



TRENDNET®



User's Guide

TEG-S2620i
H/W: V1.0R

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
1 GETTING STARTED.....	4
1.1 CONNECTING TO THE SWITCH CONSOLE PORT.....	4
1.2 PC COM PORT SETTING.....	4
1.3 CONNECTING TO THE SWITCH WEB PORT.....	4
1.4 SWITCH FUNCTION FEATURES.....	5
2 OPERATION NOTICE.....	6
2.1 COMMAND LINE EDITING.....	6
2.2 COMMAND HELP.....	7
2.3 HOW TO USE LOADER.....	8
2.3.1 Connect switch.....	8
2.3.2 Enter loader.....	8
2.3.3 Commands in loader.....	8
3 LOGIN.....	13
3.1 POWER-ON SELF-TESTING.....	13
3.2 CONSOLE LOGIN.....	13
3.3 WEB LOGIN.....	13
3.3.1 Setting IP Address by Console Port.....	13
3.3.2 Login with a Web Browser.....	13
4 CONSOLE USER INTERFACE.....	15
4.1 SYSTEM COMMANDS.....	15
4.2 SWITCH STATIC CONFIGURATION.....	16
4.2.1 Port Configuration and Status.....	16
4.2.2 Trunk.....	18
4.2.3 VLAN.....	20
4.2.4 Misc Configuration.....	27
4.2.5 Administration.....	27
4.2.5 Administration.....	28
4.2.6 Port Mirroring.....	29
4.2.7 Quality of Service.....	30
4.2.8 MAC Address Table.....	32
4.2.9 MAC Limit.....	33
4.3 PROTOCOL RELATED CONFIGURATION.....	34
4.3.1 STP/RSTP.....	34
4.3.2 MSTP.....	36
4.3.3 SNMP.....	39
4.3.4 IGMP.....	42
4.3.5 802.1x.....	43
4.3.6 DHCP Relay & Option 82.....	45
4.3.7 LLDP.....	47
4.4 SYSLOG.....	49
4.5 REBOOT SWITCH.....	49
4.5.1 Reset to Default.....	49
4.5.2 Restart.....	49
4.6 TFTP FUNCTION.....	49
4.6.1 TFTP Firmware Update.....	49
4.6.2 Restore Configure File.....	49
4.6.3 Backup Configure File.....	49
4.7 ACCESS CONTROL LIST.....	50
4.7.1 IPv4 ACL commands.....	50
4.7.2 Non-IPv4 ACL commands.....	51

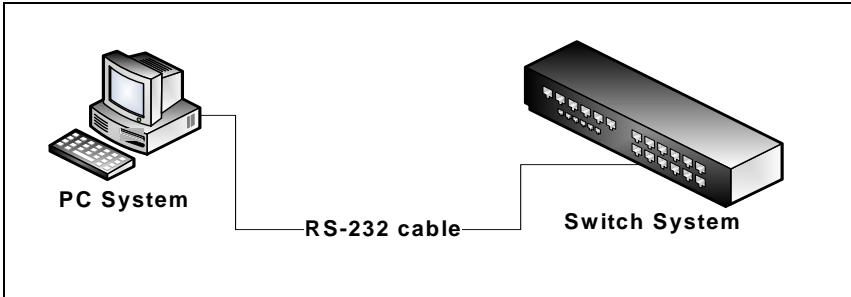
4.7.3	SIP/SMAC Binding	52
5	WEB USER INTERFACE.....	53
5.1	MAIN MENU	53
5.2	ADMINISTRATION	53
5.2.1	IP Address Setting	54
5.2.2	Switch Setting	54
5.2.3	Console Port Information	56
5.2.4	Port Configuration	57
5.2.5	SNMP Configuration	61
5.2.6	Syslog	65
5.2.7	Firmware Update	66
5.2.8	Configuration Backup	68
5.3	L2 FEATURES	69
5.3.1	VLAN Configuration	69
5.3.2	Trunking	77
5.3.3	Forwarding and Filtering	80
5.3.4	Spanning Tree	85
5.3.5	DHCP Relay and Option 82	92
5.3.6	LLDP	93
5.4	ACCESS CONTROL LIST	95
5.4.1	IPv4	96
5.4.2	Non-IPv4	98
5.4.3	Binding	99
5.4.4	QoS VoIP	100
5.5	SECURITY	101
5.5.1	Security Manager	101
5.5.2	MAC Limit	102
5.5.3	802.1x Configuration	103
5.6	QoS	105
5.6.1	QoS Configuration	105
5.6.2	Per-Port Configuration	106
5.7	MONITORING	107
5.7.1	Port Status	107
5.7.2	Port Statistics	108
5.8	RESET SYSTEM	108
5.9	REBOOT.....	108

1 Getting Started

Thanks for using the firmware for configuring EP-5926. There is two ways to access the switch management. You can use the Console mode local management and Web-based interface management.

1.1 Connecting to the Switch Console Port

- Users can use a RS-232 non-crossover serial cable to connect the PC's COM port to the switch console port.
- The switch system provides the RS-232 interface with baud rate 115200-8-n-1.
- Use terminal emulation program (e.g. Windows HyperTerminal...) to configure the switch system.

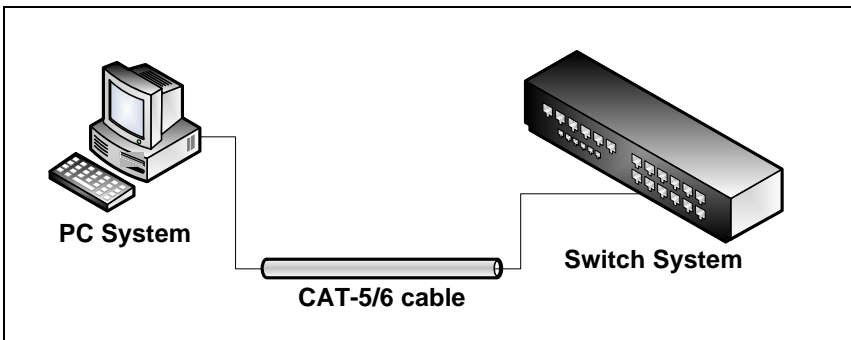


1.2 PC COM Port Setting

- Baud rate =115200
- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow control = None

1.3 Connecting to the Switch Web Port

- Users can use a CAT-5/6 cable to connect the PC's LAN port to one of the switch Ethernet port.
- Use web browser program (e.g. Internet Explorer, Mozilla Firefox) to configure the switch system.
- See section 3.3. Web login for exhaustive login information.



1.4 Switch Function Features

This system provides the following function features to facilitate network management, security and controls:

- 24 10/100Mbps RJ-45 ports and 2 10/100/1000Mbps module ports
 - 1 serial (RS-232) port for console management
 - Support up to 9KB jumbo frame
 - Command line interface (CLI) and browser-independent, secured web-based managements (HTTPS)
 - Up to 13-group and 8-member per group of static and LACP link aggregation (trunk)
 - Up to 512-group of port-based and tag-based (802.1q) VLAN
 - GVRP for tag-based VLAN
 - Per-port storm control for flooded unicast, multicast, IP multicast, broadcast and control packets
 - Spanning-tree protocols: STP (802.1d), RSTP (802.1w), MSTP (802.1s)
 - IGMP Snooping & Query (IGMP v1/v2)
 - SNMP v1/v2c/v3 management and trap function
 - Support MIB tables: MIB-II (RFC 1213), Bridge MIBs (RFC 1493), Ethernet-like MIB (RFC 1643 & RFC 2665), private-MIB, USM-MIB (RFC 2574), VACM-MIB (RFC 2575) and RMON-MIB 1, 2, 3, 9 groups (RFC 1757& RFC 2819)
 - Telnet/SSH function for remote console management (**SSH will be available soon**)
 - TFTP and HTTP firmware update and configuration backup/restore
 - Remote Syslog function
 - Static and dynamic MAC table management
 - MAC filtering function
 - MAC limit function
 - Port sniffer (mirroring)
 - Forwarding scope (Protected port)
 - Port status, control, security and statistics
 - Static or DHCP (dynamic) IP address setting
 - DHCP relay & option 82 function
 - Ingress and egress rate control with 128Kbps resolution
 - QoS with 8-level port priority to 4-level queue mapping and strict / 802.1p / WRR priority options
 - User login management
 - 802.1x port access control supporting EAP-MD5, EAP-TLS and EAP-PEAP authentication types
 - Layer 2/3/4 access control list (ACL) with 220 rule entries
 - Source IP-MAC and port binding access control
 - Q-in-Q VLAN function
 - LLDP protocol
-

2 Operation Notice

To enter the “configuration” mode, you need to be in the privileged mode, and then type the command **configure**

```
Switch# configure
```

```
Switch (config) #
```

2.1 Command Line Editing

The following generic function keys provide functions in all of the menus:

Keys	Function
<Ctrl>-B; ←	Moves the cursor back one character.
<Ctrl>-D	Deletes the character at the cursor.
<Ctrl>-E	Jumps to the end of the current command line.
<Ctrl>-F; →	Moves the cursor forward one character.
<Ctrl>-K	Deletes from the cursor to the end of the command line.
<Ctrl>-N; ↓	Enters the next command line in the command history.
<Ctrl>-P; ↑	Enters the previous command line in the command history.
<Ctrl>-U	Deletes from the cursor to the beginning of the command line.
<Ctrl>-W	Deletes the last word typed.
<Esc> B	Moves the cursor backward one word.
<Esc> D	Deletes from the cursor to the end of the word.
<Esc> F	Moves the cursor forward one word.
<Backspace>	Delete the character before the cursor.
	Delete the character at the cursor.

2.2 Command Help

You may enter `?` at any command mode, and the CLI will return possible commands at that point, along with some description of the keywords:

Switch (config) # **copy tftp?**

running-config Running configurations

flash Flash configurations

firmware Download firmware

You may use the `<Tab>` key to do keyword auto completion:

Switch (config) # **copy tftp r<Tab>**

Switch (config) # **copy tftp running-config**

You do not need to type in the entire commands; you only need to type in enough characters for the CLI to recognize the command as unique. The following example shows you how to enter the **show running-config** command:

Switch (config) # **sh ru**

2.3 How to Use Loader

2.3.1 Connect switch

Use the following setting to connect PC to Switch with RS-232 cable:

Baud Rate	115200
Data Bits	8
Parity	None
Stop bits	1
Flow Control	None

PC needs to connect one of the Switch Ethernet port with a CAT-5/5e/6 cable if loader or firmware image needs to be updated through TFTP in loader mode.

2.3.2 Enter loader

Set the HyperTerminal as top table and open the HyperTerminal first. Power on the Switch and press any key to enter into the loader mode when count down message is shown up. Then switch enters into the loader mode when the prompt is shown.

```
SDRAM Testing .....  
.....  
SDRAM Test OK  
  
Switch Register R/W Test .. PASS  
PHY Register R/W Test ..... PASS  
  
Hit any key to stop autoboot: 0  
Loader # █
```

2.3.3 Commands in loader

- **?** – alias for 'help'. To list all available commands in loader

For example:

```
Loader # ?  
tftpupdate- Update image via network using TFTP protocol  
             with user define env variables ipaddr and serverip  
kermit      - update image file over serial line (kermit mode)  
mtest      - simple RAM test  
automtest  - open simple RAM test in next booting time.  
post       - Loop POST test.  
version    - print monitor version  
help       - print online help  
?         - alias for 'help'
```

- **tftpupdate** – to update firmware or loader image through TFTP network transfer

Loader # **tftpupdate ImageFileName TftpServerIP TargetBoardIP [loader]**

Update image via network using TFTP protocol with specified parameters:

ImageFileName – the new firmware/loader image file for update.

TftpServerIP – the PC's IP who has TFTP server service.

TargetBoardIP – the switch's IP you can set it.

loader – if update loader it needed, if update firmware it not needed.

For example, to update loader image file with TFTP, PC should have TFTP server and open it.

Enter the command:

```
Loader # tftpupdate loader_v3.2.2.img 192.168.223.119 192.168.223.1 loader
```



```

Loader # tftpupdate loader_v3.2.2.img 192.168.223.119 192.168.223.1 loader
BootFile [loader_v3.2.2.img], Load addr [0xb00000]
ARP broadcast 1
ARP broadcast 2
eth addr: 00:19:5b:7d:4c:8a
Got good ARP - start TFTP

Server ethernet address 00:19:5b:7d:4c:8a
TFTP from server 192.168.223.119; our IP address is 192.168.223.1
Filename 'loader_v3.2.2.img'.
Load address: 0xb00000
Loading: #####
done
Bytes transferred = 102874 (191da hex)

```

TFTP transfer is done. Then the new image will be written into the flash if image checksum is verified.

```

Un-Protect Flash Bank # 1

## Checking Image at 00b00000 ...
  Verifying Checksum ... OK
Erasing sector 0 ...
Erasing sector 1 ...
Erasing sector 2 ...
Erasing sector 3 ...
Erasing sector 4 ...
Erasing sector 5 ...
Erasing sector 6 ...
Erasing sector 7 ...
Erasing sector 8 ...
done.
Erased 9 sectors.
Saving Image to Flash...done...
Erasing sector 1 ...
Loader # █

```

Power off and on the switch to activate the new loader.

Another example is to update new firmware file with TFTP in loader. PC should have TFTP server and open it.

Enter the command:

```
Loader # tftpupdate image.2510.img 192.168.223.119 192.168.223.1
```

```

Loader # tftpupdate image.2510.img 192.168.223.119 192.168.223.1
BootFile [image.2510.img], Load addr [0xb00000]
ARP broadcast 1
ARP broadcast 2
eth addr: 00:19:5b:7d:4c:8a
Got good ARP - start TFTP

Server ethernet address 00:19:5b:7d:4c:8a
TFTP from server 192.168.223.119; our IP address is 192.168.223.1
Filename 'image.2510.img'.
Load address: 0xb00000
Loading: #####
#####
#####
#####
done
Bytes transferred = 1294261 (13bfb5 hex)

```

TFTP transfer is done. Then the new image will be written into the flash if image checksum is verified.

```
## Checking Image at 00b00000 ...
  Verifying Checksum ... OK
Erasing sector 9 ...
Erasing sector 10 ...
Erasing sector 11 ...
Erasing sector 12 ...
Erasing sector 13 ...
Erasing sector 14 ...
Erasing sector 15 ...
Erasing sector 16 ...
Erasing sector 17 ...
Erasing sector 18 ...
Erasing sector 19 ...
Erasing sector 20 ...
Erasing sector 21 ...
Erasing sector 22 ...
Erasing sector 23 ...
Erasing sector 24 ...
Erasing sector 25 ...
Erasing sector 26 ...
Erasing sector 27 ...
Erasing sector 28 ...
done.
Erased 20 sectors.
Saving Image to Flash...done...
Erasing sector 1 ...
```

After flash writing is completed, system will be automatically rebooted to start the new firmware image:

```
## Booting image ...
  Verifying Checksum ... OK
  Uncompressing Image ... OK

Starting up the system ...

=====
24 + 2 Switch Module Slot Information
=====
      Slot 1 .... Yes
      Slot 2 .... Yes
=====

Initializing switch functions ... in default configs ... OK

Username:
```

- **kermit** – to update firmware or loader image through serial (RS-232) line transfer in Kermit mode

Loader # **kermit [loader]**- update image file over serial line (kermit mode)

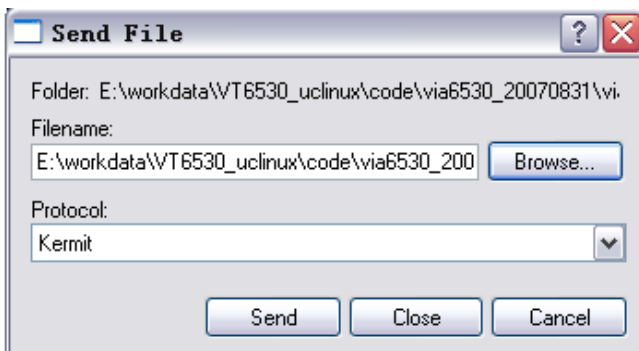
loader – if update loader it needed, if update firmware it not needed.

Here is an example to use the serial line to update new loader:

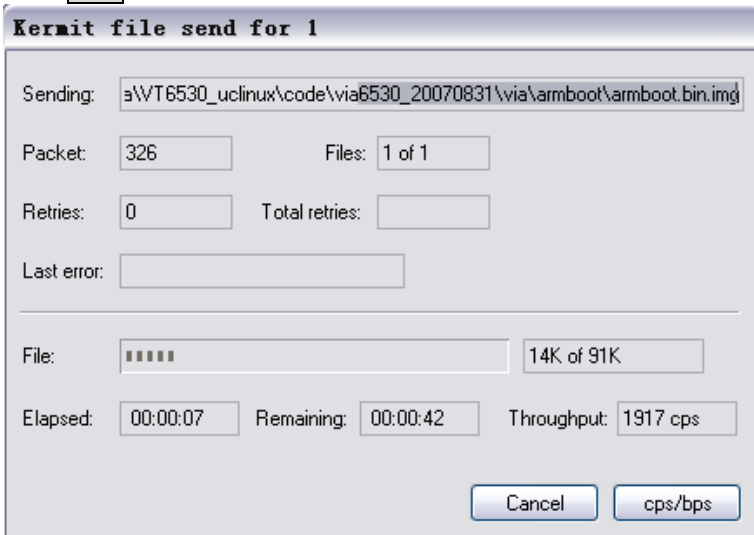
Loader # **kermit loader**

```
Loader # kermit loader
## Ready for binary (kermit) download ...
```

Select send file: filename select the loader image “armboot.bin.img” to update, Protocol “kermit”.



Press **Send** button



The following next messages will be shown when Kermit transfer is completed.

```
Loader # kermit loader
## Ready for binary (kermit) download ...
## Start Addr = 0x00500000 |
Un-Protect Flash Bank # 1

## Checking Image at 00500000 ...
  Verifying Checksum ... OK
Erasing sector 0 ...
Erasing sector 1 ...
Erasing sector 2 ...
Erasing sector 3 ...
Erasing sector 4 ...
Erasing sector 5 ...
Erasing sector 6 ...
Erasing sector 7 ...
Erasing sector 8 ...
done.
Erased 9 sectors.
Saving Image to Flash...done...
Un-Protected 1 sectors
Erasing sector 1 ...
Saving Environment to Flash...done.
Protected 1 sectors
Loader # _
```

Successfully update the loader. Finally power off and on to activate the new loader.

For updating new firmware image over serial line, use the following command:

```
Loader # kermit
## Ready for binary (kermit) download ...
```

Just like the descriptions of loader image updating, send the selected firmware image file “image.2510.img” then wait for the updating procedure is done and the system will be rebooted to activate the new firmware service.

- **version** – print monitor version

```
Loader # version
ARMboot v3.2.2
Loader #
```

- **help <command>** – print monitor version
command – the command in loader

For example:

```
Loader # help kermit
kermit [ loader ]
  - update kernel image file over serial line
  - [ loader ] update loader image file over serial line
Loader # _
```

3 Login

3.1 Power-On Self-Testing

The power-on self-testing is running immediately after the switch system is powered up. The self-testing program diagnoses the hardware components of a switch system. After hardware tests are all passed, the system will detect and display the module slot status and start the initializations. The system will be in ready state while the prompt is showing up.

```
=====
24 + 2 Switch Module Slot Information
=====
Slot 1 .... Yes
Slot 2 .... Yes
=====
Username:
```

3.2 Console Login

When you connect to the switch with a terminal emulation program, a login screen is displayed. Enter a user name and password to login to access the switch.

