

USER'S MANUAL

LAYER2 WEB SMART PLUS SWITCH

SWP-0008F

PLANEX COMMUNICATIONS INC.

First Edition V1 October 2005

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.

Table of Contents

1	Introduction	8
1.1	L2 managed features.....	8
1.2	Conventions used in this document.....	9
1.2.1	Notations	9
1.2.2	Typography	9
1.2.3	Symbols.....	9
2	Getting to know the SWP-0008F	10
2.1	Package contents	10
2.2	Front Panel	11
2.3	Technical specifications.....	12
3	Quick start guide	12
3.1	Part 1 — Installing the hardware	13
3.1.1	Installing the switch on a flat surface	13
3.2	Part 2 — Setting up the switch	13
3.2.1	Connect to the computers or a LAN.....	13
3.2.2	Attach the power adapter	13
3.3	Part 3 — Basic switch setting for management.....	14
3.3.1	Setting up through the Web interface	14
4	Management with the Web Interface	17
4.1	Log into Web user interface.....	17
4.2	Functional layout.....	19
4.2.1	Menu navigation tips	21
4.2.2	Commonly used buttons and icons.....	21
4.3	System Pages.....	22
4.3.1	Management	22
4.3.2	IP Setup.....	23
4.3.3	Administration.....	24
4.3.4	Reboot.....	26

4.3.5	Firmware Upgrade	26
4.4	Physical Interface	28
4.5	Bridge	30
4.5.1	Link Aggregation	30
4.5.2	Mirroring	32
4.5.3	Traffic Control	33
4.5.4	Dynamic Addresses	34
4.5.5	Static Addresses	35
4.5.6	Tagged VLAN	36
4.5.7	Default Port VLAN and CoS.....	38
4.5.8	CoS Queue Mapping	38
4.6	SNMP	40
4.6.1	Community Table	40
4.6.2	Host Table.....	41
4.6.3	Trap Setting	42
4.7	Security.....	43
4.7.1	Port Access Control	43
4.7.2	Dial-In User	45
4.7.3	RADIUS.....	46
4.8	Cable Diagnosis	47
4.9	Statistics Chart	48
4.9.1	Traffic Comparison.....	48
4.9.2	Error Group	49
4.9.3	Historical Status	50
4.10	Save Configuration.....	51
5	The configuration backup and restore	52
5.1	The configuration backup method	52
5.2	The configuration restore method	53
6	IP Addresses, Network Masks, and Subnets	54
6.1	IP Addresses	54
6.1.1	Structure of an IP address	54

6.1.2	Network classes	56
6.2	Subnet masks	57
7	Troubleshooting	59
7.1	Diagnosing problems using IP utilities	59
7.1.1	Ping	59
7.1.2	nslookup	61
7.2	Simple fixes	62
8	Glossary	63

List of Figures

Figure 1.	SWP-0008F Web smart plus switch package contents..	10
Figure 2.	Front panel.....	11
Figure 3.	Login Screen.....	15
Figure 4.	IP Setup	16
Figure 5.	Configuration manager login screen.....	17
Figure 6.	Home page	18
Figure 7.	Top frame	19
Figure 8.	Expanded Menu List.....	20
Figure 9.	Management.....	22
Figure 10.	IP Setup	23
Figure 11.	Administration	25
Figure 12.	Reboot	26
Figure 13.	Firmware Upgrade	27
Figure 14.	Physical Interface	29
Figure 15.	Link aggregation	31
Figure 16.	Mirroring page.....	32

Figure 17.	Traffic Control.....	33
Figure 18.	Dynamic Address	34
Figure 19.	Static Address	36
Figure 20.	Tagged VLAN.....	37
Figure 21.	Default Port VLAN and CoS	38
Figure 22.	Cos Queue Mapping	39
Figure 23.	Community Table	40
Figure 24.	Host Table	41
Figure 25.	Trap Setting.....	42
Figure 26.	Port Access Control.....	44
Figure 27.	Dial-In user	45
Figure 28.	RADIUS.....	46
Figure 29.	Cable Diagnosis	47
Figure 30.	Traffic comparison.....	48
Figure 31.	Error group	49
Figure 32.	Historical Status	50
Figure 33.	Save Configuration.....	51
Figure 34.	Using the ping utility	60
Figure 35.	Using the nslookup utility.....	61

List of Tables

Table 1.	Front panel labels and LEDs	11
Table 2.	Technical specifications.....	12
Table 3.	LED Indicators	14
Table 4.	Port color description	19
Table 5.	Commonly used buttons and icons	21
Table 6.	IP address structure	55
Table 7.	Troubleshooting.....	62

1 Introduction

Congratulations on becoming the owner of the SWP-0008F managed smart plus switch! You may now manage your LAN (local area network) through a friendly and powerful user interface.

