



# **GigaX 2008EX**

Layer 2 Managed Switch

**User Manual**

## **E2328**

First Edition V1

Nov 2005

Copyright © 2005 ASUSTeK COMPUTER INC. All Rights Reserved. No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK COMPUTER INC. (ASUS).

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or 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](http://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](mailto:tmd1@asus.com)  
Web Site: [usa.asus.com](http://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](mailto: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](mailto: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](http://www.asuscom.de/de/support) (for online support)  
Web Site: [www.asuscom.de](http://www.asuscom.de)

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	L2 managed features .....	1
1.2	Conventions used in this document .....	2
1.2.1	Notations .....	2
1.2.2	Typography.....	2
1.2.3	Symbols.....	2
<b>2</b>	<b>Getting to know the GigaX2008EX.....</b>	<b>3</b>
2.1	Package contents .....	3
2.2	Front Panel.....	4
2.3	Rear Panel .....	5
2.4	Technical specifications.....	5
<b>3</b>	<b>Quick start guide .....</b>	<b>6</b>
3.1	Part 1 — Install the hardware .....	6
3.1.1	Install the switch on a flat surface.....	6
3.1.2	Mount the switch on a rack.....	6
3.2	Part 2 — Set up the switch .....	6
3.2.1	Connect the console port.....	6
3.2.2	Connect to the computers or a LAN .....	7
3.2.3	Attach the power adapter .....	7
3.3	Part 3 — Basic switch setting for management.....	8
3.3.1	Setting up through the console port.....	8
3.3.2	Setting up through the Web interface .....	9
<b>4</b>	<b>Management with the Web Interface .....</b>	<b>11</b>
4.1	Log into Web user interface .....	11
4.2	Functional layout.....	12
4.2.1	Menu navigation tips.....	13
4.2.2	Commonly used buttons and icons .....	14

4.3	System Pages .....	14
4.3.1	Management.....	14
4.3.2	IP setup .....	15
4.3.3	Administration .....	15
4.3.4	Reboot .....	16
4.3.5	Firmware Upgrade.....	16
4.4	Physical Interface .....	17
4.5	Bridge .....	18
4.5.1	Link Aggregation.....	18
4.5.2	Mirroring .....	19
4.5.3	Traffic Control .....	20
4.5.4	Dynamic Addresses.....	20
4.5.5	Static Addresses.....	21
4.5.6	Tagged VLAN .....	22
4.5.7	Default Port VLAN and CoS .....	23
4.5.8	CoS Queue Mapping.....	23
4.6	SNMP.....	25
4.6.1	Community Table.....	25
4.6.2	Host Table.....	25
4.6.3	Trap Setting .....	26
4.7	Security .....	27
4.7.1	Port Access Control.....	27
4.7.2	Dial-In User.....	28
4.7.3	RADIUS.....	29
4.8	Power over Ethernet (PoE) .....	29
4.9	Cable diagnosis .....	30
4.10	Statistics Chart.....	31
4.10.1	Traffic Comparison .....	31
4.10.2	Error Group .....	32

4.10.3	Historical Status.....	32
4.11	Save Configuration .....	33
<b>5</b>	<b>Console Interface .....</b>	<b>34</b>
5.1	Power On Self Test .....	34
5.1.1	Boot ROM Command Mode .....	35
5.1.2	Boot ROM Commands .....	35
5.2	Login and Logout.....	36
5.3	CLI Commands .....	36
5.3.1	System Commands .....	37
5.3.2	Physical Interface Commands.....	39
5.3.3	Bridge Commands.....	39
5.3.4	SNMP .....	43
5.3.5	Security Commands .....	45
5.3.6	PoE.....	47
5.4	Miscellaneous Commands .....	49
<b>6</b>	<b>IP Addresses, Network Masks, and Subnets .....</b>	<b>50</b>
6.1	IP Addresses .....	50
6.1.1	Structure of an IP address.....	50
6.1.2	Network classes .....	51
6.2	Subnet masks .....	51
<b>7</b>	<b>Troubleshooting .....</b>	<b>53</b>
7.1	Diagnosing problems using IP utilities .....	53
7.1.1	ping.....	53
7.1.2	nslookup.....	54
7.2	Simple fixes.....	55
<b>8</b>	<b>Glossary .....</b>	<b>57</b>

## List of figures

Figure 1. GigaX2008EX L2 managed switch package contents .....	3
Figure 2. Front panel .....	4
Figure 3. Rear panel.....	5
Figure 4. Overview of hardware connections .....	8
Figure 5. Login and IP setup screen.....	10
Figure 6. Login screen.....	10
Figure 7. IP setup .....	10
Figure 8. Configuration manager login screen .....	11
Figure 9. Home page.....	12
Figure 10. Top frame .....	12
Figure 11. Expanded menu list.....	13
Figure 12. Management .....	15
Figure 13. IP Setup.....	15
Figure 14. Administration.....	16
Figure 15. Reboot.....	16
Figure 16. Firmware upgrade .....	17
Figure 17. Physical interface .....	17
Figure 18. Link aggregation.....	19
Figure 19. Mirroring page .....	19
Figure 20. Traffic control.....	20
Figure 21. Dynamic address .....	20
Figure 22. Static address .....	21
Figure 23. Tagged VLAN .....	22
Figure 24. Default port VLAN and CoS .....	23
Figure 25. Cos queue mapping .....	24
Figure 26. Community table .....	25
Figure 27. Host table .....	25



Figure 28. Trap setting .....	26
Figure 29. Port access control.....	28
Figure 30. Dial-In user .....	28
Figure 31. RADIUS .....	29
Figure 32. Power over Ethernet .....	30
Figure 33. Cable diagnosis.....	31
Figure 34. Traffic comparison.....	32
Figure 35. Error group .....	32
Figure 36. Historical status.....	32
Figure 37. Save configuration .....	33
Figure 38. CLI interface.....	34
Figure 39. Boot ROM command mode.....	35
Figure 40. System commands.....	37
Figure 41. Using the ping utility .....	53
Figure 42. Using the nslookup utility .....	54

## List of tables

Table 1. Front panel labels and LEDs .....	4
Table 2. Rear panel labels.....	5
Table 3. Technical specifications .....	5
Table 4. LED indicators .....	8
Table 5. Port color description .....	13
Table 6. Commonly used buttons and icons.....	14
Table 7. Boot ROM commands .....	35
Table 8. IP address structure.....	50
Table 9. Troubleshooting .....	55



# 1 Introduction

Congratulations on becoming the owner of the ASUS GigaX2008EX L2 managed 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 GigaX2008EX, and how to customize its configuration to get the most out of this product.

## 1.1 L2 managed features

---

- Eight 10/100 Base-TX auto-sensing Fast Ethernet ports
- One 10/100/1000Base-T auto-sensing gigabit Ethernet switching port
- One small form factor (SFP) Gigabit interface converter (GBIC) slots
- Automatic MDI/MDIX support for 10/100Base-TX and 10/100/1000Base-T ports
- 8K MAC address cache with hardware-assisted aging
- 802.3x flow control
- 802.1Q-based tagged VLAN, up to 256 VLANs
- 802.1p class of service, 4 queues per port
- 802.3ad link aggregation (manual), up to 15 trunk groups
- Port Mirroring
- 802.1x port-based network access control
- RADIUS remote authentication dial-in user service
- RMON: support 4 groups (1, 2, 3, 9)
- SNMP v1, v2
- MIB-II
- Enterprise MIB for PSU, fan, and system temperature, voltage
- Telnet remote login
- FTP for firmware update and configuration backup
- Syslog.
- Command Line Interpreter through console and telnet
- Web GUI
- LEDs for port link status
- LEDs for system and fan status

## 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 GigaX 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

- **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.