Items	Option	Default Value
Username	Max: 6, Min: 1 characters, case sensitive	admin
Password	Max: 6, Min: 1 characters, case sensitive	123

```
Username: admin
Password:
Switch#
```

3.3 Web Login

3.3.1 Setting IP Address by Console Port

When you are going to login a switch through the web page, you have to configure the IP address first. The default IP address / netmask / default gateway of a switch is **192.168.223.100 / 255.255.255.0 / 192.168.223.254**, without making any configuration changes in advance, you can login a switch with default IP address as long as the default IP address can function properly in your network environment. Otherwise, you have to re-configure the IP address, subnet mask and default gateway. The following show how to configure the IP address of a switch.

First, login with the console port.

```
Username: admin
Password:
Switch#
```

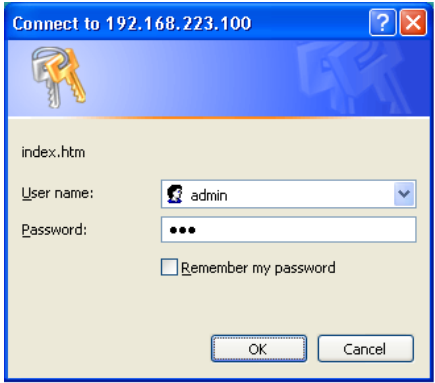
Second, you will now enter the "IP Address", then, setup the IP address, subnet mask and gateway.

```
Switch(config)# ip address 192.168.1.1 255.255.255.0
Switch(config)# ip default-gateway 192.168.1.254
```


3.3.2 Login with a Web Browser

When you connect to the switch through a web browser, a login screen is displayed. Enter a user name and password to login to access the switch.

Items	Option	Default Value
Username	Max: 6, Min: 1 characters, case sensitive	admin
Password	Max: 6, Min: 1 characters, case sensitive	123

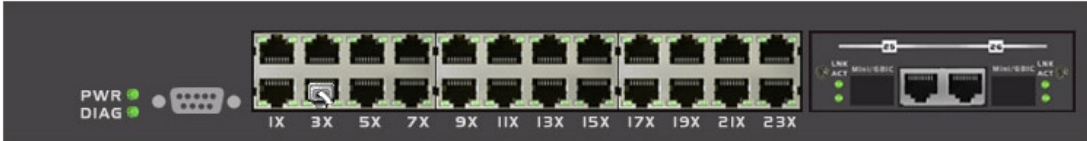


After user login verification, the homepage of the switch will be shown as below.



MENU

- Home
- [-] Administration
 - IP Address
 - Switch Setting
 - Console Port Info
 - [+] Port Configuration
 - SNMP Configuration
 - Syslog Setting
 - Firmware Update
 - Configuration Backup
- [+] L2 Features
- [+] ACL
- [+] Security
- [+] QoS
- [+] Monitoring
- Reset System
- Reboot



26-Port 10/100Mbps Layer 2 Switch

w/ Gigabit Ethernet Ports and Mini-GBIC Slots

4 Console User Interface

4.1 System Commands

show running-config

Display the running configuration of the switch.

copy running-config startup-config

Backup the switch configurations.

erase startup-config

Reset to default factory settings at next boot time.

clear arp [*<ip-addr>*] Clear entries in the ARP cache.

Parameters:

[*<ip-addr>*] specifies the IP address to be cleared. If no IP address is entered, the entire ARP cache is cleared.

show arp

Show the IP ARP translation table.

ping ip-addr [*<1..999>*] Send ICMP ECHO_REQUEST to network hosts.

Parameters:

[*<1..999>*] specifies the number of repetitions. If not entered, it will continue to ping until you press <Ctrl>-C to stop.

[**no**] **per-vlan-flooding-portmask** Enable or disable per VLAN default flooding portmask.

per-vlan-flooding-portmask **<unicast | multicast>** *<vlan-id>* *<port-list>* Set unicast or multicast per VLAN default flooding portmask.

show per-vlan-flooding-portmask

Display unicast and multicast per VLAN default flooding portmask table.

4.2 Switch Static Configuration

4.2.1 Port Configuration and Status

port state <on | off> [<port-list>]

Turn the port state on or off.

Parameters:

<port-list> specifies the ports to be turn on or off. If not entered, all ports are turn on or off.

port nego <force | auto | nway-force> [<port-list>]

Set port negotiation.

Parameters:

<port-list> specifies the ports to be set.If not entered, all ports are set.

port speed <10 | 100 | 1000> <full | half> [<port-list>]

Set port speed (in mbps) and duplex.

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port flow <enable | disable> <enable | disable> [<port-list>]

Enable or disable port flow control.

Parameters:

1st <enable | disable> enables or disables flow control in full duplex mode.

2nd <enable | disable> enables or disables flow control in half duplex mode.

<port-list> specifies the ports to be set. If not entered, all ports are set.

port rate <ingress | egress> <0..8000> [<port-list>]

Set port effective ingress or egress rate.

Parameters:

<0..8000> specifies the ingress or egress rate.<0..8000>

<port-list> specifies the ports to be set. If not entered, all ports are set.

port security <on | off> [<port-list>]

Set port priority. When port security is on, the port will stop MAC address learning, and forward only packets with MAC address in the static MAC address table.

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port protected group <1-2> [<port-list>]

Set protected port group member.

Parameters:

<port-list> specifies the group member ports.

port protected [<port-list>]

Set protected port list.

Parameters:

<port-list> specifies the protected port list.

port priority <disable | low | high> [<port-list>]

Set port priority.

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

port jumboframe <enable | disable> [<port-list>]

Set port jumbo frame. When port jumbo frame is enable, the port forward jumbo frame packet

Parameters:

<port-list> specifies the ports to be set. If not entered, all ports are set.

show port status

Show port status, including port State,Link,Trunking,VLAN,Negotiation,Speed,Duplex,Flow control, Rate control ,Priority,Security,BSF control.

show port statistics *<port-id>*

Show port statistics, including TxGoodPkt, TxBadPkt, RxGoodPkt, RxBadPkt,TxAbort, Collision, and DropPkt.

Parameters:

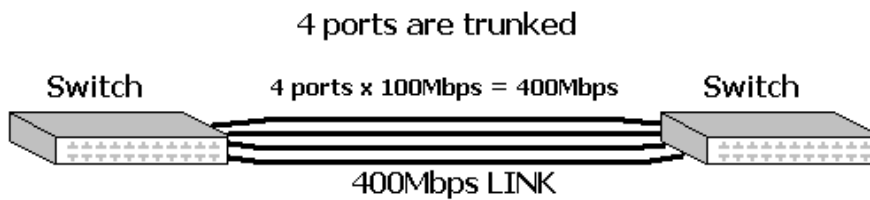
<port-id> specifies the port to be shown.

show port protection

Show protected port information.

4.2.2 Trunk

Trunk allows the switch to combine ports so that they function like a single high-speed link. It can be used to increase the bandwidth to some devices to provide a high-speed link. For example, trunk is useful when making connections between switches or connecting servers to the switch. Trunk can also provide a redundant link for fault tolerance. If one link in the trunk failed, the switch can balance the traffic among the remaining links.



NOTE:

1: The 10/100 Mbps port cannot be trunked with gigabit port (port 25~26).

2: All ports in the same trunk group will be treated as a single port. If a trunk group exists, the ports belonging to that trunk will be replaced by "TRUNK #" in the VLAN configuration screen. The following example configures port 25~26 as "TRUNK 1."

4.2.2.1 Trunking Commands

show trunk

Show trunking information.

trunk add <trunk-id> <lacp | no-lacp> <port-list> <active-port-list>

Add a new trunk group.

Parameters:

<trunk-id> specifies the trunk group to be added.

<lacp> specifies the added trunk group to be LACP enabled.

<no-lacp> specifies the added trunk group to be LACP disabled.

<port-list> specifies the ports to be set.

<active-port-list> specifies the ports to be set to LACP active.

no trunk <trunk-id>

Delete an existing trunk group.

Parameters:

<trunk-id> specifies the trunk group to be deleted.

4.2.2.2 LACP Commands

[no] lacp

Enable/disable LACP.

lacp system-priority <1..65535>

Set LACP system priority.

Parameters:

<1..65535> specifies the LACP system priority.

no lacp system-priority

Set LACP system priority to the default value 32768.

show lacp status

Show LACP enable/disable status and system priority.

show lacp

Show LACP information.

show lacp agg <trunk-id>

Show LACP aggregator information.

Parameters:

<trunk-id> specifies the trunk group to be shown.

show lacp port <port-id>

Show LACP information by port.

Parameters:

<port-id> specifies the port to be shown.

NOTE: If VLAN group exist, all of the members of static trunk group must be in same VLAN group.

4.2.3 VLAN

4.2.3.1 Virtual LANs

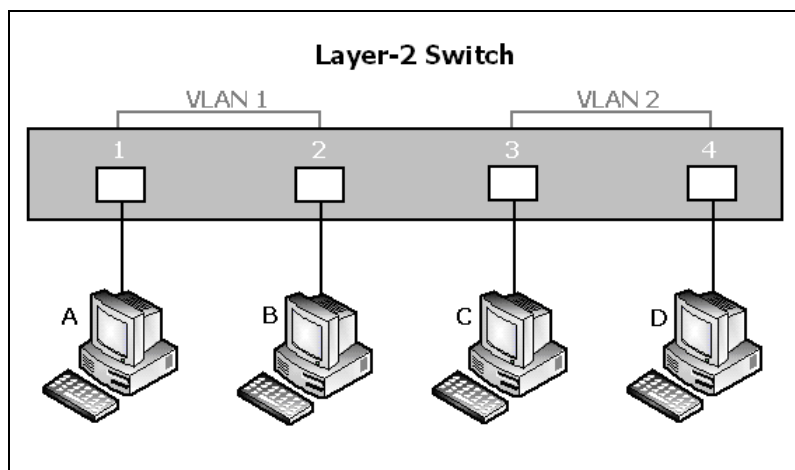
A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN within a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically. A station can belong to more than one VLAN group. VLAN prevents users from accessing network resources of another on the same LAN, thus the users can not see the hard disks and printers of another user in the same building. VLAN can also increase the network performance by reducing the broadcast traffic and enhance the security of the network by isolating groups.

This Switch supports two types of VLANs:

- Port-based
- IEEE 802.1Q (tag) -based

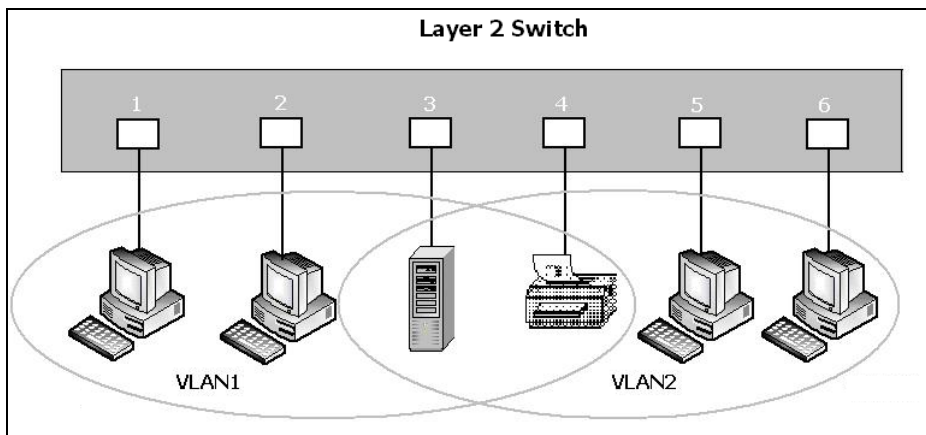
Only one of the two VLAN types can be enabled at one time.

Port-based VLANs are VLANs where the packet forwarding decision is made based on the destination MAC address and its associated port. You must define the outgoing ports allowed for each port when you use port-based VLANs. In port-based VLANs, the packets received from one port can only be sent to the ports which are configured to the same VLAN. As shown in the following figure, the switch administrator configured port 1~2 as VLAN 1 and port 3~4 as VLAN 2. The packets received from port 1 can only be forwarded to port 2. The packets received from port 2 can only be forwarded to port 1. That means the computer A can send packets to computer B, and vice versa. The same situation also occurred in VLAN 2. The computer C and D can communicate with each other. However, the computers in VLAN 1 can not see the computers in VLAN 2 since they belonged to different VLANs.

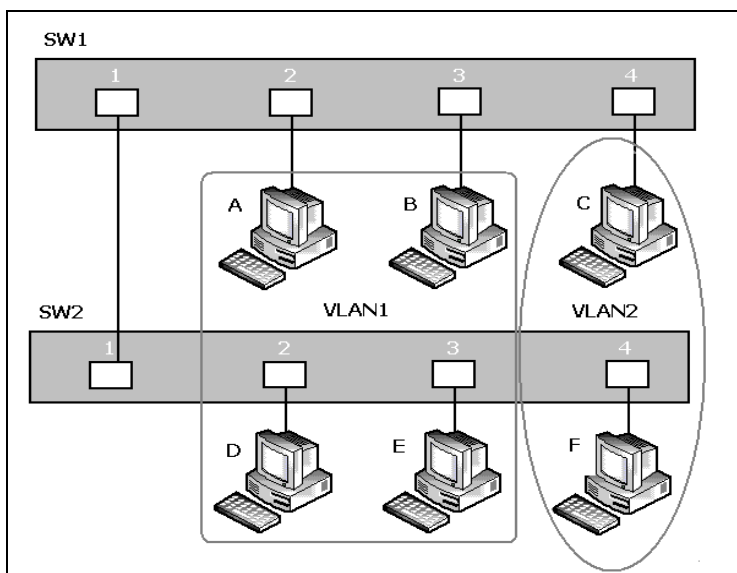


IEEE 802.1Q (tag) -based VLANs enable the Ethernet functionality to propagate tagged packets across the bridges and provides a uniform way for creating VLAN within a network then span across the network. For egress packet, you can choose to tag it or not with the associated VLAN ID of this port. For ingress packet, you can forward this packet to a specific port as long as it is also in the same VLAN group.

The 802.1Q VLAN works by using a tag added to the Ethernet packets. The tag contains a VLAN Identifier (VID) which belongs to a specific VLAN group. And ports can belong to more than one VLAN.



The difference between a port-based VLAN and a tag-based VLAN is that the tag-based VLAN truly divided the network into several logically connected LANs. Packets rambling around the switches can be forwarded more intelligently. In the figure shown below, by identifying the tag, broadcast packets coming from computer A in VLAN1 at sw1 can be forwarded directly to VLAN1. However, the switch could not be so smart in the port-based VLAN mechanism. Broadcast packets will also be forwarded to port 4 of sw2. It means the port-based VLAN can not operate a logical VLAN group among switches.



The TEG-S2620 supports both port-based VLAN and tag-based (802.1Q) VLAN modes. The default configuration is tag-based (802.1Q) VLAN. In the 802.1Q VLAN, initially, all ports on the switch belong to default VLAN, VID is 1.

NOTE: You cannot delete the default VLAN group in 802.1Q VLAN mode.

4.2.3.2 VLAN Mode

- **VLAN Mode: Port based**

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

show vlan mode

Display the current VLAN mode.

vlan mode (disabled | port-based | dot1q)

Change VLAN mode.

Parameters:

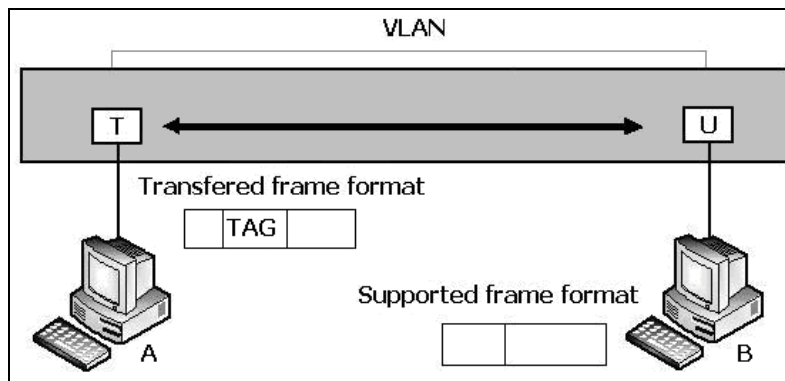
(disabled | port-based | dot1q) specifies the VLAN mode.

NOTE: Change the VLAN mode for every time, user have to restart the switch for valid value.

- **VLAN Mode: 802.1Q**

If a trunk group exists, you can see it (e.g. TRUNK1, TRUNK2...) after port 24. And, you can configure it to be a member of the VLAN group.

In the setting, port was set to Untagged if devices underneath this port do not support VLAN-tagging. Thus the switch can send untagged frames to this port. Consequently, device that do not support VLAN-tagging or do not enable VLAN tagging could successfully fetch the incoming frames and could communicate with device that transfers tagged frames, and vice versa. In the following figure, two different types of devices want to communicate with each other. Since computer A support 802.1Q VLAN and computer B do not, you have to configure two ports both beneath the same VLAN group, and set left port to "Tagged", right port to "Untagged". Therefore, two devices will receive packet type as they desired.



4.2.3.3 Advanced 802.1Q VLAN Setting

Ingress filters configuration

When a packet was received on a port, you can govern the switch to drop it or not if it is an untagged packet. Furthermore, if the received packet is tagged but not belonging to the same VLAN group of the receiving port, you can also control the switch to forward or drop the packet. The example below configures the switch to drop the packets not belonging to the same VLAN group and forward the packets not containing VLAN tags.

▪ VLAN Commands

show vlan mode

Display the current VLAN mode.

vlan mode (disabled | port-based | dot1q)

Change VLAN mode.

Parameters:

(disabled | port-based | dot1q) specifies the VLAN mode.

NOTE: Change the VLAN mode for every time, user have to restart the switch for valid value.

vlan add <1-4094> <NAME> <cpu-port | no-cpu-port> <LIST> [<LIST>]

Add or edit VLAN entry.

Parameters:

<1-4094> specifies the VLAN id or Group id (if port based VLAN mode)

<NAME> specifies the VLAN group name.

<cpu-port | no-cpu-port> specifies the CPU port belong this VLAN group.

1st <LIST> specifies the ports to be set to VLAN members.

2nd [<LIST>] specifies the ports to be set to tagged members. If not entered, all members set to untagged.

e.g. vlan add 1 vlan1 cpu-port 1-4 . This VLAN entry has four members (from port1 to port4) and all members are untagged.

no vlan <1-4094>

Delete VLAN entry.

Parameters:

<1-4094> specifies the VLAN id or group id (if port based VLAN).

e.g. no vlan 1

show vlan [<1-4094>]

Show VLAN entry information.

Parameters:

[<1-4094>] specifies the VLAN id, null means all valid entries.

e.g. show vlan 1

show vlan static

Show static VLAN entry information.

vlan pvid <LIST> <1-4094>

Set port default VLAN id.

Parameters:

<LIST> specifies the ports to be set.

<1-4094> specifies the port VLAN id.

show vlan pvid [<LIST>]

Show port default VLAN id.

Parameters:

[<LIST>] specifies the ports to be showed. If not entered, all port's PVID will be showed.

vlan filter <enable | disable> <enable | disable> <LIST>

Set ingress filter rules.

