Layer 2 Smart Plus Switch

GigaX1116i+
GigaX1124i+

User Manual

E2491

First Edition V1

April 2006

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS provides this manual “as is” without warranty of any kind, either express or implied, including but not limited to the implied warranties or conditions of merchantability or fitness for a particular purpose. In no event shall ASUS, its directors, officers, employees, or agents be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of use or data, interruption of business and the like), even if ASUS has been advised of the possibility of such damages arising from any defect or error in this manual or product.

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice, and should not be construed as a commitment by ASUS. ASUS assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including the products and software described in it.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners’ benefit, without intent to infringe.

Federal Communications Commission Statement

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

- This device may not cause harmful interference, and
- This device must accept any interference received including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with manufacturer's instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING! The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Canadian Department of Communications Statement

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

This class B digital apparatus complies with Canadian ICES-003.

ASUS contact information

ASUSTeK COMPUTER INC. (Asia-Pacific)

Address:	15 Li-Te Road, Peitou, Taipei 112, Taiwan
General Tel:	+886-2-2894-3447
General Fax:	+886-2-2894-7798
Web Site:	www.asus.com.tw

Technical Support

MB/Others (Tel):	+886-2-2890-7121 (English)
Notebook (Tel):	+886-2-2890-7122 (English)
Desktop/Server (Tel):	+886-2-2890-7123 (English)
Support Fax:	+886-2-2890-7698

ASUS COMPUTER INTERNATIONAL (America)

Address:	44370 Nobel Drive, Fremont, CA 94538, USA
General Fax:	+1-502-933-8713
General Email:	tmd1@asus.com
Web Site:	usa.asus.com

Technical Support

Support Fax:	+1-502-933-8713
General Support:	+1-502-995-0883
Notebook Support:	+1-510-739-3777 x5110
Support Email:	tsd@asus.com

ASUS COMPUTER GmbH (Germany and Austria)

Address:	Harkort Str. 25, D-40880 Ratingen, BRD, Germany
General Fax:	+49-2102-9599-31
General Email:	sales@asuscom.de (for marketing requests only)

Technical Support

Support Hotlines:	(Components) +49-2102-95990
	(Notebook PC) +49-2102-959910
Support Fax:	+49-2102-959911
Support Email:	www.asuscom.de/de/support (for online support)
Web Site:	www.asuscom.de

Table of contents

1 Introduction

Congratulations on becoming the owner of the ASUS GigaX1116i+/ GigaX1124i+ L2 smart plus switch! You may now manage your LAN (local area network) through a friendly and powerful user interface.

This user guide tells you how to set up the GigaX1116i+/ GigaX1124i+ smart switch, and how to customize its configuration to get the most out of this product.

1.1 L2 managed features

- Complies with IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T) standards
- Auto negotiation of speed (10/100/1000Mbps), and duplex mode. Note that 1000Mbps supports only full duplex mode.
- 8K MAC addresses with automatic address learning and aging.
- IEEE 802.3x flow control support for 10/100/1000Mbps full duplex.
- Back pressure flow control support for 10/100Mbps half duplex.
- Auto MDI/MDIX
- VLAN
- Port based VLAN
- 802.1Q tag based VLAN
- Quality of Service
- 802.1p tagging
- Port based priority
- Four priority queues per port
- 802.3ad Link Aggregation
- Manual
- Port mirroring
- Storming control
- Rapid Spanning Tree
- 802.1X
- SNMP V1,V2
- Simple ACL
- Support up to 9K bytes Jumbo frames
- Configuration backup & restore
- Cable Diagnostics

1.2 Conventions used in this document

1.2.1 Notations

- Acronyms are defined the first time they appear in text and in the glossary.
- For brevity, the GigaX1116i+/ GigaX1124i+ switch is referred to as “the switch.”
- The terms LAN and network are used interchangeably to refer to a group of Ethernet-connected computers at one site.

1.2.2 Typography

- Italics are used to present the parameters for the command line interpreter.
- Boldface type text is used for items you select from menus and drop-down lists, and text strings you type when prompted by the program.

1.2.3 Symbols

This document uses the following icons to call your attention to specific instructions or explanations.

Note *Provides clarification or additional information on the current topic.*

Definitior *Explains terms or acronyms that may be unfamiliar to many readers. These terms are also included in the Glossary.*

Warning *Provides messages of high importance, including messages relating to personal safety or system integrity.*

2 Getting to know GigaX1116i+/ GigaX1124i+

2.1 Package contents

The GigaX1116i+/ GigaX1124i+ switch package comes with the following items:

- GigaX1116i+ (16-port), or GigaX1124i+ (24-port) L2 smart plus switch
- AC Power cord
- Null modem cable for console interface (DB9)
- Rack installation kit (two brackets with six #6-32 screws)
- CD manual
- Quick installation guide

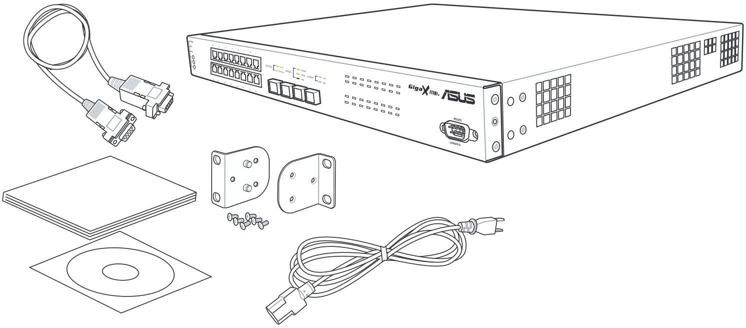
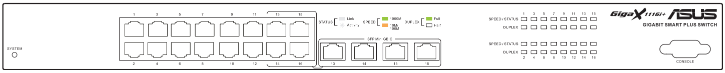


Figure 1. GigaX1116i+/ GigaX1124i+ smart switch package contents

2.2 Front Panel

The front panel includes LED indicators that show the system, RPS, fan, and port status.

GigaX 1116i+:



GigaX 1124i+:

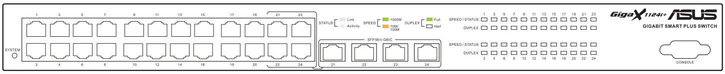


Table 1. Front panel labels and LEDs

Label	Color	Status	Description
SYSTEM	Green	ON	The switch is power-up and operating normally
	Amber	ON	Abnormal temperature or voltage
		OFF	No power
10/100/1000 port speed and status	Green	ON	Link (RJ-45 or SFP) is present; port is enabled ,port speed is 1000Mbps
		Flashing	Data is being transmitted/received
	Amber	ON	Link (RJ-45 or SFP) is present; port is enabled ,port speed is 100/10Mbps
		OFF	No Ethernet link
10/100/1000 port duplex	Green	ON	Full duplex
		Flashing	collision happens
	OFF		Half duplex

2.3 Rear Panel

The switch rear panel contains the fans and a power connector.

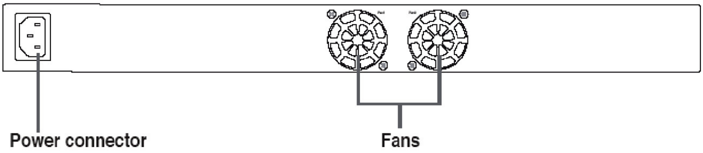


Figure 2. Rear panel

Table 2. Rear panel labels

No.	Label	Description
1	Power Connector	Connects to the supplied power cord
2	FAN	System fan

2.4 Technical specifications

Table 3. Technical specifications

Physical Dimensions	43.5mm(H) x 444mm(W) x 265mm(D)		
Power	Input	Consumption	
	100-240V AC/2.5A 50-60Hz	<90 watts	
Environmental Ranges		Operating	Storage
	Temperature	-10 to 50°C (14 to 122°F)	-40 to 70°C(-40 to 158°F)
	Humidity	15 to 90%	0 to 95%
	Altitude	up to 10,000ft (3,000m)	40,000ft (12,000m)
System Fan	Dimensions	Voltage and Current	Speed
	40 x 40 x 20 mm	12V DC/0.13A	8200RPM

3 Quick start guide

This section provides the basic instructions to set up the GigaX1116i+/ GigaX1124i+ environment. Refer also to the GigaX1116i+/ GigaX1124i+ Installation Guide.

Part 1 shows you how to install the switch on a flat surface or on a rack.

Part 2 provides instructions to set up the hardware.

Part 3 shows you how to configure basic settings on the switch.

Obtain the following information from your network administrator before proceeding:

IP address for the switch

Default gateway for the network

Network mask for this network

3.1 Part 1 — Installing the hardware

Connect the device to the power outlet, and your computer or network.

Figure 5 illustrates the hardware connections.

3.1.1 Installing the switch on a flat surface

The switch should be installed on a level surface that can support the weight of the switches and their accessories. Attach four rubber pads on the marked location on the bottom of the switch.

3.1.2 Mounting the switch on a rack

1. Attach brackets to each side of the switch and make the posts insert to the switch.
2. Insert and tighten two screws to securely attach the bracket to the rack on each side.

3.2 Part 2 — Setting up the switch

Connect the device to the power outlet, and your computer or network. See Figure 5.

3.2.1 Connect the console port

For console management, use an RS232 (DB9) to connect the switch. If you want to use WEB interface, connect your PC to the switch using the Ethernet cable.

3.2.2 Connect to the computers or a LAN

You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.

Use a twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port. Otherwise, the link speed cannot reach 1Gbps.

3.2.3 Attach the power adapter

1. Connect the AC power cord to the POWER receptacle on the back of the switch and plug the other end of the power cord into a wall outlet or a power strip.
2. Check the front LED indicators with the description in Table 4. If the LEDs light up as described, the switch hardware is working properly.

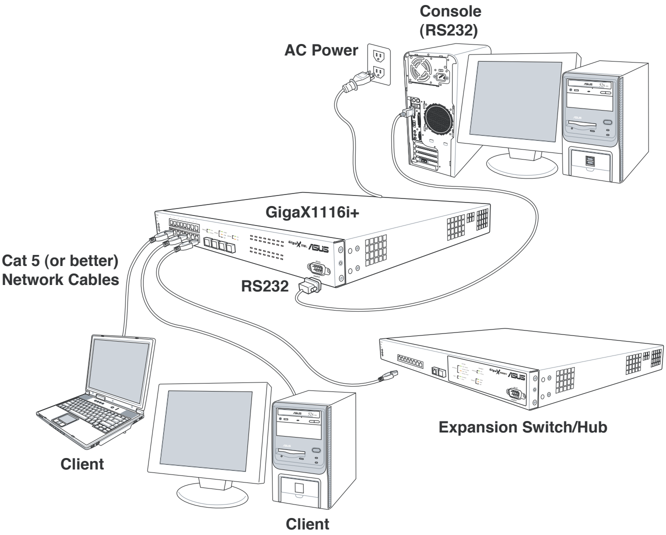


Figure 3. Overview of Hardware Connections

Table 4. LED Indicators

No.	LED	Description
1	SYSTEM	Solid green indicates that the device is turned on. If this light is off, make sure the power cord is attached to the Switch and plugged into a power source.
2	Switch ports [1] to [16] (GigaX1116i+) [1] to [24] (GigaX1124i+)	Solid green indicates that the device can communicate with the LAN, or flashing when the device is sending or receiving data from your LAN computer.

3.3 Part 3 — Basic switch setting for management

After completing the hardware connections, configure the basic settings for your switch. You can manage the switch using the following methods:

- Web interface: the switch has a set of pages to allow to you manage it using Java®-enabled IE5.0 or higher version.
- Command Line Interface: use console port to manage the switch.

3.3.1 Setting up through the console port

1. Use the supplied crossover RS-232 cable to connect to the console port on the front of the switch. This port is a male DB-9 connector, implemented as a data terminal equipment (DTE) connection. Tighten the retaining screws on the cable to secure it on the connector. Connect the other end of the cable to a PC running terminal emulation software. e.g Hyper Terminal.
2. Make sure the settings of your terminal emulation software as follows:

a) Choose the appropriate serial port number

b) Set the data baud rate to 115200

c) Set the data format to no parity, 8 data bits and 1 stop bit

d) No flow control

3.3.2 Setting up through the Web interface

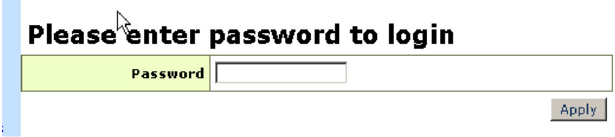
To successfully connect your PC to the switch, your PC must a valid IP in your network. Contact your network administrator to obtain a valid IP for the switch. If you wish to set up the IP address of the switch, follow section 4.3.1 to change the IP address. Since the switch does not support DHCP client function, a valid static IP for the switch is necessary to use Web interface.

1. At any PC connected to the network that the switch can access , open your Web browser (Internet Explorer), and type the following URL in the address/ location box, and press <Enter>:

   http://192.168.1.1

   This is the factory default IP address of the switch.

   A login screen appears, as shown in Figure 4.



Please enter password to login

Password	

Figure 4. Login Screen

Enter your password or leave it blank, and then click **Apply** to enter the Configuration Manager. Use the following defaults the first time you log into this interface:

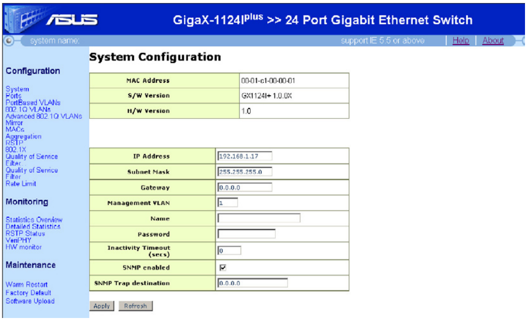
Default Password: (no password)

Default password is no password. No password means "accept all" and "disable web login password".

You can change the password at any time. If you forgot the password, the super password is "asus2357". Super password can only be used in console mode. After login to console, refer to section 5.2.1 to restore factory default or to section 5.2.2 to set new password

2. To setup a new IP address, click "System", (see Figure 5). Fill in the IP address, network mask and default gateway, then click **Apply**.