**Definition:** 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.

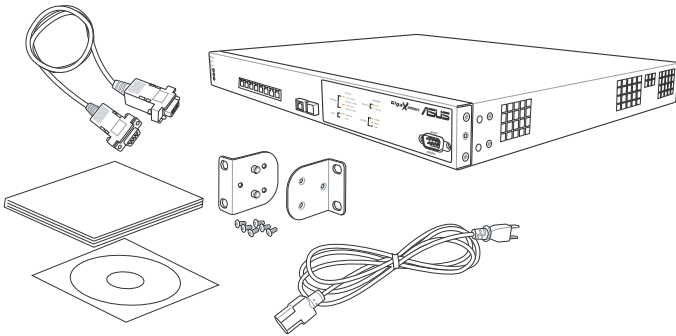
## **2 Getting to know the GigaX2008EX**

### **2.1 Package contents**

---

The GigaX2008EX switch package comes with the following items:

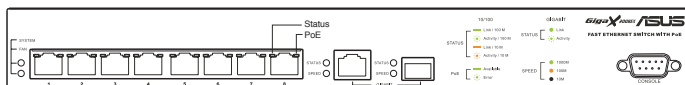
- GigaX2008EX (10-port) L2 managed switch
- AC Power cord
- Null modem cable for console interface (DB9)
- Rack installation kit (two brackets with six #6-32 screws)
- Installation CD-ROM
- User Manual
- Quick installation guide



***Figure 1. GigaX2008EX L2 managed switch package contents***

## 2.2 Front Panel

The front panel includes eight 10/100Base-TX RJ-45 port, one 10/100/1000Base-T port, one SFP GBIC slot and LED indicators that show the system, fan, and port status.



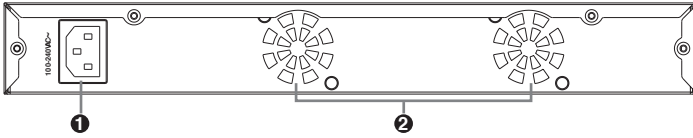
**Figure 2. Front panel**

**Table 1. Front panel labels and LEDs**

Label	Color	Status	Description
SYSTEM	Green	ON	Unit is powered on
		Flashing	Self-test, initiating, or downloading
	Amber	ON	Abnormal temperature or voltage
		OFF	No power
FAN	Green	ON	The fan is working properly
	Amber	ON	The fan stops
PoE	Green	ON	PD (Powered Devices) is connected and ready to provide power
		Flashing	PoE is off due to a fault on the port
	OFF		PD is not connected or not a valid power device
10/100 port status	Green	ON	Link is present at 100Mbps
		Flashing	Transmitting data
	Amber	ON	Link is present at 10Mbps
		Flashing	Transmitting data
	OFF		No Ethernet link
GIGABIT port status	Green	ON	Link is present
		Flashing	Transmitting data
	OFF		No Ethernet link
GIGABIT port speed	Green	ON	1000Mbps (RJ-45 or SFP)
	Amber	ON	100Mbps (RJ-45)
	OFF		10Mbps (RJ-45)

## 2.3 Rear Panel

The switch rear panel consists of the fan modules and a power connector.



**Figure 3. 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 GigaX2008EX working environment. Refer also to the GigaX2008EX Installation Guide.

Part 1 shows you how to install the GigaX2008EX 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 GigaX2008EX.

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 — Install the hardware**

---

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

#### **3.1.1 Install 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 Mount 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 — Set up the switch**

---

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

#### **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

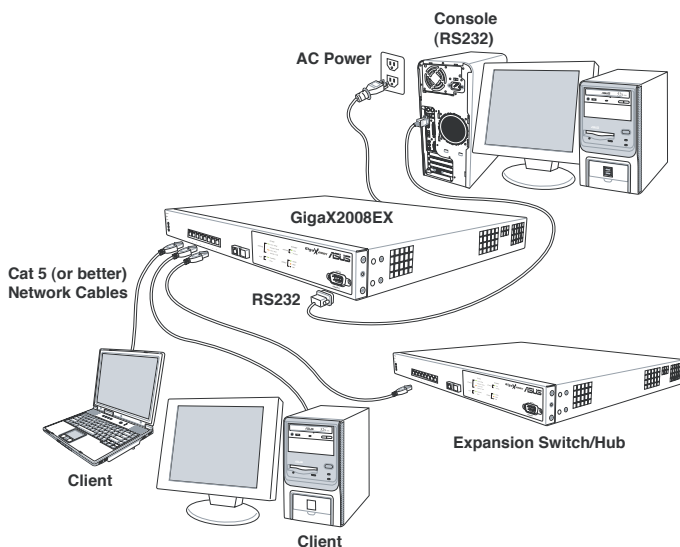
You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.



*Use a twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port. Otherwise, the link speed can not 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 4. 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	10/100 port STATUS	Solid green indicates that link is present on the port; flashing means the attached device is sending or receiving data
3	10/100 port PoE	Solid green indicates that a Power Device (PD) is connected
4	GIGABIT port STATUS	Solid green indicates that link is present; flashing means data is being transmitted; if the LED is off, no device is connected
5	GIGABIT port SPEED	Solid green means the link speed is 1000Mbps, solid amber means 100Mbps; if the LED is off, the port speed is 10Mbps
6	FAN	Solid green indicates that the system fan works properly

### **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<sup>®</sup>-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 panel of the switch. This port is a male DB-9 connector, implemented as 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 9600
  - c) Set the data format to no parity, 8 data bits and 1 stop bit
  - d) No flow control
  - e) Set VT1000 for emulation mode
3. After setting up the terminal, you can see the prompt “(ASUS)%” on the terminal.
4. Type “login” to access the command line interface. The default user name is

“admin”. Skip the password by pressing <Enter>.



*You can change the password at any time through CLI (see section 5.3.1). To protect your switch from unauthorized access, you must change the default password as soon as possible.*

5. Follow these steps to assign an IP address to the switch:

- a) Type “net interface ip sw0 <your ip address> <your network mask>”. For example, if your switch IP is 192.168.10.1 and the network mask is 255.255.255.0. Then you should type “net interface ip sw0 192.168.10.1 255.255.255.0”.
- b) If the switch has to be managed across networks, then a default gateway or a static route entry is required. Type “net route static add 0.0.0.0 <your network gateway IP> 0.0.0.0 1” as your default route entry, as shown in Figure 5.

```
(Rtus)X login
user name: admin
password: ****
user 'admin' logged in
(Rtus)X net interface ip sw0 192.168.10.1 255.255.255.0
IP address set successfully
(Rtus)X net route static add 0.0.0.0 192.168.10.254 0.0.0.0 1
Route added successfully
Specific route is added successfully
(Rtus)X _
```

*Figure 5. Login and IP setup screen*

### 3.3.2 Setting up through the Web interface

To successfully connect your PC to the switch, your PC must have a valid IP in your network. Contact your network administrator to obtain a valid IP for the switch. If you wish to change the default IP address of the switch, follow section 3.3.1 to change the IP address.

1. It is not necessary to login Web interface at the first time to use Web interface because the default configuration for Web access authentication is disabled. To secure the system configuration, please enable the authentication function at the **Administration** page under **System** category. Skip step 2 if the authentication is disabled.
2. 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 6.



**Figure 6. Login screen**

Enter your user name and password, and then click **OK** to enter the Configuration Manager. Use the following defaults the first time you log into this interface:

Default User Name:      admin

Default Password:      (no password)



*You can change the password at any time (see section 5.3.1 System Commands).*

3. To setup a new IP address, click **System**, then **IP Setup** (see Figure 7). Fill in the IP address, network mask and default gateway, then click **OK**.
4. 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.
5. To enable authentication for Web access, click **Administration** on the menu list, then select **Enabled** to start the protection.

A login window appears immediately after you click **OK**.



**Figure 7. 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.

### 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 8



**Figure 8. Configuration manager login screen**



*Login is not required if you do not enable Web authentication access (see 3.3.2)"*

2. Enter your user name and password, then click **OK**.

Use the following defaults the first time you log into the program. You can change the password at any time through CLI interface (see section 5.3.1)

Default User Name: admin

Default Password:<no password>

The home page appears each time you log into the program.(See Figures 9).



Figure 9. Home page

## 4.2 Functional layout

Typical web page consists of three separate frames. The top frame has a switch logo and front panel as shown in Figures 10. This frame remains on the top of the browser window all the times and updates the LED status periodically. See Table 4 for the LED definitions. See Table 5 for the color status description.



Figure 10. Top frame

Table 5. Port color description

Port Color	Description
Green	Ethernet link is established at 100Mbps
Black	No Ethernet link
Amber	Ethernet link is established at 10Mbps

Clicking on the port icon of the switch displays the port configuration in the lower right frame.

The left frame, a menu frame as shown in Figure 11, contains all the features available for switch configuration. These features are grouped into categories, e.g. System, Bridge, etc. You can click on any of these to display a specific configuration page.