Parameters:

1st <enable | disable> specifies the non-members packet will be forwarded or not. If set enable, forward only packets with VID matching this port's configured VID.

2nd <enable | disable> specifies the untagged frame will be dropped or not. If set enable, drop untagged frame.
<LIST> specifies the port or trunk list (eg. 3, 6-8, Trk2)

show vlan filter [<LIST>]

Show VLAN filter setting.

Parameters:

[<LIST>] specifies the ports to be showed. If not entered, all ports' filter rules will be showed.

▪ **GVRP Commands**

[no] gvrp

Enable or disable GVRP.

show gvrp status

Show GVRP enable or disable status.

[no] port gvrp <LIST>

Enable or disable GVRP by port.

Parameters:

<LIST> specifies the port or trunk list to be set

show port gvrp

Show GVRP status by port.

garp timer <join | leave | leave-all> <0..65535>

Set GARP timer.

Parameters:

<join | leave | leave-all> specifies a timer (Join, Leave, or Leave-All) to be set

<0..65535> specifies the timer in seconds.

show garp timer

Show GARP timer.

show gvrp db

Show GVRP DB.

show gvrp gip

Show GVRP GIP.

show gvrp machine

Show GVRP machine.

clear gvrp statistics <LIST>

Clear GVRP statistics by port.

Parameters:

<LIST> specifies the port or trunk list to be set

show gvrp statistics <LIST>

Show GVRP statistics by port.

Parameters:

<LIST> specifies the port or trunk list to be set

[no] gvrp debug [<sys | err | pdu | db | gen | garp | gvrp | vlan>]

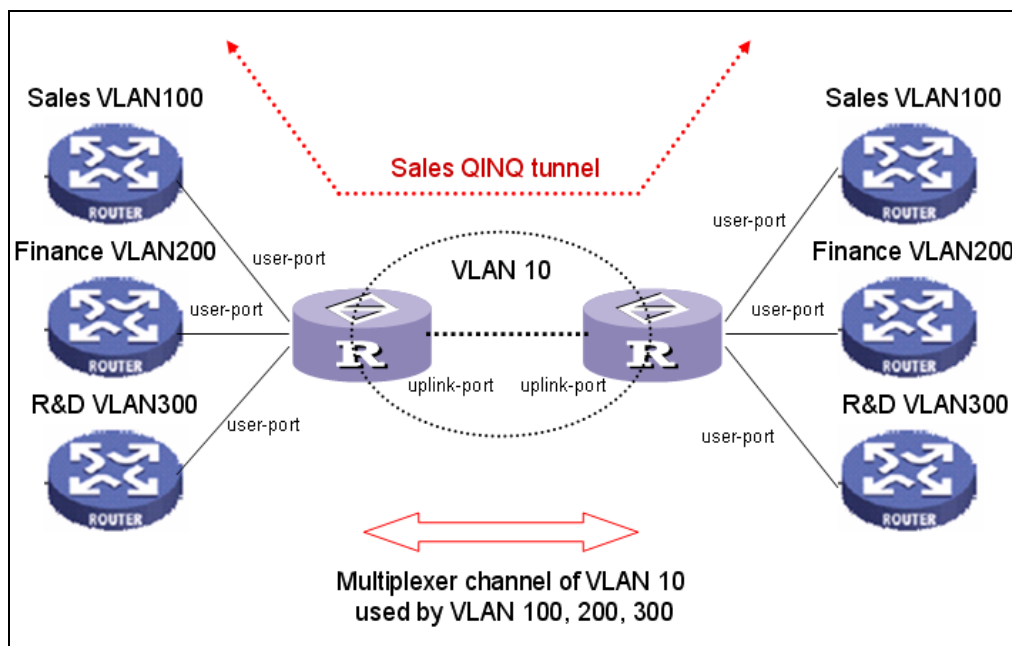
Enable/disable GVRP debugging output.

4.2.3.4 QinQ VLAN Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification. Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets.

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. QinQ is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers.

The following figure is an example of QinQ VLAN application.



▪ QinQ Commands

qinq enable

Enable QinQ.

[no] qinq

Disable QinQ.

qinq tpid <TPIDVAL>

Set QinQ tpid.

Parameters:

<TPIDVAL> specifies QinQ tpid value (Hex, 1~FFFF)

qinq userport <enable | disable> <LIST>

A port configured to support client end of QinQ tunnel is called a QinQ user-port. Use this command to enable/disable QinQ userport to specified port(s).

qinq uplinkport <enable|disable> <LIST>

A port configured to support network end of QinQ tunnel is called a QinQ uplink-port. Use this command to enable/disable QinQ uplinkport to specified port(s).

qinq tunnel add <1-25> <1-4094> <LIST>

Add QINQ tunnel.

Parameters:

<1-25> specifies the tunnel ID

<1-4094> specifies the VLAN ID

<LIST> specifies the ports to be set to QINQ tunnel.

qinq tunnel delete <1-25>

Delete QinQ tunnel.

Parameters:

<1-25> specifies the tunnel ID

show qinq configuration

Show QinQ global and portal configuration

show qinq tunnel

Show QinQ tunnel information

For example, refer to the figure of QinQ application in previous page, a QinQ tunnel using VLAN10 wants to be created for Sales VLAN100 across the public network. Port1 on left-side switch connects to Sales VLAN100 client. Port16 of switch connects to the public network. The following commands needs to be set:

```
qinq enable
qinq tpid 8100
qinq userport enable 1
qinq uplinkport enable 16
qinq tunnel add 1 10 1,16
```

4.2.4 Misc Configuration

[no] mac-age-time

Enable or disable MAC address age-out.

mac-age-time <6..1572858> Set MAC address age-out time.

Parameters:

<6..1572858> specifies the MAC address age-out time. The value must be divisible by 6. Type the number of seconds that an inactive MAC address remains in the switch's address table

show mac-age-time

Show MAC address age-out time

broadcast mode <off | 1/2 | 1/4 | 1/8 | 1/16>

Set broadcast storm filter mode to off, 1/2, 1/4, 1/8, 1/16

broadcast select <unicast/multicast | control packet | ip multicast | broadcast>

Select the Broadcast storm filter packet type:

Unicast/Multicast: Flood unicast/multicast filter

Control Packets: Control packets filter

IP multicast: Ip multicast packets filter

Broadcast Packets: Broadcast Packets filter

Collision-Retry <off | 16 | 32 | 48>

Parameters:

<off|16|32|48> In half duplex, collision-retry maximum is 16, 32 or 48 times and packet will be dropped if collisions still happen. In default (off), if collision happens, it will retry forever.

Hash <crc-hash | direct-map>

Set hash algorithm to CRC-Hash or DirectMap.

4.2.5

Administration

4.2.5.1 Change Username/Password

hostname <name-str>

Set switch name.

<name-str> specifies the switch name. If you would like to have spaces within the name, use quotes ("") around the name.

no hostname

Reset the switch name to factory default setting.

[no] password <manager | operator | all>

Set or remove username and password for manager or operator. The manager username and password is also used by the web UI.

4.2.5.2 IP Configuration

User can configure the IP setting and fill in the new value.

ip address <ip-addr> <ip-mask>

Set IP address and subnet mask.

ip default-gateway <ip-addr>

Set the default gateway IP address.

show ip

Show IP address, subnet mask, and the default gateway.

show info

Show basic information, including system info, MAC address, and firmware version.

dhcp

Set switch as dhcp client, it can get ip from dhcp server

NOTE: If this command is set, the switch will reboot.

show dhcp

show dhcp enable/disable

4.2.6 Port Mirroring

Port monitoring is a feature to redirect the traffic occurred on every port to a designated monitoring port on the switch. With this feature, the network administrator can monitor and analyze the traffic on the entire LAN segment. In EP-5926, you can specify one port to be the monitoring port and any single port to be the monitored port. You also can specify the direction of the traffic that you want to monitor. After properly configured, packets with the specified direction from the monitored ports are forwarded to the monitoring port.

NOTES:

1. The default Port Monitoring setting is disabled.
2. The analysis port is dedicated as mirroring port with duplicated traffic flow from mirrored port. The ordinary network traffic is not available for the analysis port.
3. Any trunk group and member port is not available for this function

mirror-port <rx | tx | both> <port-id> <port-list> Set port monitoring information. (RX only|TX only|both RX and TX) *Parameters:*

rx specifies monitoring rx only.

tx specifies monitoring tx only.

both specifies monitoring both rx and tx.

<port-id> specifies the analysis port ID. This port receives traffic from all monitored ports.

<port-list> specifies the monitored port list.

show mirror-port

Show port monitoring information

4.2.7 Quality of Service

There are four transmission queues with different priorities in EP-5926: Highest, SecHigh, SecLow and Lowest. The switch will take packets from the four queues according to its QoS mode setting. If the QoS mode was set to "Disable", the switch will not perform QoS on its switched network. If the QoS mode was set to "High Empty Then Low", the switch will never exhaust packets from a queue until the queues with higher priorities are empty. If the QoS mode was set to "weight ratio", the switch will exhaust packets from the queues according to the ratio. The default value of QoS mode is "weight 8:4:2:1." That means the switch will first exhaust 8 packets from the queue with highest priority, and then exhaust 4 packets from the queue with second high priority, and so on.

When the switch received a packet, the switch has to decide which queue to put the received packet into. In EP-5926, the switch will put received packets into queues according to the settings of "802.1p Priority" and "Static Port Ingress Priority." When the received packet is an 802.1p tagged packet, the switch will put the packet into a queue according to the 802.1p Priority setting. Otherwise, the switch will put the packet into a queue according the setting of Static Port Ingress Priority.

802.1p Priority: the 802.1p packet has a priority tag in its packet header. The range of the priority is 7~0. The TEG-S2620I can specify the mapping between 802.1p priority and the four transmission queues. In the default setting, the packets with 802.1p priority 0~1 are put into the queue with lowest priority, the packets with 802.1p priority 2~3 are put into queue with second low priority, and so on.

Static Port Ingress Priority: each port is assigned with one priority 7~0. The priority of the packet received from one port is set to the same priority of the receiving port. When the priority of the received packet was determined, the packet is treated as an 802.1p packet with that priority and will be put into a queue according to the 802.1p Priority setting.

4.2.7.1 QoS Configuration

■ QoS Mode:

- **First Come First Service:** The sequence of packets sent is depending on arrive orders.
- **All High before Low:** The high priority packets sent before low priority packets.
- **WRR:** Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.

■ **Qos Level:** 0~7 priority level can map to highest, second-high, second-low, lowest queue.

■ Commands:

qos priority <first-come-first-service | all-high-before-low | weighted-round-robin> [<highest-weight>][<sechigh-weight>][<sec low-weight>] [<lowest-weight>]

Set 802.1p priority.

e.g. qos priority weighted-round-robin 8,4,2,1

qos level < highest | second-high | second-low | lowest > <level-list>

Set priority levels to highest, second-high, second-low and lowest.

Parameters:

<level-list> specifies the priority levels to be high or low. Level must be between 1 and 7.

e.g. qos level highest 7

e.g. qos level lowest 4

show qos

Show QoS configurations, including 802.1p priority, priority level.

e.g. show qos

QoS configurations:

QoS mode: first come first service

Highest weight: 8

Second High weight: 4

Second Low weight: 2

Lowest weight: 1

802.1p priority[0-7]:

Lowest Lowest SecLow SecLow SecHigh SecHigh Highest Highest

4.2.7.2 Per Port Priority

port priority <disable | [0-7]> [<port-list>]

Set port priority.

Parameters:

[<port-list>] specifies the ports to be set. If not entered, all ports are set.

e.g. port priority disable 1-5

4.2.8 MAC Address Table

clear mac-address-table

Clear all dynamic MAC address table entries.

mac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

Set static unicast or multicast MAC address. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

no mac-address-table static <mac-addr> <vlan-id>

Delete static unicast or multicast MAC address table entries.

show mac-address-table

Display MAC address table entries.

show mac-address-table static

Display static MAC address table entries.

show mac-address-table multicast

Display multicast related MAC address table.

smac-address-table static <mac-addr> <vlan-id> <port-id | port-list>

Set static unicast or multicast MAC address in secondary MAC address table. If multicast MAC address (address beginning with 01:00:5E) is supplied, the last parameter must be *port-list*. Otherwise, it must be *port-id*.

show smac-address-table

Display secondary MAC address table entries.

show smac-address-table multicast

Display multicast related secondary MAC address table.

[no] filter <mac-addr> <vlan-id>

Set MAC address filter. The packets will be filtered if both of the destination MAC address and the VLAN tag matches the filter entry. If the packet does not have a VLAN tag, then it matches an entry with VLAN ID 1.

show filter

Display filter MAC address table.

4.2.9 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-serve policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an "opening" is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

User can configure the MAC limit setting and fill in the new value.

mac-limit

Enable MAC limit.

no mac-limit

Disable MAC limit.

Mac-limit <port-list> <1-64>

Set port MAC limit value, 0 to turn off MAC limit of port.

show mac-limit

Show MAC limit information, including MAC limit enable/disable, per-port MAC limit setting.

4.3 Protocol Related Configuration

4.3.1 STP/RSTP

[no] spanning-tree

Enable or disable spanning-tree.

spanning-tree forward-delay <4-30>

Set spanning tree forward delay used, in seconds.

Parameters:

<4-30> specifies the forward delay, in seconds. Default value is 15.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree hello-time <1-10>

Set spanning tree hello time, in seconds.

Parameters:

<1-10> specifies the hello time, in seconds. Default value is 2.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree maximum-age <6-40>

Set spanning tree maximum age, in seconds.

Parameters:

<6-40> specifies the maximum age, in seconds. Default value is 20.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree priority <0-61440>

Set spanning tree bridge priority.

Parameters:

<0-61440> specifies the bridge priority. The value must be in steps of 4096.

spanning-tree port path-cost <1-200000000> [<port-list>]

Set spanning tree port path cost.

Parameters:

<1-200000000> specifies port path cost.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port priority <0-240> [<port-list>]

Set spanning tree port priority.

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

[<port-list>] specifies the ports to be set. Null means all ports.

show spanning-tree

Show spanning-tree information.

show spanning-tree port [<port-list>]

Show spanning tree per port information.

Parameters:

[<port-list>] specifies the port to be shown. Null means all ports.

The remaining commands in this section are only for system with RSTP (rapid spanning tree, 802.1w) capability:

[no] spanning-tree debug

Enable or disable spanning tree debugging information.

spanning-tree protocol-version <stp | rstp>

Change spanning tree protocol version.

Parameters:

stp specifies the original spanning tree protocol (STP,802.1d).

rstp specifies rapid spanning tree protocol (RSTP,802.1w).

[no] spanning-tree port mcheck [<port-list>]

Force the port to transmit RST BPDUs. No format means not force the port to transmit RST BPDUs.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port [<port-list>]

Set the port to be edge connection. No format means set the port to be non-edge connection.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp [<port-list>]

Disable or enable spanning tree protocol on this port.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Set the port to be point to point connection.

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

[<port-list>] specifies the ports to be set. Null means all ports.

4.3.2 MSTP

[no] spanning-tree

Enable or disable multiple spanning tree.

[no] spanning-tree debug

Enable or disable multiple spanning tree debugging information.

spanning-tree forward-delay <4-30>

Set spanning tree forward delay of CIST, in seconds.

Parameters:

<4-30> specifies the forward delay, in seconds. Default value is 15.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree hello-time <1-10>

Set spanning tree hello time of CIST, in seconds.

Parameters:

<1-10> specifies the hello time, in seconds. Default value is 2.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree maximum-age <6-40>

Set spanning tree maximum age of CIST, in seconds.

Parameters:

<6-40> specifies the maximum age, in seconds. Default value is 20.

Note: The parameters must enforce the following relationships:

$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

spanning-tree priority <0-61440>

Set spanning tree bridge priority of CIST and all MSTIs.

Parameters:

<0-61440> specifies the bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree protocol-version { stp | mstp }

Set spanning tree protocol version of CIST.

Parameters:

stp specifies the original spanning tree protocol (STP,802.1d).

mstp specifies the multiple spanning tree protocol (MSTP,802.1s).

spanning-tree max-hops <1-40>

Set spanning tree bridge maximum hops of CIST and all MSTIs.

Parameters:

<1-40> specifies the bridge maximum hops. Default value is 20.

spanning-tree name [<name-string>]

Set spanning tree bridge name of CIST.

Parameters:

[<name-string>] specifies the bridge name. Default name is null.

spanning-tree revision <1-65535>

Set spanning tree bridge revision of CIST.

Parameters:

<1-65535> specifies the bridge revision. Default value is 0.

spanning-tree port path-cost <1-20000000> [<port-list>]

Set spanning tree port path cost of CIST.

Parameters:

<1-20000000> specifies port path cost.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port priority <0-240> [<port-list>]

Set spanning tree port priority of CIST.

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port mcheck [<port-list>]

Force the port of CIST to transmit MST BPDUs. No format means not force the port of CIST to transmit MST BPDUs.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port edge-port [<port-list>]

Set the port of CIST to be edge connection. No format means set the port of CIST to be non-edge connection.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

[no] spanning-tree port non-stp [<port-list>]

Disable or enable spanning tree protocol on the CIST port.

Parameters:

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree port point-to-point-mac <auto | true | false> [<port-list>]

Set the port of CIST to be point to point connection.

Parameters:

auto specifies point to point link auto connection.

true specifies point to point link true.

false specifies point to point link false.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> priority <0-61440>

Set spanning tree bridge priority of MSTI.

Parameters:

<0-15> specifies the MSTI instance ID.

<0-61440> specifies the MSTI bridge priority. The value must be in steps of 4096. Default value is 32768.

spanning-tree mst <0-15> vlan [<vlan-list>]

Set MSTI to map VLAN list.

Parameters:

<0-15> specifies the MSTI instance ID.

[<vlan-list>] specifies the mapped VLAN list. Null means all VLANs.

spanning-tree mst <0-15> port path-cost <1-20000000> [<port-list>]

Set spanning tree port path cost of MSTI.

Parameters:

<1-20000000> specifies port path cost.

[<port-list>] specifies the ports to be set. Null means all ports.

spanning-tree mst <0-15> port priority <0-240> [<port-list>]

Set spanning tree port priority of MSTI.

Parameters:

<0-240> specifies the port priority. The value must be in steps of 16.

[<port-list>] specifies the ports to be set. Null means all ports.

no spanning-tree mst <0-15>

Delete the specific MSTI.

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree

Show spanning-tree information of CIST.

show spanning-tree port [<port-list>]

Show spanning tree port information of CIST.

Parameters:

[<port-list>] specifies the port to be shown. Null means all ports.

show spanning-tree mst configuration

Show MST instance map.

show spanning-tree mst <0-15>

Show MST instance information.

Parameters:

<0-15> specifies the MSTI instance ID.

show spanning-tree mst <0-15> port <1-26>

Show specific port information of MST instance.

Parameters:

<0-15> specifies the MSTI instance ID.

<1-26> specifies port number.

show vlan spanning-tree

Show per VLAN per port spanning tree status.

4.3.3 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can be management the switch.

4.3.3.1 System Options

Snmp /no snmp

Enable or disable SNMP.

Show snmp status

Show enable or disable status of SNMP.

snmp system-name <name-str>

Set agent system name string.

Parameters:

<name-str> specifies the system name string.

e.g. snmp system-name SWITCH

snmp system-location <location-str>

Set agent location string.

Parameters:

<location-str> specifies the location string.

e.g. snmp system-location office

snmp system-contact <contact-str>

Set agent system contact string.

