      Disable
 16      Disable
 17      Disable
 18      Disable
 19      Disable
 20      Disable
 21      Disable
...(q to quit)
```

<<port>>

- **add**
  - Syntax:

    add <mac> <vid> <queue>
  - Description:

    To enable a static mac entry for a port.
  - Argument:

    <mac> : mac adress

    <vid> : vlan id

    <queue> : which queue you want to set
  - Possible value:

    <mac> : format 01-02-03-04-05-06 (alpha numeric characters)

    < vid> : 1 - 4094

    <queue> : 0 - 3
  - Example:

    ```
    ES-2126+(mac-table-port-security-port-2)#  add  22-55-
    66-78-64-88 42 3
    ```
- **del**
  - Syntax:

del <mac>

- Description:

To delete a static mac entry for a port.

- Argument:

<mac> : mac adress

- Possible value:

<mac> : format 01-02-03-04-05-06 (alpha numeric characters)

- Example:

```
ES-2126+(mac-table-port-security-port-2)#  del  22-55-66-78-64-88
```

- **show**

  - Syntax:

  show

  - Description:

  To display static mac entries for a port.

  - Argument:

  None.

  - Possible value:

  None.

  - Example:

```
ES-2126+(mac-table-port-security-port-2)# show
Port 2 static mac entry:
-----------------------------------------
 (None)
```

  <<static-mac>>

- **add**

  - Syntax:

  add <mac> <vid> <queue> <rule> <port>

  - Description:

  To add the static mac entry.

  - Argument:

  <mac>: mac address, format: 01-02-03-04-05-06

<vid>: VLAN id, from 1 to 4094

<queue>: which queue you want to set, from 0 to 3

<rule> : forwarding rule, from 0 to 2

0:static

1:drop destination address matches

2:drop source address matches

<port> : forwarded destination port, form 1 to 26

- Possible value:

<vid>: 1 to 4094

<queue>: 0 to 3

<rule>: 0 to 2

<port>: 1 to 26

- Example:

```
ES-2126+ (mac-table-static-mac)# add 00-22-44-55-66-77
1 0 0 6
```

- **del**
  - Syntax:

    del <mac>
  - Description:

    To remove the static mac entry.
  - Argument:

    <mac> : mac address, format: 00-02-03-04-05-06
  - Possible value:

    <mac> : mac address
  - Example:

```
ES-2126+(mac-table-static-mac)# del 00-02-03-04-05-06
```

- **show**
  - Syntax:

    show
  - Description:

    To display static mac entry.
  - Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(mac-table-static-mac)# show
          MAC                              VID     Queue
Forwarding Rule            Port
------ -------------------------- ------ -------- ---
--------------------------------  -------
   1)  00-40-C7-D6-00-01   200        2    Static with
Destination Drop     2
```

management

- **add**

- Syntax:

Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]

[<type> <value>] <action> <value>

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8

type h,s action a

Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

- Description:

To save the adding management policy records.

When you don't know how to set the management policy records, you can use this command as follows:

ES-2126+(management-add)# set

This command will show exhaustive operating explanation for setting the management policy records.

- Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP range.
[<port> <value>]	Incoming port.

[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

- Possible value:

[<name> <value>]	No default and it must be set.
[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any.
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any.
<action> <value>	No default and it must be set.

- Example:

```
ES-2126+(management-add)# set name Mary vid 20 ip
192.168.1.1-192.168.1.90 port 2-5,8 type h,s action a
ES-2126+(management-add)# show
 #: 1
Name : Mary                VlanID : 20          IP :
192.168.1.1-192.168.1.90
Type : Http,SNMP           Action : Accept      Port :
2,3,4,5,8
```

delete

- Syntax:

delete #

- Description:

To delete a specific record or range.

- Argument:

[#]: a specific or range management security entry(s)

- Possible value:

None.

- Example:

```
ES-2126+(management)# show

 #: 1
```

```
Name : Tom                    VlanID : 2           IP :
192.168.1.30-192.168.1.80
Type : SNMP              Action : Deny      Port : 1,2


ES-2126+(management)# delete 1


ES-2126+(management)# show


Security rule list is empty now
```

- **edit**

  the specific management policy entry.

  - Available range:

  1 to 65536.

  - Syntax:

  Usage: set [<name> <value>] [<vid> <value>] [<ip> <value>] [<port> <value>]

  [<type> <value>] <action> <value>

  Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90 port 2-5,8

  type h,s action a

  Synopsis: set name Mary vid 20 ip 192.168.1.1-192.168.1.90

  - Description:

  To edit management policy record.

  - Argument:

[<name> <value>]	ACL entry name.
[<vid> <value>]	VLAN ID.
[<ip> <value>]	IP Range.
[<port> <value>]	Incoming port.
[<type> <value>]	Access type.
<action> <value>	a(ccept) or d(eny).

  - Possible value:

[<name> <value>]	No default and it must be set.

[<vid> <value>]	The range is 1-4095 and can be set to any.
[<ip> <value>]	For example, 192.168.1.90-192.168.1.90 or any
[<port> <value>]	For example, 1 or 1-8 or 1,3-5 or any
[<type> <value>]	For example, h(ttp),s(nmp),t(elnet) or any
<action> <value>	No default and it must be set.

- Example:

```
ES-2126+(management)# edit 1

ES-2126+(management-edit-1)# set name Tom vid 2 ip
192.168.1.30-192.168.1.80 port 1-2 type s action d

ES-2126+(management-edit-1)# show

 #: 1

Name : Tom                  VlanID : 2          IP :
192.168.1.30-192.168.1.80

Type : SNMP             Action : Deny      Port : 1,2
```

- **show**
  - Syntax:

  show
  - Description:

  To show the specific management policy record.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(management)# show