**Figure 11. Expanded menu list**

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

### **4.2.1 Menu navigation tips**






- To expand a group of related menus, click on the corresponding group name. The ► sign will change to ▼ after expansion.

- To contract a group of related menus: click on the corresponding group name. The  will appear next to the group name.
- To open a specific configuration page, click on the desired menu item.

## 4.2.2 Commonly used buttons and icons

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

**Table 6. Commonly used buttons and icons**

Button/Icon	Function
	Stores any changes you have made on the current page
	Adds the existing configuration to the system, e.g. a static MAC address rule
	Modifies an existing entry
	Deletes the selected item, e.g. a static route and etc.
	Re-displays the current page with updated statistics or settings.

## 4.3 System Pages

---

System pages include management, IP setup, administration, reboot, and firmware update function.

### 4.3.1 Management

The Management page contains the following information:

**Model Name:** product name

**MAC Address:** switch MAC address

**System Name:** user assigned name to identify the system (editable)

**System Contact** (editable)

**System Location** (editable)

To save any changes and make it effective immediately, click **OK**. Use **Reload** to refresh the setting, as shown in Figure 12.





*Figure 12. Management*

### 4.3.2 IP Setup

The switch supports IP assignment. The IP Setup page contains the following editable information:

**VLAN ID:** Specify a VLAN ID to system management interface. It is necessary to be within the same VLAN for management usages.

**IP Address:** assign a static IP address to the switch management interface.

**Network Mask**

**Default Gateway**

To save any changes and make it effective immediately, click **OK**. Use **Reload** to refresh the setting, as shown in Figure 13.



*Figure 13. IP setup*

### 4.3.3 Administration

The Administration page allows you enable or disable the authentication for web user by password protection. The default setting for web access does not require any authentication.

To save any changes and make it effective immediately, click **OK**. Use **Reload** to refresh the setting, as shown in Figure 14. When you enable the password protection, you have to login again immediately.



*You can change the password at any time through the CLI interface.*



**Figure 14. Administration**

### 4.3.4 Reboot

The Reboot page contains a **Reboot** button. Click the button to reboot the system.



*Rebooting the system stops the network traffic and terminates the Web interface connection.*



**Figure 15. Reboot**

### 4.3.5 Firmware Upgrade

The Firmware page contains the following information:

**Hardware Version:** shows the hardware revision number.

**Boot ROM Version:** shows the version of the boot code

**Firmware Version:** shows the current running firmware version. This number will be updated after the firmware update.

Enter the firmware location into the firmware space directly, or click **Browse...** to choose the file name of the firmware from prompt window. Click **Upload** to update the switch firmware. See Figure 16 for reference.



*Click the upload button to load the assigned firmware to the switch. After a successful firmware update, reboot the system. You have to re-login to Web interface again*

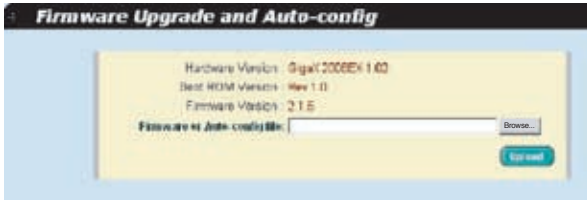


Figure 16. Firmware upgrade

## 4.4 Physical Interface

The Physical Interface displays the Ethernet port status in real time. You can configure the port in following fields:

**Port:** select the port to configure

**Admin:** disable/enable the port

**Mode:** set the speed and duplex mode

**Flow Control:** enable/disable 802.3x flow control mechanism

**Port Status Window:** displays the following information for each port

- Link status:** the link speed and duplex for an existing link, otherwise link is down
- Admin:** the setting value to disable or enable the port
- Mode:** the setting value for link speed and duplex mode
- Flow Control:** the setting value to enable or disable 802.3x flow control mechanism

Select the corresponding port number and configure the port setting, then click on the **Modify** button. The field you change will update the content of the display window. However, the new settings do not take effect until the "Save Configuration" is executed.

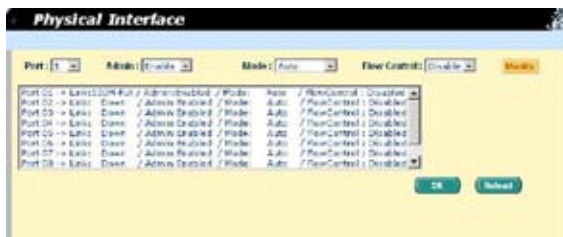


Figure 17. Physical interface

## 4.5 Bridge

---

The Bridge page group contains most layer 2 configurations, like link aggregation, mirroring etc..

### 4.5.1 Link Aggregation

The page configures the link aggregation group (port trunking). The switch can have 15 link aggregation groups.

**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.

**Name:** the group name.

**Trunk ID:** a number to identify the trunk group besides the group name.

**Remove Trunk:** Remove the selected trunk.

**Port Icons:** these port icons are listed in a way like the front panel. You have to click on the icon the select the group members. The port can be removed from the group by clicking the selected port again.

Click **OK** to make the setting send to the switch (HTTP server). Click **Reload** to refresh the settings to current value. To make the configuration effective, go to **Save Configuration** page, then click **Save**.

You have to check the runtime link speed and duplex mode to make sure the trunk is physically active. Go to Physical Interface and check the link mode in the runtime status window for the trunk ports. 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.*

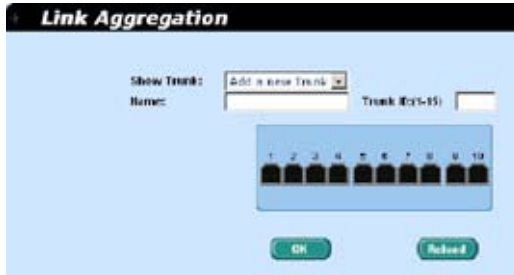


Figure 18. Link aggregation

## 4.5.2 Mirroring

Mirroring, together with a network traffic analyzer, helps you monitor network traffics. You can monitor the selected ports for egress or ingress packets.

**Mirror Mode:** Enables or disables the mirror function for the selected group.

**Monitor Port:** Receives the copies of all the traffics in the selected mirrored ports.



*The monitor port can not belong to any link aggregation group.*

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

*The monitored egress packets will be untagged*

Click **OK** to make the setting send to the switch (HTTP server). Click **Reload** to refresh the settings to current value.

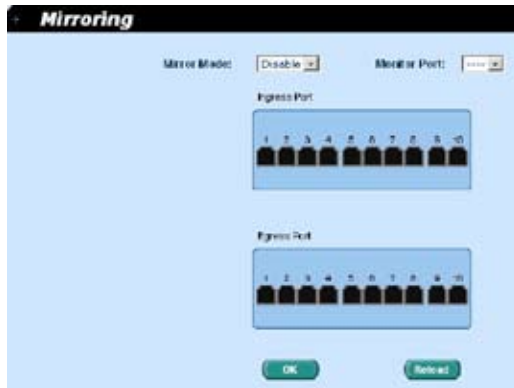


Figure 19. Mirroring page

### 4.5.3 Traffic Control

Traffic control prevents the switch bandwidth from flooding packets including broadcast packets, multicast packets. The limit number is a threshold to limit the total number of the selected type packets. For example, if broadcast/ multicast is enabled, the traffic amount of each type will not exceed the limit value. Click **OK** to save the new configuration. To make the configuration effective, go to **Save Configuration** page, then click **Save**.



Figure 20. Traffic control

### 4.5.4 Dynamic Addresses

This page displays the result of dynamic MAC address lookup by port, VLAN ID, or specified MAC address. The dynamic address is the MAC address learned by switch, it will age out from the address table if the address is not learned again during the age time. User can set the age time by entering a valid number from 15 to 3825 in seconds. Then click on **OK** to save the new age value. To make the configuration effective, please go to **Save Configuration** page, then click on **Save**.

You can look up MAC addresses by checking the port, VLAN ID, or/and MAC address, then click on **Query**. The address window will display the result of the query.



Figure 21. Dynamic address

### 4.5.5 Static Addresses

You can add a MAC address into the switch address table. The MAC address added by this way will not age out from the address table. We call it static address.