Parameters:

<contact-str> specifies the contact string.

e.g. snmp system-contact abc@sina.com

show snmp system

Show SNMP system information.

4.3.3.2 Community Strings

snmp community <read-sysinfo-only | read-all-only | read-write-all> <community-str>

Set SNMP community string.

Parameters:

<community-str> specifies the community string.

e.g. snmp community read-all-only public

no snmp community <community-str>

Delete SNMP community string.

Parameters:

<community-str> specifies the community string.

e.g. no snmp community public

show snmp community

Show SNMP community strings.

4.3.3.3 Trap Managers

snmp trap <ip-addr> [<community-str>] [<1..65535>]

Set SNMP trap receiver IP address, community string, and port number.

Parameters:

<ip-addr> specifies the IP address.

<community-str> specifies the community string.

<1..65535> specifies the trap receiver port number.

e.g. snmp trap 192.168.200.1 public

no snmp trap <ip-addr> [<1..65535>]

Remove trap receiver IP address and port number.

Parameters:

<ip-addr> specifies the IP address.

<1..65535> specifies the trap receiver port number.

e.g. no snmp trap 192.168.200.1

show snmp trap

Show all trap receivers.

4.3.3.4 SNMP V3 VACM (optional)

snmp group <group-name> <v1 | v2c | usm> <security-name>

Join a group.

Parameters:

<group-name> specifies the group name.

<v1 | v2c | usm> specifies the security model.

<security-name> specifies the security name.

e.g. snmp group test usm testuser

no snmp group <v1 | v2c | usm> <security-name>

Leave a group.

Parameters:

<v1 | v2c | usm> specifies the security model.

<security-name> specifies the security name.

e.g. no snmp group usm testuser

show snmp group

Show group list.

snmp view <view-name> <included | excluded> <view-subtree> <view-mask>

Add a view.

Parameters:

<view-name> specifies the view name.

<included | excluded> specifies the view type.

<view-subtree> specifies the view subtree (e.g. .1.3.6.1.2.1).

<view-mask> specifies the view mask, in hexadecimal digits.

e.g. snmp view testview included 1.3.6.1.2.1 0xff

no snmp view <view-name>

Delete a view.

Parameters:

<view-name> specifies the view name.

e.g. no snmp view system

show snmp view

Show view list.

snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv> <read-name> <write-name> <notify-name>

Add an access control.

Parameters:

<group-name> specifies the group name.
<v1 | v2c | usm> specifies the security model.
<noauth | auth | authpriv> specifies the security level.
<read-name> specifies the access read view name.
<write-name> specifies the access write view name.
<notify-name> specifies the access notify view name.
e.g. snmp access test usm testauth all all all

no snmp access <group-name> <v1 | v2c | usm> <noauth | auth | authpriv>

Delete an access control.

Parameters:

<group-name> specifies the group name.
<v1 | v2c | usm> specifies the security model.
<noauth | auth | authpriv> specifies the security level.
e.g. no snmp access test usm auth
show snmp access
Show access list.

4.3.3.5 SNMP V3 USM (optional)

snmp engine-id <enterprise-id> <engine-id>

Setup SNMPv3 engine ID.

Parameters:

<engine-id> specifies the engine ID, in the format of text string.
e.g. snmp engine-id 123456789123456789123456

show snmp engine-id

Show SNMPv3 engine ID.

snmp usm-user <user-name> [<md5 | none>]

Add SNMPv3 USM user.

Parameters:

<user-name> specifies the user name.
<md5 | none> specifies the authentication type.
e.g. Create a user name is testuser and password is 12345678, use auth md5 then enter CLI command:
snmp usm-user testuser md5 <cr>
New password for authentication (8<=length<=32):
12345678<cr>
Retype new password:
12345678<cr>

no snmp usm-user <user-name>

Delete SNMPv3 USM user.

Parameters:

<user-name> specifies the user name.
e.g. no snmp usm-user testuser

show snmp usm-user

Show all SNMPv3 USM users.

4.3.4 IGMP

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite.

[no] **igmp** Enable/disable IGMP snooping.

[no] **igmp fastleave** Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one second.

[no] **igmp querier** Enable/disable IGMP snooping querier.

[no] **igmp CrossVLAN** Enable/disable IGMP snooping CrossVLAN

[no] **igmp debug** Enable/disable IGMP snooping debugging output.

show igmp <status | router | groups | table>

Show IGMP snooping information.

Parameters:

status specifies IGMP snooping status and statistics information.

router specifies IGMP snooping router's IP address.

groups specifies IGMP snooping multicast group list.

table specifies IGMP snooping IP multicast table entries.

igmp clear_statistics

Clear IGMP snooping statistics counters.

4.3.5 802.1x

This switch supports IEEE 802.1x standard which provides port-based access control by validating end user's authorization through authentication (RADIUS) server. EAP- MD5/TLS/PEAP authentication types are supported for this switch.

[no] dot1x

Enable or disable 802.1x.

radius-server host <ip-addr> <1024..65535> <1024..65535>

Set radius server IP, port number, and accounting port number.

Parameters:

<ip-addr> specifies server's IP address.

1st <1024..65535> specifies the server port number.

2nd <1024..65535> specifies the accounting port number.

radius-server key <key-str>

Set 802.1x shared key.

Parameters:

<key-str> specifies shared key string.

radius-server nas <id-str>

Set 802.1x NAS identifier.

Parameters:

<id-str> specifies NAS identifier string.

show radius-server

Show radius server information, including radius server IP, port number, accounting port number, shared key, NAS identifier,

dot1x timeout quiet-period <0..65535>

Set 802.1x quiet period. (default: 60 seconds).

Parameters:

<0..65535> specifies the quiet period, in seconds.

dot1x timeout tx-period <0..65535>

Set 802.1x Tx period. (default: 15 seconds).

Parameters:

<0..65535> specifies the Tx period, in seconds.

dot1x timeout supplicant <1..300>

Set 802.1x supplicant timeout (default: 30 seconds)

Parameters:

<1..300> specifies the supplicant timeout, in seconds.

dot1x timeout radius-server <1..300>

Set radius server timeout (default: 30 seconds).

Parameters:

<1..300> specifies the radius server timeout, in seconds.

dot1x max-req <1..10>

Set 802.1x maximum request retries (default: 2 times).

Parameters:

<1..10> specifies the maximum request retries.

dot1x timeout re-authperiod <30..65535>

Set 802.1x re-auth period (default: 3600 seconds).

Parameters:

<30..65535> specifies the re-auth period, in seconds.

show dot1x

Show 802.1x information, quiet period, Tx period, supplicant timeout, server timeout, maximum requests, and re-auth period.

dot1x port <fu | fa | au | no> <port-list>

Set 802.1x per port information.

Parameters:

fu specifies forced unauthorized.

fa specifies forced authorized.

au specifies authorization.

no specifies disable authorization.

<port-list> specifies the ports to be set.

show dot1x port

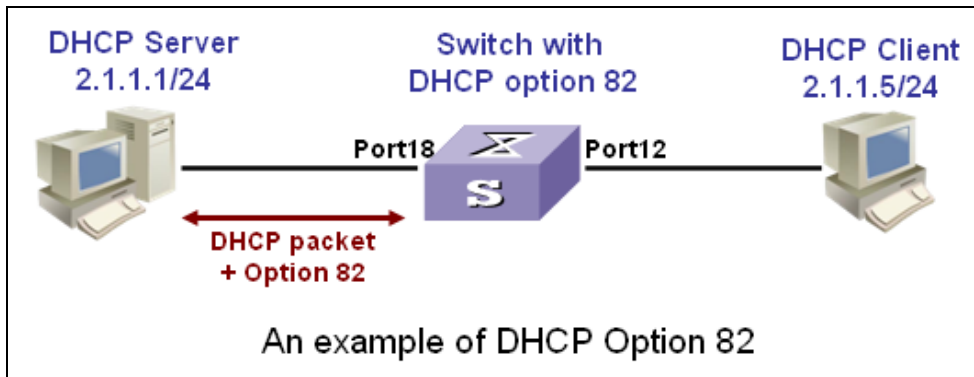
Show 802.1x per port information.

4.3.6 DHCP Relay & Option 82

DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts.

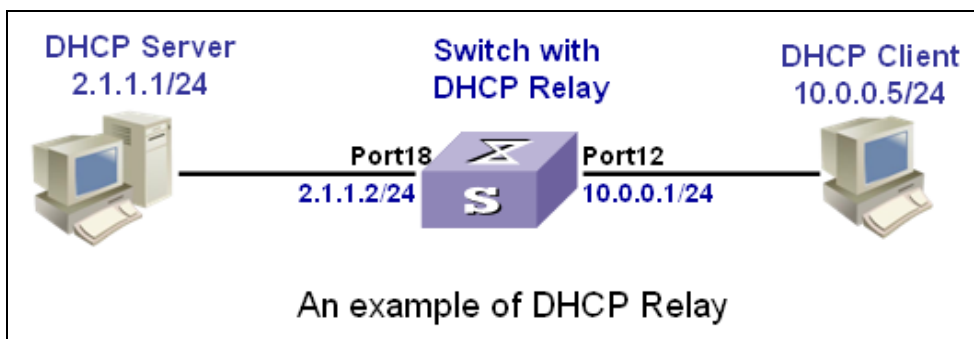
When the **DHCP Option 82** feature is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified. Option82 Information is inserted by the switch enabled option-82 feature when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers may use this information to implement IP address or other parameter assignment policies. This will significantly enhance the security of DHCP and effectively prevent the attack of DHCP flood.

The following figure is an example of DHCP Option 82:



If the **DHCP relay** feature is enabled on the switch, it forwards requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from the normal Layer 2 forwarding, in which IP datagrams are switched transparently between networks. Relay agents receive DHCP messages and generate new DHCP messages to send on output interfaces. So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

The following figure is an example of DHCP relay:



The following commands are provided for DHCP option82 / relay configuration:

[no] dhcp-option82

Enable/disable DHCP option82 function.

[no] dhcp-relay

Enable/disable DHCP relay function.

dhcp-option82 <enable | disable> <LIST>

Enable/disable port-based option82 function.

dhcp-relay <enable | disable> <LIST> <IP address>

Enable/disable port-based DHCP relay function.

dhcp router <LIST>

Set DHCP router port

show dhcp configuration

Show DHCP configuration information

For example, refer to the figure of DHCP option 82 in the previous page, use the following commands to achieve:

```
dhcp-option82
dhcp router 18
dhcp-option82 enable 12
```

Refer to the example figure of DHCP relay application, use the following commands to achieve:

```
dhcp-relay
dhcp router 18
dhcp-relay enable 10.0.0.1 12
```

4.3.7 LLDP

Link Layer Discovery Protocol (LLDP) operates on data link layer. It stores and maintains the information about the local device and the devices directly connected to it for network administrators to manage networks through NMS (network management systems). In LLDP, device information is encapsulated in LLDP PDUs in the form of TLV (meaning type, length, and value) triplets and is exchanged between directly connected devices. Information in LLDP PDUs received is restored in its MIB.

NOTE: Currently the LLDP neighbor(s) can be seen through the console only. SNMP browser will be supported in the future.

■ LLDP Operation Mode

LLDP can operate in one of the following modes.

- TxRx mode: A port in this mode sends and receives LLDP PDUs.
- Tx mode: A port in this mode only sends LLDP PDUs.
- Rx mode: A port in this mode only receives LLDP PDUs.
- Disable mode: A port in this mode does not send or receive LLDP PDUs.

LLDP is initialized when an LLDP-enabled port changes to operate in another LLDP operating mode. To prevent LLDP from being initialized too frequently, LLDP undergoes a period before being initialized on an LLDP-enabled port when the port changes to operate in another LLDP operating mode. The period is known as initialization delay, which is determined by the re-initialization delay timer.

■ Sending LLDP PDUs

A LLDP-enabled device operating in the TxRx mode or Tx mode sends LLDP PDUs to its directly connected devices periodically. It also sends LLDP PDUs when the local configuration changes to inform the neighboring devices of the change timely. In any of the two cases, an interval exists between two successive operations of sending LLDP PDUs. This prevents the network from being overwhelmed by LLDP PDUs even if the LLDP operating mode changes frequently.

To enable the neighboring devices to be informed of the existence of a device or an LLDP operating mode change (from the disable mode to TxRx mode, or from the Rx mode to Tx mode) timely, a device can invoke the fast sending mechanism. In this case, the interval to send LLDP PDUs changes to one second. After the device sends specific number of LLDP PDUs, the interval restores to the normal. (A neighbor is discovered when a device receives an LLDPDU and no information about the sender is locally available.)

■ Receiving LLDP PDUs

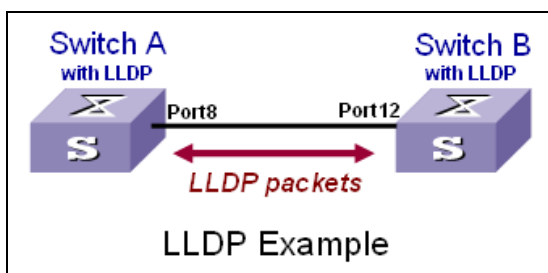
An LLDP-enabled device operating in the TxRx mode or Rx mode validates the TLVs carried in the LLDP PDUs which receive and store the valid neighboring information. An LLDP PDU also carries a TTL (time to live) setting with it. The information about a neighboring device maintained locally ages out when the corresponding TTL expires.

The TTL of the information about a neighboring device is determined by the following expression:

$$\text{TTL} = \text{LLDP hold time} \times \text{LLDP PDU sending interval (hello-time)}$$

You can set the TTL by configuring the LLDP hold-time and hello-time. Note that the TTL can be up to 65535 seconds. TTL longer than it will be rounded off to 65535 seconds.

The following figure is an example of LLDP connection:



■ LLDP Commands

[no] lldp

Enable/Disable LLDP global option

lldp hello-time <5-32768>

Set LLDP hello time which is the time interval between the transmission LLDP info packets. The range is from 5 to 32768 seconds. Default is 30 seconds.

lldp hold-time <2-10>

Set LLDP hold time. The range is from 2 to 10. Default is 4.

lldp port <rx|tx|both> [<PORT-LIST>]

Set LLDP port-based receive and transmit packet mode.

Parameters:

<rx|tx|both> **rx**: the port only receive LLDP packets; **tx**: the port only transmit LLDP packets;
both: the port can receive and transmit LLDP packets.

<PORT-LIST> specifies the ports to be set. If not specified, all ports are set.

no lldp port [<PORT-LIST>]

Disable LLDP port-based receive and transmit packet mode.

Parameters:

<PORT-LIST> specifies the ports to be set. If not specified, all ports are set.

show lldp

Show the LLDP global option, all the ports configuration and the neighbor's information.

show lldp port [<PORT-LIST>]

show LLDP port configuration and the neighbor's information..

Parameters:

<PORT-LIST> specifies the ports to be set. If not specified, all ports are set.

An LLDP example refer to the figure in previous page, the following commands will be used:

lldp (for switch A & B)

lldp port both 8 (for switch A)

lldp port both 12 (for switch B)

show lldp port 8 (for switch A to see the switch B's LLDP info learned by Switch A)

Port8 Information

State	:	RX and TX
Pkt Tx	:	3868
Pkt Rx	:	46409
Neighbor Count	:	1
Neighbor 1 information		
TTL Time	:	5879
Class ID	:	56:78:17:45:25:00
Port ID	:	port(12)
System Name	:	
System Description	:	VIA TEG-S2620ISwitch v2.16
Port Description	:	Port 12
Port SetSpeed	:	Auto
Port ActualSpeed	:	FULL-100
Port Link Aggregation	:	not support

4.4 Syslog

syslog-server <server-ip> <logging-level>

Setting the syslog server and logging level.

Parameters:

<server-ip> specifies the syslog server IP

<logging-level> specifies the logging level (0: none; 1: major; 2: all)

show syslog-server

Display the syslog server IP and logging level

4.5 Reboot switch

4.5.1 Reset to Default

erase startup-config

Reset configurations to default factory settings at next boot time.

4.5.2 Restart

boot

Reboot (warm-start) the switch.

4.6 TFTP Function

4.6.1 TFTP Firmware Update

copy tftp firmware <ip-addr> <remote-file>

Download firmware from TFTP server.

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

4.6.2 Restore Configure File

copy tftp <running-config | flash> <ip-addr> <remote-file>

Retrieve configuration from the TFTP server. If the remote file is the text file of CLI commands, use the keyword **running-config**. If the remote file is the configuration flash image of the switch instead, use the keyword **flash**.

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be downloaded from the TFTP server.

4.6.3 Backup Configure File

copy <running-config | flash> tftp <ip-addr> <remote-file>

Send configuration to the TFTP server. If you want to save the configuration in a text file of CLI commands, use the keyword **running-config**. If you want to save the configuration flash image instead, use the keyword **flash**.

Parameters:

<ip-addr> specifies the IP address of the TFTP server.

<remote-file> specifies the file to be backed up to the TFTP server.

4.7 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-IPv4 packets. This switch can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

NOTE: This function is available only in the 802.1q VLAN enabled environment.

4.7.1 IPv4 ACL commands

no acl <group id>

Delete ACL group.

Parameters:

<group id> specifies the group id (1~220).

e.g. no acl 1

no acl count <group id>

Reset the ACL group count

Parameters:

<group id> specifies the group id (1~220).

Enable/Disable acl <group id>

Reset the ACL group count

Parameters:

<group id> specifies the group id (1~220)

show acl [<group id>]

Show all or ACL group information by group id

Parameters:

<group id> specifies the group id, null means all valid groups.

e.g. show acl 1

```
Group Id      : 1
-----
Action       : Permit
Rules:
Vlan ID      : Any
IP Fragement  : Uncheck
Src IP Address : Any
Dst IP Address : Any
L4 Protocol   : Any
Port ID      : Any
Hit Octet Count : 165074
Hit Packet count : 472
```

acl (add|edit) <group id> (permit|deny) <0-4094> ipv4 <0-255> A.B.C.D A.B.C.D A.B.C.D A.B.C.D (check|unCheck) <0-65535> <0-26>

Add or edit ACL group for IPv4 packets.

Parameters:

(add|edit) specifies the operation.

<group id> specifies the group id (1~220).

(permit|deny) specifies the action. permit: permit packet cross switch; deny: drop packet.

<0-4094> specifies the VLAN id. 0 means don't care.

<0-255> specifies the IP protocol. 0 means don't care.

1st A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

2nd A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

3rd A.B.C.D specifies the Destination IP Address. 0.0.0.0 means don't care.

4th A.B.C.D specifies the Mask. 0.0.0.0 means don't care, 255.255.255.255 means compare all.

(check|unCheck) specifies the IP Fragment. check: Check IP fragment field; unCheck: Not check IP fragment field.

<0-65535> specifies the Destination port number if TCP or UDP. 0 means don't care.
<0-26> specifies the Port id. 0 means don't care.
e.g. acl add 1 deny 1 ipv4 0 192.168.1.1 255.255.255.255 0.0.0.0 0.0.0.0 unCheck 0 0
This ACL rule will drop all packet from IP is 192.168.1.1 with VLAN id=1 and IPv4.

acl (add | edit) <group id> (qosvoip) <0-4094> <0-7> <0-1F> <0-1F> <0-FF> <0-FF> <0-FFFF> <0-FFFF> <0-FFFF> <0-FFFF>
Add or edit ACL group for Ipv4.