This user guide tells you how to set up the SWP-0008F managed smart plus switch, and how to customize its configuration to get the most out of this product.

1.1 L2 managed features

- 8 10/100 BASE-TX auto-sensing Fast Ethernet ports
- Automatic MDI/MDIX support for 10/100BASE-TX
- 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, and system temperature, voltage
- Web GUI
- LEDs for port link status
- LEDs system 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 SWP-0008F switch is referred to as “the switch.”
- The terms *LAN* and *network* are used interchangeably to refer to a group of Ethernet-connected computers at one site.

1.2.2 Typography

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

1.2.3 Symbols

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



Note

Provides clarification or additional information on the current topic.



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 SWP-0008F

2.1 Package contents

The SWP-0008F switch package comes with the following items:

- SWP-0008F (8-port) L2 web smart plus switch
- AC Power cord
- CD-ROM (User's Manual, Private-MIB file)
- Warranty card
- Safety notice

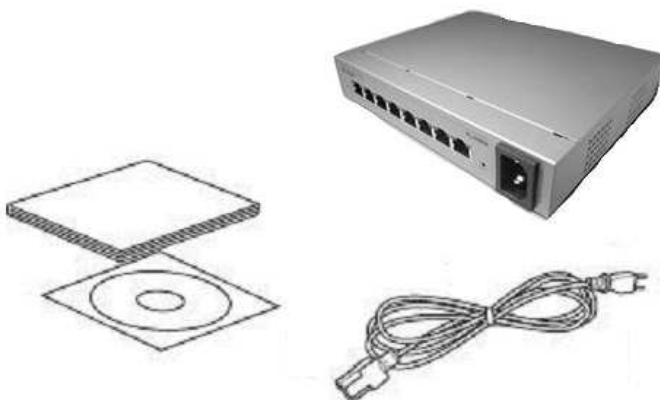


Figure 1. SWP-0008F Web smart plus switch package contents

2.2 Front Panel

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

The front panel includes a reset button to the switch configurations to the factory default. You can press the reset button about 3 ~ 5 seconds, then the switch will reboot and reset the configurations to the factory default.



Figure 2. Front panel

Table 1. Front panel labels and LEDs

Label	Color	Status	Description
Power	Green	On	Unit is powered on
		Flashing	Self-test, INIT, or downloading
	Amber	On	Abnormal temperature or voltage
	Off		No power
10/100 port status	Green	On	Link (RJ-45) is present; port is enabled
		Flashing	Data is being transmitted/received
	Off		No Ethernet link
	Amber	On	Link is present, but port is disabled manually
10/100 port speed	Green	On	100Mbps on 10/100 ports
	Off		10Mbps or link is not present

2.3 Technical specifications

Table 2. Technical specifications

Physical Dimensions	200 mm(W) X 40 mm(H) X 160 mm(D)		
Power	Input	Consumption	
	100-240V AC/2.5A 50-60Hz	< 12 watts	
Environmental Ranges		Operating	Storage
	Temperature	0 to 40°C	–25 to 70 °C
	Humidity	35 to 85%	5 to 95%
	Altitude	up to 10,000 ft (3,000m)	40,000 ft (12,000m)

3 Quick start guide

This section provides the basic instructions to set up the SWP-0008F environment. Refer also to the Series Installation Guide.

Part 1 shows you how to install the SWP-0008F on a flat surface.

Part 2 provides instructions to set up the hardware.

Part 3 shows you how to configure basic settings on the SWP-0008F.

Obtain the following information from your network administrator before proceeding:

IP address for the switch

Default gateway for the network

Network mask for this network

3.1 Part 1 — Installing the hardware

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

3.1.1 Installing the switch on a flat surface

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

3.2 Part 2 — Setting up the switch

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

3.2.1 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.

3.2.2 Attach the power adapter

1. Connect the AC power cord to the POWER receptacle on the front 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 3. If the LEDs light up as described, the switch hardware is working properly.