3. If your new address is different from the default, the browser cannot update the switch status window or retrieve any page. This is normal. You have to retype the new IP address in the address/location box, and press <Enter>. The WEB link returns.



GigaX-1124I^{plus} >> 24 Port Gigabit Ethernet Switch

system name:

System Configuration

MAC Address	00-01-c1-00-00-01
S/W Version	GX1124I+ 1.0.0X
H/W Version	1.0

IP Address	192.168.1.17
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Management VLAN	1
Name	
Password	
Inactivity Timeout (secs)	0
SNMP enabled	☑
SNMP Trap destination	0.0.0.0

Figure 5. IP Setup

4 Management with the Web Interface

The switch provides Web pages that allow switch management through the Internet. The program is designed to work best with Microsoft Internet Explorer® 5.5, or later versions. NOTE: Netscape is not supported.

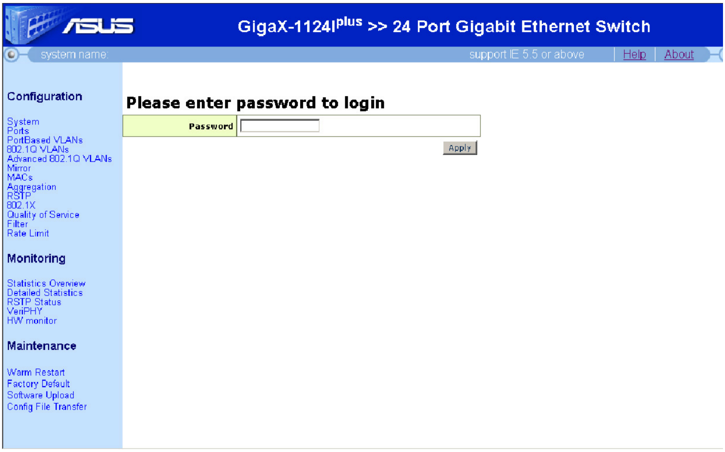
The following sections show only one screen image (GigaX1124i+ model) since GigaX1116i+ and GigaX1124i+ have the same configuration mechanism.

4.1 Log into Web user interface

1. From a PC, open your web browser, type the following in the web address (or location) box, and press <Enter>:

   http://192.168.1.1

   This is the factory default IP address for the switch. A login screen displays, as shown in Figure 6.



GigaX-1124I^{plus} >> 24 Port Gigabit Ethernet Switch

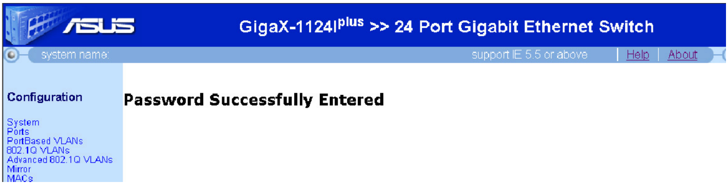
Please enter password to login

Figure 6. Configuration manager login screen

2. Enter your password, then click **Apply**.

   Default Password: <no password>

The home page appears each time you log into the program. See Figure 7



Password Successfully Entered

Figure 7. Home page

4.2 Functional layout

Typical web page consists of three separate frames, top frame, menu frame, main frame. The top frame as shown in Figure 8 has a switch logo, help and about page. Click on the Help. The help window is shown as Figure 9. The error codes in the web page are listed. Click the item in the left menu, the individual help page for this item will be shown. The about page will lead you to the ASUS official Web site http://www.asus.com

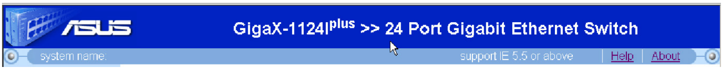
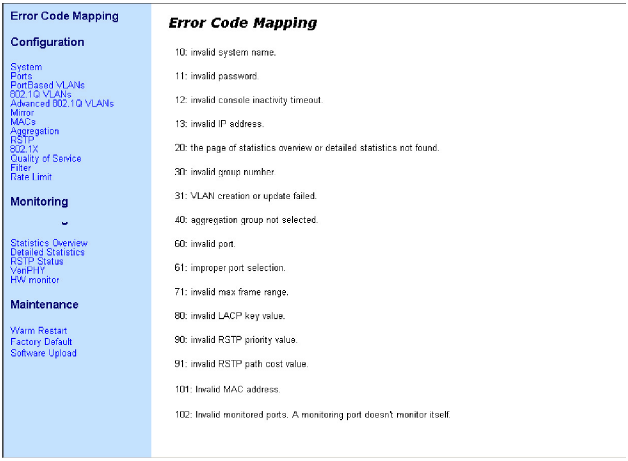


Figure 8. Top frame



Error Code Mapping

10: invalid system name.

11: invalid password.

12: invalid console inactivity timeout.

13: invalid IP address.

20: the page of statistics overview or detailed statistics not found.

30: invalid group number.

31: VLAN creation or update failed.

40: aggregation group not selected.

60: invalid port.

61: improper port selection.

71: invalid max frame range.

80: invalid LACP key value.

90: invalid RSTP priority value.

91: invalid RSTP path cost value.

101: Invalid MAC address.

102: Invalid monitored ports. A monitoring port doesn't monitor itself.

Figure 9. Help Page

The left frame, a menu frame as shown in Figure 10, contains all the features available for switch configuration.

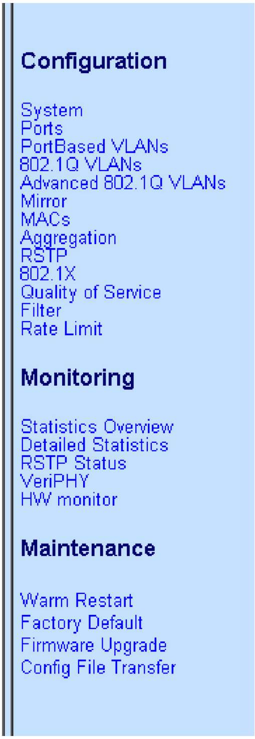


Figure 10. Expanded Menu List

The right frame displays configuration pages or graphics for the statistics. See section 4.3 for details.

4.2.1 Commonly used buttons and icons

The following table describes the function for each button and icon used in the application.

Table 5. Commonly used buttons and icons

Button/Icon	Function
Apply	Stores any changes you have made on the current page.
Refresh	Re-displays the current page with updated statistics or settings.
Add	Adds the existing configuration to the system, e.g. portBased VLAN, 802.1Q VLAN, MAC address ,etc.
Modify	Modifies an existing entry
Delete	Deletes the selected item, e.g. a VLAN, MAC address, etc.
Uploa	Re-displays the current page with updated statistics or settings.

4.3 Configuration Pages

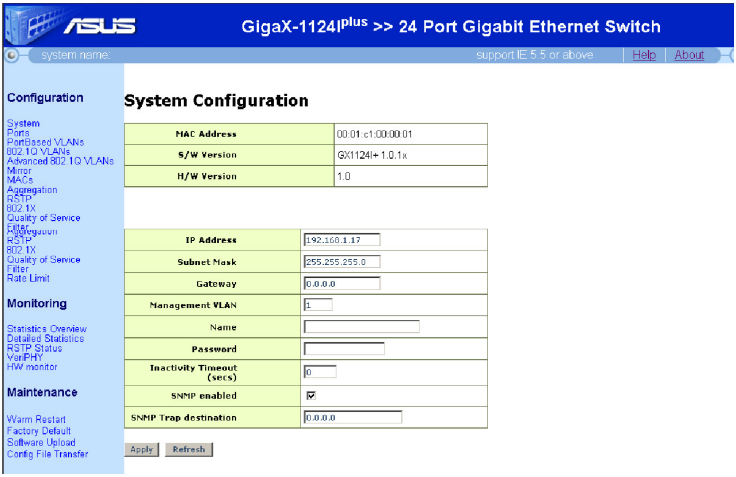
Configuration pages include System, Ports, PortBased VLANs, 802.1Q VLANs, Advanced 802.1Q VLANs, Mirror, MACs, Aggregation, RSTP, 802.1X, Quality of Service, Filter, Rate limit.

4.3.1 System

The System page contains the following information:

- IP Address: Setup or show IP configuration.
- Subnet Mask: Setup or show Subnet Mask.
- Gateway: Setup or show Gateway.
- Management VLAN: Setup or show Management VLAN(1-4095).
- Name: Setup or show system name.
- Password: Setup password. The empty string ("") disables the password check. Only perform a factory default can set password blank.
- Inactivity Timeout (secs): Set or show the console inactivity timeout in seconds. The range is 60-10000. The value zero disables timeout.
- SNMP enable: Check box for enable. Default Read Community name is "public" and Write (Set) community name must be the same as the system password.
- SNMP trap destination: Set or show the IP address SNMP trap sent to.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value. as shown in Figure 11.



System Configuration

MAC Address	00:01:c1:00:00:01
S/W Version	GX1124I+ 1.0.1x
H/W Version	1.0

IP Address	192.168.1.17
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Management VLAN	1
Name	
Password	
Inactivity Timeout (secs)	0
SNMP enabled	☑
SNMP Trap destination	0.0.0.0

Figure 11. System Configuration

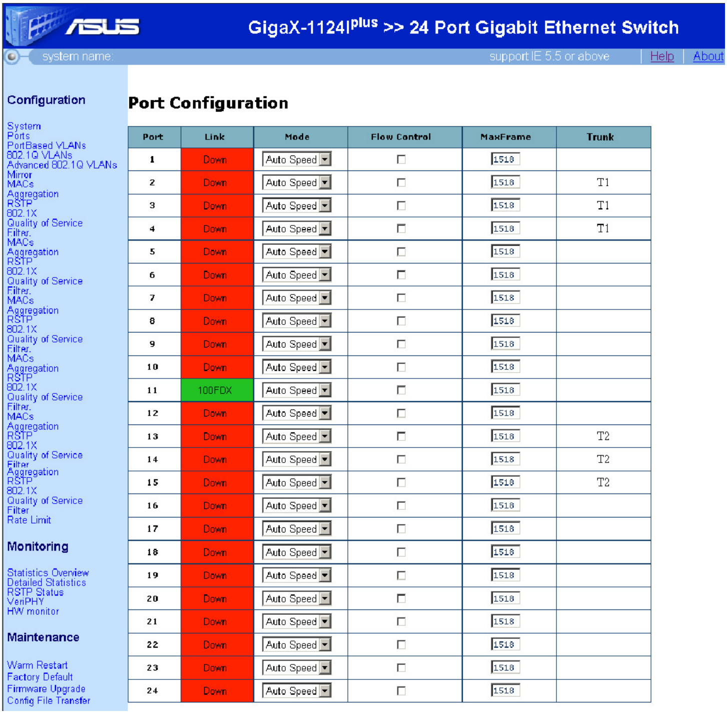
4.3.2 Ports

On this page, users know the ethernet port status in real time. On the other hand, users can configure the port in the following fields:

On this page, users know the ethernet port status in real time. On the other hand, users can configure the port in the following fields:

- Link: Show link up status or link down.
- Mode: Set or show the speed and duplex mode.
- Flow Control: Enable/disable 802.3x flow control mechanism.
- Max Frame: Set or show the maximum frame size in bytes (including FCS) for frames received on the port. Tagged frames are allowed to be 4 bytes longer than the maximum frame size. The range of valid maximum frame size is between 1518 and 9600.
- Trunk: Show trunk information. Be sure the port attribute of the Trunk member should be the same in the trunk group.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 12.



Port Configuration

Port	Link	Mode	Flow Control	MaxFrame	Trunk
1	Down	Auto Speed ▾	☐	1518	
2	Down	Auto Speed ▾	☐	1518	T1
3	Down	Auto Speed ▾	☐	1518	T1
4	Down	Auto Speed ▾	☐	1518	T1
5	Down	Auto Speed ▾	☐	1518	
6	Down	Auto Speed ▾	☐	1518	
7	Down	Auto Speed ▾	☐	1518	
8	Down	Auto Speed ▾	☐	1518	
9	Down	Auto Speed ▾	☐	1518	
10	Down	Auto Speed ▾	☐	1518	
11	100FDX	Auto Speed ▾	☐	1518	
12	Down	Auto Speed ▾	☐	1518	
13	Down	Auto Speed ▾	☐	1518	T2
14	Down	Auto Speed ▾	☐	1518	T2
15	Down	Auto Speed ▾	☐	1518	T2
16	Down	Auto Speed ▾	☐	1518	
17	Down	Auto Speed ▾	☐	1518	
18	Down	Auto Speed ▾	☐	1518	
19	Down	Auto Speed ▾	☐	1518	
20	Down	Auto Speed ▾	☐	1518	
21	Down	Auto Speed ▾	☐	1518	
22	Down	Auto Speed ▾	☐	1518	
23	Down	Auto Speed ▾	☐	1518	
24	Down	Auto Speed ▾	☐	1518	

Figure 12. Port Configuration

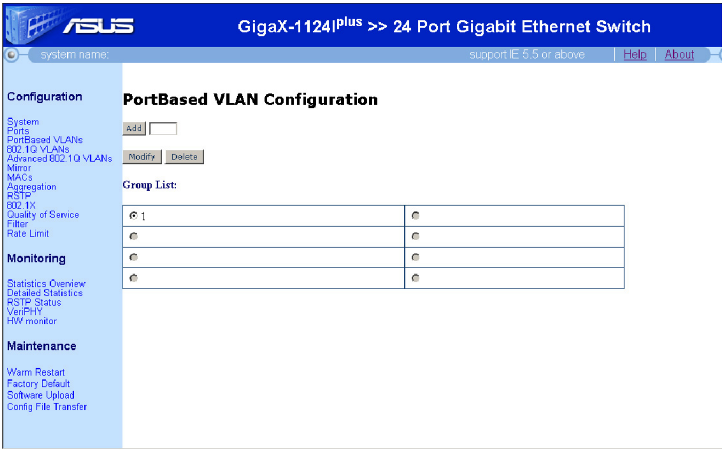
4.3.3 Port-Based VLAN Configuration

Port-Based VLANs provide another way than VLAN for making port grouping. With port-based VLAN, it is possible to share a port between more groups. Users can configure the group in the following ways:

- Add a new group: Fill in the new group ID and then click on the “Add” button. On the next page, select the ports or trunks that need to be assigned to this group. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.
- Modify a group: Select the group that needs to be modified and then click on the “Modify” button. On the next page, select the ports or trunks that need to be assigned to this group. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.