#: 1

Name : Tom                  VlanID : 2          IP :
192.168.1.30-192.168.1.80

Type : SNMP             Action : Deny      Port : 1,2
```

DE

poe

- **set priority**
  - Syntax:

    set priority <port-range> <priority>
  - Description:

    To set the PoE priority on ports.
  - Argument:

    <port-range>¡G

    <priority>: set priority as 0:Low, 1:Normal, 2:High
  - Possible value:

    <port range>: 1 to 24

    <priority>: 0, 1 or 2
  - Example:

    ```
    ES-2126+(poe)# set priority 1-12 2
    ```
- **set state**
  - Syntax:

    set state <port-range> <state>
  - Description:

    To set the PoE state on ports.
  - Argument:

    <port-range>¡G

    <state>: enable or disable PoE function. 0:Disable 1:Enable
  - Possible value:

    <port-range>¡G

    <state>: 0 or 1
  - Example:

    ```
    ES-2126+(poe)# set state 11 0
    ```
- **show**
  - Syntax:

    show
  - Description:

    To display the PoE status.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(poe)# show

Vmain          : 48.3 V

Imain          : 0.0 A

Pconsume       : 0.0 W

Power Limit    : 185 W

Temperature    : 37 'C / 98 'F


Port No                 | 1  2  3  4  5  6  7  8  9  10  11  12
------------------------ | -  -  -  -  -  -  -  -  -  -
--  --  --
Port On                  | X  X  X  X  X  X  X  X  X  X   X   X
AC Disconnect Port Off     | X  X  X  X  X  X  X  X  X
X   X   X
DC Disconnect Port Off     | X  X  X  X  X  X  X  X  X
X   X   X
Overload Port Off          | X  X  X  X  X  X  X  X  X
X   X   X
Short Circuit Port Off     | X  X  X  X  X  X  X  X  X
X   X   X
Over Temp. Protection      | X  X  X  X  X  X  X  X  X
X   X   X
Power Management Port Off | X  X  X  X  X  X  X  X  X
X   X   X



Port No                    | 13 14 15 16 17 18 19 20 21
22  23  24
```

DE

```
------------------------ | -- -- -- -- -- -- -- -- --
--  --  --
Port On                  | X  X  X  X  X  X  X  X  X  X  X  X
AC Disconnect Port Off   | X  X  X  X  X  X  X  X  X
X   X   X
DC Disconnect Port Off   | X  X  X  X  X  X  X  X  X
X   X   X
Overload Port Off        | X  X  X  X  X  X  X  X  X
X   X   X
Short Circuit Port Off   | X  X  X  X  X  X  X  X  X
X   X   X
Over Temp. Protection    | X  X  X  X  X  X  X  X  X
X   X   X
Power Management Port Off | X  X  X  X  X  X  X  X  X
X   X   X

Port Status  State  Priority Power(W) Current(mA) Class
---- ------ ------- -------- -------- ----------- -----
  1  Normal Enable   Normal     0.0       0         0
  2  Normal Enable   Normal     0.0       0         0
  3  Normal Enable   Normal     0.0       0         0
  4  Normal Enable   Normal     0.0       0         0
  5  Normal Enable   Normal     0.0       0         0
  6  Normal Enable   Normal     0.0       0         0
  7  Normal Enable   Normal     0.0       0         0
  8  Normal Enable   Normal     0.0       0         0
  9  Normal Enable   Normal     0.0       0         0
 10  Normal Enable   Normal     0.0       0         0
 11  Normal Enable   Normal     0.0       0         0
 12  Normal Enable   Normal     0.0       0         0
 13  Normal Enable   Normal     0.0       0         0
 14  Normal Enable   Normal     0.0       0         0
```

```
15  Normal Enable   Normal     0.0        0          0
16  Normal Enable   Normal     0.0        0          0
17  Normal Enable   Normal     0.0        0          0
18  Normal Enable   Normal     0.0        0          0
19  Normal Enable   Normal     0.0        0          0
20  Normal Enable   Normal     0.0        0          0
21  Normal Enable   Normal     0.0        0          0
22  Normal Enable   Normal     0.0        0          0
23  Normal Enable   Normal     0.0        0          0
24  Normal Enable   Normal     0.0        0          0
```


port

- **clear counter**
  - Syntax:

    clear counter
  - Description:

    To clear all ports' counter (include simple and detail port counter) information.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+(port)# clear counter
    ```
- **disable state**
  - Syntax:

    disable state <range>
  - Description:

    To disable the communication capability of the port.
  - Argument:

    <range>: port range, syntax 1,5-7, available from 1 to 26
  - Possible value:

<range>: 1 ~ 26

- Example:

```
ES-2126+(port)# disable state 12
```

- **enable state**
  - Syntax:

    enable state
  - Description:

    To enable the communication capability of the port.
  - Argument:

    <range>: port range, syntax 1,5-7, available from 1 to 26
  - Possible value:

    <range>: 1 ~ 26
  - Example:

```
ES-2126+(port)# enable state 3-10
```

- **set description**
  - Syntax:

    set flow-control <range> <description>
  - Description:

    To enter port description.
  - Argument:

    <range>: port range, syntax 1,5-7, available from 1 to 26

    <description> : port description
  - Possible value:

    <range>: 1 to 26

    <description> : 47 alpha numeric characters
  - Example:

```
ES-2126+(port)# set description 22 port22
```

- **set flow-control**
  - Syntax:

    set flow-control <range> <symmetric|asymmetric>
  - Description:

    To set up the flow control function of all ports.

- Argument:

<range>:port range, syntax 1,5-7, available from 1 to 26

<symmetric>: set its flow control as symmetric

<asymmetric>: set its flow control as asymmetric

- Possible value:

<range>: 1 to 26

- Example:

```
ES-2126+(port)# set flow-control 3-6 symmetric
```

set speed-duplex

- Syntax:

set speed-duplex <range> <auto>|[<10|100|1000> <half|full>]

- Description:

To set up the speed and duplex of all ports.

- Argument:

<range>:port range, syntax 1,5-7, available from 1 to 26

<port-speed>:

auto : set auto-negotiation mode

10 : set speed to 10M

100 : set speed to 100M

1000 : set speed to 1000M

<port-duplex> :

half : set to half duplex

full : set to full duplex

- Possible value:

<range>: 1 to 26

<port-speed> : auto, 10, 100, 1000

<port-duplex> : full, half

- Example:

```
ES-2126+(port)# set speed-duplex 8 100 full
```

show conf

- Syntax:

show conf

- Description:

To display the each port's configuration about state, speed-duplex and flow control.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(port)# show conf
```

- **show desciption**
  - Syntax:

show description

- Description:

To display the ports' descriptions.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126P+(port)# show description
 Port  Description
------------------
 1
 2
 3
 4
 5
 6
 7
 8
```

```
9
10
11
12
13
14
15
16
17
18
19
20
21
22  port22
23
24
25
26
```

- **show detail-counter**
  - Syntax:

    show detail-counter <#>
  - Description:

    To display the detail-counter for each port.
  - Argument:

    <#> : port
  - Possible value:

    <#> : 1 - 26
  - Example:

    ```
    ES-2126+(port)# show detail-counter
    ```
- **show media**
  - Syntax:

show media <port>

- Description:

To display the module 25 or 26 information.