Table 3. LED Indicators

No.	LED	Description
1	Power	Solid green indicates that the device is turned on. If this light is off, check if the power adapter is attached to the switch and plugged into a power source.
2	Switch ports [1] to [8]	Solid green indicates that the device can communicate with the LAN, or flashing when the device is sending or receiving data from your LAN computer.

3.3 Part 3 — Basic switch setting for management

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

- Web interface: the switch has a set of pages to allow to you manage it using Java[®]-enabled IE5.5 or higher version.

3.3.1 Setting up through the Web interface

To successfully connect your PC to the switch, your PC must a valid IP in your network. Contact your network administrator to obtain a valid IP for the switch. If you wish to 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 3.




Figure 3. Login Screen

Enter your user name and password, and then click  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)

3. To setup a new IP address, click **"System"**, then **"IP Setup"** (see Figure 4). Fill in the IP address, network mask and default gateway, then click .
4. If your new address is different from the default, the browser can not 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 . See the figures on the next page.

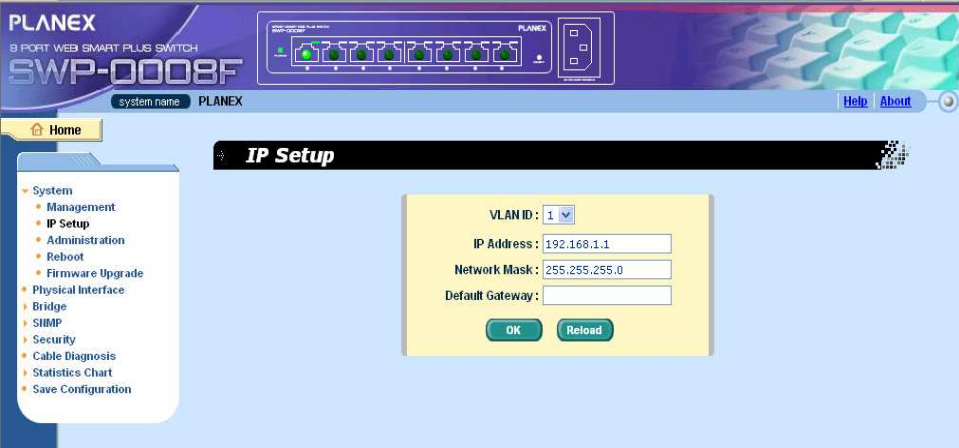


Figure 4. IP Setup

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 5.



Figure 5. Configuration manager login screen



Login is not required if you do not enable Web authentication access (see 3.3.1)"

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

Use the following defaults the first time you log into the program.

- Default User Name: admin
- Default Password: <no password>

The home page appears each time you log into the program. (See Figure 6).

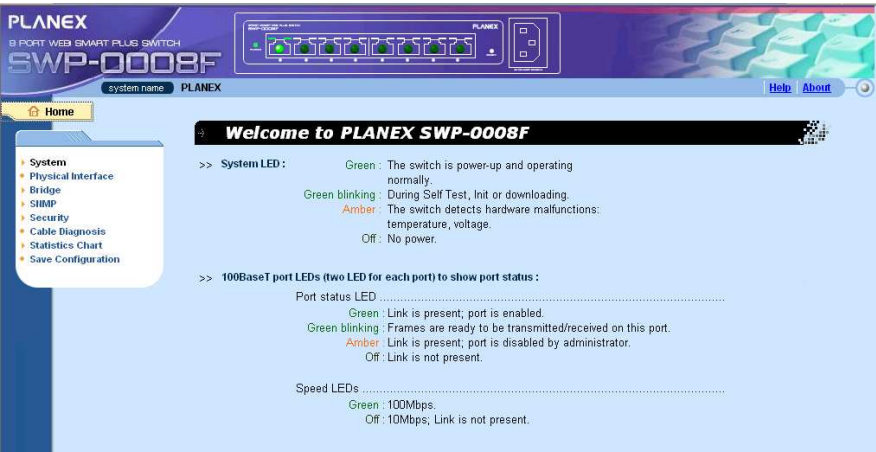


Figure 6. Home page

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 Figure 7. This frame remains on the top of the browser window all the times and updates the LED status periodically. See Table 3 for the LED definitions. See Table 4 for the color status description.