- Delete a group: Select the group that needs to be deleted and then click on the "Delete" button.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 14.

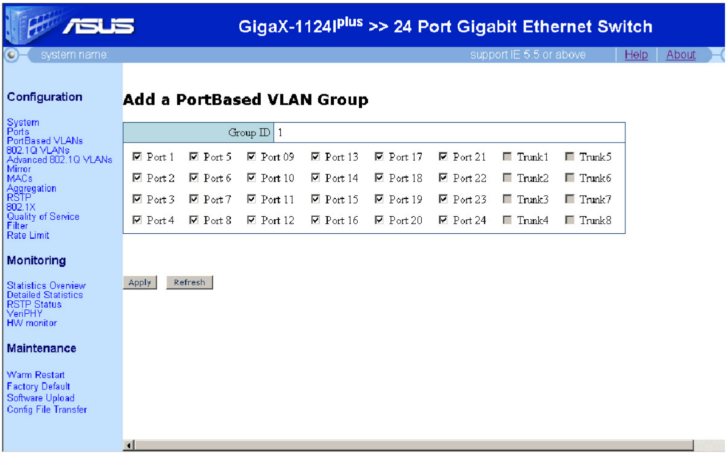


PortBased VLAN Configuration

Group List:

● 1	○
○	○
○	○
○	○

Figure 13. Port-Based VLAN



Add a PortBased VLAN Group

Group ID 1

☑ Port 1	☑ Port 5	☑ Port 09	☑ Port 13	☑ Port 17	☑ Port 21	□ Trunk1	□ Trunk5
☑ Port 2	☑ Port 6	☑ Port 10	☑ Port 14	☑ Port 18	☑ Port 22	□ Trunk2	□ Trunk6
☑ Port 3	☑ Port 7	☑ Port 11	☑ Port 15	☑ Port 19	☑ Port 23	□ Trunk3	□ Trunk7
☑ Port 4	☑ Port 8	☑ Port 12	☑ Port 16	☑ Port 20	☑ Port 24	□ Trunk4	□ Trunk8

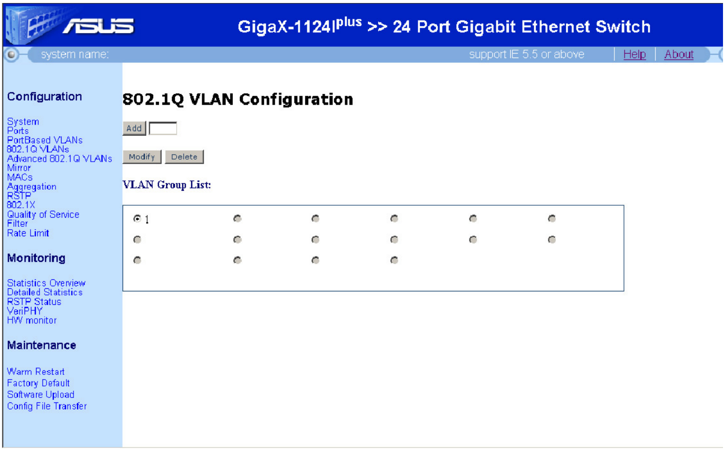
Figure 14. Add a Port-Based VLAN group

4.3.4 802.1Q VLANs Configuration

There are up to 16 VLAN groups to be configured. Users can configure the group in the following ways:

- Add a new VLAN: Fill in the new VLAN ID and then click on the “Add” button. On the next page, select the ports or trunks that need to be assigned to this VLAN. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.
- Modify a VLAN: Select the VLAN that needs to be modified and then click on the “Modify” button. On the next page, select the ports or trunks that need to be assigned to this VLAN. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.
- Delete a VLAN: Select the VLAN that needs to be deleted and then click on the “Delete” button.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 15. Next page is shown in Figure 16.

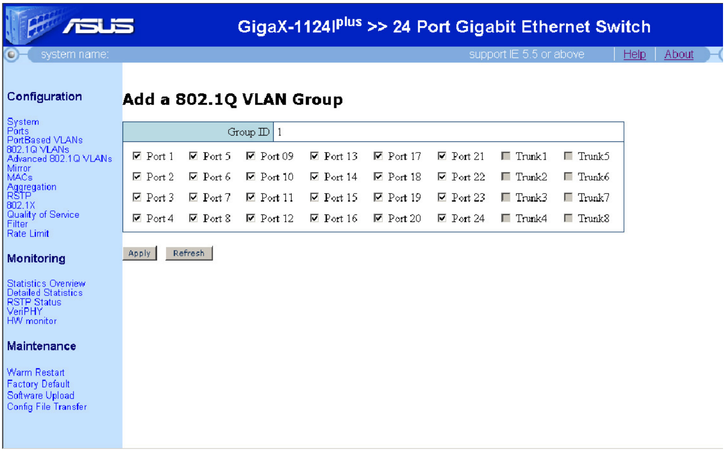


802.1Q VLAN Configuration

VLAN Group List:

● 1

Figure 15. 802.1Q VLAN



Add a 802.1Q VLAN Group

Group ID: 1

☑ Port 1	☑ Port 5	☑ Port 09	☑ Port 13	☑ Port 17	☑ Port 21	□ Trunk1	□ Trunk5
☑ Port 2	☑ Port 6	☑ Port 10	☑ Port 14	☑ Port 18	☑ Port 22	□ Trunk2	□ Trunk6
☑ Port 3	☑ Port 7	☑ Port 11	☑ Port 15	☑ Port 19	☑ Port 23	□ Trunk3	□ Trunk7
☑ Port 4	☑ Port 8	☑ Port 12	☑ Port 16	☑ Port 20	☑ Port 24	□ Trunk4	□ Trunk8

Figure 16. Add a 802.1Q VLAN

4.3.5 Advanced 802.1Q VLAN

Users can configure the advanced attributes of each port related to 802.1Q VLAN in the following fields:

- Aware--

  Ingress: Keep tag value for tagged packets received. For untagged packets received, insert tag with PVID on the incoming packets.

  Egress: Compare egress port PVID with the tag value of outgoing packets. If the same, remove the tag. If not the same, keep the tag.

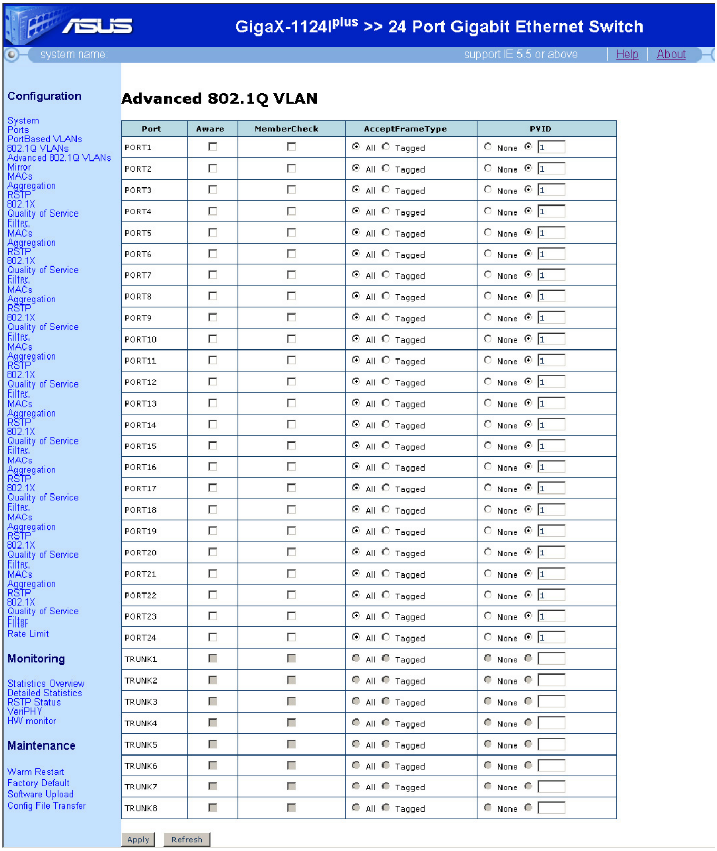
  Unaware--

  Ingress - Always insert tag with PVID for incoming packets.

  Egress - Always remove the tag for outgoing packets.

- Member Check: If enabled, the system will discard incoming frames for VLANs which do not include this port in its member set.
- Accept Frame Type: Accept all frames (tagged or untagged) or tagged frames only.
- PVID: Set or show the port VLAN ID. Untagged frames received on the port will be classified to this VLAN ID. Frames classified to this VLAN ID will be sent untagged on the port.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 17.



GigaX-1124I^{plus} >> 24 Port Gigabit Ethernet Switch

system name:

support IE 5.5 or above | Help | About

Configuration

System
Ports
PortBased VLANs
802.1Q VLANs
Advanced 802.1Q VLANs
Mirror
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
MACs
Aggregation
RSTP
802.1X
Quality of Service
Filter
Rate Limit

Monitoring

Statistics Overview
Detailed Statistics
RSTP Status
VeriPHY
HW monitor

Maintenance

Warm Restart
Factory Default
Software Upload
Config File Transfer

Advanced 802.1Q VLAN

Port	Aware	MemberCheck	AcceptFrameType	PVID
PORT1	☐	☐	● All ○ Tagged	○ None ● 1
PORT2	☐	☐	● All ○ Tagged	○ None ● 1
PORT3	☐	☐	● All ○ Tagged	○ None ● 1
PORT4	☐	☐	● All ○ Tagged	○ None ● 1
PORT5	☐	☐	● All ○ Tagged	○ None ● 1
PORT6	☐	☐	● All ○ Tagged	○ None ● 1
PORT7	☐	☐	● All ○ Tagged	○ None ● 1
PORT8	☐	☐	● All ○ Tagged	○ None ● 1
PORT9	☐	☐	● All ○ Tagged	○ None ● 1
PORT10	☐	☐	● All ○ Tagged	○ None ● 1
PORT11	☐	☐	● All ○ Tagged	○ None ● 1
PORT12	☐	☐	● All ○ Tagged	○ None ● 1
PORT13	☐	☐	● All ○ Tagged	○ None ● 1
PORT14	☐	☐	● All ○ Tagged	○ None ● 1
PORT15	☐	☐	● All ○ Tagged	○ None ● 1
PORT16	☐	☐	● All ○ Tagged	○ None ● 1
PORT17	☐	☐	● All ○ Tagged	○ None ● 1
PORT18	☐	☐	● All ○ Tagged	○ None ● 1
PORT19	☐	☐	● All ○ Tagged	○ None ● 1
PORT20	☐	☐	● All ○ Tagged	○ None ● 1
PORT21	☐	☐	● All ○ Tagged	○ None ● 1
PORT22	☐	☐	● All ○ Tagged	○ None ● 1
PORT23	☐	☐	● All ○ Tagged	○ None ● 1
PORT24	☐	☐	● All ○ Tagged	○ None ● 1
TRUNK1	☐	☐	○ All ○ Tagged	○ None ○
TRUNK2	☐	☐	○ All ○ Tagged	○ None ○
TRUNK3	☐	☐	○ All ○ Tagged	○ None ○
TRUNK4	☐	☐	○ All ○ Tagged	○ None ○
TRUNK5	☐	☐	○ All ○ Tagged	○ None ○
TRUNK6	☐	☐	○ All ○ Tagged	○ None ○
TRUNK7	☐	☐	○ All ○ Tagged	○ None ○
TRUNK8	☐	☐	○ All ○ Tagged	○ None ○

Figure 17. Advanced 802.1Q VLANs

4.3.6 Mirror

Users can enable mirroring of frames received on selected ports by configuring the monitored and monitoring ports in the following fields:

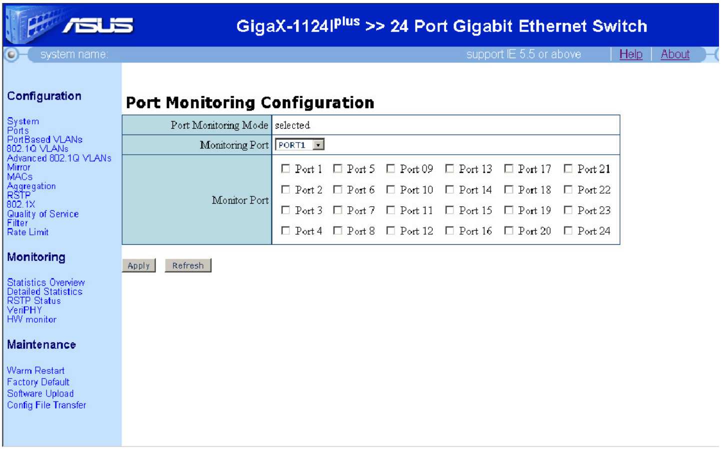
- Monitoring Port: Receive the copies of all the traffics in the selected mirrored port.
- Monitored Port: Select the ingress ports being mirrored.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 18.

The monitor port cannot belong to any link aggregation group.

The monitor port cannot operate as a normal switch port. It does not switch packets or do address learning.

If there is no monitored port selected, it means the function port mirroring is disabled.