- Argument:

<port>: available 25, 26

- Possible value:

<port>: 25, 26

- Example:

```
ES-2126+(port)# show media 25
Port 25 Fiber Media Information
-------------------------------------------------------
---------------
Connector Type        : SFP - LC
Fiber Type            : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate             : 1G
Vendor OUI            : 00:40:c7
Vendor Name           : APAC Opto
Vendor PN             : KM28-C3S-TC-N
Vendor Rev            : 0000
Vendor SN             : 5425011140
Date Code             : 050530
Temperature           : none
Vcc                   : none
Mon1 (Bias) mA        : none
Mon2 (TX PWR)         : none
Mon3 (RX PWR)         : none
```

show simple-counter

- Syntax:

show simple-counter

- Description:

To display the summary counting of each port's traffic.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(port)# show simple-counter
```

show status

- Syntax:

show status

- Description:

To display the port's current status.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(port)# show status
Port Media Link  State  Auto Nego. Speed/Duplex Rx Pause
Tx Pause
---- ----- ---- ------- ---------- ------------ ------
-- --------
  1    TP    Down  Enable    Enable    ----/----      ----
----
  2    TP    Down  Enable    Enable    ----/----      ----
----
  3    TP    Down  Enable    Enable    ----/----      ----
----
  4    TP    Down  Enable    Enable    ----/----      ----
----
 5   TP    Up   Enable   Enable   100M/Full      ON     ON
```

DE

```
  6    TP    Down   Enable    Enable    ----/----      ----
----
  7    TP    Down   Enable    Enable    ----/----      ----
----
                                 :
                              :
                              :
 24    TP    Down   Enable    Enable    ----/----      ----
----
 25    TP    Down   Enable    Enable    ----/----      ----
----
 26    TP    Down   Enable    Enable    ----/----      ----
----
```

qos

- **disable 1p**
  - Syntax:

    disable 1p
  - Description:

    To disable 802.1p qos.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    `ES-2126+(qos)# disable 1p`
- **disable dscp**
  - Syntax:

    disable dscp
  - Description:

    To disable IP DSCP qos.
  - Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(qos)# disable dscp
```

- **disable qos**
  - Syntax:

disable qos

  - Description:

To disable qos function.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(qos)# disable qos
```

- **disable tos**
  - Syntax:

disable tos

  - Description:

To disable IP TOS qos.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(qos)# disable tos
```

- **enable 1p**
  - Syntax:

enable 1p

  - Description:

To enable 802.1p qos.

DE

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(qos)# enable 1p
```

- **enable dscp**
  - Syntax:

enable dscp

- Description:

To enable IP DSCP qos.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(qos)# enable dscp
```

- **enable qos**
  - Syntax:

enable qos

- Description:

To enable qos function.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(qos)# enable qos
```

- **enable tos**
  - Syntax:

enable tos

- Description:

To enable IP TOS qos.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(qos)# enable tos
```

- **set dscp**
  - Syntax:

    set dscp [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

  - Description:

    To set IP DSCP qos weighting for 4 queues.

  - Argument:

    <q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

    <priority>: priority level. One queue has been assigned 2 different priorities.

    You don't need to use all of queue, but must assign queue in order.

    Syntax: 1,2 or 2,5-7, available from 0 to 63.

  - Possible value:

    <priority>: 0 to 63

  - Example:

```
ES-2126+(qos)# set dscp q0 2 q1 2 q2 2 q3 3
```

- **set pri-tag**
  - Syntax:

    set pri-tag [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

  - Description:

    To set 802.1p qos weighting for 4 queues.

  - Argument:

    <q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

    <priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queues, but must assign queues in order.

- Syntax: 1,2 or 2,5-7, available from 0 to 7.
- Possible value:

<priority>: 0 to 7.

- Example:

```
ES-2126+(qos)# set pri-tag q0 0 q1 2 q3 4
```

- **set sche**
  - Syntax:

set sche <wrr|strict> <wrr_0> <wrr_1> <wrr_2> <wrr_3>

  - Description:

To set qos schedule and weight for 4 queues.

  - Argument:

<wrr> : scheduling weighted round robin method

<strict> : scheduling strict method.

<wrr_0 to 3>: weighted for every queue. Weighted range : 1-55.

  - Possible value:

<wrr|strict>: wrr or strict

<wrr_0 to 3>: 1-55.

  - Example:

```
ES-2126+(qos)# set sche wrr 1 2 8 16
```

- **set tos**
  - Syntax:

set tos <type_value> [<q0><priority>] [<q1><priority>] [<q2><priority>]

[<q3><priority>]

  - Description:

To set IP tos qos weighting for 4 queues.

  - Argument:

<type_value>: Delay Priority: 0;

Throughput Priority: 1;

Reliability Priority: 2;

Monetary Cost Priority: 3.

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queues, but must assign queues in order (from low queue to high queue).

- Syntax: 1,2 or 2,5-7, available from 0 to 7.
- Possible value:

<type_value>: 0~3

<priority>: 0 to 7.

- Example:

```
ES-2126+(qos)# set tos 0 q0 1 q1 2 q2 4 q3 6
```

- **set vip**
  - Syntax:

set vip <port_range> <mode>

  - Description:

To set vip port for strict priority.

  - Argument:

<port_range>: syntax 1,5-7, available from 1 to 26

<mode>: enable/disable vip port for each port. 1: enable. 0: disable.

  - Possible value:

<port_range>: 1 to 26

<mode>: 1 or 0

  - Example:

```
ES-2126+(qos)# set vip 1-6 1
```

- **show dscp**
  - Syntax:

show dscp

  - Description:

To show IP DSCP Qos configuration.

  - Argument:

None.

  - Possible value:

DE

None.

- Example:

```
ES-2126+(qos)# show dscp
ip diffserv classification
====================
Global QoS mode: Enable QoS
                 Disable 802.1p Priority
                 Disable ip tos classification
                 Enable ip diffserv classification
Scheduling:      weighted round robin method.
weight:          wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                 weighted range: 1~55.
P0~63:           Priority 0~63.
Default mode:    Queue0: P0~15; Queue1: P16~31; Queue2:
P32~47; Queue3: P48~63.