**MAC Address:** enter the MAC address

**VLAN ID:** enter the VLAN ID that the MAC belongs

**Port Selection:** select the port which the MAC belongs

Click on **Add** when you create a new static MAC address by the above information. Then you will see the new added entry shows in the address window. In one page, 15 entries can be displayed in the address window. When you create more than 15 entries, the new added entries will display in the next page. You can click on First, Previous, Next, or Last to go through the pages of static MAC address, or input the page number and then click on Go. You can remove the existed address by selecting the entry with the mouse, then clicking on **Remove**. The **Modify** button updates the existed MAC address entries. You can look up a static MAC addresses by input the MAC address and VLAN ID, then click on **Query**. The address window will mark the result of the query. Click **OK** to save effective. Click **Reload** to refresh the settings to current value. To make the configuration effective, please go to **save configuration** page, then click **Save**.



Figure 22. Static address

## 4.5.6 Tagged VLAN

You can set up to 256 VLAN groups and show VLAN group in this page. There is a default VLAN created by the switch. It cannot be removed at all. This feature prevents the switch from malfunctions. You can remove any existed VLAN except the default VLAN.

You can assign the port to be a tagged port or an untagged port by toggling the port button. There are three types of button displays:

**“U” type:** untagged port that will remove VLAN tags from the transmitted packets.

**“T” type:** All packets transmitted from this port will be tagged.

**“Blank” type:** This port is not a member of the VLAN group.

If one untagged port belongs to two or more VLAN groups at the same time, it will confuse the switch and cause flooding traffics. To prevent it, the switch only allows one untagged port belongs to one VLAN at the same time. That is, the untagged port belongs to the VLAN group which is called “PVID” and configured in the “Default Port VLAN & CoS” page. If you want to assign an untagged port from one VLAN to another, you have to remove it from the original VLAN, or change it to be tagged in the original VLAN first.

**Show VLAN:** select the existed VLAN to display or select “Add a new VLAN” to create a new VLAN group

**Name:** the VLAN name

**VLAN ID:** this field requires user to enter the VLAN ID when a new VLAN is created

**Remove VLAN:** Remove a existed VLAN. This field disappears in VLAN creation page.

Click on **OK** to save the configuration. To make the configuration effective, go to **Save Configuration** page, then click on **Save**.



*Figure 23. Tagged VLAN*



### 4.5.7 Default Port VLAN and CoS

Some VLAN tag related field settings for each port are included in this page. It includes:

**Port:** select the port to configure

**PVID:** port-based VLAN ID. Every untagged packet received from this port will be tagged with this VLAN group ID

**CoS (Class of Service) value:** every untagged packet received from this port will be assigned to this CoS in the VLAN tagged.

Click on **Modify** to change the content in the port list window. Click on **OK** to save the configuration. To make the configuration effective, go to “Save Configuration” page, then click **Save**.



Figure 24. Default port VLAN and CoS

### 4.5.8 CoS Queue Mapping

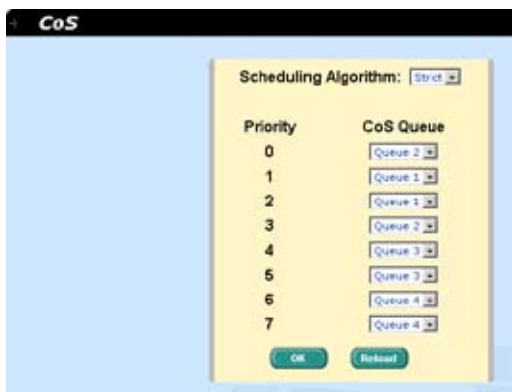
The switch supports 4 egress queues for each port. For each queue, you can specify the scheduling types as follows:

**Strict priority scheduling:** each CoS value can map into one of the four queues. The queue 4 has the highest priority to transmit the packets. And packets in the low-priority queue do not transmit until all the high-priority queues become empty. In Strict priority scheduling, weight settings are always zero.

**Weighted round-robin (WRR) scheduling:** WRR scheduling requires you to specify a number that indicates the importance (weight) of the queue relative to other CoS queues. WRR scheduling prevents the low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduling transmits some packets from each queue in turn. The number of packets it sends corresponds to the relative importance of the queue. For example, if Queue1 has a weight of 1 and Queue2 has a weight of 2, one

packet is sent from the Queue1 for every two that are sent from the Queue2. By using this scheduling, low-priority queues have the opportunity to send packets even through the high-priority queues are not empty. The fixed weights are 1,2,4,8.

Click **OK** to save the configuration. Click on **Reload** to refresh the settings to current value. To make the configuration effective, go to **Save Configuration** page, then click **Save**.



**Figure 25. Cos queue mapping**

## 4.6 SNMP

This group offers the SNMP configuration including Community Table, Host Table, and Trap Setting.

### 4.6.1 Community Table

You can type different community names and specify whether the community has the privilege to make a setting (write access) by checking the box. Click **OK** to save the configuration permanently or **Reload** to refresh the page.

Community Name	Set
private	<input checked="" type="checkbox"/>
public	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>
	<input type="checkbox"/>

OK Reload

Figure 26. Community table

### 4.6.2 Host Table

This page links host IP address to the community name that is entered in Community Table page. Type an IP address and select the community name from the drop-down list. Click **OK** to save the configuration permanently or **Reload** to refresh the page.

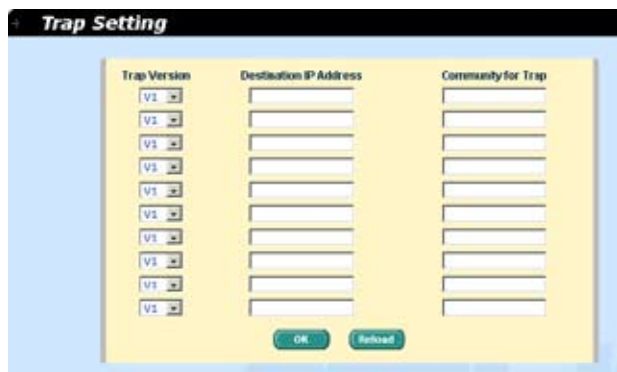
Host IP Address	Community
172.16.1.1	private
192.168.1.1	private
192.168.1.2	private
	private
	private
	private
	private
	private
	private
	private

OK Reload

Figure 27. Host table

### 4.6.3 Trap Setting

By setting trap destination IP addresses and community names, you can enable SNMP trap function to send trap packets in different versions(v1 or v2). Click **OK** to save the configuration permanently or **Reload** to refresh the page.



The image shows a web-based configuration window titled "Trap Setting". It contains three columns: "Trap Version", "Destination IP Address", and "Community for Trap". Each column has eight rows of input fields. The "Trap Version" column has a dropdown menu in each row, all currently set to "V1". The "Destination IP Address" and "Community for Trap" columns have empty text input fields. At the bottom of the window are two buttons: "OK" and "Reload".

Trap Version	Destination IP Address	Community for Trap
V1		
V1		
V1		
V1		
V1		
V1		
V1		
V1		

OK Reload

Figure 28. Trap setting

## 4.7 Security

---

The switch has the 802.1x port-based security feature. Only authorized hosts are allowed to access the switch port. Traffic is blocked for hosts failed to authenticate themselves. The authentication service is provided by a RADIUS server or the local database in the switch.

The switch also supports dynamic VALN assignment through 802.1x authentication process. The VLAN information for the users/ports should be configured in the authentication server properly before enabling this feature.

### 4.7.1 Port Access Control

Port Access Control is used to configure various 802.1x parameters. 802.1x uses either RADIUS server or local database to authenticate port users.

The first part is the Bridge (Global) settings:

**Reauthentication:** Once enabled, the switch will try to authenticate the port user again when the re-authentication time is up.

**Reauthentication Time:** If 'Reauthentication' is enabled, this is the interval for the switch to re-send authentication request to the port user.(see above)

**Authentication Method:** RADIUS or Local database can be used to authenticate the port user.

**Quiet Period:** If authentication failed either from RADIUS or local database, the switch waits upon this time period before sending another authentication request to the port user.

**Retransmission Time:** If the port user failed to respond to authentication request from the switch, the switch waits upon this time period before sending another authentication request to the port user.

**Max Reauthentication Attempts:** Retry count if the port user failed to respond to authentication requests from the switch.

The second part is the port settings. Please click **Modify** when you have finished the modifications.