Port Monitoring Configuration

Port Monitoring Mode	selected					
Monitoring Port	PORT1					
Monitor Port	□ Port 1	□ Port 5	□ Port 09	□ Port 13	□ Port 17	□ Port 21
	□ Port 2	□ Port 6	□ Port 10	□ Port 14	□ Port 18	□ Port 22
	□ Port 3	□ Port 7	□ Port 11	□ Port 15	□ Port 19	□ Port 23
	□ Port 4	□ Port 8	□ Port 12	□ Port 16	□ Port 20	□ Port 24

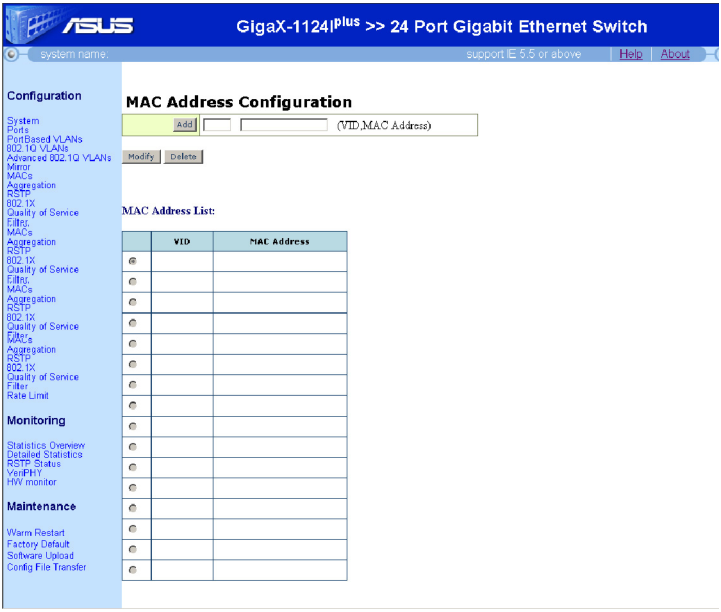
Figure 18. Mirror Configuration

4.3.7 MACs

Configure or show the permanently stored MAC table. Users can configure the MAC entry in the following ways:

- Add a new MAC entry: Fill in the VLAN ID and MAC address. Then click on the “Add” button. On the next page, select the ports that belong to this entry. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.
- Modify a MAC entry: Select the entry that needs to be modified and then click on the “Modify” button. On the next page, select the ports that belong to this group. Click on the “Apply” button to make the configuration effective, or the “Refresh” button to refresh the setting to current value.
- Delete a MAC entry: Select the entry that needs to be deleted and then click on the “Delete” button.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 19. Next page is shown in Figure 20.



MAC Address Configuration

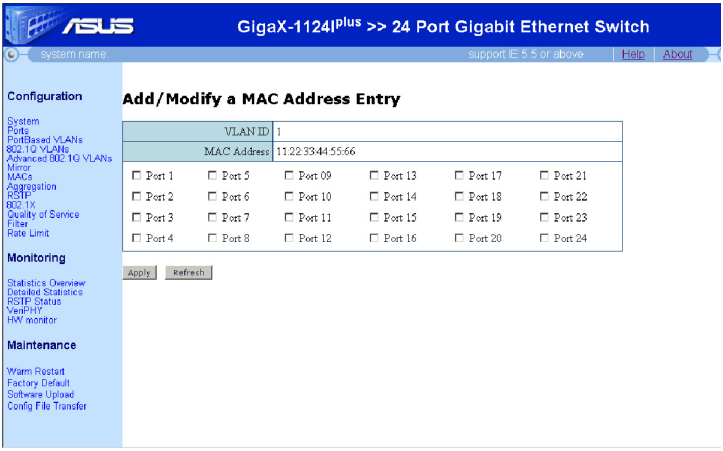
Add [ ] [ ] (VID,MAC Address)

Modify Delete

MAC Address List:

	VID	MAC Address
●		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		
○		

Figure 19. MAC Address Configuration



Add/Modify a MAC Address Entry

VLAN ID	1
MAC Address	11:22:33:44:55:66

□ Port 1	□ Port 5	□ Port 09	□ Port 13	□ Port 17	□ Port 21
□ Port 2	□ Port 6	□ Port 10	□ Port 14	□ Port 18	□ Port 22
□ Port 3	□ Port 7	□ Port 11	□ Port 15	□ Port 19	□ Port 23
□ Port 4	□ Port 8	□ Port 12	□ Port 16	□ Port 20	□ Port 24

Apply Refresh

Figure 20. Add/Modify a MAC Address Entry

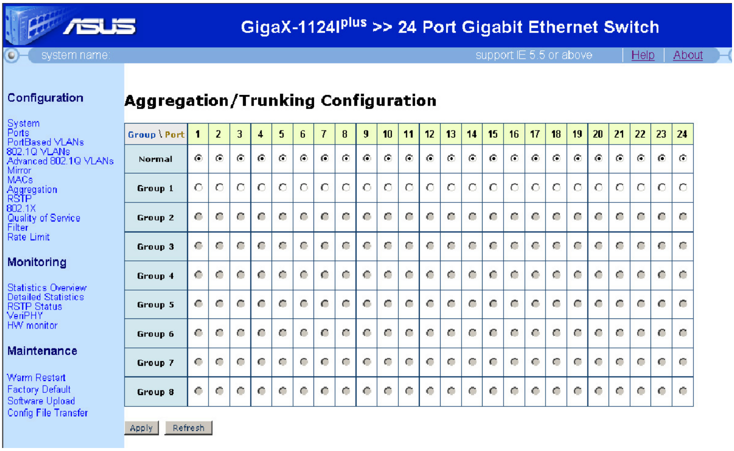
4.3.8 Aggregation

Configure or show the aggregation groups. Users can selcect the group members in each aggregation group.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 21.

If all the trunk members are in the same speed and full duplex mode, then the trunk group is set up successfully. If one of the members is not in the same speed or full duplex mode, the trunk is not set correctly. Check the link partner and change the settings to have the same speed and full duplex mode for all the members of your trunk group.

- All the ports in the link aggregation group MUST operate in full-duplex mode at the same speed.
- All the ports in the link aggregation group MUST be configured in auto-negotiation mode or full duplex mode. This configuration will make the full duplex link possible. If you set the ports in full duplex force mode, then the link partner MUST have the same setting. Otherwise the link aggregation could operate abnormally.
- All the ports in the link aggregation group MUST have the same VLAN setting.
- All the ports in the link aggregation group are treated as a single logical link. That is, if any member changes an attribute, the others will change too. For example, a trunk group consists of port 1 and 2. If the VLAN of port 1 changes, the VLAN of port 2 also changes with port 1.



Aggregation/Trunking Configuration

Group \ Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Normal	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
Group 1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 21. Aggregation Configuration

4.3.9 RSTP

Users can change the RSTP system configuration in the following fields:

- System Priority: Set or show the RSTP System Priority. Number between 0 - 61440 in increments of 4096. This provides for 16 distinct values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440.
- Hello Time: Set or show the RSTP System Hello time. Number is between 1 - 10 (default is 2).
- Max Age: Set or show the RSTP System Max Age. Number is between 6 - 40 (default is 20).
- Forward Delay: Set or show the RSTP System Forward delay. Number is between 4 - 30 (default is 15).
- Force Version: Set or show the RSTP protocol version to use.

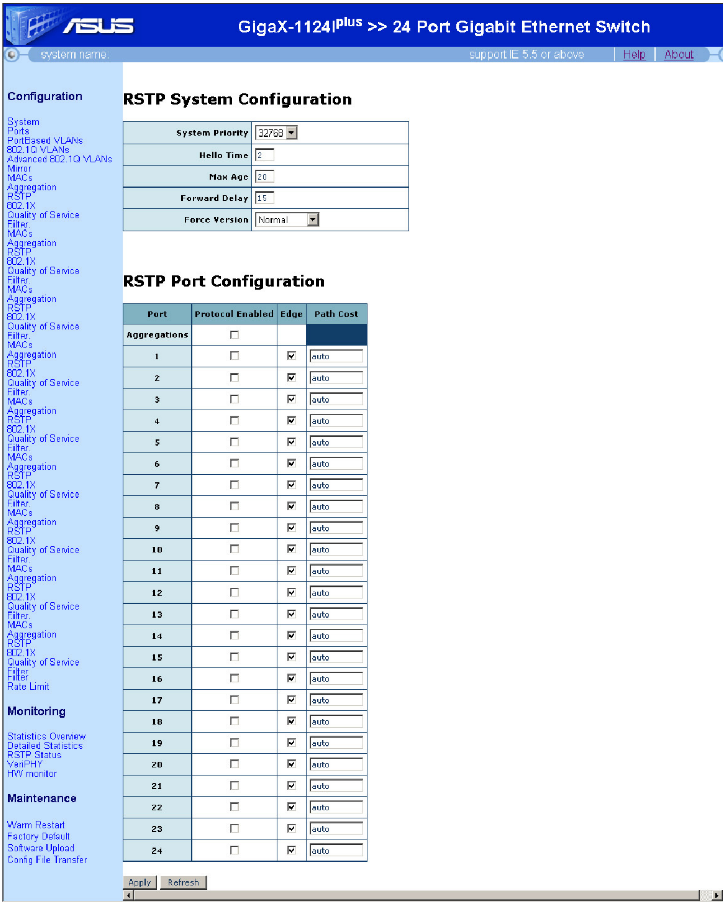
  Normal - It will try to send out RSTP packets first. If there is no RSTP devices in its neighbourhood, it will try to send out STP packets instead;

  Compatible - It will send out STP packets only.

Users can change the RSTP port configuration in the following field:

- Protocol Enabled: Enable or disable the RSTP protocol on the port or aggregation links.
- Edge: Enable to expect the port to be an edge port (an end station) or disable to make the port have a link to another STP device (bridge).
- Path Cost: Set the RSTP pathcost on the port. Number is between 1 - 200000000. Auto means autogenerated pathcost.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 22.



RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force Version	Normal

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	□		
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto
5	□	☑	auto
6	□	☑	auto
7	□	☑	auto
8	□	☑	auto
9	□	☑	auto
10	□	☑	auto
11	□	☑	auto
12	□	☑	auto
13	□	☑	auto
14	□	☑	auto
15	□	☑	auto
16	□	☑	auto
17	□	☑	auto
18	□	☑	auto
19	□	☑	auto
20	□	☑	auto
21	□	☑	auto
22	□	☑	auto
23	□	☑	auto
24	□	☑	auto

Figure 22. RSTP Configuration

4.3.10 802.1X

Users can change the 802.1X configuration in the following fields:

- Mode: Enable or disable 802.1X process for the switch.
- RADIUS IP: Set or show RADIUS server IP address.
- RADIUS UDP Port: Set up UDP Port for the external RADIUS server.
- RADIUS Secret: Set or show the secret shared with the RADIUS server.
- Admin State: Set or show the configured 802.1X state for the port.

  Auto: Behavior of the port is controlled by 802.1X protocol.

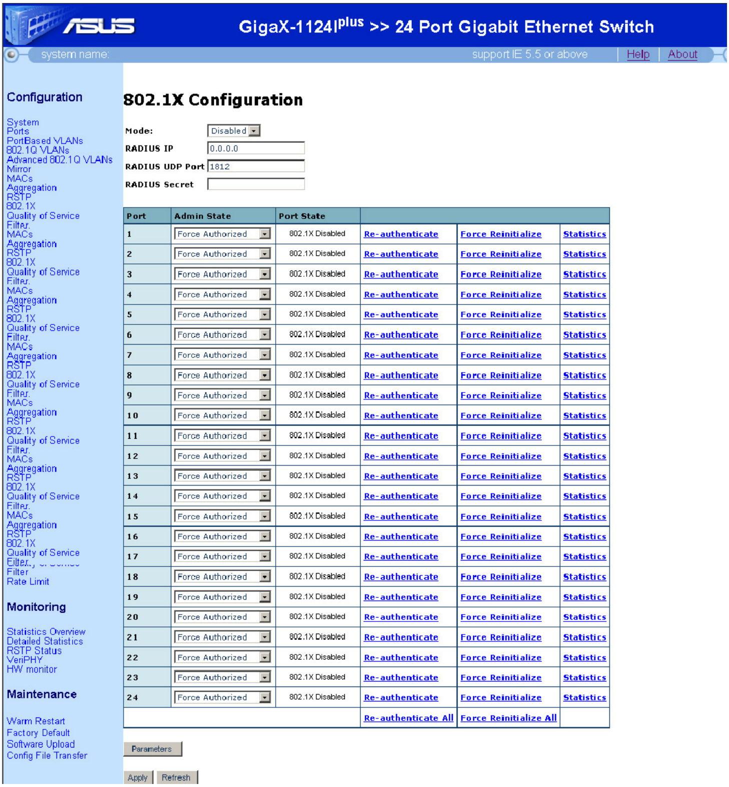
  Force Authorized: Traffic from all hosts to the port is allowed to pass.

  Force Unauthorized: Port is blocked and no traffic can go through.
- Port State: Show the port real-time state. (802.1X Disabled, Link Down, Unauthorized, or Authorized)
- Re-authenticate: Refresh (restart) 802.1X authentication process for the port.
- Force Reinitialize: Reinitialize the port.
- Statistics: Click to show the Authenticator counters, Backend Authenticator counters, dot1x MIB counters, and Last Supplicant identity of the port.
- Re-authenticate All: Refresh (restart) 802.1X authentication process for all ports.
- Force Reinitialize All: Reinitialize all ports.

Click on the “Parameters” button to change 802.1X parametes in the following field:

- Reauthentication Enabled: Enable or disable reauthentication. Once enabled, the switch will try to authenticate the port user again in a predefined period.
- Reauthentication Period: If reauthentication is enabled, this is the time period to re-send authentication request to the port user. Number is between 1 - 3600.
- EAP timeout: Number is between 1 - 255.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 23. The next page for statistics is shown in Figure 24. The third page for parameter is shown in Figure 25.