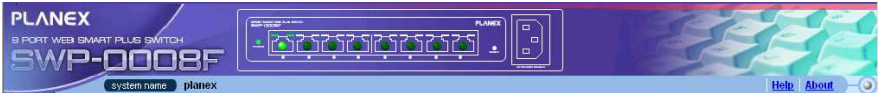


Figure 7. Top frame

Table 4. Port color description

Port Color	Description
Green port	Ethernet link is established
Black	No Ethernet link
Amber port	Link is present but port is disabled manually

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 8, 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.

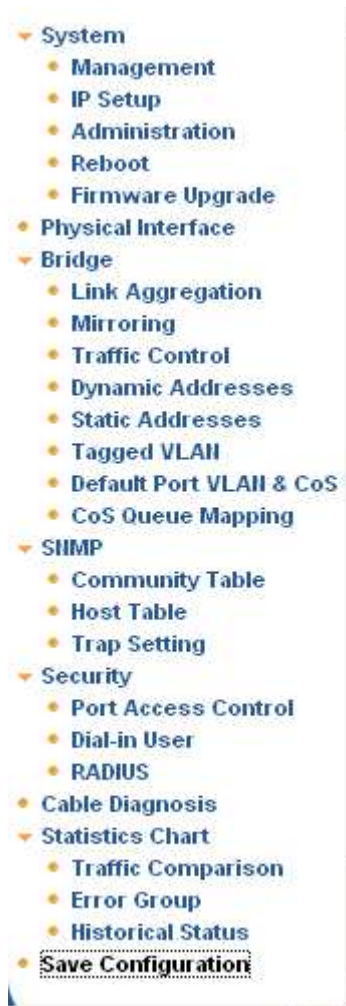


Figure 8. Expanded Menu List

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 ► sign 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 5. 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 and etc.
	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 . Use  to refresh the setting, as shown in Figure 9.

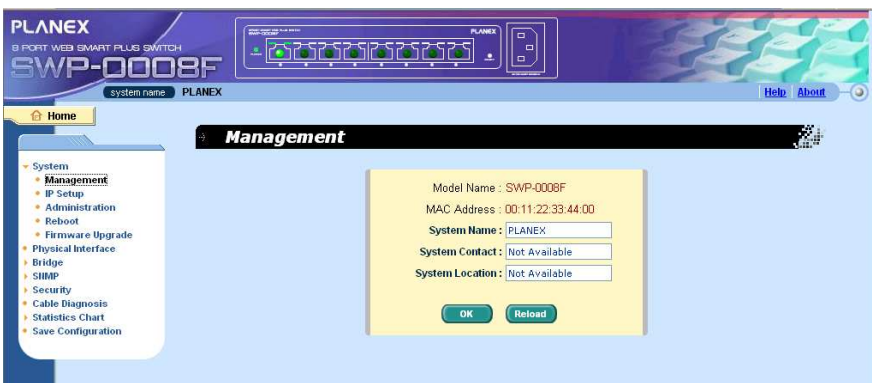


Figure 9. Management

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 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 10.

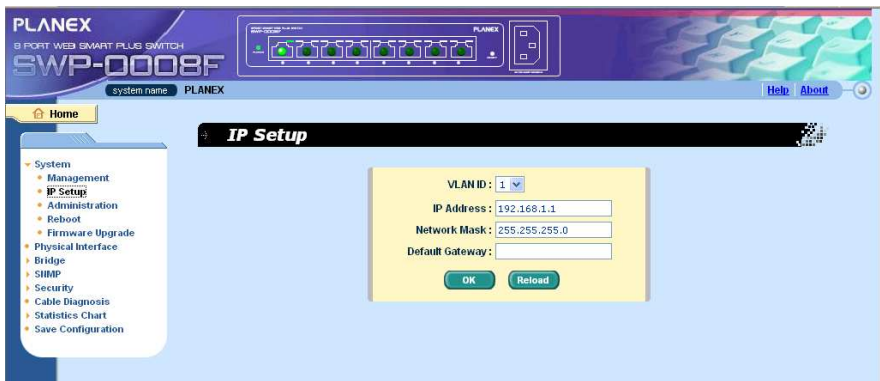


Figure 10. IP Setup

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.

Password Protection is : Enable or Disable the authentication for web user by Password protection.

User Name : New user Name.