**Port:** Specify which port to be configured.

**Multi-host:** If enabled, all hosts connected to the selected port are allowed to use the port if one of the hosts passed the authentication. If disabled, only one host among other hosts passed the authentication is allowed to use the port.

**Authentication Control:** If 'force authorized' is selected, the selected port is forced to be authorized. Thus, traffic from all hosts is allowed to pass. Otherwise, if 'force unauthorized' is selected, the selected port is blocked and no traffic can

go through. If 'Auto' is selected, the behavior of the selected port is controlled by 802.1x protocol. All ports should be set to 'Auto' under normal conditions.

**Guest VLAN:** Specify a guest VLAN to clients that are not 802.1x-capable.

Click **OK** to make the settings effective permanently. Click **Reload** to refresh the settings to current value.



Figure 29. Port Access Control

## 4.7.2 Dial-In User

Dial-in User is used to define users in the local database of the switch.

**User Name:** New user name.

**Password:** Password for the new user.

**Confirm Password:** Enter the password again.

**Dynamic VLAN:** Specify the VLAN ID assigned to the 802.1x- authenticated clients.

Please click **Add** to add the new user. Click **Modify** when you have finished the modifications. Click **Remove** when you want to remove the selected user. Click **OK** to make the settings effective permanently. Click **Reload** to refresh the settings to current value.



Figure 30. Dial-In user

### 4.7.3 RADIUS

In order to use external RADIUS server, the following parameters are required to be setup:

**Authentication Server IP:** The IP address of the RADIUS server.

**Authentication Server Port:** The port number for the RADIUS server is listening to.

**Authentication Server Key:** The key is used for communications between GigaX and the RADIUS server.

**Confirm Authentication Key:** Re-type the key entered above.



*The VLAN of the RADIUS server connected to the switch must be the same as the VLAN of the system management interface.*

Please click **OK** to make the settings permanent. Click **Reload** to refresh the settings to current value.

Figure 31. RADIUS

## 4.8 Power over Ethernet (PoE)

PoE provides a way to distribute low-voltage power across the network using existing copper Ethernet cable to an endpoint PD (Powered Device). This centralized, reliable source of power allows network devices such as IP telephones, wireless LAN access points, surveillance cameras, and other embedded appliances to operate without additional power adapters or AC outlets. You can configure the port power as follows:

**Port:** select the port to configure

**Port State:** enable/disable the port power

**Priority:** set the port priority. Low numeric value indicates a high priority. Assigning the same priority to different ports will arrange the ports according to their physical order, with the lower numeric port having the highest priority. The valid value is from 0 to 47.

**Port Status Window:** displays the following information for each port

a) **Link status**: whether the PD is connected or not

b) **Priority**: display the port power priority setting

Select the corresponding port number and configure the port power setting, then click on the **Modify** button. The field you change will update the content of the display window. However, the new settings do not take effect until the **Save Configuration** is executed.

Click **OK** to make the settings effective permanently. Click **Reload** to refresh the settings to current value. To make the configuration effective, please go to **Save Configuration** page, and then click on **Save**.

You can look up the detailed port power information by selecting the port, then click **Query**. The port diagnostic window will display the result of the query.



Figure 32. Power over Ethernet

## 4.9 Cable diagnosis

The major function of Cable Diagnosis is to detect cable fault (open or short) and report the estimated fault location. Moreover, Cable Diagnosis can also detect PHY type (100M, 1000M or 10000M) as well as estimated cable length of normal cable. Cable length estimation only supports Giga speed mode.

Just select a port number and click **Go**. Test result shall be displayed accordingly.



*When you enable the Cable Diagnosis on a port, the connection of this port will be disconnected during the diagnosis.*





Figure 33. Cable diagnosis

## 4.10 Statistics Chart

The Statistics Chart pages provide network flow in different charts. You can specify the period time to refresh the chart. You can monitor the network traffic amount in different graphic chart by these pages. Most MIB-II counters are displayed in these charts.

Click **Auto Refresh** to set the period for retrieving new data from the switch. You can differentiate the statistics or ports by selecting **Color**. Finally, click on **Draw** to let the browser to draw the graphic chart. Each new Draw will reset the statistics display.

### 4.10.1 Traffic Comparison

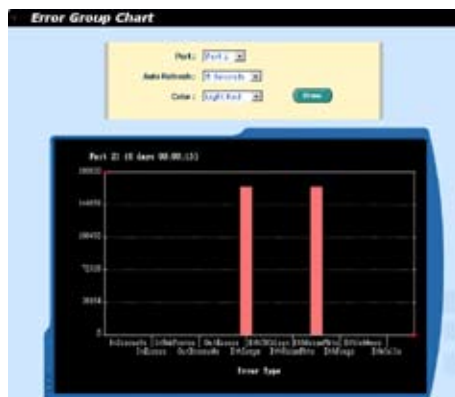
This page shows the one statistics item for all the ports in one graphic chart. Specify the statistics item to display and click the **Draw**, the browser will show you the update data and refresh the graphic periodically.



Figure 34. Traffic comparison

#### 4.10.2 Error Group

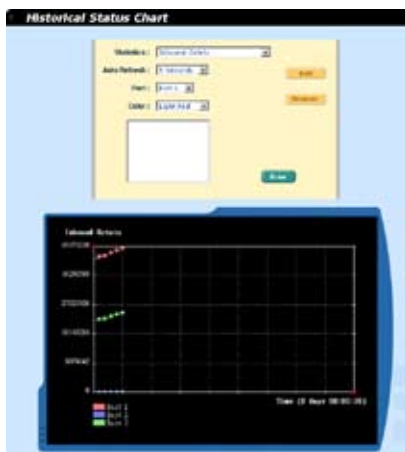
Select the **Port** and display **Color**, then click **Draw**, the statistics window shows you all the discards or error counts for the specified port. The data is updated periodically.



**Figure 35. Error group**

### 4.10.3 Historical Status

You can display information for different ports and statistics items in this chart. Since this shows the history of the statistics information, the chart can keep the old data even it is refreshed.



**Figure 36. Historical status**

## 4.11 Save Configuration

To save configuration permanently, you should click **Save**. The setting also takes effective after a successful save.

Sometimes you may want to reset the switch configuration, you can click on **Restore** to reset the configuration file to factory default. Of course, a system reboot will follow this restoration process.



*You will lose all the configurations when you choose to restore the factory default configurations.*



**Figure 37. Save configuration**

## 5 Console Interface

This chapter describes how to use console interface to configure the switch. The switch provides RS232 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 9600, 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. This is very useful when you are not familiar with the CLI commands. The CLI mode times out when idle for 10 minutes. You have to login again to enter CLI mode after the timeout.

All the CLI commands are case sensitive. 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 “sys” before any sub-commands. For example, “sys” is a command category including a lot of sub-commands. You don't have to type “sys” for the sub-commands once you change your working category to “sys” by typing “sys”. The prompt will become “(system name) sys%” when your working category is “sys”.

### 5.1 Power On Self Test

---

POST is executing during the system booting time. It tests system memory, LED and hardware chips on the switchboard. It displays system information as the result of system test and initialization. You can ignore the information until the prompt, “(ASUS) %”, appears (see Figure 38).

```
Step 4
>>>>> ASUS OS Initialization Start(Phase 2)

System Parameters Reloading ..... [ DONE ]
Layer 2 Functions Initialization ..... [ DONE ]
CLI Command Tree Initialization ..... [ DONE ]
In-ROM File System Initialization ..... [ DONE ]
RBDIUSd Initialization ..... [ DONE ]
SNMPd Initialization ..... [ DONE ]
Telnetd Initialization ..... [ DONE ]
HTTPd Initialization ..... [ DONE ]
FTPd Initialization ..... [ DONE ]
SSHd Initialization ..... [ DONE ]

ASUS OS Initialization Success.

Step 5
>>>>> Entering COM(CLI Command Mode) ...

Login is required!
(ASUS)%
```

*Figure 38. CLI interface*

### 5.1.1 Boot ROM Command Mode

During the POST process, you can enter a “Boot ROM Command” mode by pressing <ENTER> key as shown in Figure 39.

Figure 39 shows dual images in the switch.

Enter the “?” key to show the help messages for all available commands.