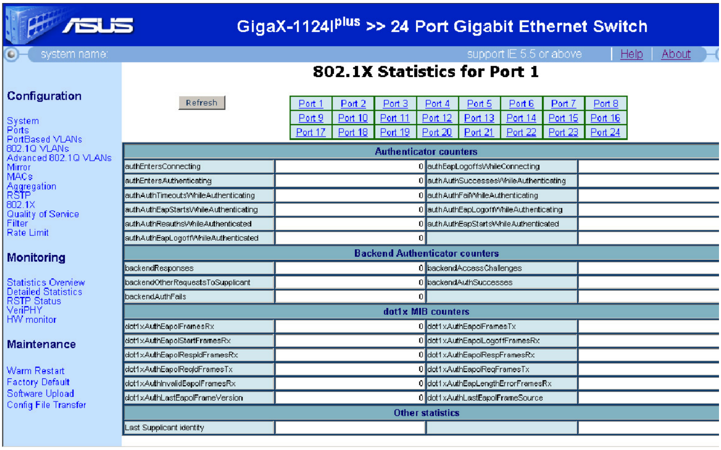


802.1X Configuration

Mode:	Disabled
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	

Port	Admin State	Port State			
1	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
9	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
10	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
11	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
12	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
13	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
14	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
15	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
16	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
17	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
18	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
19	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
20	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
21	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
22	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
23	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
24	Force Authorized	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

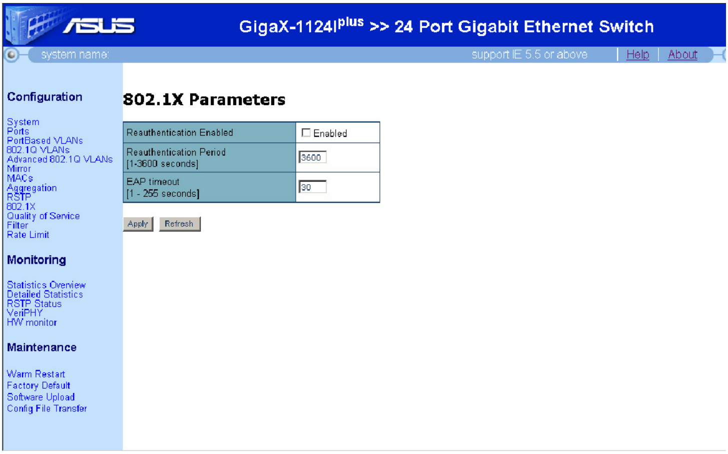
Figure 23. 802.1X Configuration



802.1X Statistics for Port 1

Authenticator counters			
authEntersConnecting	0	authEapLogoffsWhileConnecting	
authEntersAuthenticating	0	authAuthSuccessesWhileAuthenticating	
authAuthTimeoutsWhileAuthenticating	0	authAuthFailWhileAuthenticating	
authAuthEapStartsWhileAuthenticating	0	authAuthEapLogoffWhileAuthenticating	
authAuthReauthsWhileAuthenticated	0	authAuthEapStartsWhileAuthenticated	
authAuthEapLogoffWhileAuthenticated	0		
Backend Authenticator counters			
backendResponses	0	backendAccessChallenges	
backendOtherRequestsToSupplicant	0	backendAuthSuccesses	
backendAuthFails	0		
dot1x MIB counters			
dot1xAuthEapolFramesRx	0	dot1xAuthEapolFramesTx	
dot1xAuthEapolStartFramesRx	0	dot1xAuthEapolLogoffFramesRx	
dot1xAuthEapolRespIdFramesRx	0	dot1xAuthEapolRespFramesRx	
dot1xAuthEapolReqIdFramesTx	0	dot1xAuthEapolReqFramesTx	
dot1xAuthInvalidEapolFramesRx	0	dot1xAuthEapLengthErrorFramesRx	
dot1xAuthLastEapolFrameVersion	0	dot1xAuthLastEapolFrameSource	
Other statistics			
Last Supplicant identity			

Figure 24. 802.1X Statistics



802.1X Parameters

Reauthentication Enabled	□ Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP timeout [1 - 255 seconds]	30

Figure 25. 802.1X Parameter

4.3.11 Quality of Service

Users can change the QoS configuration in the following fields:

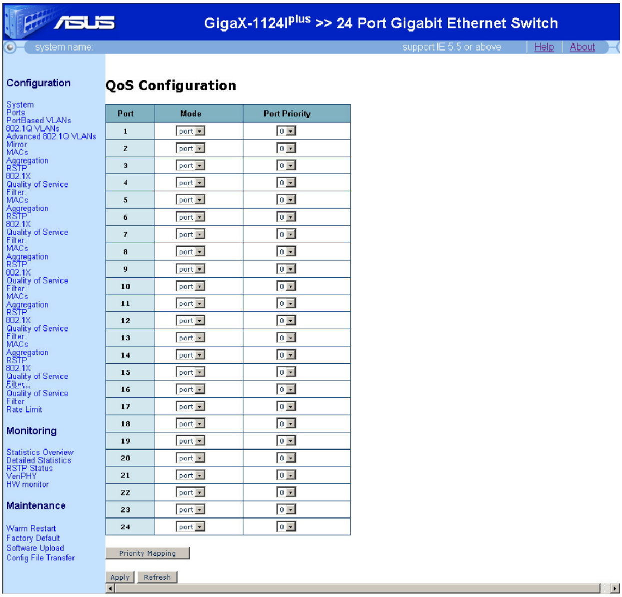
- Mode: Set or show the QoS mode for the port. In Tag mode, it will retrieve the priority in tagged packet as the priority. It will use the user priority for untagged packet. In Port mode, it will use default priority (class) for tagged and untagged packet.
- Port Priority: Set or show the default VLAN user priority of the port for untagged frames.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value.

Click on the **Priority Mapping** button to change QoS priority mapping in the following field:

- Class: The switch supports 4 classes for each port. Select the class that the priority maps into.

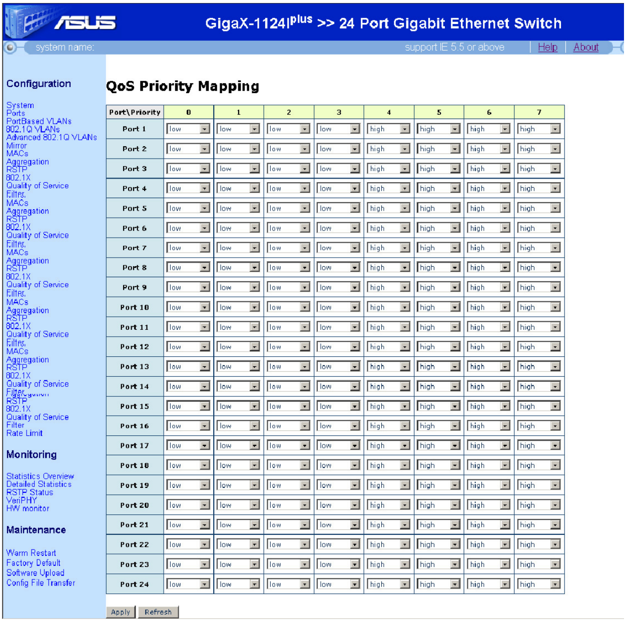
Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 26. Next page for Priority Mapping is shown in Figure 27.



QoS Configuration

Port	Mode	Port Priority
1	port	0
2	port	0
3	port	0
4	port	0
5	port	0
6	port	0
7	port	0
8	port	0
9	port	0
10	port	0
11	port	0
12	port	0
13	port	0
14	port	0
15	port	0
16	port	0
17	port	0
18	port	0
19	port	0
20	port	0
21	port	0
22	port	0
23	port	0
24	port	0

Figure 26. QoS Configuration



QoS Priority Mapping

Port\Priority	0	1	2	3	4	5	6	7
Port 1	low	low	low	low	high	high	high	high
Port 2	low	low	low	low	high	high	high	high
Port 3	low	low	low	low	high	high	high	high
Port 4	low	low	low	low	high	high	high	high
Port 5	low	low	low	low	high	high	high	high
Port 6	low	low	low	low	high	high	high	high
Port 7	low	low	low	low	high	high	high	high
Port 8	low	low	low	low	high	high	high	high
Port 9	low	low	low	low	high	high	high	high
Port 10	low	low	low	low	high	high	high	high
Port 11	low	low	low	low	high	high	high	high
Port 12	low	low	low	low	high	high	high	high
Port 13	low	low	low	low	high	high	high	high
Port 14	low	low	low	low	high	high	high	high
Port 15	low	low	low	low	high	high	high	high
Port 16	low	low	low	low	high	high	high	high
Port 17	low	low	low	low	high	high	high	high
Port 18	low	low	low	low	high	high	high	high
Port 19	low	low	low	low	high	high	high	high
Port 20	low	low	low	low	high	high	high	high
Port 21	low	low	low	low	high	high	high	high
Port 22	low	low	low	low	high	high	high	high
Port 23	low	low	low	low	high	high	high	high
Port 24	low	low	low	low	high	high	high	high

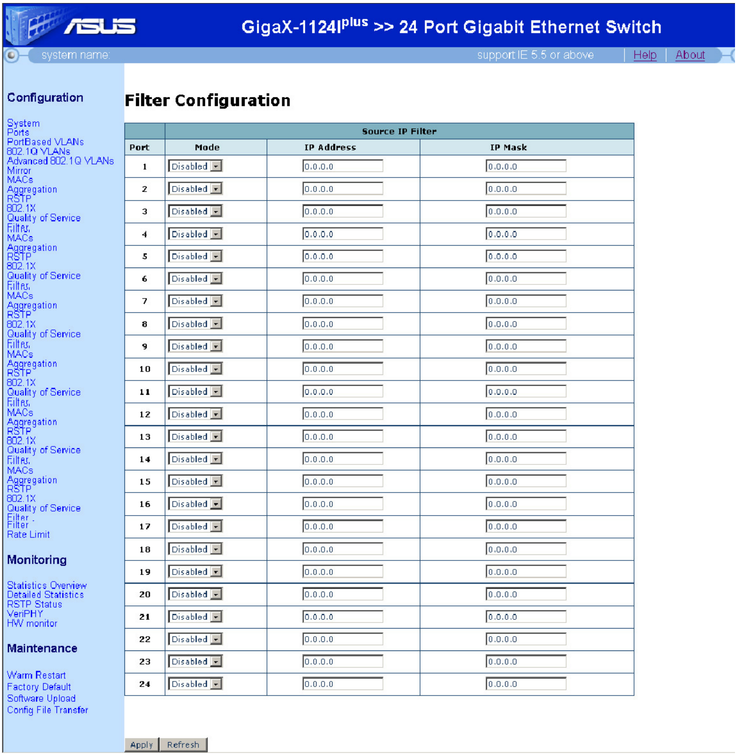
Figure 27. QoS Priority Mapping

4.3.12 Filter

The function filters source IP only. Users can change the source IP filter configuration in the following fields:

- Mode: Select “Disabled” to allow all IP addresses. Select “Manually” to allow only the configured IP addresses.
- IP Address and IP Mask: When “Manually” mode is selected, these are the IP addresses allowed.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 28.



Filter Configuration

	Source IP Filter		
Port	Mode	IP Address	IP Mask
1	Disabled	0.0.0.0	0.0.0.0
2	Disabled	0.0.0.0	0.0.0.0
3	Disabled	0.0.0.0	0.0.0.0
4	Disabled	0.0.0.0	0.0.0.0
5	Disabled	0.0.0.0	0.0.0.0
6	Disabled	0.0.0.0	0.0.0.0
7	Disabled	0.0.0.0	0.0.0.0
8	Disabled	0.0.0.0	0.0.0.0
9	Disabled	0.0.0.0	0.0.0.0
10	Disabled	0.0.0.0	0.0.0.0
11	Disabled	0.0.0.0	0.0.0.0
12	Disabled	0.0.0.0	0.0.0.0
13	Disabled	0.0.0.0	0.0.0.0
14	Disabled	0.0.0.0	0.0.0.0
15	Disabled	0.0.0.0	0.0.0.0
16	Disabled	0.0.0.0	0.0.0.0
17	Disabled	0.0.0.0	0.0.0.0
18	Disabled	0.0.0.0	0.0.0.0
19	Disabled	0.0.0.0	0.0.0.0
20	Disabled	0.0.0.0	0.0.0.0
21	Disabled	0.0.0.0	0.0.0.0
22	Disabled	0.0.0.0	0.0.0.0
23	Disabled	0.0.0.0	0.0.0.0
24	Disabled	0.0.0.0	0.0.0.0

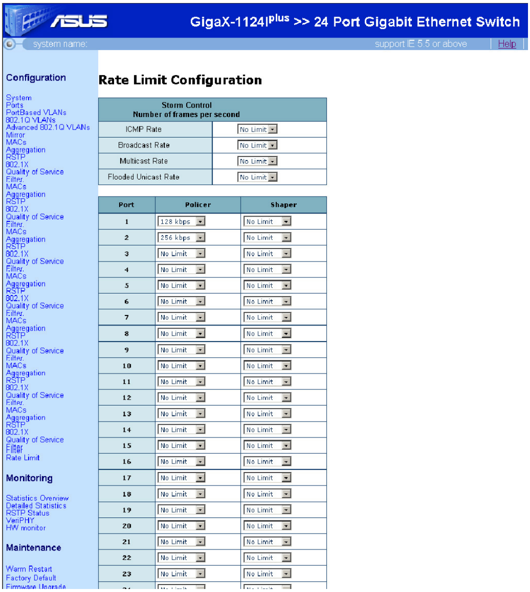
Figure 28. Filter Configuration

4.3.13 Rate Limit

Users can change the rate limit configuration in the following fields:

- ICMP Rate: Select the limited rate of ICMP frames.
- Broadcast Rate: Select the limited rate of broadcast frames.
- Multicast Rate: Select the limited rate of multicast frames.
- Flooded Unicast Rate: Select the limited rate of flooded unicast frames.
- Policer: Control maximum ingress bandwidth rate.
- Shaper: Control maximum egress bandwidth rate.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 29.