Parameters:

(add | edit) specifies the operation.
<group id> specifies the group id (1~220).
(qosvoip) specifies the action, do qos voip packet adjustment.
<0-4094> specifies the VLAN id. 0 means don't care.
<0-1F> specifies the port ID value.
<0-1F> specifies the port ID mask.
<0-FF> specifies the protocol value.
<0-FF> specifies the protocol mask.
<0-FFFF> specifies the source port value.
<0-FFFF> specifies the source port mask.
<0-FFFF> specifies the destination port value.
<0-FFFF> specifies the destination mask.

e.g. acl add 1 qosvoip 1 7 1 1 0 0 0 0 0

4.7.2 Non-IPv4 ACL commands

no acl <group id> and **show acl [<group id>]** commands are the same as in Ipv4 ACL commands.

acl (add | edit) <1-220> (permit | deny) <0-4094> nonipv4 <0-65535>

Add or edit ACL group for non-Ipv4.

Parameters:

(add | edit) specifies the operation.
<group id> specifies the group id (1~220).
(permit | deny) specifies the action. permit: permit packet cross switch; deny: drop packet.
<0-4094> specifies the VLAN id. 0 means don't care.
<0-65535> specifies the Ether Type. 0 means don't care.

e.g. acl add 1 deny 0 nonipv4 2054

This ACL rule will drop all packets for ether type is 0x0806 and non-IPv4

4.7.3 SIP/SMAC Binding

Source IP (SIP) / Source MAC (SMAC) address binding is another type of ACL rule to provide secured access to the switch. Only the traffic which matches all criteria of specified source IP address, source MAC address, VLAN ID and port number can be allowed to access to the switch. This function is also called IP-MAC lock.

bind

Enable binding function.

no bind

Disable binding function.

no bind <group id>

Delete Binding group.

Parameters:

<group id> specifies the group id (1~220).

e.g. no bind 1

show bind [<group id >]

Show Binding group information.

Parameters:

<group id> specifies the group id (1~220), null means all valid groups.

e.g. show bind 1

bind add < group id > A:B:C:D:E:F <0-4094> A.B.C.D <1-26>

Add Binding group.

Parameters:

< group id > specifies the group id (1~220).

1st A.B.C.D specifies the MAC address.

<0-4094> specifies the VLAN id. 0 means don't care.

2nd A.B.C.D specifies the Source IP address. 0.0.0.0 means don't care.

3rd A.B.C.D specifies the IP Address.

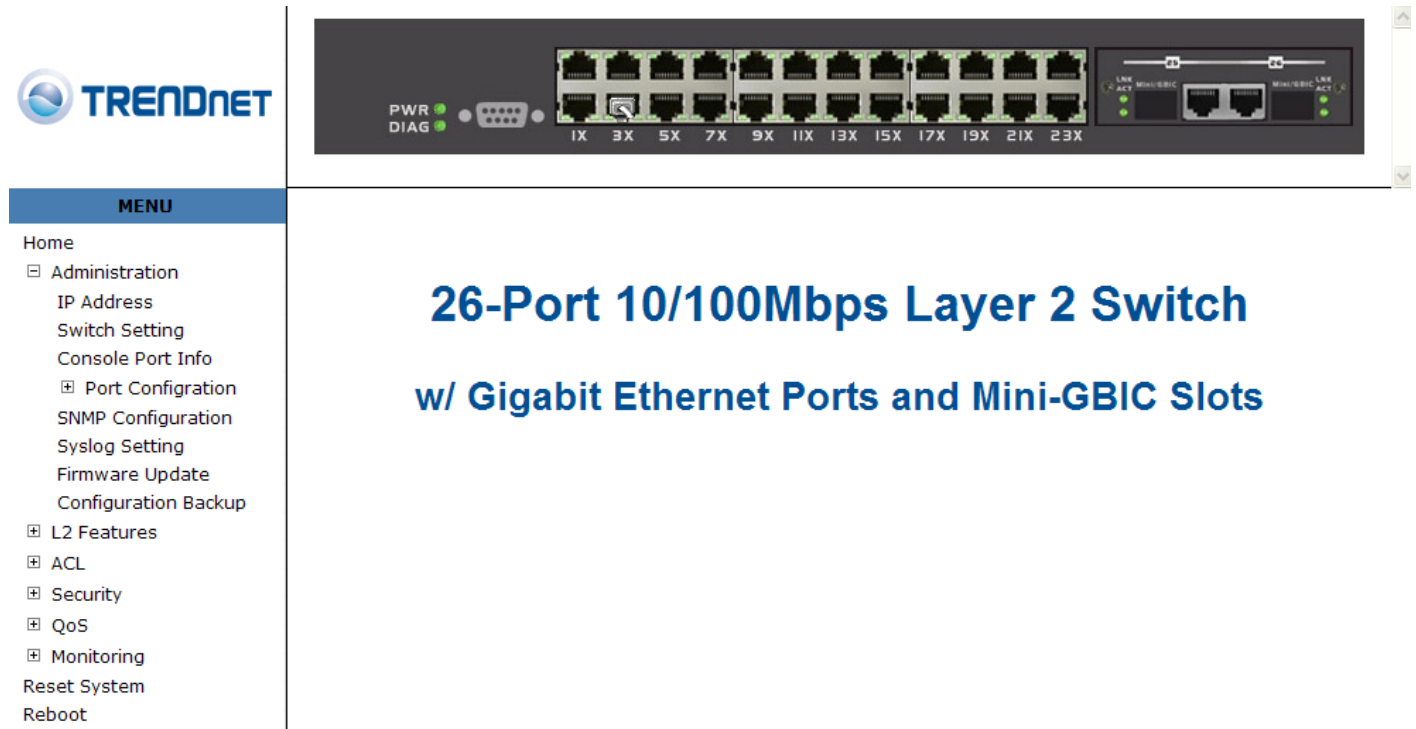
<1-26> specifies the Port id.

e.g. bind add 1 00:11:22:33:44:55 0 192.168.1.1 1. This Binding rule will permit all packet cross switch from device's IP is 192.168.1.1 and MAC is 00:11:22:33:44:55 and this device connect to switch port id=1.

5 Web User Interface

5.1 Main Menu

This is the main menu of the switch firmware in web interface.



The screenshot displays the TrendNet web interface. On the left is a navigation menu with the following items: Home, Administration (with sub-items: IP Address, Switch Setting, Console Port Info, Port Configuration, SNMP Configuration, Syslog Setting, Firmware Update, Configuration Backup), L2 Features, ACL, Security, QoS, Monitoring, Reset System, and Reboot. The main content area features a product image of a 26-port switch and the following text:

26-Port 10/100Mbps Layer 2 Switch w/ Gigabit Ethernet Ports and Mini-GBIC Slots

5.2 Administration

There are many management functions can be set or performed if you expand the submenus of **Administrator** in MENU area. These functions are:

- IP address Setting
- Switch Settings
- Console Port information
- Port Controls
- SNMP Configuration
- Security Manager
- 802.1x Configuration
- Quality of Service (QoS)
- Syslog Setting
- Firmware Update
- Configuration Backup

5.2.1 IP Address Setting

User can see and modify the IP address, subnet mask and default gateway in this page, then clicks “Apply” button to confirm (save) the settings, then the switch **reboot** must be done to activate the updates. The IP address can be statically set or dynamically be assigned by enabling DHCP option.

NOTE: If any of the value is changed in this field, reboot is necessary.

IP Address Setting

DHCP: ▾

IP Address	<input type="text" value="192.168.1.172"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.1.254"/>

5.2.2 Switch Setting

5.2.2.1 Basic

All information in **Basic** page is all read only, user can't modify the contents.

Model name: Display the switch's model name.

Description: Display the name of device type.

MAC Address: The unique hardware address assigned by manufacturer (default)

Firmware version: Display the switch's firmware version.

Switch Setting

Basic	Module Info	Misc Config
--------------	--------------------	--------------------

Model name	TEG-S2620i
Description	Intelligent 24+2G Switch
MAC Address	00:0A:17:02:21:00
Firmware version	2.19

5.2.2.2 Module Info

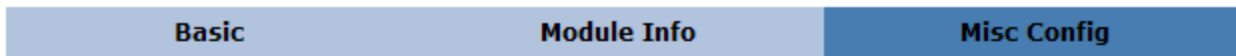
All information in this field is read only, user can't modify its contents. It is only to display the module port information.

	TYPE	DESCRIPTION
Module1	8	GIGA COMBO
Module2	8	GIGA COMBO

5.2.2.3 MISC CONFIG

This page is to provide miscellaneous settings:

Switch Setting



MAC Table Address Entry
Age-Out Time: seconds (6~1572858,must multiple of 6,default is 300s)

Broadcast Storm Filter Mode: ▾

Broadcast Storm Filter Packet select

Broadcast Packets

IP Multicast

Control Packets

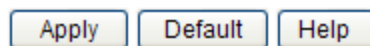
Flooded Unicast/Multicast Packets

Collisions Retry Forever : ▾

Hash Algorithm : ▾

IP/MAC Binding : ▾

802.1x Protocol : ▾



MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 6~1572858 seconds. Default is 300 seconds. The value is a multiple of 6.

Broadcast Storm Filter Mode: To configure broadcast storm control, enable it and set the upper threshold for individual ports.

The threshold is the percentage of the port's ingress bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 1/2, 1/4, 1/8, 1/16, and off.

Broadcast Storm Filter Packets Select: To select broadcast storm Filter Packets type. If no packets type by selected, mean can not filter any packets .The Broadcast Storm Filter Mode will show OFF.

Collisions Retry Forever: In half duplex, collision-retry maximum is 16, 32, or 48 times and packet will be dropped if collisions still happen. In default (Disable), system will retry forever if collisions happen.

Hash Algorithm: Select Hash Algorithm.

IP/MAC Bing: Enable or disable SMAC and SIP binding.

802.1x Protocol: Enable or disable 802.1x protocol.

5.2.3 Console Port Information

Console is a standard UART (RS-232) interface to communicate with Serial Port.

User can use windows HyperTerminal program to link the switch. Connect To -> Configure:

Bits per seconds: 115200

Data bits: 8

Parity: none

Stop Bits: 1

Flow control: none

Console Information

Baurate(bits/sec)	115200
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

Help

5.2.4 Port Configuration

5.2.4.1 Port Controls

The following webpage is to provide the display and modification for the port settings. Use the dropdown in Port field to select one or multiple ports in the upper control area. The lower display area will show the port settings for the selected port(s). Use the other control fields in the upper area to modify the port settings for the selected port(s). Press **Apply** to save and activate the port settings.

Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
						Ingress	Egress			
Port1 <input type="checkbox"/> Port2 <input type="checkbox"/> Port3 <input type="checkbox"/> Port4 <input type="checkbox"/>	Enable <input type="button" value="v"/>	Auto <input type="button" value="v"/>	1000 <input type="button" value="v"/>	Full <input type="button" value="v"/>	Enable <input type="button" value="v"/>	0 <input type="text"/>	0 <input type="text"/>	<input type="checkbox"/>	Enable <input type="button" value="v"/>	Enable <input type="button" value="v"/>

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit: 128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			

State: User can disable or enable this port.

Negotiation: User can set auto negotiation mode is Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation), Force of per port.

Speed: User can set 100Mbps or 10Mbps speed on Port1~Port24. User can set 1000Mbps, 100Mbps or 10Mbps speed on Port25~Port26 (depend on module card mode).

Duplex: User can set full-duplex or half-duplex mode of per port.

Flows control:

- **Full:** User can set flow control function is enable or disable in full mode.
- **Half:** User can set backpressure is enable or disable in half mode.

Rate Control: port1 ~ port 24, supports by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. Device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

- **Ingress:** Type the port effective ingress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.
0: disable rate control.
1 ~ 8000: valid rate value
- **Egress:** Type the port effective egress rate. The valid range is 0 ~ 8000. The unit is 128Kbps.
0: disable rate control.
1 ~ 8000: valid rate value.

Port Security: A port in security mode will be “locked” without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. User can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click

Apply to change on this page.

BSF: User can disable/Enable port broadcast storm filtering option by port. The filter mode and filter packets type can be select in Switch Setting > Misc Config page.

Jumbo Frame: User can disable/Enable port jumbo frame option by port. When port jumbo frame is enable, the port forward jumbo frame packet

5.2.4.2 Port Sniffer

The Port Sniffer (mirroring) is a method for monitor traffic in switched networks. Traffic through a port can be monitored by one specific port. That is, traffic goes in or out a monitored port will be duplicated into sniffer port.

Sniffer Type: Select a sniffer mode: Disable / Rx / Tx / Both.

Analysis (Monitoring) Port: It' means Analysis port can be used to see the traffic on another port you want to monitor. You can connect Analysis port to LAN analyzer or netxray.

Monitored Port: The port you want to monitor. The monitor port traffic will be copied to Analysis port. You can select one monitor ports in the switch. User can choose which port that they want to monitor in only one sniffer type.

NOTE:

1. The Analysis port is dedicated for monitoring usage. That is the ordinary port function will be unavailable.
2. If you want to disable this function, you must select monitor port to none.

Port Sniffer

Sniffer Type: BOTH <input type="button" value="v"/>	
Analysis Port: Port1 <input type="button" value="v"/>	
Port	Monitor
Port1	<input type="radio"/>
Port2	<input type="radio"/>
Port3	<input type="radio"/>
Port4	<input type="radio"/>
Port5	<input type="radio"/>
Port6	<input type="radio"/>
Port7	<input type="radio"/>
Port8	<input type="radio"/>
Port9	<input type="radio"/>
Port10	<input type="radio"/>
Port11	<input type="radio"/>
Port12	<input type="radio"/>
Port13	<input type="radio"/>
Port14	<input type="radio"/>
Port15	<input type="radio"/>

5.2.4.3 Protected Port

There are two protected port groups. Ports in different groups can't communicate each other.

In the same group, protected ports can't communicate each other, but can communicate with unprotected ports. Unprotected ports can communicate with any ports, including protected ports. In default, all ports are in Group1 and not protected.

Portected Port Setting

Port ID	Protected	Group1	Group2
Port1	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port4	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port5	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port6	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port7	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port8	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port9	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port10	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port11	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port12	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port13	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port14	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port15	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port16	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>
Port17	<input type="checkbox"/>	<input checked="" type="radio"/>	<input type="radio"/>

For example, in the above configuration page for protected port, Port4 in Group2, other ports in Group1, and both Port1& Port2 are protected. These settings provide Port4 can't communicate with other ports in Group1. Port1 & Port2 can't communicate each other but can communicate with other ports in Group1.

5.2.5 SNMP Configuration

Any Network Management platform running the simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a Protocol that governs the transfer of information between management station and agent.

5.2.5.1 System Options

Use this page to define management stations as trap managers and to enter SNMP community strings. User can also define a name, location, and contact person for the switch. Fill in the system options data, and then click **Apply** to update the changes on this page.

Name: Enter a name to be used for the switch.

Location: Enter the location of the switch.

Contact: Enter the name of a person or organization.

SNMP Status: Enable/Disable SNMP Function

SNMP Configuration

System Options

Name:	<input type="text" value="Layer 2 Switch"/>
Location:	<input type="text" value="No Location"/>
Contact:	<input type="text" value="No Contact"/>
SNMP Status:	<input type="text" value="Disable"/> ▾

5.2.5.2 Community strings

Serve as passwords and can be entered as one of the following:

RO: Read only. Enables requests accompanied by this string to display MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

Community Strings

Current Strings:		New Community String:
<div style="border: 1px solid black; padding: 5px; min-height: 50px;">(none)</div>	<input type="button" value=" << Add <<"/> <input type="button" value=" Remove"/>	String: <input type="text"/> <input checked="" type="radio"/> RO <input type="radio"/> RW

5.2.5.3 Trap Manager

Trap Manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.

Trap Managers

Current Managers:		New Manager:
(none)	<input data-bbox="500 464 659 501" type="button" value=" << Add << "/> <input data-bbox="500 533 651 571" type="button" value=" Remove "/>	IP Address: <input data-bbox="911 474 1125 512" type="text"/> Community: <input data-bbox="911 527 1125 564" type="text"/>

5.2.5.4 SNMPv3 Group

Maintain SNMPv3 group.

Group Name: specifies the group name.

v1 | v2c | USM: specifies the security model.

Security Name: specifies the security name.

V3 Group

Current Strings:		SNMP Group
root_v1_root admin_v1_admin public_v1_public root_v2c_root admin_v2c_admin public_v2c_public	<input data-bbox="492 1205 651 1243" type="button" value=" << Add << "/> <input data-bbox="492 1274 643 1312" type="button" value=" Remove "/>	Group Name: <input data-bbox="927 1184 1149 1222" type="text" value="Input group-name"/> V1 V2c USM: <input data-bbox="927 1247 1027 1285" type="text" value="v1"/> Security Name: <input data-bbox="927 1304 1149 1341" type="text" value="Input security-name"/>

5.2.5.5 SNMPv3 View

Maintain SNMPv3 view.

View Name: specifies the view name.

Included | Excluded: specifies the view type.

View Subtree: specifies the view subtree (e.g. .1.3.6.1.2.1).

View Mask: specifies the view mask, in hexadecimal digits.

V3 View

Current Strings:		SNMP View
<pre>all_included_1_80 mib2_included_1.3.6.1.2.1_fc system_included_1.3.6.1.2.1.1_fe</pre>	<p><< Add <<</p> <p>Remove</p>	<p>View Name: <input type="text" value="Input view-name"/></p> <p>Included Excluded: <input type="button" value="included"/> ▾</p> <p>View Subtree(eg: 1.3.6.1.2.1) <input type="text" value="Input view-subtree"/></p> <p>View Mask(Hex Adecimal Digits): <input type="text" value="Input view-mask"/></p>

5.2.5.6 SNMPv3 Access

Maintain SNMPv3 access control.

Group Name: specifies the group name.

v1 | v2c | USM: specifies the security model.

SNMP Access: specifies the security level (**noauth | auth | authpriv**)

Read View: specifies the access read view name.

Write Name: specifies the access write view name.

Notify Name: specifies the access notify view name.

V3 Access

Current Strings		SNMP Access
<pre>root_v1_noauth_all_all_all root_v2c_noauth_all_all_all admin_v1_noauth_all_none_all admin_v2c_noauth_all_none_all public_v1_noauth_system_none_system public_v2c_noauth_system_none_system</pre>	<p><< Add <<</p> <p>Remove</p>	<p>Group Name: <input type="text" value="Input group-name"/></p> <p>V1 V2c USM: <input type="button" value="v1"/> ▾</p> <p>SNMP Access: <input type="button" value="noauth"/> ▾</p> <p>Read View: <input type="text" value="Input read-view"/></p> <p>Write View: <input type="text" value="Input write-view"/></p> <p>Notify View: <input type="text" value="Input notify-view"/></p>

5.2.5.7 SNMPv3 USM-User

Maintain SNMPv3 USM-user.