*Although the commands are helpful in some situation, we **STRONGLY** suggest users not to use them if you don't know the command function.*

```

30000> Switch Software Information

Switch Type ..... GigaX 2008EX
Boot ROM Version ..... Ver 1.0
Boot ROM Build Date ..... Oct 10 2009 22:18:33

30000> Firmware slot 0 Information

Firmware Address ..... 0xFFFF0000
Firmware Age ..... 9602
Firmware Status ..... PASS
Firmware Version ..... 3.3.3
Firmware Creation Date ..... 12/4/2005 20:28:30
Firmware Size ..... 1560784 bytes
Firmware Checksum ..... 0x3d8f
Firmware Starting Address ..... 0x000000
Firmware Web File Size ..... 195830 bytes

30000> Firmware slot 1 Information

Firmware Address ..... 0xFFFF0000
Firmware Age ..... 9603
Firmware Status ..... PASS
Firmware Version ..... 3.3.3
Firmware Creation Date ..... 12/4/2005 20:28:30
Firmware Size ..... 1560784 bytes
Firmware Checksum ..... 0x3d8f
Firmware Starting Address ..... 0x000000
Firmware Web File Size ..... 195830 bytes

Hit any Key to Enter Command Mode in 2 Second(s)

[Press OK Button]

```

**Figure 39. Boot ROM Command Mode**

### 5.1.2 Boot ROM Commands

Type “?” in the boot mode to display the valid commands list.

**Table 7. Boot ROM commands**

Command	Parameters	Usage
a	NONE	Display MAC address
b	Slot 0/1/a	Change boot slot
c	IP address	Configure TFTP client IP address
g	NONE	Load and execute firmware
h	NONE	Display online help
m	mask	Configure network mask
p	NONE	Display current configuration
r	NONE	System reboot

Command	Parameters	Usage
s	IP address	Configure TFTP server IP address
t	NONE	Toggle safe mode
u	File name	Upload boot module/firmware via network using TFTP protocol
v	NONE	Display boot rom version
w	NONE	Toggle administrator password reset

---

## 5.2 Login and Logout

By typing “login” to enter the CLI mode, you have to give a valid user name and password. As the first time login, you can enter “**admin**” as the user name and bypass the password. For security reason, please change the user name and password after login. Once you forget the use name and password, you may contact ASUS support team or erase the whole configuration file in the **Boot ROM Command** mode. If you take the second choice, the whole system configuration is lost at the same time. That is, you have to configure the switch again.

You type “**logout**” to leave the CLI mode safely. This action allows you to secure the CLI mode. The next user has to do login again with authorized user name and password.

---

## 5.3 CLI Commands

The switch provides CLI commands for all managed functions. The command uses are listed in the categories as the WEB management interface. This way, you can follow the instructions and set up the switch correctly as easily as using WEB interface to configure the switch. “save” command is used to save the configuration to flash. Some CLI command is only effective after “save” command is executed.



*Always use “?” to get the available commands list and help.*

*Always use “/” to get back to the root directory.*

*Always use “..” to get back to parent directory.*

*Type the command only to get help for the command*

### 5.3.1 System Commands

#### [System Name]

Displays the given name of the switch. This is an RFC-1213 defined MIB object in System Group, and provides administrative information on the managed node.

**CLI command:** sys info name <system name description>

If you put a name in the name description field, the switch system name will be changed into the new one.

#### [System Contact]

Displays the detail information of contact about the switch. This is an RFC-1213 defined MIB object in System Group, and provides contact information on the managed node.

**CLI command:** sys info contact <system contact description>

If you put the contact description in the contact description field, the switch contact information will be changed to the new one.

#### [System Location]

Displays the physical location of the switch. This is an RFC-1213 defined MIB object in System Group, and provides the location information on the managed node.

**CLI command :** sys info location <system location description>

Type the location description in the location description field to change the location.

```
(ASUS) %
(ASUS) %
(ASUS) %
(ASUS) %
(ASUS) %
(ASUS) %
(ASUS) %
(ASUS) % sys
(ASUS) % sys info
(ASUS) % sys/info? name
CURRENT system name is ASUS

(ASUS) % sys/info? v
Available commands are:
/          Change to root directory
..         Change to parent directory
name       Set/show system name
contact    Set/show contact person name
location   Set/show system location
version    Show version information
save       Save the configuration permanently

(ASUS) % sys/info?
```

**Figure 40. System commands**

#### [VLAN ID]

Display the VLAN ID for the switch. It is necessary to be within the same VLAN for management .

**CLI command:** net interface vlan sw0 <VLAN ID>

### **[IP Address]**

Displays the static IP address for the switch. This IP address is used for manageable purpose, i.e.; network applications such as, http server, SNMP server, ftp server, telnet server and SSH server of the switch are all using this IP address.

**CLI command:** net interface ip sw0 < IP address> <netmask>

### **[Network Mask]**

Displays the subnet mask for the switch.

**CLI command:** net interface ip sw0 < IP address> <netmask>

### **[Default Gateway]**

Displays the IP address of the default gateway. This field is necessary if the switch network contains one or more routers.

**CLI command:** net route static add <destination subnet/IP> <gateway>  
<netmask> <metric>

### **[Password Protection is] [Enabled/Disabled]**

When the password protection is enabled, the web interface will request a user name and password authentication while user accesses the switch through the browser.

**CLI command:** sys web set <enable/disable>

### **[New Password] / [Verify Password]**

The default user name is admin. By default, a password is not required. You may set a password by configuring these fields.

**CLI command:** sys users modify <user name, 'admin' by default>

**user name** (old user name, 'admin' by default): <new user name>

**password** (old password,): <new password>

### **[Reboot]**

User can reboot the switch by issuing the reboot command.

**CLI command:** sys reboot

### **[Upload]**

No CLI command for this function. Refer to Boot ROM commands for this function.



### 5.3.2 Physical Interface Commands

#### **[Admin]** [Enable/Disable]

Displays the port admin status and allows user to turn the port on or off.

**CLI command:** l2 port admin <port number> <enable/disable>

#### **[Mode]** [Auto/10M-Half/10M-Full/100M-Half/100M-Full/1G-Full]

Displays the current speed and duplex mode of the port. The speed and duplex mode can be automatically detected when auto-negotiation is enabled on a port.

**CLI command:** l2 port autoneg <port number> <enable/disable>

**CLI command:** l2 port speed <port number> <10/100/1000>

**CLI command:** l2 port duplex <port number> <full/half>

#### **[Flow Control]** [Enable/Disable]

Displays the IEEE802.3x flow control setting of a port. Note that this flow control is operating only in full duplex mode.

**CLI command:** l2 port flow <port number> <enable/disable>

#### **[Reload]**

Restores the previous port settings from the configuration file.

**CLI command:** l2 port retrieve

### 5.3.3 Bridge Commands

#### **[Show Trunk]**

Displays a specific trunk group settings. User can create a new trunk group by specify a unique trunk ID, a trunk name description, the port selection criterion (rtag), and its trunk group member ports.

**CLI command:** l2 trunk show <trunk id>

#### **[Create Trunk]**

Creates a new trunk group by giving trunk ID, rtag, name, and port numbers.

**CLI command:** l2 trunk create <trunk id> <trunk name> <port list>

#### **[Add/Remove Trunk]**

Trunk group port members can be added to or removed from an existing trunk group.

**CLI command:** l2 trunk add <trunk id> <port list>

**CLI command:** l2 trunk remove <trunk id> <port list>

#### **[Reload]**

Restores the previous saved settings of trunk from configuration file.

**CLI command:** l2 trunk retrieve

#### **[Mirror Mode] [Enable/Disable]**

#### **[Monitor Port] [port number]**

Displays the mirroring settings of the switch.

**CLI command:** l2 mirror create <monitor port no> <enable/disable>

**CLI command:** l2 mirror ingress <port list>

**CLI command:** l2 mirror egress <port list>

**CLI command:** l2 mirror remove <ingress/egress> <port list>

#### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** l2 mirror retrieve

#### **[Limit Rate]**

User can limit the broadcast, multicast, and flooding (due to destination lookup failed) traffic rate by turning the traffic control on.

**CLI command:** l2 rate set <enable/disable> [<mode (1:broadcast only, 2: broadcast and multicast, 3:broadcast, multicast and unknown unicast )> <limit rate (70~250000 Kbps/sec)>]

#### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** l2 rate retrieve

#### **[Aging Time]**

User can set the ARL (Address Resolution Logic) entries aging time by setting the aging time value.