 DiffServ   Queue   DiffServ   Queue   DiffServ   Queue
DiffServ   Queue
---------- ------- ---------- ------- ---------- -----
-- ---------- ------
     0          0        1          0        2          0
3          0
     4          0        5          0        6          0
7          0
     8          0        9          0       10          0
11         0
    12          0       13          0       14          0
15         0
    16          1       17          1       18          1
19         1
    20          1       21          1       22          1
23         1
```

```
    24          1       25          1       26          1
27          1
    28          1       29          1       30          1
31          1
    32          2       33          2       34          2
35          2
    36          2       37          2       38          2
39          2
    40          2       41          2       42          2
43          2
    44          2       45          2       46          2
47          2
    48          3       49          3       50          3
51          3
    52          3       53          3       54          3
55          3
    56          3       57          3       58          3
59          3
    60          3       61          3       62          3
63          3
```

- **show port**
  - Syntax:

    show port
  - Description:

    To show VIP port configuration.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(qos)# show port

Port Based Priority

====================
```

```
Global QoS mode: Enable QoS
                 Enable 802.1p Priority
                 Disable ip tos classification
                 Disable ip diffserv classification
 Port No  Mode    Port No   Mode
-------- -------  --------- -------
    1     Enable       2     Enable
    3     Enable       4     Enable
    5     Enable       6     Enable
            :
            :
   23    Disable      24    Disable
   25    Disable      26    Disable
```

- **show priority-tag**
  - Syntax:

  show priority-tag
  - Description:

  To show 802.1p Qos configuration.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(qos)# show priority-tag
802.1p priority
====================
Global QoS mode: Enable QoS
                 Enable 802.1p Priority
                 Disable ip tos classification
                 Disable ip diffserv classification
Scheduling:      weighted round robin method.
```

```
weight:          wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                 weighted range: 1~55.
P0~7:            Priority 0~7.
Default mode:    Queue0: P0,P1; Queue1: P2,P3; Queue2:
P4,P5; Queue3: P6,P7.
```

	P0	P1	P2	P3	P4	P5	P6	P7
Queue	0	0	1	1	2	2	3	3

- **show tos**
  - Syntax:

  show tos
  - Description:

  To show IP tos Qos configuration.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(qos)# show tos
ip tos classification
====================
Global QoS mode: Enable QoS
                 Disable 802.1p Priority
                 Enable ip tos classification
                 Disable ip diffserv classification
```

```
Scheduling:       weighted round robin method.
weight:           wrr 0 = 1; wrr 1 = 1; wrr 2 = 8; wrr 3
= 16.
                  weighted range: 1~55.
P0~7:             Priority 0~7.
Default mode:     Queue0: P0,P1; Queue1: P2,P3; Queue2:
P4,P5; Queue3: P6,P7.

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Delay Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Throughput Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Reliability Priority

        P0   P1   P2   P3   P4   P5   P6   P7
       ---- ---- ---- ---- ---- ---- ---- ----
Queue  0    0    1    1    2    2    3    3
TOS type: Monetary Cost Priority
```

reboot

- **reboot**
  - Syntax:

    reboot
  - Description:

    To reboot the system.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+# reboot
    ```

security

<<isolated-group>>

- **set**
  - Syntax:

    set <port>
  - Description:

    To set up the function of the isolated group.
  - Argument:
  - <port> : isolated port; range syntax: 1,5-7, available from 0 to 26

    set 0 as disabled
  - Possible value:

    <port>:0 to 26
  - Example:

    ```
    ES-2126+(security-isolated-group)# set 2,3,4
    ```
- **show**
  - Syntax:

    show
  - Description:

    To display the current setting status of isolated group.
  - Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(security-isolated-group)# show
Isolated group:
2 3 4
<<mirror>>
```

- **disable**
  - Syntax:

disable

  - Description:

To disable the function of mirror.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(security-mirror)# disable
```

- **enable**
  - Syntax:

enable

  - Description:

To enable the function of mirror.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(security-mirror)# enable
```

- **set**
  - Syntax:

set <spy> <ingress> <egress>

- Description:

To set up the monitoring port and monitored ports of the mirror function. User can monitor the ports that receive or transmit the packets.

- Argument:

<spy>: monitoring port

- <ingress>: monitored ingress port; range syntax: 1,5-7, available from 0 to 26
- <egress>: monitored egress port; range syntax: 1,5-7, available from 0 to 26

  set ingress/egress to 0 as ingress/egress disabled

- Possible value:

<ingress>: 0 to 26

<egress>: 0 to 26

- Example:

```
ES-2126+(security-mirror)# set 1 4 2-3
```

show

- Syntax:

show

- Description:

To display the current setting status of mirror.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(security-mirror)# show
Mirror:
Monitoring Port  :1
Monitored Ingress :4
Monitored Egress  :2 3
```

DE

snmp

- **disable**
  - Syntax:

    disable set-community

    disable snmp
  - Description:

    The Disable here is used for the de-activation of snmp or set-community.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+(snmp)# disable set-community
    ES-2126+(snmp)# disable snmp
    ```
- **enable**
  - Syntax:

    enable set-community

    enable snmp
  - Description:

    The Enable here is used for the activation snmp or set-community.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+(snmp)# enable set-community
    ES-2126+(snmp)# enable snmp
    ```
- **set**
  - Syntax:

    set get-community <community>

    set set-community <community>

    set trap <#> <ip> [port] [community]

- Description:

The Set here is used for the setup of get-community, set-community, trap host ip, host port and trap- community.

- Argument:

<#>: trap number, range: 1 to 6

<ip>: ip address or domain name

<port>: trap port

<community>: community name

- Possible value:

<trap number> : 1 to 6

<port> :1~65535

- Example:

```
ES-2126+(snmp)# set get-community public
ES-2126+(snmp)# set set-community private
ES-2126+(snmp)# set trap 1 192.168.1.1 162 public
```

- **show**
  - **Syntax**:

show

  - Description:

The Show here is to display the configuration of SNMP.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(snmp)# show
SNMP          : Enable
Get Community: public
Set Community: private [Enable]
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community:
public
```

```
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community:
public
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community:
public
```

stp

- **MCheck**
  - Syntax:

    MCheck <range>
  - Description:

    To force the port to transmit RST BPDUs.
  - Argument:

    <range>: syntax 1,5-7, available from 1 to 26
  - Possible value:

    <range>: 1 to 26
  - Example:

```
ES-2126+(stp)# Mcheck 1-8
```

- **disable**
  - Syntax:

    disable
  - Description:

    To disable the function of STP.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(stp)# disable
```

- **enable**
  - Syntax:

    enable
  - Description:

    To enable the function of STP.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(stp)# enable
```

- **set config**
  - Syntax:

    set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>
  - Description:

    To set up the parameters of STP.
  - Argument:

    <Bridge Priority>: priority must be a multiple of 4096,available from 0 to 61440.

    <Hello Time>: available from 1 to 10.

    <Max. Age>: available from 6 to 40.

    <Forward Delay>: available from 4 to 30.

    Note: 2*(Forward Delay -1) >= Max Age

    Max Age >= 2*(Hello Time +1)
  - Possible value:

    <Bridge Priority>: 0 to 61440.

    <Hello Time>: 1 to 10.

    <Max. Age>: 6 to 40.

    <Forward Delay>: 4 to 30.
  - Example:

```
ES-2126+(stp)# set config 61440 2 20 15
```

DE

- **set port**
  - Syntax:

    set port <range> <path cost> <priority> <edge_port> <admin p2p>
  - Description:

    To set up the port information of STP.
  - Argument:

    <range>: syntax 1,5-7, available from 1 to 26

    <path cost>: 0, 1-200000000. The value zero means auto status

    <priority>: priority must be a multiple of 16, available from 0 to 240

    <edge_port>: Admin Edge Port, <yes|no>

    <admin p2p>: Admin point to point, <auto|true|false>
  - Possible value:

    <range> :1 to 26 <path cost>: 0, 1-200000000.

    <priority> : 0 to 240 <edge_port> : yes / no

    <admin p2p>: auto / true / false
  - Example:

    ```
    ES-2126+(stp)# set port 1-16 0 128 yes auto
    ```
- **set version**
  - Syntax:

    set version <stp|rstp>
  - Description:

    To set up the version of STP.
  - Argument:

    <stp|rstp>:stp / rstp
  - Possible value:

    <stp|rstp>:stp / rstp
  - Example:

    ```
    ES-2126+(stp)# set version rstp
    ```
- **show config**
  - Syntax:

    show config
  - Description:

To display the STP configuration data.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(stp)# show config

STP State Configuration :

Spanning Tree Protocol    : Enabled

Bridge Priority (0-61440) : 61440

Hello Time (1-10 sec)     : 2

Max. Age (6-40 sec)       : 20

Forward Delay (4-30 sec)  : 15

Force Version             : RSTP
```

show port

- Syntax:

show port

- Description:

To display the port information of STP.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(stp)# show port

Port  Port  Status  Path  Cost  Priority  Admin  Edge  Port
Admin Point To Point

====  ==========  =========  ========  ===============
====================

   1   DISCARDING      2000000      128             Yes
Auto
```

DE

```
   2   DISCARDING      2000000      128              Yes
Auto
   3   DISCARDING      2000000      128              Yes
Auto
   4   DISCARDING      2000000      128              Yes
Auto
   5   DISCARDING      2000000      128              Yes
Auto
                  :
                  :
                  :
  23   DISCARDING       200000      128               No
Auto
  24   DISCARDING       200000      128               No
Auto
  25   DISCARDING        20000      128               No
Auto
  26   DISCARDING        20000      128               No
Auto
```

- **show status**
  - Syntax:

    show status
  - Description:

    To display of the status of STP.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(stp)# show status
STP Status :
STP State                          : Enabled
Bridge ID                          : 00:40:C7:D8:09:1D
```

```
Bridge Priority                      : 61440
Designated Root                    : 00:40:C7:D8:09:1D
Designated Priority                  : 61440
Root Port                            : 0
Root Path Cost                       : 0
Current Max. Age(sec)                : 20
Current Forward Delay(sec)           : 15
Hello Time(sec)                      : 2
STP Topology Change Count            : 0
Time Since Last Topology Change(sec) : 848
```

system

- **set contact**
  - Syntax:

    set contact <contact>
  - Description:

    To set the contact description of the switch.
  - Argument:

    <contact>:string length up to 40 characters.
  - Possible value:

    <contact>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.
  - Example:

    ES-2126+(system)# set contact Taipei
- **set device-name**
  - Syntax:

    set device-name <device-name>
  - Description:

    To set the device name description of the switch.
  - Argument:

    <device-name>: string length up to 40 characters.
  - Possible value:

    <device-name>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

DE

- Example:

ES-2126+(system)# set device-name CR-2600

- **set location**
  - Syntax:

set location <location>

  - Description:

To set the location description of the switch.

  - Argument:

<location>: string length up to 40 characters

  - Possible value:

<location>: A, b, c, d, ... ,z and 1, 2, 3, …. etc.

  - Example:

```
ES-2126+(system)# set location Taipei
```

- **show**
  - Syntax:

show

  - Description:

To display the basic information of the switch.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(system)# show
Model Name                      : ES-2126+
System Description               : 24-Port 10/100BaseT/TX
Managed PoE Switch
Location                        :
Contact                         :
Device Name                     : ES-2126+
System Up Time              : 0 Days 0 Hours 4 Mins 50 Secs
Current Time                    : Wed Feb 08 16:55:29 2006
```

```
BIOS Version                  : v1.05
Firmware Version              : v2.07
Hardware-Mechanical Version   : v1.01-v1.01
Serial Number                 : 031203000004
Host IP Address               : 192.168.1.1
Host MAC Address              : 00-00-8c-00-d8-00
Device Port                 : UART * 1  TP *24  Fiber * 2
RAM Size                      : 16 M
Flash Size                    : 2 M
```

tac-plus

- **show access**
  - Syntax:

    show access
  - Description:

    Shows the access configuration.
  - Example:

```
ES-2126+(tac-plus)# show access
Access retry : 3
Access    Login    Login
          Primary  Secondary
-------   -------  ---------
Console   Local    None
Telnet    TACACS   Local
Web       TACACS   Local
```

- **show tac-plus**
  - Syntax:

    show tac-access
  - Description:

    Shows the TACACS+ configuration.
  - Example:

```
ES-2126+(tac-plus)# show tac-plus
```

```
Authorization                  : Enable
Fallback to Local Authorization: Enable
Accounting                     : Enable
Secret Key: secret
#    Server IP
- ---------------
1  10.1.1.1
2  0.0.0.0
```

- **enable**
  - Syntax:

    enable <argument>
  - Description:

    Enables the TACACS+ functions for accounting, authorization and fallback to local authorization.
  - Arguments:

    Accounting: enables the TACACS+ accounting.

    Authorization: enables the TACACS+ authorization.

    Fallback-author: enables the fallback to local authorization.
- **disable**
  - Syntax:

    disable <argument>
  - Description:

    Disables the TACACS+ functions for accounting, authorization and fallback to local authorization.
  - Arguments:

    Accounting: disables the TACACS+ accounting.

    Authorization: disables the TACACS+ authorization.

    Fallback-author: disables the fallback to local authorization.
- **set console-access**
  - Syntax:

    set console-access <method1> <method2>
  - Description:

Sets the primary and secondary access mode for the login via console (outband).

- Arguments:

Method from 0 to 2:

0: Authentication via local user accounts of the device.

1: Authentication via TACACS+-Server.

2: No authentication required (for method 2 only).

- Example:

```
ES-2126+(tac-plus)#  set console-access 1 0

Sets the primary access mode for the login via console
to TACACS+ and the secondary access mode to local user
accounts.
```

set host

- Syntax:

set host <#> <ip>

- Description:

Sets the IP addresses for the first and secondary TACACS+ server.

- Arguments:

#: Number from 1 (first TACACS+ server) to 2 (secondary TACACS+ server).

ip: IP address of the TACACS+ server

- Example:

```
ES-2126+(tac-plus)#  set host 1 10.1.1.1

Sets the IP address of the primary TACACS+ server to
"10.1.1.1".
```

set key

- Syntax:

set key <secret-key>

- Description:

Sets the encryption key for the communication with the TACACS+ server. This key must correspond with the encryption key which is configured in the TACACS+ server.

- Arguments:

secret-key: maximum 31 characters.

- Example:

```
ES-2126+(tac-plus)#  set key secret

Sets the encryption key to "secret".
```

- **set retry**
  - Syntax:

    set retry <retry>
  - Description:

    Sets the access retry value. When the login failed for the number of retries, the secondary login method will be used.

    If TACACS+ is defined as primary access mode, the secondary TACACS+ server is used after the number of login failures has reached the access retry value. After the number of login failures has reached the access retry value even on the secondary TACACS+ server, the secondary login method will be used.
  - Arguments:

    retry: 1 to 3.
  - Example:

```
ES-2126+(tac-plus)#  set retry 2

Sets the access retry value to "2".
```

- **set telnet-access**
  - Syntax:

    set telnet-access <method1> <method2>
  - Description:

    Sets the primary and secondary access mode for the login via telnet.
  - Arguments:

    Method from 0 to 2:

    0: Authentication via local user accounts of the device.

    1: Authentication via TACACS+-Server.

    2: No authentication required (for method 2 only).
  - Example:

```
ES-2126+(tac-plus)#  set telnet-access 1 0
```

```
Sets the primary access mode for the login via telnet
to TACACS+ and the secondary access mode to local user
accounts.
```

- **set web-access**
  - Syntax:

    set web-access <method1> <method2>
  - Description:

    Sets the primary and secondary access mode for the login via web browser.
  - Arguments:

    Method from 0 to 2:

    0: Authentication via local user accounts of the device.

    1: Authentication via TACACS+-Server.

    2: No authentication required (for method 2 only).
  - Example:

```
ES-2126+(tac-plus)#  set web-access 1 0
```

```
Sets the primary access mode for the login via web
browser to TACACS+ and the secondary access mode to
local user accounts.
```

tftp

- **set server**
  - Syntax:

    set server <ip>
  - Description:

    To set up the IP address of tftp server.
  - Argument:

    <ip>: the IP address of tftp server
  - Possible value:

    <ip>: tftp server IP
  - Example:

```
ES-2126+(tftp)# set server 192.168.3.111
```

DE

- **show**
  - Syntax:

    show
  - Description:

    To display the information of tftp server.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(tftp)# show
Tftp Server : 192.168.3.111
```

time

- **set daylightsaving**
  - Syntax:

    set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>
  - Description:

    To set up the daylight saving.
  - Argument:

```
<hr>   : daylight saving hour, range: -5 to +5
<MM>   : daylight saving start Month (01-12)
<DD>   : daylight saving start Day (01-31)
<HH>   : daylight saving start Hour (00-23)
<mm>   : daylight saving end Month (01-12)
<dd>   : daylight saving end Day (01-31)
<hh>   : daylight saving end Hour (00-23)
```
  - Possible value:

```
<hr>   : -5 to +5
<MM>   : (01-12)
<DD>   : (01-31)
<HH>   : (00-23)
```

```
<mm>   : (01-12)
<dd>   : (01-31)
<hh>   : (00-23)
```

- Example:

```
ES-2126+(time)# set daylightsaving 3 10/12/01 11/12/01
```

- **set manual**
  - Syntax:

    set manual <YYYY/MM/DD> <hh:mm:ss>
  - Description:

    To set up the current time manually.
  - Argument:

```
<YYYY> : Year   (2000-2036)    <MM>  : Month  (01-12)
<DD>   : Day    (01-31)        <hh>  : Hour   (00-23)
<mm>   : Minute (00-59)        <ss>  : Second (00-59)
```

  - Possible value:

```
<YYYY>: (2000-2036)           <MM>  : (01-12)
<DD>   : (01-31)               <hh>  : (00-23)
<mm>   : (00-59)               <ss>  : (00-59)
```

  - Example:

```
ES-2126+(time)# set manual 2005/04/21 16:18:50
```

- **set ntp**
  - Syntax:

    set ntp <ip> <timezone>
  - Description:

    To set up the current time via NTP server.
  - Argument:

    <ip>: ntp server ip address or domain name

    <timezone>: time zone (GMT), range: -12 to +13
  - Possible value:

    <timezone>: -12,-11…,0,1…,13
  - Example:

```
ES-2126+(time)# set ntp clock.via.net 8
```

```
Synchronizing...(1)
Synchronization success
```

- **show**
  - Syntax:

    show
  - Description:

    To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”,
    ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(time)# show
Current Time          : Wed Apr 21 06:16:22 2005
NTP Server            : 209.81.9.7
Timezone              : 8
Day light Saving      : 4 Hours
Day light Saving Start: Mth: 2 Day: 20 Hour: 10
Day light Saving End  : Mth: 3 Day: 20 Hour: 10
```

trunk

- **del trunk**
  - Syntax:

    del trunk <port-range>
  - Description:

    To remove the trunk port.
  - Argument:

    <port-range> : syntax 1,5-7, available from 1 to 26
  - Possible value:

    <port-range> : 1 to 26
  - Example:

```
ES-2126+(trunk)# del trunk 1
```

- **set hash**
  - Syntax:

  set hash <method>
  - Description:

  To set up trunk hash method.
  - Argument:

  <method>: lacp hash method

  0: DA and SA

  1: SA

  2: DA

  Note : This hash method applies to both LACP and static trunk.
  - Possible value:

  <method>: 0~2
  - Example:

```
ES-2126+(trunk)# set hash 2
```

- **set priority**
  - Syntax:

  set priority <range>
  - Description:

  To set up the LACP system priority.
  - Argument:

  <range>:available from 1 to 65535.
  - Possible value:

  <range>:1 to 65535.
  - Example:

```
ES-2126+(trunk)# set priority 33333
```

- **set trunk**
  - Syntax:

  set trunk <port-range> <method> <group> <active LACP>
  - Description:

DE

To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.

- Argument:

<port-range> : syntax 1,5-7, available from 1 to 26

<method>: <static|lacp>

static : adopt the static link aggregation

lacp : adopt the dynamic link aggregation- link aggregation control protocol

<group>: 1-3.

<active LACP>: <passive|active>

active : set the LACP to active mode

passive : set the LACP to passive mode

- Possible value:

<port-range> : 1 to 26

<method>: static or lacp

<group>: 1-3.

<active LACP>: active or passive

- Example:

```
ES-2126+(trunk)# set trunk 2-5 lacp 1 active
```

- **show aggtr-view**
  - Syntax:

show aggtr-view

- Description:

To display the aggregator list.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(trunk)# show aggtr-view


Aggregator  1) Method: None
```

```
                    Member Ports: 1
                    Ready Ports:1

Aggregator  2) Method: LACP
                    Member Ports: 2
                    Ready Ports:
                      :
                      :
                      :
```