Password : Password for the new user ,and modify password.

Confirm Password: Enter the password again.

Please click  to add the new user. Click  when you have finished the modifications. Click  when you want to remove the selected user. Click  to make the settings effective permanently. Click  to refresh the setting to current value.

As shown in Figure 11. When you enable the password protection, you have to login again immediately.

User name , default password is shown as below.

Default User Name:	Admin
Default Password:	<no password>

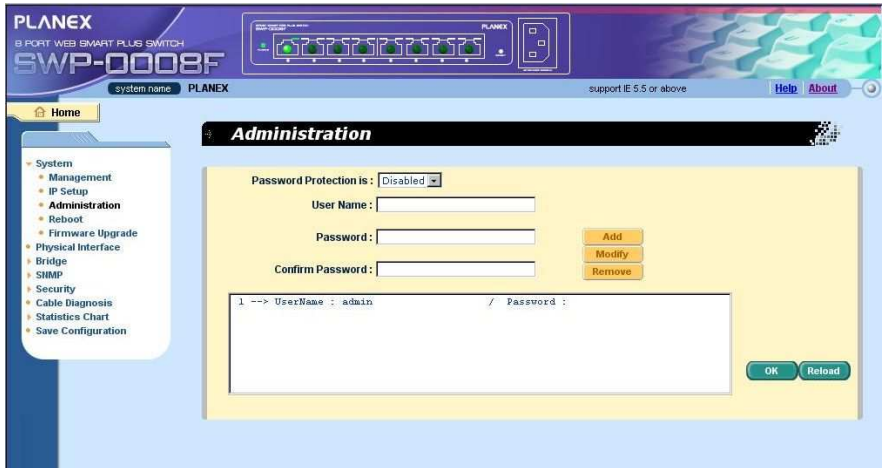



Figure 11. Administration

4.3.4 Reboot

The **Reboot** page contains a  button. Clicking the button reboots the system.



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

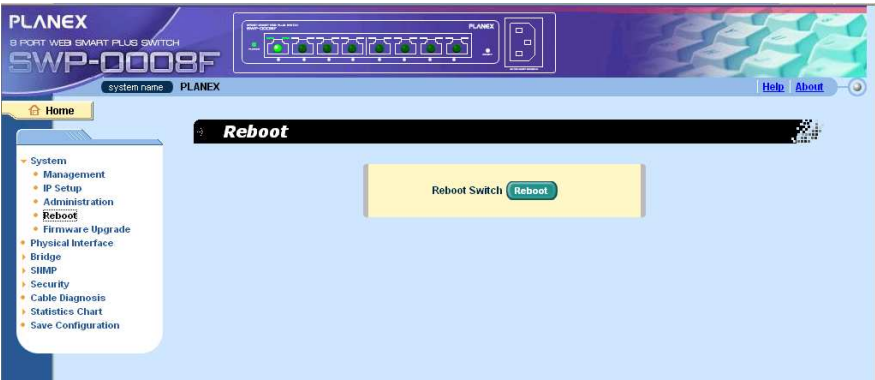


Figure 12. Reboot



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  to choose the file name of the firmware from prompt window. Click  to update the switch firmware. See Figure 13 for reference.



Clicking the upload button loads the assigned firmware to the switch, then reboot system after a successful firmware update. You have to re-login to Web interface again

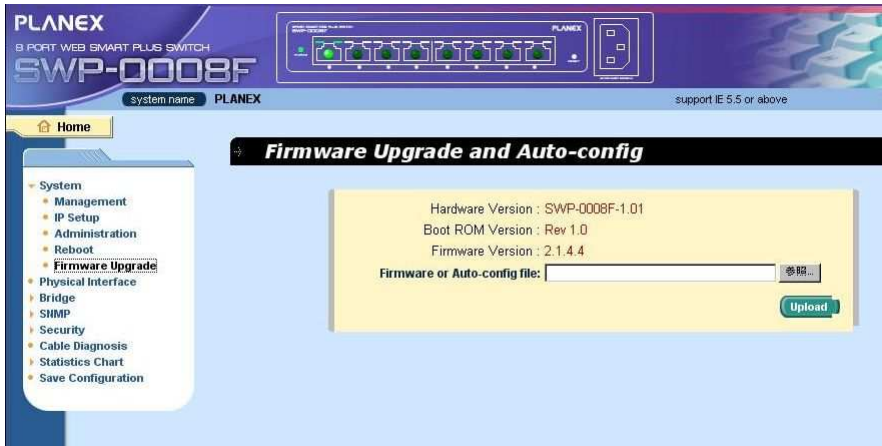


Figure 13. Firmware Upgrade

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

- a) Link status: the link speed and duplex for an existing link, otherwise link is down
- b) Admin: the setting value to disable or enable the port
- c) Mode: the setting value for link speed and duplex mode
- d) 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  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.