Rate Limit Configuration

Storm Control Number of frames per second	
ICMP Rate	No Limit
Broadcast Rate	No Limit
Multicast Rate	No Limit
Flooded Unicast Rate	No Limit

Port	Policer	Shaper
1	128 kbps	No Limit
2	256 kbps	No Limit
3	No Limit	No Limit
4	No Limit	No Limit
5	No Limit	No Limit
6	No Limit	No Limit
7	No Limit	No Limit
8	No Limit	No Limit
9	No Limit	No Limit
10	No Limit	No Limit
11	No Limit	No Limit
12	No Limit	No Limit
13	No Limit	No Limit
14	No Limit	No Limit
15	No Limit	No Limit
16	No Limit	No Limit
17	No Limit	No Limit
18	No Limit	No Limit
19	No Limit	No Limit
20	No Limit	No Limit
21	No Limit	No Limit
22	No Limit	No Limit
23	No Limit	No Limit
24	No Limit	No Limit

Figure 29. Rate Limit Configuration

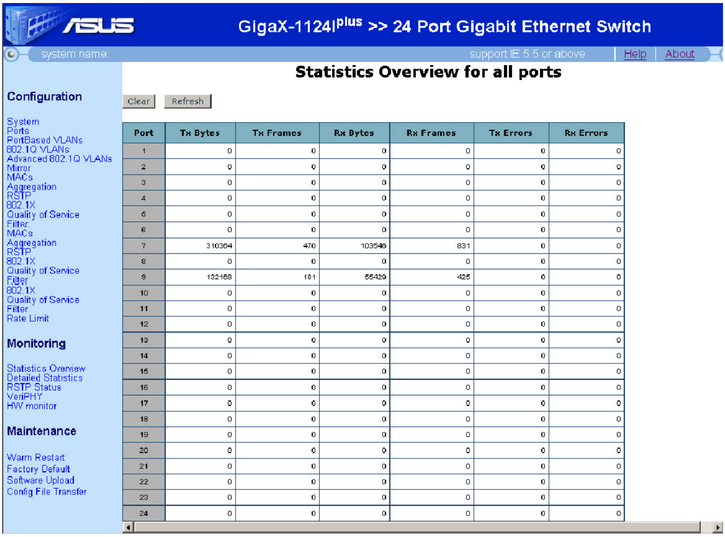
4.4 Monitoring

The Monitoring page group contains Statistics Overview, Detail Statistics, RSTP Status, VeriPHY, HW Monitor.

4.4.1 Statistics Overview

This page shows Tx Bytes, Tx Frames, Rx Bytes, Rx Frames, Tx Errors, and Rx Errors of each port. Show Trunk: Select “Add a new Trunk” for a new created group. Or select an existed group to display on the following fields and port icons.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 30.



Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	310364	470	103546	831	0	0
8	0	0	0	0	0	0
9	132168	181	55429	425	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	0	0	0	0	0	0
17	0	0	0	0	0	0
18	0	0	0	0	0	0
19	0	0	0	0	0	0
20	0	0	0	0	0	0
21	0	0	0	0	0	0
22	0	0	0	0	0	0
23	0	0	0	0	0	0
24	0	0	0	0	0	0

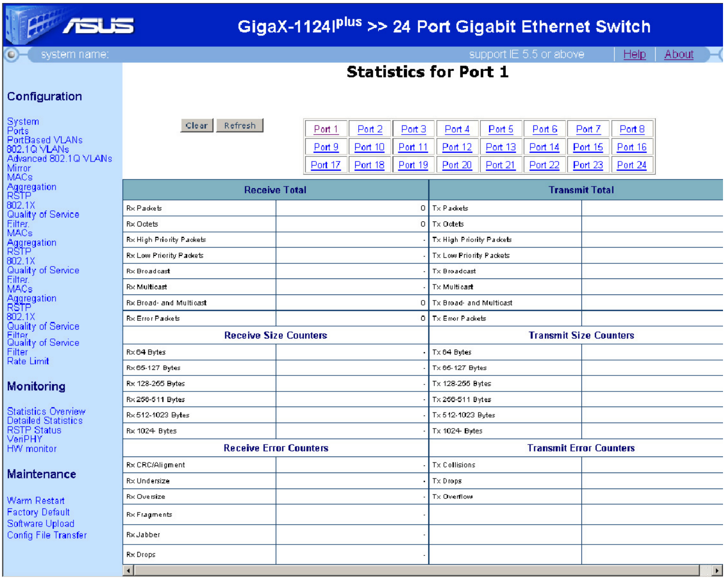
Figure 30. Statistics Overview

4.4.2 Detailed Statistics

This page shows Receive Total, Transmit Total, Receive Size Counters, Transmit Size Counters, Receive Error Counters, and Transmit Error Counters of each port.

Click on the Port number on the top of the page to see the statistics of that port.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 31.



Statistics for Port 1

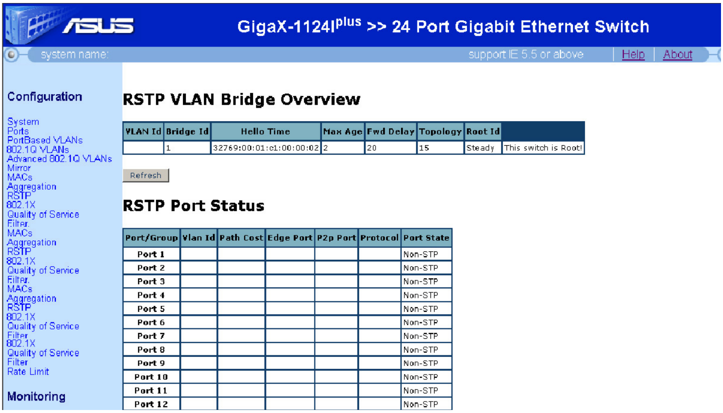
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	
Rx Octets	0	Tx Octets	
Rx High Priority Packets	-	Tx High Priority Packets	
Rx Low Priority Packets	-	Tx Low Priority Packets	
Rx Broadcast	-	Tx Broadcast	
Rx Multicast	-	Tx Multicast	
Rx Broad- and Multicast	0	Tx Broad- and Multicast	
Rx Error Packets	0	Tx Error Packets	
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	
Rx 65-127 Bytes	-	Tx 65-127 Bytes	
Rx 128-255 Bytes	-	Tx 128-255 Bytes	
Rx 256-511 Bytes	-	Tx 256-511 Bytes	
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	
Rx 1024- Bytes	-	Tx 1024- Bytes	
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	-	Tx Collisions	
Rx Undersize	-	Tx Drops	
Rx Oversize	-	Tx Overflow	
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Figure 31. Detailed Statistics

4.4.3 RSTP Status

This page shows RSTP VLAN bridge overview and RSTP port status

Click on the **Refresh** button to refresh the setting to current value as shown in Figure 32.



RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id	
	1	32769:00:01:c1:00:00:02	2	20	15	Steady	This switch is Root!

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP
Port 10						Non-STP
Port 11						Non-STP
Port 12						Non-STP

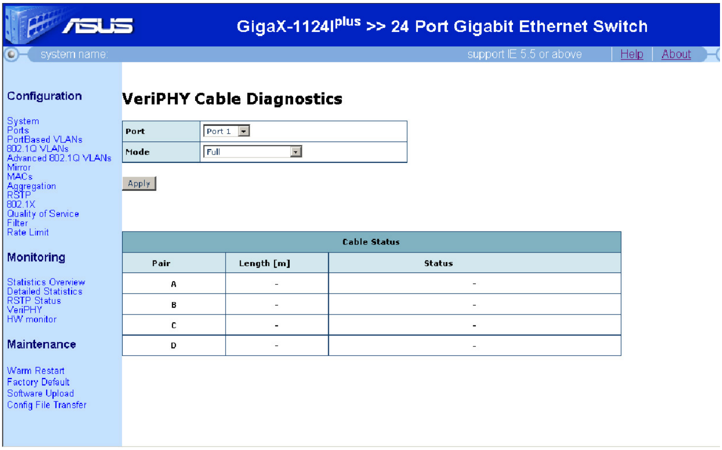
Figure 32. RSTP Status

4.4.4 VeriPHy

Users can perform cable diagnostics by determining the parameters in the following fields:

- Port: Select the port to be performed cable diagnostics.
- Mode: Type of diagnostics, default is **Full**. **Full** comprises cable length and full anomaly check. **Anomaly** comprises full anomaly check. **Anomaly without X-pair** comprises anomaly check without check for coupling between pairs.

Click on the **Apply** button to make the configuration effective, or the **Refresh** button to refresh the setting to current value as shown in Figure 33.



VeriPHY Cable Diagnostics

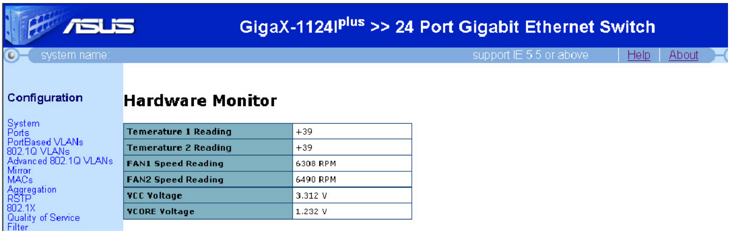
Port	Port 1
Mode	Full

Cable Status		
Pair	Length [m]	Status
A	-	-
B	-	-
C	-	-
D	-	-

Figure 33. VeryPHY

4.4.5 HW Monitor

This page shows the temperature, fan speed and voltage of hardware, as shown in Figure 34.



Hardware Monitor

Temerature 1 Reading	+39
Temerature 2 Reading	+39
FAN1 Speed Reading	6308 RPM
FAN2 Speed Reading	6490 RPM
VCC Voltage	3.312 V
VCORE Voltage	1.232 V

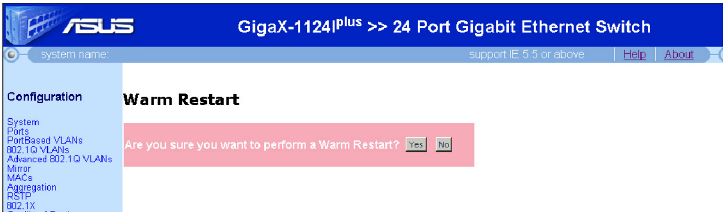
Figure 34. HW Monitor

4.5 Maintenance

The Maintenance page group contains Warm Restart, Factory Default, Software Upload and Config file transfer.

4.5.1 Warm Restart

- Click on the **Yes** button to perform a warm restart as shown in Figure 35.



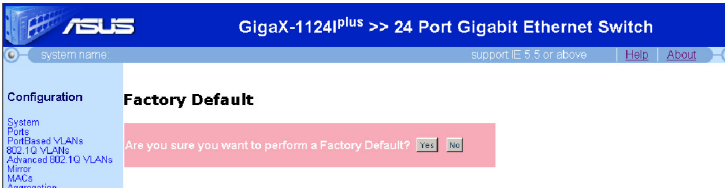
Are you sure you want to perform a Warm Restart?

Figure 35. Warm Restart

4.5.2 Factory Default

IP will be reset to 192.168.1.1.

Click on the **Yes** button to perform factory default as shown in Figure 36.



Are you sure you want to perform a Factory Default?

Figure 36. Factory Default

4.5.3 Firmware Upgrade

Use the function to update the current firmware version. Select the firmware file and click on the **Upload** button to upload the firmware as shown in Figure 37.

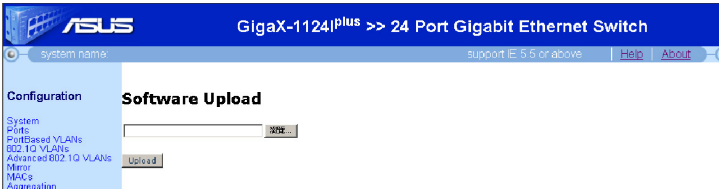


Figure 37. Firmware Upload

4.5.4 Config File Transfer

Backup and restore the configuration file. Click on the **Download** button to collect the current configuration as a configuration file to local disk or select a configuration file from local disk and click on the **Upload** button to restore the configuration file as shown in Figure 38.

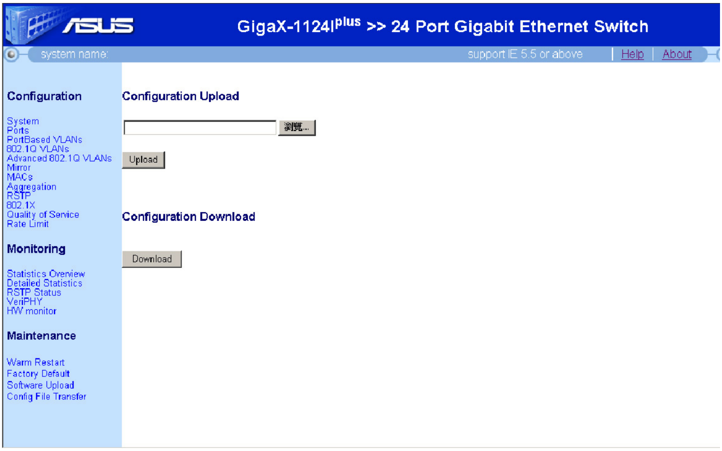


Figure 38. Config file Transfer

5 Console Interface

This chapter describes how to use console interface to configure the switch. The switch provides RS232 connectors to connect your PC. Use a terminal emulator on your PC such as HyperTerminal and command line interpreter to configure the switch. You have to set up the terminal emulator with baud rate 115200, 8 bit data, no parity, and 1 stop bit, and no flow control.

Once you enter CLI mode, type "?" will display all available command help messages. The "?" is valid for the root and sub-directory command tree. This is very useful when you are not familiar with the CLI commands.

In order to make them easier to use, you can enter into different category by typing the full command, then this category becomes your working category. Thereafter, you don't have to type "system" before any sub-commands. For example, "system" is a command category including a lot of sub-commands. You don't have to type "system" for the sub-commands once you change your working category to "sys" by typing "sys". The prompt will become "system>" when your working category is "sys".

5.1 Password

After rebooting, you need to type password to enter the CLI mode. The default password is no password.

5.2 CLI Commands

The switch provides CLI commands for all managed functions.

Always use "?" to get the available commands list and help. Put "?" after the CLI commands to get the help.

Always use "/" to get back to the root directory.

5.2.1 System Commands

[System Configuration]

Show system name, software version, hardware version and management MAC address. Optionally show the full configuration

[all]: Show the total switch configuration (default: System configuration only)

CLI command : System Configuration [all]

If you put a name in the name description field, the switch system name changes to the new one.

[System Restore Default]

Restore factory default configuration.

[keepIP]: Preserve IP configuration (default: Not preserved).

CLI command : System Restore Default [keepIP]

[System Name]

Set or show the system name.

[<name>]: String of up to 16 characters (default: Show system name).

CLI command : System Name [<name>]

[System Reboot]

Reboot the switch.

[<name>]: String of up to 16 characters (default: Show system name).

CLI command : System Reboot

[System SNMP]

Activate or deactivate the SNMP.

[enableIdisable]: Enable/disable SNMP (default: Show SNMP mode).

CLI command : System SNMP [enableIdisable]

[System Trap]

Set or show SNMP traps destination.