- **show lacp-config**
  - Syntax:

    show lacp-config
  - Description:

    To display the value of LACP Priority.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(trunk)# show lacp-config
LACP System Priority : 33333
Hash Method      : DA
```

- **show lacp-detail**
  - Syntax:

    show lacp-detail <aggtr>
  - Description:

    To display the detailed information of the LACP trunk group.
  - Argument:

    <aggtr> : aggregator, available from 1 to 26
  - Possible value:

    <aggtr> : 1 to 26

DE

- Example:

```
ES-2126+(trunk)# show lacp-detail 2


Aggregator 2 Information:
              Actor                                Partner
--------------------------------  --------------------
-------------
System Priority    MAC Address    System Priority    MAC
Address
---------------  -----------------  ---------------  ----
-------------
     32768       00-40-c7-e8-00-02       32768       00-
00-00-00-00-00


 Port    Key      Trunk Status        Port             Key
------  --------  -----------------  ---------------  ----
-------------
   2     257           ---              2                0
```

show status

- Syntax:

show status

- Description: Description:

To display the aggregator status and the settings of each port.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(trunk)# show status
         Trunk Port Setting           Trunk Port Status
-------------------------------------  ----------------
------
```

DE

```
 port    Method    Group    Active LACP    Aggtregator
Status
======  ========  =======  =============  =============
========
  1     None      0       Active           1        Ready
  2     LACP      1        Active           2         ---
  3     LACP      1        Active           3         ---
  4     LACP      1        Active           4         ---
  5     LACP      1        Active           5         ---
  6     None      0        Active           6         ---
  7     None      0        Active           7         ---
  8     None      0        Active           8         ---
  9     None      0        Active           9         ---
 10     None      0        Active          10         ---
 11     None      0        Active          11         ---
 12     None      0        Active          12         ---
 13     None      0        Active          13         ---
 14     None      0        Active          14         ---
 15     None      0        Active          15         ---
 16     None      0        Active          16         ---
 17     None      0        Active          17         ---
 18     None      0        Active          18         ---
 19     None      0        Active          19         ---
 20     None      0        Active          20         ---
 21     None      0        Active          21         ---
 22     None      0        Active          22         ---
 23     None      0        Active          23         ---
 24     None      0        Active          24         ---
 25     None      0        Active          25         ---
 26     None      0        Active          26         ---
```

DE

VLAN

- **del port-group**
  - Syntax:

    del port-group <name>
  - Description:

    To delete the port-based VLAN group.
  - Argument:

    <name>: port-VLAN name
  - Possible value:

    <name>: port-VLAN name
  - Example:

    ```
    ES-2126+(VLAN)# del port-group VLAN-2
    ```
- **del tag-group**
  - Syntax:

    del tag-group <vid>
  - Description:

    To delete the tag-based VLAN group.
  - Argument:

    <vid>: VLAN ID, available from 1 to 4094
  - Possible value:

    <vid>: 1 to 4094
  - Example:

    ```
    ES-2126+(VLAN)# del tag-group 2
    ```
- **disable double-tag**
  - Syntax:

    disable double-tag
  - Description:

    To disable double-tag.
  - Argument:

    None.
  - Possible value:

    None.

- Example:

```
ES-2126+(VLAN)# disable double-tag
```

- **disable drop-untag**
  - Syntax:

    disable drop-untag <port_range>
  - Description:

    To disable drop-untag.
  - Argument:
  - <port_range>: which port(s) you want not to drop untagged frames. Syntax: 1,5-7, available from 1 to 26
  - Possible value:

    <port_range>: 1 to 26
  - Example:

```
ES-2126+(VLAN)# disable drop-untag 2,4,5-7
```

- **disable svl**
  - Syntax:

    disable svl
  - Description:

    To enable Independent VLAN Learning.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

```
ES-2126+(VLAN)# disable svl
```

- **disable symmetric**
  - Syntax:

    disable symmetric
  - Description:

    To Not drop frames from the non-member port.
  - Argument:

    None.

- Possible value:

None.

- Example:

```
ES-2126+(VLAN)# disable symmetric
```

- **enable double-tag**
  - Syntax:

enable double-tag

  - Description:

To enable double-tag.

  - Argument:

None.

  - Possible value:

None.

  - Example:

```
ES-2126+(VLAN)# enable double-tag
```

- **enable drop-untag**
  - Syntax:

enable drop-untag <port_range>

  - Description:

To enable drop-untag.

  - Argument:
  - <port_range>: which port(s) you want to drop untagged frames. Syntax: 1,5-7, available from 1 to 26
  - Possible value:

<port_range>: 1 to 26

  - Example:

```
ES-2126+(VLAN)# enable drop-untag 2,4,5-7
```

- **enable svl**
  - Syntax:

enable svl

  - Description:

To enable Shared VLAN Learning.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(VLAN)# enable svl
```

■ **enable symmetric**

- Syntax:

enable symmetric

- Description:

To drop frames from the non-member port.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(VLAN)# enable symmetric
```

■ **set mgt-vlan**

- Syntax:

set mgt-vlan <state> <vid>

- Description:

To set configuration of port-based vlan.

- Argument:

<state> : 0 for disable, 1 for enable

<vid> : vlan id, from 1 to 4094

- Possible value:

<state> : 0 - 1

<vid> : 1 - 4094

- Example:

```
ES-2126+(VLAN)# set mgt-vlan 1 300
```

■ **set mode**

- Syntax:

set mode <port|tag>

- Description:

To switch VLAN mode between port-based and tag-based modes.

- Argument:

<port|tag>: port or tag

tag: set tag-based VLAN

port: set port-based VLAN

- Possible value:

<port|tag>: port or tag

- Example:

```
ES-2126+(VLAN)# set mode tag
```

set port-group

- Syntax:

set port-group <name> <range>

- Description:

To add or edit a port-based VLAN group.

- Argument:

<name>: port-VLAN name

- <range>: VLAN group members, syntax: 1,5-7, available from 1 to 26
- Possible value:

<range>: 1 to 26

- Example:

```
ES-2126+(VLAN)# set port-group VLAN-1 2-5,6-10
```

set pvid

- Syntax:

set pvid <port_range> <pvid> <default_priority>

- Description:

To set VLAN PVID and port pripority.

- Argument:

<port_range>: which port(s) you want to set PVID(s). Syntax 1,5-7, available from 1 to 26

<pvid>: which PVID you want to set, available from 1 to 4094

<default_priority>: which priority you want to set, available from 0 to 7

- Possible value:

<port_range>: 1 to 26

<pvid>: 1 to 4094

<default_priority>: 0 to 7

- Example:

```
ES-2126+(VLAN)# set pvid 3,5,6-8 5 6
```

- **set tag-group**
  - Syntax:

set tag-group <vid> <name> <member_range> <untag_range>

  - Description:

To add or edit the tag-based VLAN group.