User Name: Specifies the user name (should be the security name defined in group)

Auth Type: Specifies the authentication type (**md5 / none**)

Auth-Key: Specifies the authentication key (8~32 chars)

Private Key: Specifies the encrypt key (8~32 chars)

V3 usm-user

Current Strings:		SNMP usm-user
<div data-bbox="131 510 250 961" style="border: 1px solid black; padding: 5px;">(none)</div>	<div data-bbox="423 680 581 720" style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;"><< Add <<</div> <div data-bbox="423 751 574 791" style="border: 1px solid gray; padding: 2px;">Remove</div>	<div data-bbox="654 632 1130 667">SMMP User Name: <input data-bbox="906 632 1130 667" type="text" value="Input user-name"/></div> <div data-bbox="654 688 1013 724">Auth Type: <input data-bbox="906 688 1013 724" style="border: none; background-color: #f0f0f0; padding: 2px 5px;" type="text" value="none"/> ▼</div> <div data-bbox="654 745 1130 781">Auth Key(8~32): <input data-bbox="906 745 1130 781" type="text" value="Input auth-key"/></div> <div data-bbox="654 802 1130 837">Private Key(8~32): <input data-bbox="906 802 1130 837" type="text" value="Input priv-key"/></div>

5.2.6 Syslog

This system supports syslog sent to a remote syslog server. Currently system will do syslog for 3 events: **cold start, warm start and link change**. In this page, user needs to setup the following parameters to activate the syslog:

Syslog server IP: The IP address of remote syslog server

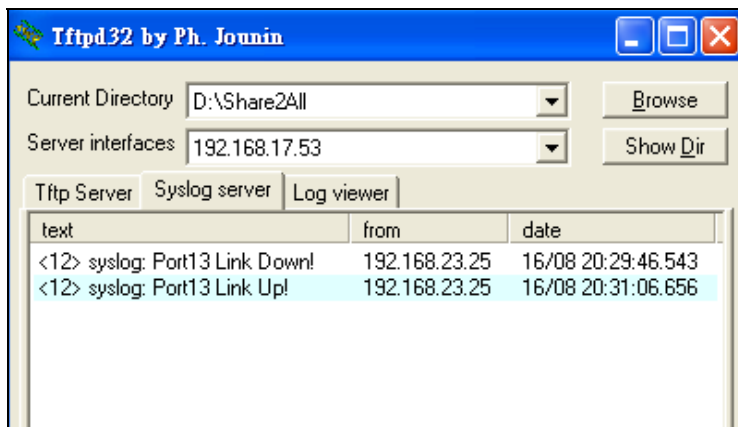
Log level: None / Major / All

Then click **Apply** button to activate the syslog function.

Syslog Setting

Syslog server IP	<input type="text"/>
Log level	None <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

The following example figure shows the syslog server application (e.g. Tftpd32.exe) got the messages from switch which link status is changed on port13.



5.2.7 Firmware Update

This system supports firmware update through two different ways: TFTP and HTTP.

5.2.7.1 TFTP Update

Use this page to assign a TFTP server IP address and an existing firmware image file. Then press **Apply** button to start the firmware update process.

Firmware Update

TFTP Firmware Update

TFTP Server IP Address	<input type="text"/>
Firmware File Name	<input type="text"/>

Apply **Help**

The firmware image will first update to the RAM area in system. Hit the **Update Firmware** button to confirm to write to the system's flash memory.

Image download complete.
Would you make sure to update firmware?

Update Firmware

When the whole process is completed, system needs to be rebooted by pressing the **reboot** button to activate the new firmware.

Reboot Switch System

reboot **Help**

5.2.7.2 HTTP Update

An alternative for firmware updating is using HTTP transfer. Just like the file copy in Windows, select the valid firmware image file to be uploaded to the switch and hit **Submit** to start the updating process. This is easier than ordinary TFTP file transfer.

HTTP Firmware Update

**Note: Firmware update needs several minutes.
Please wait a while, then manually refresh the webpage.**

When the firmware image is completely uploaded, system will automatically be rebooted.

5.2.8 Configuration Backup

Just like the firmware update, this system also supports configuration backup/restore through either TFTP or HTTP transfer.

5.2.8.1 TFTP Restore Configuration

Use this page to assign a TFTP server IP address and an existing configuration filename to be restored. Then press **Apply** button to start the restore process.

Configuration Restore

TFTP Restore Configuration

TFTP Backup Configuration

TFTP Server IP Address	<input type="text"/>
Restore File Name	<input type="text"/>

Apply **Help**

5.2.8.2 TFTP Backup Configuration

Use this page to assign a TFTP server IP address and a filename to be stored. Then press **Apply** button to start the backup process.

Configuration Restore

TFTP Restore Configuration

TFTP Backup Configuration

TFTP Server IP Address	<input type="text" value="10.99.100.228"/>
Restore File Name	<input type="text" value="flash.dat"/>

Apply **Help**

5.3 L2 Features

This switch provides the following L2 features:

- VLAN Configuration
- Trunking (Port Aggregation)
- Forwarding & Filtering
- Spanning Tree (STP)
- DHCP Relay & Option 82
- LLDP (**optional**)

5.3.1 VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

This switch supports port-based, 802.1Q (tagged-based) or no VLAN in web management page. In default, 802.1Q VLAN is enabled for common and advanced operations.

In VLAN configuration, there are three categories to configure:

- Static VLAN
- GVRP VLAN
- QinQ VLAN

5.3.1.1 Static VLAN

5.3.1.1.1 Port Based VLAN

VLAN Configuration

VLAN Operation Mode: Port Based VLAN ▾

VLAN Information

DEFAULT	1
TestLAN02	2

First select Port-based VLAN in VLAN Operation Mode. Then click **Add** to create a new VLAN group.

Enter the VLAN name, group ID and select the members for the new VLAN. Then click **Apply** to activate the setting.

If there are many groups that over the limit of one page, you can click the [Next Page](#) to view other VLAN groups.


NOTE: If the trunk groups exist, you can see it (ex: TRK1, TRK2...) in select menu of ports, and you can configure it is the member of the VLAN or not.

5.3.1.1.2 802.1Q VLAN

In this page, user can create 802.1Q (tag-based) VLAN.

There are up to 512 VLAN groups to provide configuration. While VLAN Operation Mode is changed to 802.1Q VLAN, all ports on the switch belong to default VLAN group which VID is 1. The default VLAN group can't be deleted.

VLAN Configuration

VLAN Operation Mode: 

Basic | **VLAN filter**

VLAN Information

DEFAULT ___ 1

Basic | **VLAN filter**

VLAN Name:

VID:

Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10 Port11 Port12	<input type="button" value="Add >>"/>	<input type="button" value="<< Remove"/>
---	---	--

CPU Port

▪ **Basic**

Create a VLAN and add tagged member ports to it.

1. From the main menu, click Administrator → VLAN configuration, click Add then you will see the page as follow.
2. Type a name for the new VLAN.
3. Type a VID (1~4094). The default is 1.
4. From the Available ports box, select ports to add to the switch and click “Add >>”. If the trunk groups exist, you can see it in here (ex: TRK1, TRK2...), and you can configure it is the member of the VLAN or not.
5. Click Next. Then you can view the page as follow :

6. Uses this page to set the outgoing frames are VLAN-Tagged frames or no. Then click Apply.
Tag: outgoing frames with VLAN-Tagged.
Untag: outgoing frames without VLAN-Tagged.

▪ **VLAN Filters**

Basic | **VLAN filters**

Ingress Filtering Rule 1
 (Forward only packets with VID matching this port's configured VID)
Ingress Filtering Rule 2
 (Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
<ul style="list-style-type: none"> Port1 Port2 Port3 Port4 	1	Enable	Disable

Apply | Default | Help

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
Port1	1	ENABLE	DISABLE
Port2	1	ENABLE	DISABLE
Port3	1	ENABLE	DISABLE

Port NO.

Port number(s) to be assigned to see or configure the settings.

Port VID (PVID)

Port VLAN ID will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. This switch allows user to set one PVID for each port, the range is

1~4094, default PVID is 1. The PVID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. This switch has two ingress filtering rules as follows:

Ingress Filtering Rule 1: A forward only packet with VID matching this port's configured VID.

Ingress Filtering Rule 2: Drop Untagged Frame.

5.3.1.2 GVRP VLAN

5.3.1.2.1 GVRP Setting

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch, the switch will automatically add that device to the existing VLAN

GVRP can be enabled per port basis. To enable GVRP function for a port, both global GVRP and special port GVRP are required to configure.

GVRP Configuration

GVRP Setting

[GVRP Table](#)

GVRP Disable ▾	
Port	GVRP
Port1	<input type="checkbox"/>
Port2	<input type="checkbox"/>
Port3	<input type="checkbox"/>
Port4	<input type="checkbox"/>
Port5	<input type="checkbox"/>
Port6	<input type="checkbox"/>
Port7	<input type="checkbox"/>
Port8	<input type="checkbox"/>
Port9	<input type="checkbox"/>
Port10	<input type="checkbox"/>
Port11	<input type="checkbox"/>
Port12	<input type="checkbox"/>
Port13	<input type="checkbox"/>
Port14	<input type="checkbox"/>
Port15	<input type="checkbox"/>
Port16	<input type="checkbox"/>
Port17	<input type="checkbox"/>
Port18	<input type="checkbox"/>

5.3.1.2.2 GVRP Table

GVRP Configuration

GVRP Setting		GVRP Table
No	VLAN ID	Port members
1	50	17

In this page, the VLAN group(s) dynamically created by GVRP can be displayed with VID and port member(s).

5.3.1.3 QinQ VLAN

5.3.1.3.1 QinQ Port Setting

Business customers of service providers often have specific requirements for VLAN IDs and the number of VLANs to be supported. The VLAN ranges required by different customers in the same service-provider network might overlap, and traffic of customers through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations and could easily exceed the VLAN limit (4096) of the IEEE 802.1Q specification.

Using the QinQ feature, service providers can use a single VLAN to support customers who have multiple VLANs. Customer VLAN IDs are preserved, and traffic from different customers is segregated within the service-provider network, even when they appear to be in the same VLAN. Using QinQ expands VLAN space by using a VLAN-in-VLAN hierarchy and retagging the tagged packets. A port configured to support QinQ is called a QinQ user-port. A port configured to support QinQ Uplink is called a QinQ uplink-port.

To enable QinQ function, the global **QinQ** option, QinQ **Tpid** and specified port-based QinQ **User** or **Uplink** port option need to be configured.

QinQ Configuration

QinQ Port Setting

[QinQ Tunnel Setting](#)

QinQ Disable <input type="button" value="v"/>		
QinQ Tpid <input type="text" value="8100"/>		
Port	QinQ	QinQ Uplink
Port1	<input type="checkbox"/>	<input type="checkbox"/>
Port2	<input type="checkbox"/>	<input type="checkbox"/>
Port3	<input type="checkbox"/>	<input type="checkbox"/>
Port4	<input type="checkbox"/>	<input type="checkbox"/>
Port5	<input type="checkbox"/>	<input type="checkbox"/>
Port6	<input type="checkbox"/>	<input type="checkbox"/>
Port7	<input type="checkbox"/>	<input type="checkbox"/>
Port8	<input type="checkbox"/>	<input type="checkbox"/>
Port9	<input type="checkbox"/>	<input type="checkbox"/>
Port10	<input type="checkbox"/>	<input type="checkbox"/>
Port11	<input type="checkbox"/>	<input type="checkbox"/>
Port12	<input type="checkbox"/>	<input type="checkbox"/>
Port13	<input type="checkbox"/>	<input type="checkbox"/>
Port14	<input type="checkbox"/>	<input type="checkbox"/>
Port15	<input type="checkbox"/>	<input type="checkbox"/>
Port16	<input type="checkbox"/>	<input type="checkbox"/>
Port17	<input type="checkbox"/>	<input type="checkbox"/>

5.3.1.3.2 QinQ Tunnel Setting

Virtual private networks (VPNs) provide enterprise-scale connectivity on a shared infrastructure, often Ethernet-based, with the same security, prioritization, reliability, and manageability requirements of private networks. QinQ tunnel is a feature designed for service providers who carry traffic of multiple customers across their networks and are required to maintain the VLAN and Layer 2 protocol configurations of each customer without impacting the traffic of other customers. When you configure QinQ tunnel, you assign the QinQ user-port and uplink-port to a VLAN ID that is dedicated to QinQ tunnel.

To add QinQ tunnel, you first select QinQ Tunnel ID, then fill VLAN ID QinQ dedicated to QinQ tunnel, and select user-port and uplink-port to be added to QinQ tunnel.

QinQ Configuration

[QinQ Port Setting](#)

QinQ Tunnel Setting

Tunnel ID	Tunnel1 ▾	<< Get
Tunnel VID	4	
Port4 Port5 Port6 Port7	<< Add << Remove>>	Port1 ▲ Port2 Port3 ≡ Port8 Port9 Port10 Port11 Port12 Port13 ▾

Apply Delete Help

5.3.2 Trunking

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode**, more detail information refers to IEEE 802.3ad.

5.3.2.1 Aggregator Setting

Trunking

Aggregator Setting	Aggregator information	State Activity												
<table border="1"><thead><tr><th>LACP</th><th>System Priority</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td><input type="text" value="32768"/></td></tr></tbody></table>			LACP	System Priority	<input type="checkbox"/>	<input type="text" value="32768"/>								
LACP	System Priority													
<input type="checkbox"/>	<input type="text" value="32768"/>													
<table border="1"><thead><tr><th>Group ID</th><td>Group4 <input type="button" value="v"/></td><td><input type="button" value="<< Get"/></td></tr><tr><th>Lacp</th><td>Enable <input type="button" value="v"/></td><td></td></tr><tr><th>Work Ports</th><td><input type="text" value="6"/></td><td></td></tr><tr><td><ul style="list-style-type: none">Port18Port19Port20Port21Port22Port23</td><td><input type="button" value="<< Add <<"/> <input type="button" value="Remove >>"/></td><td><ul style="list-style-type: none">Port12 <input type="button" value="v"/>Port13Port14Port15Port16Port17Port24Mod1Mod2 <input type="button" value="v"/></td></tr></thead></table>			Group ID	Group4 <input type="button" value="v"/>	<input type="button" value="<< Get"/>	Lacp	Enable <input type="button" value="v"/>		Work Ports	<input type="text" value="6"/>		<ul style="list-style-type: none">Port18Port19Port20Port21Port22Port23	<input type="button" value="<< Add <<"/> <input type="button" value="Remove >>"/>	<ul style="list-style-type: none">Port12 <input type="button" value="v"/>Port13Port14Port15Port16Port17Port24Mod1Mod2 <input type="button" value="v"/>
Group ID	Group4 <input type="button" value="v"/>	<input type="button" value="<< Get"/>												
Lacp	Enable <input type="button" value="v"/>													
Work Ports	<input type="text" value="6"/>													
<ul style="list-style-type: none">Port18Port19Port20Port21Port22Port23	<input type="button" value="<< Add <<"/> <input type="button" value="Remove >>"/>	<ul style="list-style-type: none">Port12 <input type="button" value="v"/>Port13Port14Port15Port16Port17Port24Mod1Mod2 <input type="button" value="v"/>												

| | | |

System Priority: A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.

Group ID: There are up to 7 trunk groups can be configured. Choose the "Group ID" and click to retrieve the trunk group.

LACP: If enabled, the group is LACP static trunk group. If disabled, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.

Work ports: Allow max eight ports can be aggregated at the same time. If LACP static trunk group, the exceed ports is standby and able to aggregate if work ports fail. If local static trunk group, the number must be as same as the group member ports. Select the ports to join the trunk group. Allow max 8 ports can be aggregated at the same time. If LACP enabled, you can configure LACP Active/Passive status in each port on State Activity page.

5.3.2.2 Aggregator Information

When you are setting LACP aggregator, you can see relation information in here. The following page shows no group active and no LACP related data.

Trunking

Aggregator Setting	Aggregator information	State Activity
--------------------	------------------------	----------------

The following information provides a view of LACP current status.

This page shows some static trunk groups are created.

Trunking

Aggregator Setting	Aggregator information	State Activity
--------------------	------------------------	----------------

The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	10
Port_No	15 16

This page shows actor and partner trunks one group.

Trunking

Aggregator Setting	Aggregator information	State Activity
--------------------	------------------------	----------------

Port	LACP State Activity	Port	LACP State Activity
1	N/A	2	N/A
3	N/A	4	N/A
5	<input checked="" type="checkbox"/> Active	6	<input checked="" type="checkbox"/> Active
7	<input checked="" type="checkbox"/> Active	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	<input checked="" type="checkbox"/> Active
19	<input checked="" type="checkbox"/> Active	20	<input checked="" type="checkbox"/> Active
21	<input checked="" type="checkbox"/> Active	22	<input checked="" type="checkbox"/> Active
23	<input checked="" type="checkbox"/> Active	24	N/A
25	N/A	26	N/A

5.3.2.3 State Activity

Active (select): The port automatically sends LACP protocol packets.

N/A (no select): The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

1. A link that has either two active LACP ports or one active port can perform dynamic LACP trunking.

A link has two N/A LACP ports will not perform dynamic LACP trunking because both ports are waiting for and LACP protocol packet from the opposite device.

2. If you are active LACP's actor, when you are select trunking port, the active status will be created automatically.

Port	LACP State Activity	Port	LACP State Activity
1	N/A	2	N/A
3	N/A	4	N/A
5	<input checked="" type="checkbox"/> Active	6	<input checked="" type="checkbox"/> Active
7	<input checked="" type="checkbox"/> Active	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	<input checked="" type="checkbox"/> Active
19	<input checked="" type="checkbox"/> Active	20	<input checked="" type="checkbox"/> Active
21	<input checked="" type="checkbox"/> Active	22	<input checked="" type="checkbox"/> Active
23	<input checked="" type="checkbox"/> Active	24	N/A
25	N/A	26	N/A

Apply

Help

5.3.3 Forwarding and Filtering

In this submenu, the following functions related to forwarding and filtering are provided:

- IGMP Snooping
- Dynamic MAC Table
- Static MAC Table
- MAC Filtering

5.3.3.1 IGMP Snooping

This switch supports multicast IP, one can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information in this page, you can view difference multicast group, VID and member port in here, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

Forwarding and Filtering

IGMP Snooping

Dynamic MAC Table

Static MAC Table

MAC Filtering

Multicast Group

Ip_Address _____ VID _____ MemberPort _____

239.255.255.250	1	**3*****
-----------------	---	----------

IGMP Protocol: ▾

IGMP fastleave: ▾

IGMP Querier: ▾

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the queries (IGMP router or switch) asking for a response from each host belonging multicast group.
Report	A message sent by a host to the queries to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the queries to indicate that the host has quit being a member of a specific multicast group.

IGMP protocol: Enable/disable IGMP snooping.

IGMP fast leave: Enable/disable IGMP snooping fast leave. If enable, switch will fast delete member who send leave report, else wait one second.

IGMP Querier: Enable/disable IGMP snooping querier. If select disable, the switch can't send query report.

5.3.3.2 Dynamic MAC Address

The switch will dynamically learn the device's MAC address when it corresponding with the switch. MAC address will be stored in MAC address table. Dynamic MAC Table shows the MAC addresses learned by the switch. The table will be shown by pages if larger than 500 MAC Addresses.

Forwarding and Filtering

IGMP Snooping

Dynamic MAC Table

Static MAC Table

MAC Filtering

Click "Clear" will clear Dynamic addresses from the switch .

Clear

Dynamic addresses currently learned on the switch are listed below.

NO	MAC	PORT	VID	TYPE
1	00:04:76:4A:1C:A4	3	1	Dynamic

Top

Prev

Next

There are total 1 Mac Addresses.

Click **Clear** to clear Dynamic MAC address table.

Click **Top** to show the first page of MAC address table.

Click **Prev** to show the previous page of MAC address table. If there is nothing to shown or NO is 1, it is the first page.

Click **Next** to show the next page of MAC address table. If there is nothing to shown, it is the end page.