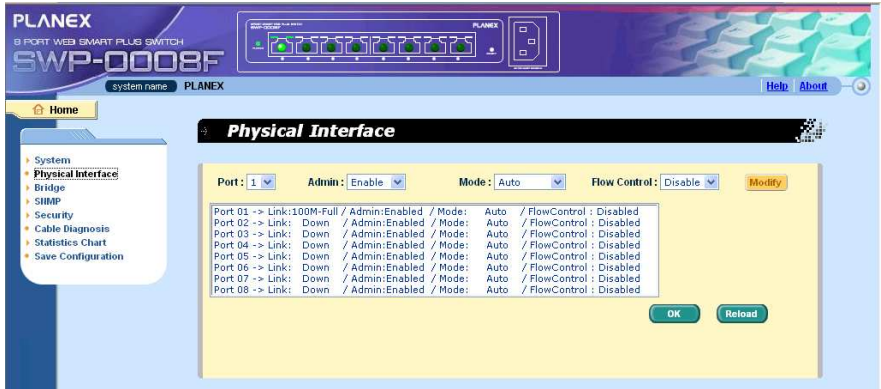


Figure 14. Physical Interface

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

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.

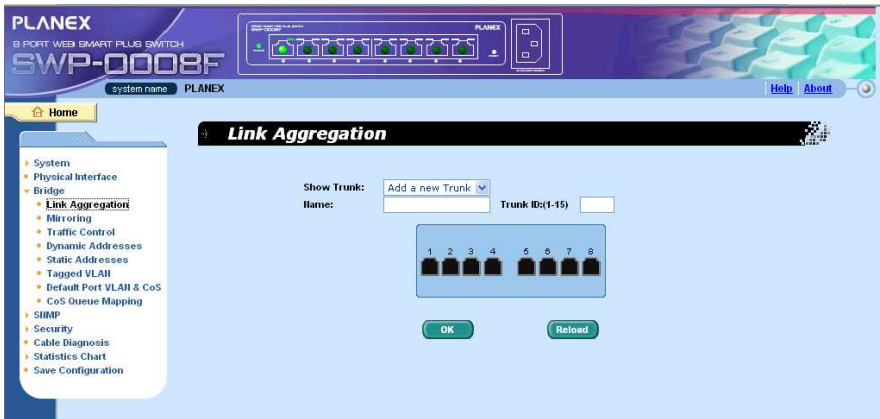


Figure 15. Link aggregation

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 untag.

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

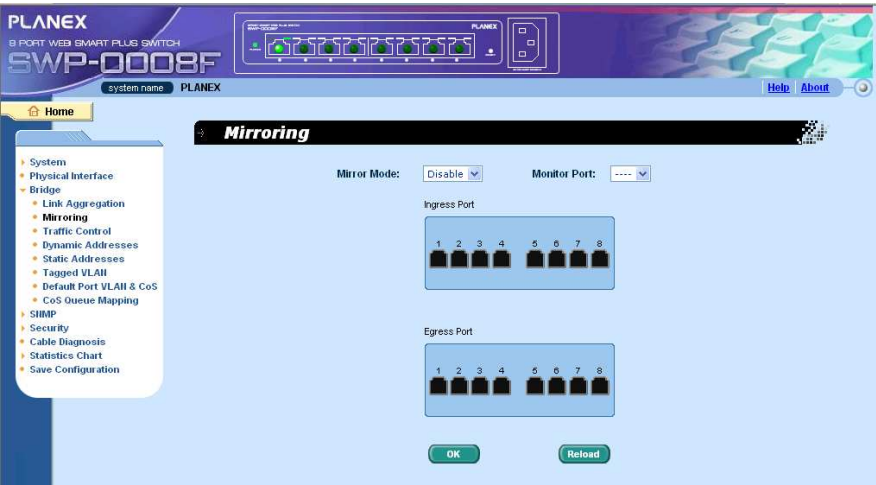


Figure 16. Mirroring page

4.5.3 Traffic Control



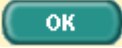


Traffic control prevents the switch bandwidth from flooding packets including broadcast packets, multicast packets. The limit number is a threshold to limit the total number of the checked type packets. For example, if broadcast / multicast is enabled, the traffic amount of each type will not exceed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



Figure 17. 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  to save the new age value. To make the configuration effective, please go to “Save Configuration” page, then click on .