  - Argument:

<vid>: VLAN id, from 1 to 4094

<name>: tag-VLAN group name

  - <member_range>: member port; syntax: 1,5-7, available from 1 to 26
  - <untag_range>: untagged out port; syntax: 1,5-7, available from 0 to 26

    set untag_range to 0 as none of the ports are force untagged

  - Possible value:

<vid>: 1 to 4094

<member_range>: 1 to 26

<untag_range>: 0 to 26

  - Example:

```
ES-2126+(VLAN)# set tag-group 2 VLAN-2 2-5,6,15-13 0
```

- **show config**
  - Syntax:

show config

  - Description:

To display the current VLAN mode, Symmetric VLAN, SVL and Double tag states.

DE

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(VLAN)# show config

Current VLAN mode:Tag-based VLAN
Global setting:
Symmetric VLAN  : Disable (Asymmetric)
SVL             : Disable (IVL)
Double tag      : Disable
```

show group

- Syntax:

show group

- Description:

To display VLAN mode and VLAN group.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(VLAN)# show group

Vlan mode is tag-based.

1)  Name   :default
    VID    :1
    Member:1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24
           25 26
```

```
    Untag :1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
19 20 21 22 23 24
          25 26
2)  Name  :VLAN-2
    VID   :2
    Member:2 3 4 5 6 13 14 15
    Untag :
```

- **show pvid**
  - Syntax:

  show pvid
  - Description:

  To display pvid, priority and drop untag result.
  - Argument:

  None.
  - Possible value:

  None.
  - Example:

```
ES-2126+(VLAN)# show pvid
 Port   PVID   Priority   Drop Untag
------ ------ ---------- ------------
   1       1        0      Disable
   2       1        0      Disable
   3       5        6      Disable
   4       1        0      Disable
   5       5        6      Disable
   6       5        6      Disable
   7       5        6      Disable
   8       5        6      Disable
   9       1        0      Disable
  10       1        0      Disable
  11       1        0      Disable
```

DE

```
12          1          0          Disable
13          1          0          Disable
14          1          0          Disable
15          1          0          Disable
16          1          0          Disable
17          1          0          Disable
18          1          0          Disable
19          1          0          Disable
20          1          0          Disable
21          1          0          Disable
22          1          0          Disable
23          1          0          Disable
24          1          0          Disable
25          1          0          Disable
26          1          0          Disable
```

vs

- **disable**
  - Syntax:

    disable
  - Description:

    To disable the virtual stack.
  - Argument:

    None.
  - Possible value:

    None.
  - Example:

    ```
    ES-2126+(vs)# disable
    ```
- **enable**
  - Syntax:

    enable
  - Description:

To enable the virtual stack.

- Argument:

None.

- Possible value:

None.

- Example:

```
ES-2126+(vs)# enable
```

- **set gid**
  - Syntax:

set gid <gid>

  - Description:

To set the group id.

  - Argument:

<gid>: group ID

  - Possible value:

<gid>: a-z,A-Z,0-9

  - Example:

```
ES-2126+(vs)# set gid group1
```

- **set role**
  - Syntax:

set role <master|slave>

  - Description:

To set role.

  - Argument:

<master|slave>: master: act as master, slave : act as slave

  - Possible value:

<master|slave>: master or slave

  - Example:

```
ES-2126+(vs)# set role master
```

- **show**
  - Syntax:

show

- Description:

To display the configuration of the virtual stack.

- Argument:

None.

- Possible value:

None.

- Example:

ES-2126+(vs)# show

```
Virtual Stack Config:
State      : Enable
Role       : Master
Group ID   : group1
```

6 Appendix

6.1 Performance data and specifications

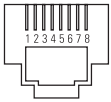
		LANCOM ES-2126+	LANCOM ES-2126P+
Performance	Switching technology	Store and forward with latency less than 5 µs	
	MAC addresses	Support of max 8K MAC addresses	
	Throughput	max. 8.8 Gbps on the backplane	
	Virtual Stacking Management (VSM)	Supports stacking of up to 16 devices, several switches can be managed via one ip address	
	VLAN	Port based and IEEE 802.1q tag based VLAN with up to 4096 VLAN and up to 256 active VLANs; Supports ingress and egress packet filter in port based VLAN	
LAN protocols	Link Aggregation Control Protocol (LACP)	2 Fast- and 1 Gigabit Ethernet groups, max 4 member per group, supports DA, SA and DA+SA MAC based trunking with automatic failover	
	Multicasting	Supports IGMP snooping inkluding active and passive mode	
	GVRP/GARP	802.1q with GVRP/GARP	
	Spanning Tree Protokoll (STP) / Rapid STP	802.1d/1w	
802.3af Features	Ports		24x 802.3af PoE ports
	Power		185 Watt total power with dynamic load balancing on all ports (i.e. up to 15.4 watt for 12 ports or 7.7 watt für 24 ports)
	Priorisation		Supports port based priority and PoE status setting
	Status information		Monitoring via LED, displaying the actual power consumption per port in web interface
Interfaces	Ethernet ports	24 ports 10/100 Mbps fast ethernet, 2 Combo ports TP/SFP 10/100/1000 Mbps	
	Serial interface	Serial configuration interface	
Power supply		Internal power supply unit (110–230 V, 50-60 Hz)	
Housing		Robust metal housing, 19" 1U (440 x 44 x 209 mm) with removable mounting brackets, network connectors on the front	

		LANCOM ES-2126+ LANCOM ES-2126P+
CE		CE conformity according to EN 55022, EN 55024, EN 60950
Environment		Temperature range 0–40°C; humidity 5–90%; non-condensing
Accessories		■ 1000Base-SX SFP module, LANCOM SFP-SX-LC1, item no. 61556 ■ 1000Base-LX SFP module, LANCOM SFP-LX-LC1, item no. 61557
Service		5 years
Support		via Hotline and Internet

6.2 Connector wiring

6.2.1 Ethernet interface 10/100Base-TX

8-pin RJ45 sockets (ISO 8877, EN 60603-7)

Connector	Pin	Line
	1	T+
	2	T-
	3	R+
	4	PoE/G
	5	PoE/G
	6	R-
	7	PoE/ -48 V
	8	PoE/ -48 V

6.3 CE-declarations of conformity

CE

LANCOM Systems herewith declares that the devices of the type described in this documentation are in agreement with the basic requirements and other relevant regulations of the 1995/5/EC directive.

The CE declarations of conformity for your device can be found on the relevant product page on the LANCOM Web site (www.lancom-systems.com).