**CLI command:** l2 arl age [aging time value]

#### **[Query by Port]**

ARL entries existed in ARL table can be queried according to port number.

**CLI command:** l2 arl port <port number>

### **[Query by VLAN ID]**

ARL entries existed in ARL table can be queried according to VLAN ID.

**CLI command:** `l2 arl vlan <vlan id>`

### **[Query by MAC Address]**

ARL entries existed in ARL table can be queried according to MAC address.

**CLI command:** `l2 arl mac <mac address> [vlan id]`

### **[MAC Address]**

### **[VLAN ID]**

### **[Port Selection]**

User can add or modify a static ARL entry by specifying a MAC address, VLAN ID, port number, and trunk ID.

**CLI command:** `l2 arl static <mac> <vlan id> <port no> <trunk id>`

### **[Remove]**

Static ARL entries can be deleted by indicating the MAC address and its VLAN ID. These two-field combination is formed as unique entry in ARL table.

**CLI command:** `l2 arl delete <mac address> <vlan id>`

### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** `l2 arl retrieve`

### **[Show VLAN]**

Displays the existing VLAN information of the switch.

**CLI command:** `l2 vlan show <vlan id>`

### **[Name]**

### **[VLAN ID]**

Allows user to config the VLAN settings. User may create a new VLAN by giving a unique VLAN ID, a VLAN description name, and its port member list, note that the port member here is indicated as tagged port member. To specify a VLAN port member as untagged port, CLI command `utportadd` can achieve this purpose. User may use CLI command `add` or `remove` to further add some port members to a VLAN or exclude some existing port members from a VLAN.

**CLI command:** `l2 vlan create <vlan id> <vlan name> <port list>`

**CLI command:** `l2 vlan add <vlan id> <port list>`

**CLI command:** l2 vlan remove <vlan id> <port list>

**CLI command:** l2 vlan utportadd <vlan id> <untagged port list>

### **[Remove VLAN]**

Allows user to completely destroy an existing VLAN.

**CLI command:** l2 vlan delete <vlan id>

### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** l2 vlan retrieve

### **[Show Port]**

Displays the port configuration

**CLI command:** l2 port show <port id or \* for all ports>

### **[PVID]**

Sets the default VLAN for a port by giving a VLAN ID and its associated port member list.

**CLI command:** l2 port vlan <vlan id, 4095 to disable the port-based vlan>  
<port list>

### **[CoS Value]**

Sets the Class of Service for a port by assigning it a priority (with range of 0-7) criteria value for untagged packets..

**CLI command:** l2 port priority <CoS> <port list>

### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** l2 port retrieve

### **[CoS] [Map]**

Allows user to map the CoS priority (with range of 0-7) for a buffer queue (total of 4, with queue ID of 1-4).

**CLI command:** l2 cos map <queue id (1-4)> <cos (0-7)>

### **[Scheduling Algorithm] [Strict/WRR]**

Allows user to set scheduling with strict priority based or weight priority based.

**CLI command:** l2 cos sched <mode (1: strict 2: weighted round robin)>

**[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** l2 cos retrieve

### 5.3.4 SNMP

**[Community Name] [Set]**

A community entry contains a community description string and a set of privileges. Get privilege are turned on by default, and user can specify whether to give it the Set Privilege while create a new entry.

**CLI command:** snmp community add

**New community string:** <new community string>

**Get privileges:** [y, always turn on by default]

Set privileges? (y/n):[n] <set privilege, y for 'yes'; n for 'no'>

User can modify a community entry in the table by reassigning its community string and privileges.

**CLI command:** snmp community set

**Community entry (table index):** <entry id to config>

**Community string (old community string):** <new community string>

This action will modify all hosts with community string from 'old community' to 'new community'.

**Are you sure? (y/n):** [y] <y for 'yes'; n for 'no'>

**Get privileges:** [y, always turn on by default]

Set privileges? (y/n): [n] <set privilege, y for 'yes'; n for 'no'>

Allows user to delete a community entry from community table.

**CLI command:** snmp community delete

**Community entry (table index):** <entry id to delete>

This action will delete all hosts in community string with 'delete community'.

Are you sure? (y/n): [y] <y for 'yes'; n for 'no'>

**[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** snmp community retrieve

**[Host IP Address] [Community]**

A host entry contains a host IP address, network mask and its dedicated community string.

**CLI command:** snmp host add

**Host IP/Subnet:** <IP address>

**Netmask:** <netmask>

**Community:** <community string>

User can modify a host entry in the table by reassigning its allowed IP address, network mask and community string.

**CLI command:** snmp host set

**Host table entry (table index):** <entry id to config>

**Host IP/Subnet (old IP address):** <new IP address>

**Netmask (old netmask):** <new netmask>

**Community (old community string):** <new community string>

Allows user to delete a host entry from host table.

**CLI command:** snmp host delete

**Entry id (table index):** <entry id to delete>

#### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** snmp host retrieve

#### **[Trap Version] [v1/v2c]**

##### **[Destination]**

##### **[Community for Trap]**

A trap entry contains SNMP version (currently support version 1 and version 2c), a destination IP address and the remote community string.

**CLI command:** snmp trap add

**SNMP version? (1/2c):** [1, by default] <snmp version>

**Destination IP:** <IP address>

**Community:** <community string>

User can modify a trap entry in the table by reassigning its SNMP version, destination IP address and community string.

**CLI command:** snmp trap set

**Trap table entry (table index):** <entry id to config>

**SNMP version?** (1/2c): [old snmp version] <new snmp version>

**Destination IP** (old IP address): <new IP address>

**Community** (old community string): <new community string>

Allows user to delete a trap entry from trap table.

**CLI command:** snmp trap delete

**Trap table entry** (table index): <entry id to delete>

#### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** snmp trap retrieve

### **5.3.5 Security Commands**

#### **[Reauthentication]**

Allows user to open or close periodic reauthentication.

**CLI command:** security dot1x bridge reauth <enable / disable>

#### **[Reauthentication Time]**

Allows user to set up the reauthentication time.

**CLI command:** security dot1x bridge reauthtime <reauthentication time (1-4294967295 sec)>

#### **[Authentication Method]**

Allows user to set up the authentication method (RADIUS or Local database).

**CLI command:** security dot1x bridge authmeth <type (1:local 2:radius)>

#### **[Quiet Period]**

Allows user to set up the quiet period.

**CLI command:** security dot1x bridge quietperiod <quiet period (1-65535 sec)>

#### **[Retransmission Time]**

Allows user to set up the retransmission time.

**CLI command:** security dot1x bridge retxttime <retransmission time (1-65535 sec)>

#### **[Max Reauthentication Attempts]**

Allows user to set up the max number of the reauthentication attempts.

**CLI command:** security dot1x bridge reauthmax <max reauthentication attempts (1-10)>

#### **[Multi-host]**

Allows user to enable or disable Multi-host on some specific ports.

**CLI command:** security dot1x port multihost <enable/disable> <port list/\*>

#### **[Authentication Control]**

Allows user to set up the authentication control of some specific ports.

**CLI command:** security dot1x port authctrl <type (1: force\_authorized 2: force\_unauthorized 3: auto)><port list/\*>

#### **[Guest VLAN]**

Allows user to set up the guest VLAN ID of some specific ports.

**CLI command:** security dot1x bridge port guestvlan <vlan id (0:no guest vlan)> <port list/\*>

#### **[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** security dot1x retrieve

#### **[User Name]**

#### **[Password]**

#### **[Confirm Password]**

#### **[Dynamic VLAN]**

Create users in the local database of the switch for 802.1x authentication. A user entry contains a user name, password and dynamic VLAN.

**CLI command:** security dialinuser create

**User Name:** <user name string>

**Password:** <password string>

**Confirm Password:** <confirm password string>

**Dynamic VLAN:** <dynamic VLAN>

**CLI command:** security dialinuser remove <user name/\*>

Allows user to delete a user entry from the local database.

**CLI command:** security dialinuser modify <user name/\*>

Allows user to modify a user entry from the local database. It contains a user name, password and dynamic VLAN.



**User Name:** <new user name string>

**Password:** <new password string>

**Confirm Password:** <new confirm password string>

**Dynamic VLAN:** <new dynamic VLAN>

**[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** security dialinuser retrieve

**[Authentication Server IP]**

**[Authentication Server Port]**

**[Authentication Server Key]**

**[Confirm Authentication Key]**

Allows user to config the RADIUS server IP, server port and server key .