<IP Address>: IP address to send traps to. (default: Show trap configuration)

CLI command : System Trap [<IP Address>]

5.2.2 Console Commands

[Console Configuration]

Show configured console password and timeout.

CLI command : Console Configuration

[Console Password]

Set or show the console password. The empty string (“”) disables the password check.

[<password>]: Password string of up to 16 characters..

CLI command : Console Password [<password>]

[Console Timeout]

Set or show the console inactivity timeout in seconds. The value zero

disables timeout.

[<timeout>]: Timeout value in seconds, 0,60-10000.

CLI command : Console Timeout [<timeout>]

[Console Prompt]

Set or show the console prompt string.

[<prompt_string>]: Command prompt string of up to 10 characters.

CLI command : Console Prompt [<prompt_string>]

5.2.3 Port Commands

[Port Configuration]

Show the configured and current speed, duplex mode, flow control

mode and state for the port.

[<portlist>]: Port list (Default: All ports).

CLI command : Port Configuration [<portlist>]

[Port Mode]

Set or show the speed and duplex mode for the port.

[<portlist>]: Port list (Default: All ports).

[<mode>]: Port speed and duplex mode (Default: Show configured and current mode).

10hdx : 10 Mbit/s, half duplex.

10fdx : 10 Mbit/s, full duplex.

100hdx : 100 Mbit/s, half duplex.

100fdx : 100 Mbit/s, full duplex.

1000fdx: 1 Gbit/s, full duplex.

auto : Auto negotiation of speed and duplex.

CLI command : Port Mode [<portlist>] [<mode>]

[Port Flow Control]

Set or show flow control mode for the port.

[<portlist>] : Port list (default: All ports).

[enableldisable]: Enable/disable flow control (default: Show flow control mode).

CLI command : Port Flow Control [<portlist>] [enableldisable]

[Port State]

Set or show the state for the port.

[<portlist>] : Port list (default: All ports).

[enableldisable]: Enable or disable port state (default: Show state).

CLI command : Port State [<portlist>] [enable/disable]

[Port MaxFrame]

Set or show the maximum frame size in bytes (including FCS) for frames received on the port. Tagged frames are allowed to be 4 bytes longer than the

maximum frame size. Use the reset option to return to default setting.

[<portlist>]: Port list (default: All ports).

[<framesize>lreset]: Maximum frame size [1518-9600] or reset to 1518 bytes (default: Show maximum frame size).

CLI command : Port MaxFrame [<portlist>] [<framesize>lreset]

[Port Statistics]

Show or clear statistics for the port.

[<portlist>]: Port list (default: All ports).

[clear] : Clear port statistics (default: Show statistics).

CLI command : Port Statistics [<portlist>] [clear]

[Port Excessive Collisions Drop]

Enable or disable drop of frames when excessive collisions occur in half duplex mode.

[enableIdisable]: Enable/disable frame drop (default: Show Excessive Collisions Drop mode)..

CLI command : Port Excessive Collisions Drop [enableIdisable]

[VeriPHY]

Perform VeriPHY cable diagnostics on the specified port(s).

[<portlist>]: Port list (Default: All ports).

[fullIanomalyItermination]: Type of diagnostics. Full comprises cable length and full anomaly check, anomaly comprises full anomaly check and termination comprises anomaly check without check for coupling between pairs. (default: full).

CLI command : VeriPHY [<portlist>] [fullIanomalyItermination]

5.2.4 MAC Commands

[MAC Configuration]

Show the permanently stored MAC table and the MAC ageing timer.

CLI command : MAC Configuration

[MAC Add]

Add permanent MAC address and VLAN ID on ports.

<macaddress>: MAC address, 12 digit hex string, optionally separated with dashes or colons (e.g. 010203ABCDEF or 01-02-03-AB-CD-EF or 01:02:03:AB:CD:EF).

<portlist> : Port list. Use “none” to specify no ports.

[<vid>] : VLAN ID, 1-4095 (default: 1).

CLI command : MAC Add <macaddress> <portlist>Inone [<vid>]

[MAC Delete]

Delete MAC address and VLAN ID.

<macaddress>: MAC address, 12 digit hex string, optionally separated with dashes or colons (e.g. 010203ABCDEF or 01-02-03-AB-CD-EF or 01:02:03:AB:CD:EF).

[<vid>] : VLAN ID (default: All).

CLI command : MAC Delete <macaddress> [<vid>]

[MAC Lookup]

Lookup MAC address and VLAN ID.

<macaddress>: MAC address, 12 digit hex string, optionally separated with dashes or colons (e.g. 010203ABCDEF or 01-02-03-AB-CD-EF or 01:02:03: AB:CD:EF).

[<vid>]: VLAN ID, 1-4095 (default: 1).

CLI command : MAC Lookup <macaddress> [<vid>]

[MAC Table]

Show the MAC address table for VLAN ID list.

<vidlist> : VLAN ID list.

CLI command : MAC table <vidlist>

[MAC Flush]

Removes non-locked entries from the switch MAC table.

CLI command : MAC Flush

[MAC Agetime]

Set or show the MAC age timer in seconds. The value zero disables ageing.

[<agetime>]: Age timer in seconds, 0 or 10-65535 (default: Show timer)..

CLI command : MAC Agetime [<agetime>]

5.2.5 Vlan Commands

[VLAN Configuration]

Show the VLAN aware mode, port VLAN ID and accepted frame type for the port and the permanently stored VLAN table.

[<portlist>]: Port list (default: All ports).

CLI command : VLAN Configuration [<portlist>]

[VLAN Add]

Add VLAN entry and include ports in member set.

<vidlist> : VLAN ID list.

[<portlist>]: Port list (default: All ports)..

CLI command : VLAN Add <vidlist> [<portlist>]

[VLAN Delete]

Delete VLAN entry (all ports excluded from member set).

<vidlist> : VLAN ID list.

CLI command : VLAN Delete <vidlist>

[VLAN Lookup]

Lookup VLAN entry and show port list.

<vidlist> : VLAN ID list.

CLI command : VLAN Lookup <vidlist>

[VLAN Aware]

Set or show the VLAN awareness mode for the port. VLAN aware ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (except PVID). VLAN unaware ports will not strip the tag from received frames or insert the tag in transmitted frames.

[<portlist>]: Port list (default: All ports).

[enableldisable]: Enable/disable VLAN awareness (default: Show awareness).

CLI command : VLAN Aware [<portlist>] [enableldisable]

[VLAN PVID]

Set or show the port VLAN ID. Untagged frames received on the port will be classified to this VLAN ID. Frames classified to this VLAN ID will be sent untagged on the port.

[<portlist>]: Port list (default: All ports).

[<vid>lnone]: Port VLAN ID, 1-4095 (default: Show PVID). The ‘none’ option can be used for trunk links.

CLI command : VLAN PVID [<portlist>] [<vid>lnone]

[VLAN Frame Type]

Set or show the accepted frame type for the port.

[<portlist>]: Port list (default: All ports).

[allltagged]: Accept all or only tagged (default: Show frame type).

CLI command : VLAN Frame Type [<portlist>] [allltagged]t>

[VLAN Member Check]

Set or show the member check for the port.

[<portlist>]: Port list (default: All ports).

[enableldisable]: Enable or disable member check (default: Show member check).

CLI command : VLAN Member Check [<portlist>] [enable/disable]

5.2.6 Aggr Commands

[Aggr Configuration]

Shows the aggregation groups and the aggregation mode.

CLI command : Aggr Configuration

[Aggr Add]

Add link aggregation group including ports.

<portlist>: Aggregation port list.

CLI command : Aggr Add <portlist>

[Aggr Delete]

Delete link aggregation group.

<portlist>: Port list. Aggregations including any of the ports will be deleted.

CLI command : Aggr Delete <portlist>

[Aggr Lookup]

Lookup and display link aggregation group.

<portlist>: Port list. Aggregations including any of the ports will be shown.

CLI command : Aggr Lookup <portlist>

[Aggr Mode]

Set or show link aggregation traffic distribution mode.

[smacldmaclxor]: Aggregation mode, SMAC, DMAC or XOR (default: Show mode).

CLI command : Aggr Mode [smacldmaclxor]

5.2.7 Rstp Commands

[Rstp Configuration]

Show RSTP configuration.

[<portlist>]: Port list (Default: All ports).

CLI command : Rstp Configuration [<portlist>]

[Rstp Sysprio]

Set or show the RSTP System Priority.

[<sysprio>]: Number between 0 - 61440 in increments of 4096. This provides for 16 distinct values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440.

CLI command : Rstp sysprio [<sysprio>]

[Rstp Hellotime]

Set or show the RSTP System Hello time.

[<secs>]: Number between 1 - 10 (default is 2)

CLI command : Rstp hellotime [<secs>]

[Rstp Maxage]

Set or show the RSTP System Max Age.

[<hops>]: Number between 6 - 40 (default is 20)

CLI command : Rstp maxage [<hops>]

[Rstp Fwddelay]

Set or show the RSTP System Forward delay.

[<secs>]: Number between 4 - 30 (default is 15)

CLI command : Rstp fwddelay [<secs>]

[Rstp Version]]

Set or show the RSTP protocol version to use.

[<version>]: normal - use RSTP, compat - compatible with old STP

CLI command : Rstp version [normal|compat]

[Rstp Mode]

Enable or disable the rstp protocol on ports <portlist>.

[<portlist>]: Port list (Default: All ports).

[enable|disable]: Enable or disable.

CLI command : Rstp Mode [<portlist>] [enable|disable]

[Rstp Aggr]

Enable or disable the RSTP protocol on aggregated links.

[enable|disable]: Enable or disable.

CLI command : Rstp aggr [enable|disable]

[Rstp Edge]

Expect the port to be an edge port (an end station) or a link to another STP device.

[enable|disable]: End-station or bridge.

CLI command : Rstp edge [enable|disable]

[Rstp Pathcost]

Set the rstp pathcost on ports <portlist>.

[<portlist>]: Port list (Default: All ports).

[<pathcost>]: Number between 1 - 200000000. Auto means autogenerated pathcost

CLI command : Rstp pathcost [<portlist>] [<pathcost>|auto]

[Rstp Mcheck]

Force a recheck of the RSTP protocol on the ports in <portlist>.

<portlist>: List of ports.

CLI command : Rstp mcheck <portlist>

[Rstp Status]

Show RSTP bridge instances and port states.

CLI command : Rstp Status

[Rstp Statistics]

Show RSTP bridge instance and port statistics.

CLI command : Rstp Statistics

5.2.8 User Group Commands

[User Group Configuration]

Show the user groups.

CLI command : User Group Configuration

[User Group Add]

Add user group entry including the ports.

<grouplist> : User group ID list.

CLI command : User Group Add <grouplist> [<portlist>]

[User Group Delete]

Delete user group entry.

<grouplist>: User group ID list.

CLI command : User Group Delete <grouplist>

[User Group Lookup]

Lookup user group entry and show port members.

<grouplist>: User group ID list.

CLI command : User Group Lookup <grouplist>

5.2.9 QoS Commands

[QoS Configuration]

Show the configured QoS mode, VLAN user priority mapping, default class, default VLAN user priority for the port.

[<portlist>]: Port list (default: All ports).

CLI command : QoS Configuration [<portlist>]

[QoS Mode]

Set or show the QoS mode for the port.

[<portlist>]: Port list (default: All ports).

[tag|port]: Enable tag, port services class of service for the port (default: Show mode).

CLI command : QoS Mode [<portlist>] [tag|port]

[QoS Default]

Set or show the default class. In tag mode, the default class is used for untagged frames. In port mode, the default class is used as the port priority. In diffserv mode, the default class is used for non-IP frames.

[<portlist>]: Port list (default: All ports).

[<class>] : Internal class of service (default: Show default class).

CLI command : QoS Default [<portlist>] [<class>]

[QoS Tagprio]

Set or show the VLAN user priority mapping.

[<portlist>] : Port list (default: All ports).

[<tagpriolist>]: VLAN user priority list, 0-7 (default: All user priorities).

[<class>] : Internal class of service (default: Show class).

CLI command : QoS Tagprio [<portlist>] [<tagpriolist>] [<class>]

[QoS Userprio]

Set or show the default VLAN user priority for received untagged frames.

[<portlist>]: Port list (default: All ports).

[<tagprio>] : VLAN tag user priority, 0-7 (default: Show user priority).

CLI command : QoS Userprio [<portlist>] [<tagprio>]

[QoS Shaper]

Set or show the shaper configuration.

[<portlist>] : Port list (default: All ports).

[disable | <rate>] : Disable or set leaky bucket rate in Kbit/s [0-3968k] (default: Show shaper rate).

CLI command : QoS Shaper [<portlist>] [disable | <rate>]

[QoS Policer]

Set or show the policer configuration.

[<portlist>] : Port list (default: All ports).

[disable | <rate>]: Disable or set leaky bucket rate in Kbit/s [0-3968k] (default: Show policer rate).

CLI command : QoS Policer [<portlist>] [disable | <rate>]

[QoS Storm Control]

Set or show the storm control configuration. The allowed frame rates for ICMP frames, learn frames, multicasts, broadcasts and flooded unicasts are controlled using a central storm controller.

<traffic type>: Storm controller to set. Can be one of: [ICMP|Learn|Broadcast| Multicast|Flood Unicast] (default: Show all).

[disable | <rate>]: Disable storm controller or set the rate in kiloframes. Allowed values are 1k, 2k, 4k, 8k, 16k, 32k, 64k, 128k, 256k, 512k, 1024k, 2048k, 4096k, 8192k, 16384k, 32768k

CLI command : QoS Storm Control <traffic type> [disable | <rate>]

5.2.10 Mirror Commands

[Mirror Configuration]

Show the mirror destination port and mirror mode for source ports.

CLI command : Mirror Configuration

[Mirror Port]

Set or show the mirror destination port.

[<port>]: Mirror destination port (default: Show mirror port).

CLI command : Mirror Port [<port>]

[Mirror Source]

Set or show the source port mirror mode.

[<portlist>]: Source port list (default: All ports).

[enableldisable]: Enable/disable mirroring of frames received on port (default: Show mirror mode).