5.3.3.3 Static MAC Table

When you add a static MAC address, it permanently remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again.

This table can associate with the **Security** field in **Port Controls** configuration to achieve the access control by source MAC / port / VID binding. That is only ingress traffic with matched lookup (with specified MAC address, port number and VID) in this table can be allowed to access to the switch.

Forwarding and Filtering

IGMP Snooping

Dynamic MAC Table

Static MAC Table

MAC Filtering

Dynamic addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address _____ PORT _____ VID _____

00:04:76:4A:1C:A4	3	1
-------------------	---	---

Mac Address

Port num

Vlan ID

NO	MAC	PORT	VID	TYPE
1	00:04:76:4A:1C:A4	3	1	Static

The following parameters can be associated to setup the Static MAC table:

MAC Address: Static MAC address in a MAC entry

Port number: Switch port number to associate with the MAC address in a MAC entry

Vlan ID: If tag-based (IEEE 802.1Q) VLANs are enabled, static MAC address can be associated with individual VLANs. Type the VID in this field to associate with the MAC address.

Click to add a new entry. Click to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

5.3.3.4 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination MAC addresses.

Forwarding and Filtering



Specify a MAC address to filter.

00:04:76:4A:1C:A4	1
-------------------	---

Mac Address

Vlan ID

NO	MAC	SOURCE	VID	TYPE
1	00:04:76:4A:1C:A4	Filter	1	Static

MAC Address: MAC address that wants to be filtered.

Vlan ID: If tag-based (802.1Q) VLAN are enabled, type the VID in this field to associate with the MAC address.

Click to add a new entry. Click to remove a specified entry.

The MAC entries in this table can be sorted by clicking the column NO / MAC / PORT / VID / TYPE.

5.3.4 Spanning Tree

5.3.4.1 STP system

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1d) for avoiding loops in switching networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network. You can enable STP on web management's switch setting advanced item, select enable STP. We are recommended that you enable STP on all switches ensures a single active path on the network. You can view STP information about the Root Bridge. Such as following screen.

Root Bridge Information

Priority	32768
MAC Address	00:0A:17:02:21:00
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view STP port status about the switch. Such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Forwarding	NO	NO	NO
Port2	2000000	128	Forwarding	NO	NO	NO
Port3	200000	128	Forwarding	NO	NO	YES
Port4	2000000	128	Forwarding	NO	NO	NO
Port8	2000000	128	Forwarding	NO	NO	NO
Port9	2000000	128	Forwarding	NO	NO	NO
Port10	2000000	128	Forwarding	NO	NO	NO
Port11	2000000	128	Forwarding	NO	NO	NO
Port12	2000000	128	Forwarding	NO	NO	NO
Port13	2000000	128	Forwarding	NO	NO	NO
Port14	2000000	128	Forwarding	NO	NO	NO
Port17	2000000	128	Forwarding	NO	NO	NO
Port24	2000000	128	Forwarding	NO	NO	NO
Mod1	2000000	128	Forwarding	NO	NO	NO
Mod2	2000000	128	Forwarding	NO	NO	NO
Trk3	20000000	128	Forwarding	NO	NO	NO
Trk4	20000000	128	Forwarding	NO	NO	NO
Trk10	20000000	128	Forwarding	NO	NO	NO

You can configure STP parameters, then click Apply button to set the values. Such as following screen.

Configure Spanning Tree Parameters

STP State (Default DISABLE)	<input checked="" type="checkbox"/>
STP protocol version (Default MSTP)	STP
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

You can select STP state item to enable STP. If you want to disable STP, please cancel the item. Default value of STP state is disabled.

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root. Value range <1-10>. Default value is 2.
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

NOTE: The above parameters must enforce the following relationships:
 $2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$

The following parameters can be configured on each port, click Apply button to set the values.

Port Number	Path Cost (1-20000000)	Priority (0 - 240; Default 128)
Port1 Port2 Port3 Port4 Port8	200000	128

You can select one port in the Port Number item to configure the parameters of the port.

Parameter	Description
-----------	-------------

Path Cost	The contribution of the path through this port, when the port is the root port, to the total cost of the path to the root for this bridge. Value range <1-65535>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has the highest priority. Value range <0-240>, the value must be in steps of 16. Default value is 128.

5.3.4.2 RSTP system

The Rapid Spanning Tree Protocol (RSTP) is a standardized method (IEEE 802.1W) that supersedes the Spanning Tree Algorithm and Protocol (STP) described as above and provides significantly faster reconfiguration. RSTP is compatible for STP, so the following content is mostly the same as the above STP description, adding some enhanced performance.

You can view RSTP information about the Root Bridge. Such as following screen.

Root Bridge Information

Priority	32768
MAC Address	00:0A:17:02:21:00
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view RSTP port status about the switch. Such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Disabled	NO	NO	NO
Port2	2000000	128	Disabled	NO	NO	NO
Port3	200000	128	Forwarding	NO	NO	YES
Port4	2000000	128	Disabled	NO	NO	NO
Port8	2000000	128	Disabled	NO	NO	NO
Port9	2000000	128	Disabled	NO	NO	NO
Port10	2000000	128	Disabled	NO	NO	NO
Port11	2000000	128	Disabled	NO	NO	NO
Port12	2000000	128	Disabled	NO	NO	NO
Port13	2000000	128	Disabled	NO	NO	NO
Port14	2000000	128	Disabled	NO	NO	NO
Port17	2000000	128	Disabled	NO	NO	NO
Port24	2000000	128	Disabled	NO	NO	NO
Mod1	2000000	128	Disabled	NO	NO	NO
Mod2	2000000	128	Disabled	NO	NO	NO
Trk3	20000000	128	Disabled	NO	NO	NO
Trk4	20000000	128	Disabled	NO	NO	NO
Trk10	20000000	128	Disabled	NO	NO	NO

Besides STP Debug and STP protocol version items, the remaining items are the same as STP describing above. You can select STP Debug item to output RSTP debug information. If you want to disable the debug, please cancel the item. Default value of STP Debug is disabled.

STP protocol version item has two values for you to choose. If you want the protocol version to be STP, you can choose STP. If you want the protocol version to be RSTP, you can choose RSTP. Default value of STP protocol version is RSTP.

The following parameters can be configured on each port, click Apply button to set the values.

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1-200000000)	Priority (0 - 240; Default 128)	Admin Edge (Default NO)	Admin Non-STP (Default NO)	Admin P2P (Default AUTO)
<div style="border: 1px solid #ccc; padding: 2px;"> Port1 ▲ Port2 ▲ Port3 ▲ Port4 ▲ Port8 ▼ </div>	200000	128	NO ▼	NO ▼	AUTO ▼
<input type="button" value="Apply"/> <input type="button" value="Help"/>					

You can select one port in the Port Number item to configure the parameters of the port. Besides Path Cost and Priority items, the remaining items are newly enhanced performance. Priority item is just the same as STP, and the value range of Path Cost item is different from STP.

Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the total cost of the path to the root for this bridge. Value range <1-200000000>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has the highest priority. Value range <0-240>, the value must be in steps of 16. Default value is 128.
Admin Edge	You can choose the value of YES if you want the port to be edge port. If the port is edge port, when the port becomes a Designated Port it can rapidly transition to the Forwarding Port State. Value range <NO YES>. Default value is NO.
Admin Non -STP	If you want to disable spanning tree protocol on the port, you can choose the value of YES to this port. Value range <NO YES>. Default value is NO.
Admin P2P	If you want point-to-point link auto detection on the port, you can choose the value of AUTO to this port. If you want point-to-point link of the port always be true, you can choose the value of YES to this port. If you want point-to-point link of the port always be false, you can choose the value of NO to this port. Value range <AUTO NO YES>. Default value is AUTO.

5.3.4.3 MSTP system

The Multiple Spanning Tree Protocol (MSTP) is a standardized method (IEEE 802.1S) for providing simple and full connectivity for frames assigned to any given VLAN throughout a Bridged Local Area Network comprising arbitrarily interconnected Bridges, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. These Regions and the other Bridges and LANs are connected into a single Common Spanning Tree (CST). You can enable MSTP on web management's switch setting advanced item, select enable MSTP. We are recommended that you enable MSTP on all switches ensures a single active path on the network.

You can view MSTP information about the CIST Root Bridge. Such as following screen.

Root Bridge Information

Priority	32768
MAC Address	00:0A:17:02:21:00
Root Path Cost	0
Root Port	0
Maximum Age	20
Hello Time	2
Forward Delay	15

You can view MSTP CIST port status about the switch. Such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState	PortEdge	PortNonSTP	PortP2P
Port1	2000000	128	Disabled	NO	NO	NO
Port2	2000000	128	Disabled	NO	NO	NO
Port3	200000	128	Forwarding	NO	NO	YES
Port4	2000000	128	Disabled	NO	NO	NO
Port8	2000000	128	Disabled	NO	NO	NO
Port9	2000000	128	Disabled	NO	NO	NO
Port10	2000000	128	Disabled	NO	NO	NO
Port11	2000000	128	Disabled	NO	NO	NO
Port12	2000000	128	Disabled	NO	NO	NO
Port13	2000000	128	Disabled	NO	NO	NO
Port14	2000000	128	Disabled	NO	NO	NO
Port17	2000000	128	Disabled	NO	NO	NO
Port24	2000000	128	Disabled	NO	NO	NO
Mod1	2000000	128	Disabled	NO	NO	NO
Mod2	2000000	128	Disabled	NO	NO	NO
Trk3	20000000	128	Disabled	NO	NO	NO
Trk4	20000000	128	Disabled	NO	NO	NO
Trk10	20000000	128	Disabled	NO	NO	NO

You can configure MSTP parameters, then click Apply button to set the values. Such as following screen.

Configure Spanning Tree Parameters

STP State (Default DISABLE)	<input checked="" type="checkbox"/>
STP protocol version (Default MSTP)	MSTP ▾
Priority (0-61440; Default 32768)	32768
Maximum Age (6-40; Default 20)	20
Hello Time (1-10; Default 2)	2
Forward Delay (4-30; Default 15)	15

You can select STP state item to enable MSTP. If you want to disable MSTP, please cancel the item. Default value of STP state is disabled.

You can select STP Debug item to output MSTP debug information. If you want to disable the debug, please cancel the item. Default value of STP Debug is disabled.

STP protocol version item has two values for you to choose. If you want the protocol version to be STP, you can choose STP. If you want the protocol version to be MSTP, you can choose MSTP. Default value of STP protocol version is MSTP.

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Value range <0-61440>, the value must be in steps of 4096. Default value is 32768.
Max Age	You can change Max Age value. The maximum age of received protocol information before it is discarded. Value range <6-40>. Default value is 20.
Hello Time	You can change Hello time value. The time interval between the transmission of Configuration BPDUs by a Bridge that is attempting to become the Root or is the Root. Value range <1-10>. Default value is 2.
Forward Delay time	You can change forward delay time. The time spent by a Port in the Listening State and the Learning State before moving to the Learning or Forwarding State, respectively. It is also the value used for the ageing time of dynamic entries in the Filtering Database, while received BPDU indicate a topology change. Value range <4-30>. Default value is 15.

NOTE: The above parameters must enforce the following relationships:

$$2 * (\text{hello-time} + 1) \leq \text{maximum-age} \leq 2 * (\text{forward-delay} - 1)$$

The following parameters can be configured on each CIST port, click Apply button to set the values.

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1-20000000)	Priority (0 - 240; Default 128)	Admin Edge (Default NO)	Admin Non-STP (Default NO)	Admin P2P (Default AUTO)
Port1 ▾ Port2 ▾ Port3 ▾ Port4 ▾ Port8 ▾	200000	128	NO ▾	NO ▾	AUTO ▾

You can select one port in the Port Number item to configure the parameters of the CIST port.

Parameter	Description
Path Cost	The contribution of the path through this port, when the port is the root port, to the total cost of the path to the root for this bridge. Value range <1-200000000>.
Port Priority	You can make it more or less likely to become the root port, the lowest number has the highest priority. Value range <0-240>, the value must be in steps of 16. Default value is 128.
Admin Edge	You can choose the value of YES if you want the port to be edge port. If the port is edge port, when the port becomes a Designated Port it can rapidly transition to the Forwarding Port State. Value range <NO YES>. Default value is NO.
Admin Non -STP	If you want to disable spanning tree protocol on the port, you can choose the value of YES to this port. Value range <NO YES>. Default value is NO.
Admin P2P	If you want point-to-point link auto detection on the port, you can choose the value of AUTO to this port. If you want point-to-point link of the port always be true, you can choose the value of YES to this port. If you want point-to-point link of the port always be false, you can choose the value of NO to this port. Value range <AUTO NO YES>. Default value is AUTO.

5.3.5 DHCP Relay and Option 82

The Relay Agent Information option (Option 82) is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server (RFC 3046). Servers recognizing the Relay Agent Information option may use the information to implement IP address or other parameter assignment policies. The DHCP Relay can forward the DHCP broadcast packets to a DHCP server in a different subnet (RFC 1542). So DHCP server can provide IP addresses to clients spanning multiple subnets instead of deploying a DHCP server on every subnet.

5.3.5.1 DHCP Option 82

To enable DHCP option 82 function, need to enable global option 82 and special port option 82. Then select DHCP router port.

DHCP Relay & Option 82

DHCP Option 82 Enable ▼		
DHCP Relay Disable ▼		
DHCP Option 82 Router Port Port4 ▼		
DHCP Opt.82 Port	Option	Relay IP
Port1	<input type="checkbox"/>	0.0.0.0
Port2	<input type="checkbox"/>	0.0.0.0
Port3	<input type="checkbox"/>	0.0.0.0
Port4	<input type="checkbox"/>	0.0.0.0
Port8	<input type="checkbox"/>	0.0.0.0

5.3.5.2 DHCP Relay

To enable DHCP relay function, need to enable global dhcp-relay and special port dhcp-relay. Then select DHCP router port.

DHCP Option 82 Disable ▼		
DHCP Relay Enable ▼		
DHCP Option 82 Router Port Port4 ▼		
DHCP Opt.82 Port	Option	Relay IP
Port1	<input type="checkbox"/>	10.99.0.196
Port2	<input type="checkbox"/>	172.0.19.108
Port3	<input type="checkbox"/>	140.155.22.90
Port4	<input type="checkbox"/>	0.0.0.0
Port8	<input type="checkbox"/>	0.0.0.0
Port9	<input type="checkbox"/>	0.0.0.0

5.3.6 LLDP

This switch supports LLDP (Link Layer Discovery Protocol) function. Please refer to the section **4.3.7** which has descriptions about the LLDP function and operation in console. Here is the web UI to configure this function.

5.3.6.1 LLDP Configuration

This page is to provide the global parameters for LLDP for configuration.

LLDP Configuration

LLDP Configuration

PerPort Configuration

Configure LLDP Parameters:

LLDP status:	Enable ▾
LLDP hello time:(5-32768)	100
LLDP hold time:(2-10)	10

Apply Help

LLDP Status: Enable/Disable LLDP.

LLDP hello time: LLDP hello time value which is time interval between the transmission LLDP info packets. Value range is from 5 to 32768. Default value is 30.

LLDP hold time: LLDP hold time value. Value range is from 2 to 10. Default value is 4.

TTL (time to live) is a period of time for keeping the information about a neighboring device. The information will be aged out when the corresponding TTL expires. TTL can be calculated by configuring LLDP hello time and hold time according to the following expression:

$$\text{TTL} = \text{LLDP hello time} \times \text{LLDP hold time}$$

5.3.6.2 PerPort Configuration

PerPort LLDP configuration is in this page:

LLDP Configuration

LLDP Configuration

PerPort Configuration

Configure Port Status

Port Number	Port Status
Port1 ▴	
Port2 ▾	
Port3 ▾	
Port4 ▾	
Port8 ▾	
	Tx_and_Rx ▾

Apply Help

Port Number: specify the port(s) to be configured in the switch.

Port Status: specify one of four port mode to operate LLDP for specified port(s)

- **Tx_only:** LLDP transmit the packet of the port only
- **Rx_only:** LLDP receive the packet of the port only.
- **Tx_and_Rx:** LLDP transmit and receive the packets of the port.
- **Disable:** LLDP do not transmit and receive the packets of the port.

PerPort LLDP configuration status can be shown in the lower area of this page like the following example:

Port Status

PortNum	Status
Port1	Tx_and_Rx
Port2	Tx_and_Rx
Port3	Tx_and_Rx
Port4	Tx_and_Rx
Port8	Tx_and_Rx
Port9	Tx_and_Rx
Port10	Tx_and_Rx
Port11	Tx_and_Rx
Port12	Tx_and_Rx
Port13	Tx_and_Rx
Port14	Tx_and_Rx
Port17	Tx_and_Rx
Port24	Tx_and_Rx
Mod1	Tx_and_Rx
Mod2	Tx_and_Rx
Trk3	Disable
Trk4	Disable
Trk10	Disable

5.4 Access Control List

Packets can be forwarded or dropped by ACL rules include IPv4 or non-Ipv4. TEG-S2620I can be used to block packets by maintaining a table of packet fragments indexed by source and destination IP address, protocol, and so on.

Group Id	<input type="text" value=""/> (1~220)		
Action	Permit <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)		
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094;Any means Vid=0 if uses binding)		
Packet Type / Binding	<input checked="" type="radio"/> IPv4	<input type="radio"/> Non-IPv4	<input type="radio"/> Binding
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	Ether Type	Any <input type="text" value=""/> Type# <input type="text" value=""/>
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>		MAC Address <input type="text" value="00:11:22:33:44:55"/>
IP Fragment	<input type="checkbox"/> Uncheck <input type="checkbox"/>		IP Address <input type="text" value="0.0.0.0"/>
L4 Protocol	<input checked="" type="radio"/> Any <input type="radio"/> TCP <input type="text" value="Any"/> Port#: <input type="text" value=""/> <input type="radio"/> UDP <input type="text" value="Any"/> Port#: <input type="text" value=""/>	QoS VoIP	Port Id <input type="text" value="1"/> (1~26)
		Priority# <input type="text" value="7"/>	
		PortID# Value (Hex,0~1F) <input type="text" value="0"/> Mask (Hex,0~1F) <input type="text" value="0"/>	
		Protocol# Value (Hex,0~FF) <input type="text" value="0"/> Mask (Hex,0~FF) <input type="text" value="0"/>	
		Source Port# Value (Hex,0~FFFF) <input type="text" value="0"/> Mask (Hex,0~FFFF) <input type="text" value="0"/>	
		Destination Port# Value (Hex,0~FFFF) <input type="text" value="0"/> Mask (Hex,0~FFFF) <input type="text" value="0"/>	

There are 2 main ACL rule types to setup: **Packet Type** (IPv4 and Non-IPv4) and **Binding** (SIP-SMAC-Port).

Port Id	<input type="text" value="0"/> (1~26,0:don't care)
Current List	<input type="text"/>

Enable/Disable ACL rule: Select an ACL entry which you want to enable/disable in the Current List. Then click / to execute.

Reset ACL count: Select an ACL entry which you want to reset its counts (**octetcnt** and **packetcnt** fields) in the Current List. Then click to do the action.

5.4.1 IPv4

In "Packet Type / Binding" box should select "IPv4".