**CLI command:** security radius set

**authentication server ip <ip/none>:** (old server ip)<new server ip >

**authentication server port <port/default>:** (old server port)<new server port>

**authentication server key <key/none>:** <server key>

**confirm authentication key <key/none>:** <confirm server key>

**[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** security radius retrieve

### **5.3.6 PoE**

**[Admin]**

Set port power to enable or disable.

**CLI command:** poe admin < enable / disable > < port list/\* >

**[Prio]**

Set port priority.

**CLI command:** poe admin < priority[0-47] > < port list/\* >

**[heat]**

Show temperature of the devices.

**CLI command:** poe heat

**[pse]**

Show PSE system Information.

**CLI command:** poe pse

**[diag]**

Show diagnostic result for port power.

**CLI command:** poe diag

**[display]**

Display real-time port power information.

**CLI command:** poe display < port list/\* >

**[show]**

Show the PoE configuration.

**CLI command:** poe show

**[save]**

Save the PoE configuration into the flash.

**CLI command:** poe save

**[Reload]**

Restores the previous saved settings from configuration file.

**CLI command:** poe retrieve

## **5.4 Miscellaneous Commands**

---

**sys time uptime:** shows the time since the system boot up.

**sys time date:** shows the current date and time

**sys time settime:** sets the current time

**sys files config backup:** backup configuration files

**sys files config default:** restore factory default configuration files

**sys monitor auto:** enable or disable fan auto detection

**sys monitor set:** Set fan speed command (1~255)

**sys monitor show:** Show the status of system environment

**net ping:** ping remote host

**net route show:** displays the entries in the routing table

## 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 8. IP address structure**

	Field1	Field2	Field3	Field4
<b>Class A</b>	Network ID	Host ID		
<b>Class B</b>	Network ID		Host ID	
<b>Class C</b>	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

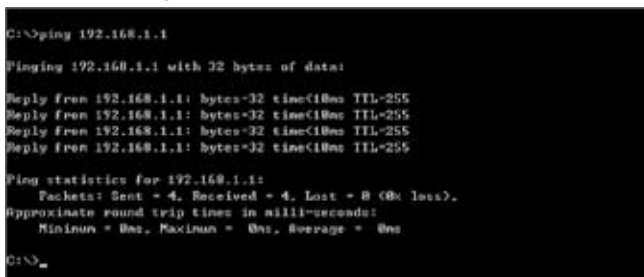
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer 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 you know on your LAN or a public IP address for an Internet site.

If the target computer receives the message, a Command Prompt window appears as shown in Figure 45.



```
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 milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

**Figure 41. 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](http://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

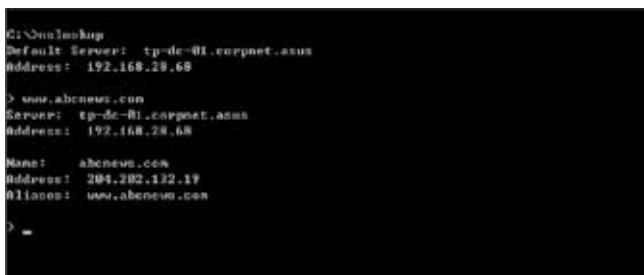
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred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

Clicks **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](http://www.absnews.com).

The window displays the associate IP address you know. See Figure 46.



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

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

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

> _
```

**Figure 42. 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 9. Troubleshooting**

Problem	Suggested Action
<b>LEDs</b>	
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.
FAN LED is amber blinking	Check the fan on the back of the switch.
Gigabit Ethernet Link LED does not illuminate after an Ethernet cable is attached.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Verify if your cable is sufficient for your network requirements. A 1000 Mbps network (1000BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.</li> </ol>
<b>Network Access</b>	
PC cannot access another host in the same network	<ol style="list-style-type: none"> <li>1. Check the Ethernet cabling is good and the LED is green.</li> <li>2. If the port LED is amber, check if this port is disabled.</li> </ol>
PCs cannot display web configuration pages.	<ol style="list-style-type: none"> <li>1. The switch is powered up and the connecting port is enabled. The factory default IP for the switch is 192.168.1.1.</li> <li>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.</li> <li>3. Ping "switch IP" from the PC, if it still fails, repeat step 2.</li> <li>4. If ping is successful but the web configuration still fails, connecting PC through the console port by a RS232 cable, check if any filter rule or static MAC address is set to block the WEB traffics.</li> </ol>

Problem	Suggested Action
<b>Web Configuration Interface</b>	
You forgot/lost your WEB configuration interface user ID or password.	<p>1.If you have not changed the password from the default, try using "admin" as the user ID and bypassing password.</p> <p>2. a) Power on the switch and enter BootROM mode.  b) Input "w" to enable administrator password reset and then input "g" to continuously execute firmware program.  Note: The method allows you to use default username and password to login just once and would not allow you to use it to login again after system reboots. Other configuration will not be changed.  c) Login to CLI using default username "admin" (no password) Type command "sys users show" to show username and password you had saved.</p>
Some pages do not display completely	<p>1.Verify that you are using Internet Explorer v5.5 or later. Netscape is not supported. Support for Javascript® must be enabled in your browser. Support for Java may also be required.</p> <p>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.</p>
Changes to Configuration are not being retained.	Be sure to click on <b>Save</b> button in the <b>Save Configuration</b> page to save any changes.
<b>Console Interface</b>	
Cannot show the texts on the terminal emulator.	<p>1.The factory default baud rate is 9600, no flow control, 8 bit data, no parity check and stop bit is one.</p> <p>2.Change your terminal emulator setup to this number.</p> <p>3.Check if the cable is good.</p>

## 8 Glossary

<b>10BASE-T</b>	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.
<b>100BASE-T</b>	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.
<b>1000BASE-T</b>	A designation for the type of wiring used by Ethernet networks with a data rate of 1000 Mbps.
<b>binary</b>	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.
<b>bit</b>	Short for “binary digit,” a bit is a number that can have two values, 0 or 1. See also binary.
<b>bps</b>	bits per second
<b>CoS</b>	Class of Service. Defined in 802.1Q, the value range is from 0 to 7.
<b>broadcast</b>	To send data to all computers on a network.
<b>Ethernet</b>	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.
<b>FTP</b>	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.
<b>host</b>	A device (usually a computer) connected to a network.
<b>ICMP</b>	Internet Control Message Protocol  An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.

<b>IGMP</b>	Internet Group Management Protocol  An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers. A multicast group of computers is one whose members have designated as interested in receiving specific content from the others. Multicasting to an IGMP group can be used to simultaneously update the address books of a group of mobile computer users or to send company newsletters to a distribution list.
<b>IGMP Snooping</b>	Snoop the IGMP packets on each port and associate the port with a layer 2 muticast group.
<b>mask</b>	See network mask.
<b>Multicast</b>	To send data to a group of network devices.
<b>Mbps</b>	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
<b>Monitor</b>	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.
<b>network mask</b>	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.
<b>NIC</b>	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.
<b>packet</b>	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).
<b>ping</b>	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.

<b>port</b>	A physical access point to a device such as a computer or router, through which data flows into and out of the device.
<b>protocol</b>	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.
<b>remote</b>	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
<b>RJ-45</b>	Registered Jack Standard-45  The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
<b>RMON</b>	Remote Monitoring  Extensions to SNMP, provide comprehensive network monitoring capabilities.
<b>routing</b>	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.
<b>SNMP</b>	Simple Network Management Protocol  The TCP/IP protocol used for network management.
<b>STP</b>	Spanning Tree Protocol  The bridge protocol to avoid packet looping in a complicate network.
<b>subnet</b>	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.
<b>subnet mask</b>	A mask that defines a subnet. See also network mask.
<b>TCP</b>	See TCP/IP.
<b>TCP/IP</b>	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.
<b>Telnet/SSH</b>	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 / SSH allows you to log into and use a computer from a remote location.
<b>TFTP</b>	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.
<b>Trunk</b>	Two or more ports are combined as one virtual port, also called as Link Aggregation.
<b>TTL</b>	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.
<b>twisted pair</b>	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.
<b>upstream</b>	The direction of data transmission from the user to the Internet.
<b>VLAN</b>	Virtual Local Area Network
<b>WAN</b>	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.
<b>Web browser</b>	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.