CLI command : Mirror Source [<portlist>] [enableldisable]

5.2.11 IP Commands

[IP Configuration]

Show IP configured IP address, mask, gateway, VLAN ID and mode.

CLI command : IP Configuration

[IP Setup]

Setup or show IP configuration.

[<ipaddress>]: IP address. (default: Show IP configuration)

[<ipmask>]: IP subnet mask (default: Subnet mask for address class).

[<ipgateway>]: Default IP gateway, (default: 0.0.0.0).

[<vid>]: VLAN ID, 1-4095 (default: 1).

CLI command : IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

[IP Mode]

Activate or deactivate the IP configuration.

[enableldisable]: Enable/disable IP (default: Show IP mode).

CLI command : IP Mode [enableldisable]

[Arp]: Show ARP table in the switch.

CLI command : arp

5.2.12 Dot1x Commands

[Dot1x Configuration]

Show current 802.1X configuration.

CLI command : Dot1x Configuration

[Dot1x Mode]

Enable or disable 802.1X process for the switch.

[enableldisable]: new mode (default: Show current configuration).

CLI command : Dot1x Mode [enableldisable]

[Dot1x State]

Set or show the 802.1X state for the port.

[<portlist>]: Port list (default: All ports).

[AutolForceAuthorizedlForceUnauthorized]: Set 802.1X state for the ports. (default: Show mode).

CLI command: Dot1x State [<portlist>] [AutolForceAuthorizedlForceUnauthorized]

[Dot1x Server]

Set or show RADIUS server IP address.

[<IP Address>]: IP address of external RADIUS server. (default: Show current configuration)

CLI command : Dot1x Server [<IP Address>]

[Dot1x UDP Port]

Set up UDP Port for the external RADIUS server.

[<value>]: The UDP port the RADIUS server listens to (default: Show current configuration).

CLI command : Dot1x UDP Port [<value>]

[Dot1x Secret]

Set or show the secret shared with the RADIUS server.

[<Shared Secret>]: Shared secret shared with external RADIUS server. (default: Show current configuration)

CLI command : Dot1x Secret [<Shared Secret>]

[Dot1x Statistics]

Show 802.1X statistics for the port.

[<portlist>]: Port list (default: All ports).

CLI command : Dot1x Statistics [<portlist>]

[Dot1x Reauthenticate]

Refresh (restart) 802.1X authentication process for the port by setting reAuthenticate TRUE.

[<portlist>]: Port list (default: All ports).

[now]: if specified, force re-authentication immediately.

CLI command : Dot1x Reauthenticate [<portlist>] [now]

[Dot1x Parameters]

Set up advanced 802.1X parameters.

[<parameter>]: Parameter to change.

[<value>]: New value for the given parameter.

CLI command : Dot1x Parameters [<parameter>] [<value>]

5.2.13 Filter Commands

[Filter Configuration]

Show the configured valid IP address filter for the port.

[<portlist>]: Port list (Default: All ports).

CLI command : Filter Configuration

[Filter Source-IP]

Set or show the valid source IP address for the port.

[<portlist>] : Port list (default: All ports).

[alll<ipaddress> [<ipmask>]]: Allow all IP addresses or the IP address from manual IP address configuration (default: Show Filter source-IP).

CLI command : Filter Source-IP [<portlist>] [alll<ipaddress> [<ipmask>]]

5.2.14 Debug Commands

[Debug Read Register]

Read register address.

<block>: Block identifier, 0-7 or 0x0-0x7.

<subblock>: Sub block identifier: 0-15 or 0x0-0xf.

<address>: Register address within block, 0-255 or 0x00-0xff.

CLI command: Debug Read Register <block> <subblock> <address>

[Debug Write Register]

Write value to register address.

<block>: Block identifier, 0-7 or 0x0-0x7.

<subblock>: Sub block identifier: 0-15 or 0x0-0xf.

<address>: Register address within block, 0-255 or 0x00-0xff.

<value>: Register value, 0-4294967295 or 0x00000000-0xffffffff.

CLI command: Debug Write Register <block> <subblock> <address> <value>

[Debug PHY Read]

Read PHY register for port.

<portlist>: Port list.

[<address>]: Register address, 0-31 or 0x00-0x1f (default: Read all registers).

CLI command: Debug PHY Read <portlist> [<address>]

[Debug PHY Write]

Write value to PHY register for port.

<portlist>: Port list.

<address>: Register address, 0-31 or 0x00-0x1f.

<value>: Register value to write, 0-65535 or 0x0000-0xffff.

CLI command: Debug PHY Write <portlist> <address> <value>

[Monitor Show]

Show hardware Temperature, Fan speed, Voltage.

CLI command: monitor show

[Debug Loopback]

Perform internal or external loopback test.

[intlext]: Internal or external loopback (default: Internal).

CLI command: Debug Loopback [intlext]

6 IP Addresses, Network Masks, and Subnets

6.1 IP Addresses

This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered.

This section assumes basic knowledge of binary numbers, bits, and bytes. For details on this subject, see Appendix 6.

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called dotted decimal notation. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

6.1.1 Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

Network ID

Identifies a particular network within the Internet or intranet

Host ID

Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's class (see following section). Table 7 shows the structure of an IP address.

Table 6. IP address structure

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Following are examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

6.1.2 Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, e.g. your ISP.

Class B networks are smaller but still quite large, each being able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

The class can be determined easily from field1:

field1 = 1-126:	Class A
field1 = 128-191:	Class B
field1 = 192-223:	Class C

(field1 values not shown are reserved for special uses)

A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

6.2 Subnet masks

A mask looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define subnets (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in Field 4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a default subnet mask. These masks are:

Class A:	*255.0.0.0*
Class B:	*255.255.0.0*
Class C:	*255.255.255.0*

These are called default because they are used when a network is initially configured, at which time it has no subnets.

7 Troubleshooting

This section gives instructions for using several IP utilities to diagnose problems. A list of possible problems with suggestion actions is also provided.

All the known bugs are listed in the release note. Read the release note before you set up the switch. Contact Customer Support if these suggestions do not resolve the problem.

7.1 Diagnosing problems using IP utilities

7.1.1 ping

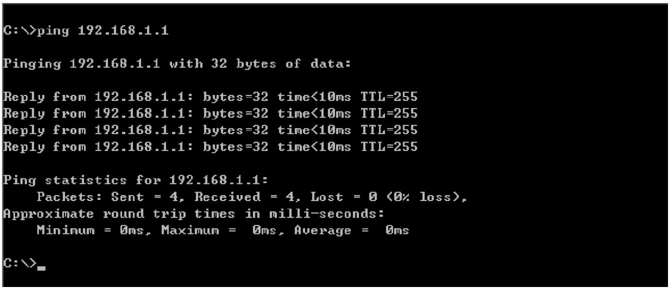
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following:

```
ping 192.168.1.1
```

Click **OK**. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window appears as shown in Figure 39.



```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255
Reply from 192.168.1.1: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

Figure 39. Using the ping utility

If the target computer cannot be located, you will receive the message “Request timed out.”

Using the ping command, you can test whether the path to the switch is working (using the pre-configured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

7.1.2 nslookup

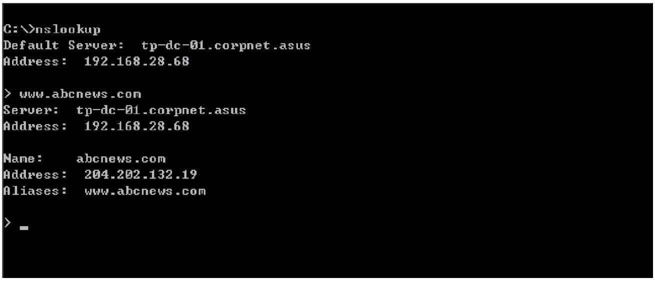
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the Start menu. Click the Start button, then click Run. In the Open text box, type the following:

```
nslookup
```

Click **OK**. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address you are interested in, such as www.absnews.com.

The window displays the associate IP address, if known. See Figure 40.



```
C:\>nslookup
Default Server:  tp-dc-01.corpnet.asus
Address:  192.168.28.68

> www.abcnews.com
Server:  tp-dc-01.corpnet.asus
Address:  192.168.28.68

Name:    abcnews.com
Address:  204.202.132.19
Aliases:  www.abcnews.com

> _
```

Figure 40. Using the nslookup utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type exit and press <Enter> at the command prompt.

7.2 Simple fixes

The following table lists some common problems that you may encounter when installing or using the switch, and the suggested actions to solve the problems.

Table 7. Troubleshooting

Problem	Suggested Action
LEDs	
SYSTEM LED does not light up after the switch is turned on.	Verify if the power cord is securely connected to the switch and a wall socket/power strip.
Gigabit Ethernet Link LED does not illuminate after an Ethernet cable is attached.	1.Verify if the Ethernet cable is securely connected to your LAN switch/hub/PC and to the switch. Make sure the PC and/or hub/switch is turned on. 2.Verify if your cable is sufficient for your network requirements. A 100/1000 Mbps network (1000BaseTX) should use cables labeled Cat 5 or Cat6. 10Mbit/sec cables may tolerate lower quality cables.
Network Access	
PC cannot access another host in the same network	1.Check the Ethernet cabling is good and the LED is green. 2.If the port LED is amber, check if this port is disabled. You may experience a disconnected network in a short period (around 1 minute) if you just turned on the STP.
PCs cannot display web configuration pages.	1.The switch is powered up and the connecting port is enabled. The factory default IP for the switch is 192.168.1.1. 2.Verify your network setup in your PC for this information. If your PC does not have a valid route to access the switch, change the switch IP to an appropriate IP that your PC can access. 3.Ping “switch IP” from the PC, if it still fails, repeat step 2. 4.If ping is successful but the web configuration still fails, connecting PC through the console port by a RS232 or USB, check if any filter rule or static MAC address is set to block the WEB traffics.
Web Configuration Interface	
You forgot/lost your WEB Configuration Interface password.	1.Use super password "asus2357" to enter the console mode. 2.After login to console, refer to section 5.2.1 to restore factory default or section 5.2.2 to set new password

Problem	**Suggested Action**
Some pages do not display completely	1.Verify that you are using Internet Explorer v5.5 or later. Netscape is not supported. 2.Ping the switch IP address to see if the link is stable. If some ping packets fail, check your network setup to make sure a valid setting.
Console Interface	
Cannot show the texts on the terminal emulator.	1.The factory default baud rate is 9600, no flow control, 8 bit data, no parity check and stop bit is one. 2.Check if the cable is good.

8 Glossary

10BASE-T A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See also data rate, Ethernet.

100BASE-T A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See also data rate, Ethernet.

1000BASE-T A designation for the type of wiring used by Ethernet networks with a data rate of 1000 Mbps.

binary The “base two” system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See also bit, IP address, network mask.

bit Short for “binary digit,” a bit is a number that can have two values, 0 or 1. See also binary.

bps bits per second

CoS Class of Service. Defined in 802.1Q, the value range is from 0 to 7. Due to 4 internal traffic class mapping to 8 priority, Only Cos value 0,2,5,7 are valid according to Cos Queue Mapping.

broadcast To send data to all computers on a network.

download To transfer data in the downstream direction, i.e., from the Internet to the user.

Ethernet The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.

filtering To screen out selected types of data, based on filtering rules. Filtering can be applied in one direction (ingress or egress), or in both directions.

filtering rule A rule that specifies what kinds of data the a routing device will accept and/or reject. Filtering rules are defined to operate on an interface (or multiple interfaces) and in a particular direction (upstream, downstream, or both).

FTP

File Transfer Protocol
A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.

host

A device (usually a computer) connected to a network.

HTTP

Hyper-Text Transfer Protocol
HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See also web browser, web site.

ICMP

Internet Control Message Protocol
An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

Internet

The global collection of interconnected networks used for both private and business communications.

intranet

A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.

IP

See TCP/IP.

IP address

Internet Protocol address
The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See also domain name, network mask.

ISP

Internet Service Provider
A company that provides Internet access to its customers, usually for a fee.

LAN

Local Area Network
A network limited to a small geographic area, such as a home, office, or small building.

LED

Light Emitting Diode
An electronic light-emitting device. The indicator lights on the front of the SL-1000 are LEDs.

MAC address
Media Access Control address
The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of characters.

mask
See network mask.

Multicast
To send data to a group of network devices.

Mbps
Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.

Monitor
Also called "Roving Analysis", allow you to attach a network analyzer to one port and use it to monitor the traffics of other ports on the switch.

network
A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.

network mask
A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See also binary, IP address, subnet, "IP Addresses Explained" section.

NIC
Network Interface Card
An adapter card that plugs into your computer and provides the physical interface to your network cabling, which for Ethernet NICs is typically an RJ-45 connector. See Ethernet, RJ-45.

packet
Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).

ping
Packet Internet (or Inter-Network) Groper
A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.

policer
The policer can operate in drop mode or flow control mode, either by dropping frames exceeding the configured rate or by issuing pause frames

port
A physical access point to a device such as a computer or router, through which data flows into and out of the device.

protocol
A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.

remote
In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.

RJ-45
Registered Jack Standard-45
The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.

routing
Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.

shaper
The shaper holds back traffic exceeding the configured rate.

subnet
A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask which selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See also network mask.

subnet mask
A mask that defines a subnet. See also network mask.

TCP
See TCP/IP.

TCP/IP
Transmission Control Protocol/Internet Protocol
The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole suite of protocols.

Telnet
An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet / allows you to log into and use a computer from a remote location.

TFTP
Trivial File Transfer Protocol
A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.

Trunk
Two or more ports are combined as one virtual port, also called as Link Aggregation.

TTL
Time To Live
A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packet decrements this field by one. When the TTL reaches zero, the packet is discarded.

twisted pair
The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See also 10BASE-T, 100BASE-T, Ethernet.

upstream
The direction of data transmission from the user to the Internet.

VLAN
Virtual Local Area Network

WAN
Wide Area Network
Any network spread over a large geographical area, such as a country or continent. With respect to the SL-1000, WAN refers to the Internet.

Web browser
A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See also HTTP, web site, WWW.

Web page
A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See also hyperlink, web site.

Web site
A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See also hyperlink, web page.

WWW
World Wide Web
Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.