Group Id	<input type="text" value=""/> (1~220)		
Action	Permit <input type="checkbox"/> <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)		
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094;Any means Vid=0 if uses binding)		
Packet Type / Binding	<input checked="" type="radio"/> IPv4 <input type="radio"/> Non-IPv4 <input type="radio"/> Binding		
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>	Ether Type	Any <input type="text" value=""/> Type# <input type="text" value=""/> MAC Address <input type="text" value="00:11:22:33:44:55"/>
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> Mask <input type="text" value="255.255.255.255"/>		IP Address <input type="text" value="0.0.0.0"/>
IP Fragment	<input type="checkbox"/> Uncheck <input type="checkbox"/>		Port Id <input type="text" value="1"/> (1~26)
L4 Protocol	<input checked="" type="radio"/> Any <input type="checkbox"/> TCP Any <input type="checkbox"/> UDP Any Protocol#: <input type="text"/> Port#: <input type="text"/> Port#: <input type="text"/>	QoS VoIP	Priority# <input type="text" value="7"/> PortID# <input type="text" value="0"/> Value (Hex,0~1F) <input type="text" value="0"/> Mask (Hex,0~1F) <input type="text" value="0"/> Protocol# <input type="text" value="0"/> Value (Hex,0~FF) <input type="text" value="0"/> Mask (Hex,0~FF) <input type="text" value="0"/> Source Port# <input type="text" value="0"/> Value (Hex,0~FFFF) <input type="text" value="0"/> Mask (Hex,0~FFFF) <input type="text" value="0"/> Destination Port# <input type="text" value="0"/> Value (Hex,0~FFFF) <input type="text" value="0"/> Mask (Hex,0~FFFF) <input type="text" value="0"/>
Port Id	<input type="text" value="0"/> (1~26,0:don't care)		
Current List	<input type="text" value="ENABLE_(gid#1)_permit_(vid#any)_(sip#any)_(dip#any)_(l4#any)_(frg#uncheck)_(portId#any)_(octetcnt#22979)_(packetcnt#33)"/>		

The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. a. Permit : Permit packet cross switch. b. Deny: Drop packet.	Permit
VLAN	Any / VID. a. Any: Any Vlan id. b. VID: 1~4094. A certain vlan id.	Any
Packet Type	IPv4 / Non-IPv4 / Binding a. IPv4: Set Ipv4 packet field. b. Non-IPv4: Set non-Ipv4 packet field. c. Binding: Set binding entry.	IPv4
Src IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address.	Any

	Mask: *.*.*.*.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255 Notice: This is not subnet mask.	
Dst IP Address	(Set this field if Packet Type is IPv4, else ignore.) Any / IP and Mask a. Any: Any IP address. b. IP :A certain IP address. Mask: *.*.*.*.*.*.*.*.*.* * is represent a digit from 0~9, *** is range from 0 to 255	Any
IP Fragment	(Set this field if Packet Type is IPv4, else ignore.) Uncheck / Check a. Uncheck: Not check IP fragment field. b. Check: Check IP fragment field.	Uncheck
L4 Protocol	(Set this field if Packet Type is IPv4, else ignore.) Any / ICMP(1) / IGMP(2) / TCP(6) / UDP(17)	Any
Protocol	(Set this field if Packet Type is IPv4, else ignore.) 0~255. If protocol not find in L4 Protocol field, you can direct assign number.	
TCP	(Set this field if Packet Type is IPv4, else ignore.) Any / FTP(21) / HTTP(80)	Any
Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If TCP port not find in TCP field, you can direct assign number.	
UDP	(Set this field if Packet Type is IPv4, else ignore.) Any / DHCP(67) / TFTP(69) / NetBios(137)	Any
Port	(Set this field if Packet Type is IPv4, else ignore.) 0~65535 If UDP port not find in UDP field, you can direct assign number.	
Port Id	Source port id, from 1~26, 0 means don't care.	0
Current List	You create ACL and Binding groups.	
Count	The octetcnt is octet number of the packets hitting the ACL rule. The packetcnt is the packet number Hiting the ACL rule.	0

5.4.2 Non-IPv4

In “Packet Type / Binding” box should select “Non-IPv4”.

Action	<input type="button" value="Permit"/> <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)		
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094;Any means Vid=0 if uses binding)		
Packet Type / Binding	<input checked="" type="radio"/> IPv4 <input type="radio"/> Non-IPv4 <input type="radio"/> Binding		
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP <input type="text" value="0.0.0.0"/> <input type="text" value="Mask 255.255.255.255"/>	Ether Type	<input type="text" value="Any"/> <input type="text" value="Type#"/> <input type="text" value="MAC Address 00:11:22:33:44:55"/>

The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. c. Permit : Permit packet cross switch. d. Deny: Drop packet.	Permit
Vlan	Any / VID. c. Any: Any Vlan id. d. VID: 1~4094. A certain vlan id.	Any
Packet Type	IPv4 / Non-IPv4 / Binding d. IPv4: Set Ipv4 packet field. e. Non-IPv4: Set non-Ipv4 packet field. f. Binding: Set binding function.	IPv4
Ether Type	(Set this field if Packet Type is Non-IPv4, else ignore.) Any / ARP(0x0806) / IPX(0x8137)	Any
Type	(Set this field if Packet Type is Non-IPv4, else ignore.) 0~0xFFFF If ether type not find in Ether Type field, you can direct assign number.	
Current List	You create ACL and Binding groups.	

5.4.3 Binding

Let device that has specific IP address and MAC address can use network. We can set specific IP address, MAC address, VLAN id and port id to bind, and device can cross switch if all conditions match.

Use binding function; we should enable it first in following page.

In "Packet Type / Binding" box should select "Binding".

Action	Permit <input type="button" value="v"/> <input type="checkbox"/> QoS VoIP (QoS mode "All High Before Low" is required in QoS webpage)
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID 1 (1~4094;Any means Vid=0 if uses binding)
Packet Type / Binding	<input checked="" type="radio"/> IPv4 <input type="radio"/> Non-IPv4 <input type="radio"/> Binding
Src IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP 0.0.0.0 Mask 255.255.255.255
Dst IP Address	<input checked="" type="radio"/> Any <input type="radio"/> IP 0.0.0.0 Mask 255.255.255.255
IP Fragment	Uncheck <input type="button" value="v"/>
Ether Type	Any <input type="button" value="v"/> Type# <input type="text"/>
MAC Address	00:11:22:33:44:55
IP Address	0.0.0.0
Port Id	1 (1~26)

The related parameters are shown in the following table:

Items	Option	Default value
Group ID	1 ~ 220 (max. 220 ACL group)	
Action	Permit / Deny. e. Permit : Permit packet cross switch. f. Deny: Drop packet.	Permit
Vlan	Any / VID. e. Any: Any Vlan id. f. VID: 1~4094. A certain vlan id.	Any
Packet Type	IPv4 / Non-IPv4 / Binding g. IPv4: Set Ipv4 packet field. h. Non-IPv4: Set non-Ipv4 packet field. i. Binding: Set binding function.	IPv4
Mac address	***.***.***.***.***.*** * is represent a digit from 0~9 and A~F, *** is range from 0 to FF.	00:11:22:33:44:55
IP address	***.***.***.*** * is represent a digit from 0~9, *** is range from 0 to 255.	0.0.0.0
Port Id	Source port id, from 1~26.	1
Current List	You create ACL and Binding groups.	

5.4.4 QoS VoIP

QoS VoIP option in Action field is to provide ingress VoIP packets can be forwarded out with higher priority through the ACL function.

NOTE: To make this function work, the QoS mode “All High Before Low” in QoS Configuration is required.

In “Action” box select the “QoS VoIP” checkbox to make QoS VoIP parameter area available to configure.

Action	Permit <input type="checkbox"/> QoS VoIP (QoS mode “All High Before Low” is required in QoS webpage)
VLAN	<input checked="" type="radio"/> Any <input type="radio"/> VID <input type="text" value="1"/> (1~4094;Any means Vid=0 if uses binding)

The QoS VoIP related parameters are shown in the following table:

QoS VoIP Parameter	Option	Default value
Priority	0 ~ 7	7
PortID	0~1F	0
PortID Mask	0~1F	0
Protocol	0~FF	0
Protocol Mask	0~FF	0
Source Port	0~FFFF	0
Source Port Mask	0~FFFF	0
Destination Port	0~FFFF	0
Destination Port Mask	0~FFFF	0

All parameters with HEX format provide settings in continuous range.

For example, if we want VoIP packets, with UDP protocol type (17) and source port number is in range of 10000~10015, to be forwarded out with highest priority while network congestion happens, an ACL rule can be created like the following setting:

Parameter	Value
GID	1
Action	QoS VoIP
VLAN	Any
Priority	7
PortID	0
PortID Mask	0
Protocol	11h
Protocol Mask	1Fh
Source Port	2710h
Source Port Mask	FF00h
Destination Port	0
Destination Port Mask	0

5.5 Security

5.5.1 Security Manager

In this page, user can change user name and password with the following parameters.

User Name: Type the new user name.

Assign/Change password: Type the new password.

Reconfirm password: Retype the new password.

Security Manager

User Name	<input type="text"/>
Assign/Change password	<input type="password"/>
Reconfirm password	<input type="password"/>

Click to activate the setting.

5.5.2 MAC Limit

MAC limit allows users to set a maximum number of MAC addresses to be stored in the MAC address table. The MAC addresses chosen to be stored in MAC address table is the result of first-come-first-save policy. Once a MAC address is stored in the MAC address table, it stays in until it is aged out. When an “opening” is available, the switch stored the first new MAC address it sees in that opening. All packets from MAC addresses not in the MAC address table should be blocked.

MAC Limit

Configure MAC Limit

MAC Limit	<input type="checkbox"/>
Port Number	Limit (1-64,0 to turn off MAC limit)
Port1 Port2 Port3 Port4 Port5	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

MAC Limit Port Status

Port Number	Limit
Port1	off
Port2	off
Port3	off
Port4	off
Port5	off
Port6	off
Port7	off
Port8	off
Port9	off

MAC Limit: enable/disable MAC limit function

Limit: select port number and input Limit value (0~64, 0 to turn off MAC limit)

Click **Apply** to activate the setting.

5.5.3 802.1x Configuration

802.1x makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

In the beginning, 802.1x configuration page is disabled because 802.1x is disabled in default. To enable 802.1x, go to **Administration** → **Switch setting** → **Misc Configs** page to enable the **802.1x protocol** field. After clicked **Apply**, the 802.1x configuration page will be shown up.

5.5.3.1 System Configuration

In this page, the parameters related to authentication (Radius) server are provided:

802.1x Configuration

System Configuration

PerPort Configuration

Misc Configuration

Configure 802.1x Parameters

Radius Server IP:	<input type="text" value="192.168.200.99"/>
Server Port:	<input type="text" value="1812"/>
Accounting Port:	<input type="text" value="1813"/>
Shared Key:	<input type="text"/>
NAS,Identifier:	<input type="text" value="NAS_L2_SWITCH"/>

Radius Server IP: the IP address of the authentication server.

Server Port: The UDP port number used by the authentication server to authenticate (default: 1812).

Accounting Port: The UDP port number used by the authentication server to retrieve accounting information (default: 1813).

Shared Key: A key shared between this switch and authentication server.

NAS, Identifier: A string used to identify this switch.

5.5.3.2 Perport Configuration

In this page, you can select the specific port and configure the authorization state. There are 4 kinds of authorization state to provide for each port.

Configure 802.1x Per Port State

Port Number	Port State
Port1 <input type="button" value="▲"/>	
Port2 <input type="button" value="☰"/>	
Port3	
Port4	
Port8 <input type="button" value="▼"/>	Au <input type="button" value="▼"/>

Fu: Force the specific port to be unauthorized.

Fa: Force the specific port to be authorized.

Au: The state of the specific port was determined by the outcome of the authentication.

No: The specific port didn't support 802.1x function.

5.5.3.3 Misc Configuration

In this page, you can change the default configuration for the 802.1x standard:

802.1x Configuration

System Configuration	PerPort Configuration	Misc Configuration
----------------------	-----------------------	--------------------

Configure 802.1x misc configuration

Quiet period:	<input type="text" value="60"/>
Tx period:	<input type="text" value="15"/>
Supplicant timeout:	<input type="text" value="30"/>
Server timeout:	<input type="text" value="30"/>
Max requests:	<input type="text" value="2"/>
Reauth period:	<input type="text" value="3600"/>

Quiet Period: Used to define periods of time during which it will not attempt to acquire a supplicant (default time: 60 seconds).

Tx Period: Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).

Supplicant Timeout: Used to determine timeout conditions in the exchanges between the supplicant and authentication server (default value: 30 seconds).

Server Timeout: Used to determine timeout conditions in the exchanges between the authenticator and authentication server (default value: 30 seconds).

ReAuthMax: Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (default value: 2 times).

Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (default value: 3600 seconds).

5.6 QoS

This switch provides quality of service (QoS) to prioritize the packet forwarding when traffic congestion happens. This switch supports port-based (4-level output queue) and 802.1p (8-level priority to 4-level queue mapping) QoS functions. Strict and weight round robin (WRR) QoS mode are supported.

5.6.1 QoS Configuration

This page is mainly to set the QoS mode (First Come First Service, All High before Low, and WRR) and 8-level priority to 4-level queue mapping.

QoS Configuration

Qos Configuration

PerPort Configuration

Priority Queue Service:

Qos Mode							
<input type="radio"/> First Come First Service							
<input type="radio"/> All High before Low							
<input checked="" type="radio"/> WRR	Highest 8	SecHigh 4	SecLow 2	Lowest 1			
802.1p priority [0-7]							
Lowest ▾	Lowest ▾	SecLow ▾	SecLow ▾	SecHigh ▾	SecHigh ▾	Highest ▾	Highest ▾

Apply

Default

Help

First Come First Service: The sequence of packets sent is depending on arrive orders. This mode can be regarded as QoS is disabled.

All High before Low: The high priority packets sent before low priority packets.

WRR: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of higher priority packets sent before one lower priority packet is sent. For example, 8 Highest : 4 second-high means that the switch sends 8 highest-priority packets before sending 4 second-high priority packets.

QoS Priority: 8-level (0~7) priority can be mapped to 4-level (Highest, Second-High, Second-Low, Lowest) queue.

5.6.2 Per-Port Configuration

Per-port priority can be configured and shown in this page.

Qos Configuration	PerPort Configuration								
Configure Port Priority									
<table border="1"><thead><tr><th>Port Number</th></tr></thead><tbody><tr><td>Port1</td></tr><tr><td>Port2</td></tr><tr><td>Port3</td></tr><tr><td>Port4</td></tr><tr><td>Port8</td></tr></tbody></table>	Port Number	Port1	Port2	Port3	Port4	Port8	<table border="1"><thead><tr><th>Port Priority</th></tr></thead><tbody><tr><td>Disable</td></tr></tbody></table>	Port Priority	Disable
Port Number									
Port1									
Port2									
Port3									
Port4									
Port8									
Port Priority									
Disable									
<input type="button" value="Apply"/> <input type="button" value="Help"/>									

Port Number: the ports in the switch.

Port Priority: port priority can be disable or 0-7.

Per-Port priority setting can be displayed like the following figure.

Port Priority	
PortNum	Priority
Port1	Disable
Port2	Disable
Port3	Disable
Port4	Disable
Port8	Disable
Port9	Disable
Port10	Disable
Port11	Disable
Port12	Disable
Port13	Disable
Port14	Disable
Port17	Disable
Port24	7
Mod1	Disable
Mod2	Disable
Trk3	Disable
Trk4	Disable

5.7 Monitoring

The following items are provided in Monitoring section:

- Port status
- Port statistics

5.7.1 Port Status

This page provides current status of every port that depends on user's setting and the negotiation result.

Port Status

The following information provides a view of the current status of the unit.

Port	State	Link	Negotiation	Speed	Duplex	Flow Control	Rate Control (Unit:128Kbps)		Security	BSF	Jumbo Frame
							Ingress	Egress			
Port1	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port2	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port3	On	Up	Auto	100	Full	Off	Off	Off	Off	On	On
Port4	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port8	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port9	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port10	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port11	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port12	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port13	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port14	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port17	On	Down	---	---	---	Off	Off	Off	Off	On	On
Port24	On	Down	---	---	---	Off	Off	Off	Off	On	On
Mod1	On	Down	---	---	---	On	Off	Off	Off	On	On
Mod2	On	Down	---	---	---	On	Off	Off	Off	On	On
Trk3	On	Down	---	---	---	Off	Off	Off	Off	On	On
Trk4	On	Down	---	---	---	Off	Off	Off	Off	On	On
Trk10	On	Down	---	---	---	Off	Off	Off	Off	On	On

State: Display port statuses: **disable or enable**. "Unlink" will be treated as "off".

Link Status: Down means "No Link"; Up means "Link up".

Auto Negotiation: Display the auto negotiation mode: auto/force/nway-force.

Speed status: Display 1000Mbps or 100Mbps or 10Mbps speed, port 1- 24 are 10/100Mbps, Port 25-26 are 10/100/1000Mbps.

Duplex status: Display full-duplex or half-duplex mode.

Flow Control: Display the flow control state

Full: Display the flow control is enabled or disabled in full mode.

Half: Display the backpressure is enabled or disabled in half mode.

Rate Control: Display the rate control setting.

Ingress: Display the port effective ingress rate of user setting.

Egress: Display the port effective egress rate of user setting.

Port Security: Display the port security is enabled or disabled.

BSF: Display the port broadcast storm filter control is enable or disable.

Jumbo Frame: Display the jumbo frame is supported or not for the port.

NOTE: You can click the **Browser's Refresh button** or press <F5> to update to the latest status.

5.7.2 Port Statistics

The following information provides a view of the current status of the whole unit.
Press **Reset** button to clean all count.

Port Statistics

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
Port1	On	Down	0	0	0	0	0	0	0
Port2	On	Down	0	0	0	0	0	0	0
Port3	On	Up	91	0	82	0	0	0	0
Port4	On	Down	0	0	0	0	0	0	0
Port8	On	Down	0	0	0	0	0	0	0
Port9	On	Down	0	0	0	0	0	0	0
Port10	On	Down	0	0	0	0	0	0	0
Port11	On	Down	0	0	0	0	0	0	0
Port12	On	Down	0	0	0	0	0	0	0
Port13	On	Down	0	0	0	0	0	0	0
Port14	On	Down	0	0	0	0	0	0	0
Port17	On	Down	0	0	0	0	0	0	0
Port24	On	Down	0	0	0	0	0	0	0
Mod1	On	Down	0	0	0	0	0	0	0
Mod2	On	Down	0	0	0	0	0	0	0
Trk3	On	Down	0	0	0	0	0	0	0
Trk4	On	Down	0	0	0	0	0	0	0
Trk10	On	Down	0	0	0	0	0	0	0

5.8 Reset System

The page to reset the switch to default configuration is shown as below.

Reset System

Reset Switch to Default Configuration

5.9 Reboot

The page to reboot (warm restart) the switch is shown as below.

Reboot Switch System



TRENDnet[®]

TRENDnet Technical Support

US • Canada

Toll Free Telephone: 1(866) 845-3673

24/7 Tech Support



Europe (Germany • France • Italy • Spain • Switzerland • UK)

Toll Free Telephone: +00800 60 76 76 67

English/Espanol - 24/7

Francais/Deutsch - 11am-8pm, Monday - Friday MET

Worldwide

Telephone: +(31) (0) 20 504 05 35

English/Espanol - 24/7

Francais/Deutsch - 11am-8pm, Monday - Friday MET

Product Warranty Registration

Please take a moment to register your product online.

Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet[®]

20675 Manhattan Place

Torrance, CA 90501

USA