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

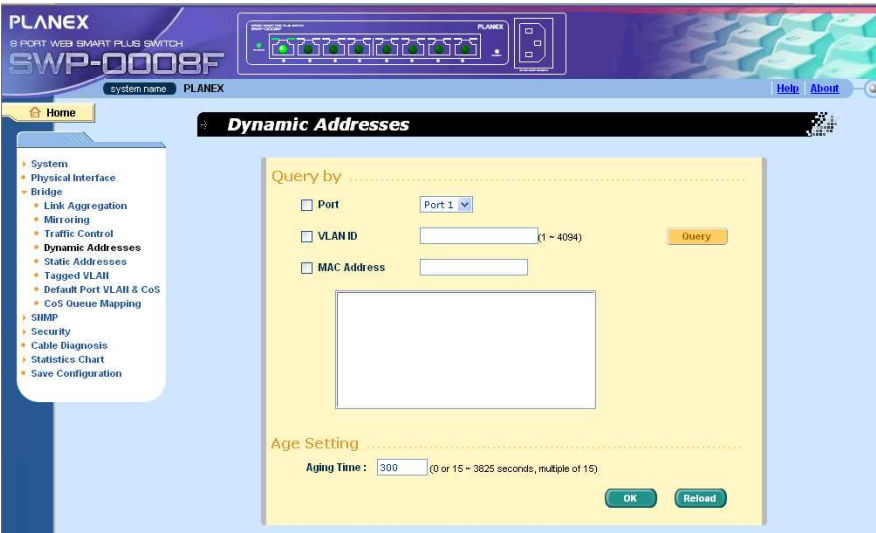


Figure 18. Dynamic Address

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

Discard on: you can do packet filtering when the MAC address appears in the packets as destination address.

Click on  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 . The  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 . The address window will mark the result of the query. Click  to save effective. Click  to refresh the settings to current value. To make the configuration effective, please go to "save configuration" page, then click .

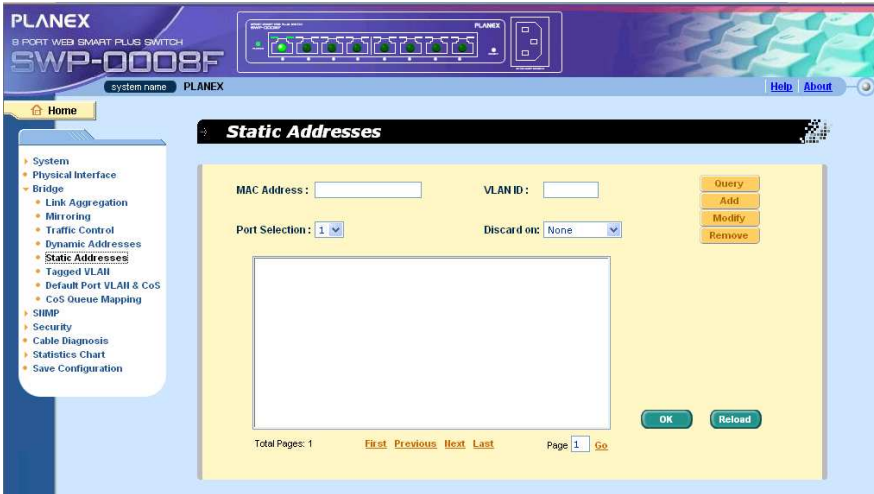


Figure 19. Static Address

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.

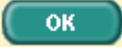

If one untagged port belongs to two or more VLAN groups at the same time, it will confuse the switch and cause flooding traffics. To prevent it, the switch only allows one untagged port belongs to one VLAN at the same time. That is, the untagged port belongs to the VLAN group which is called “PVID” and 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  to save the configuration. To make the configuration effective, go to “Save Configuration” page, then click on .

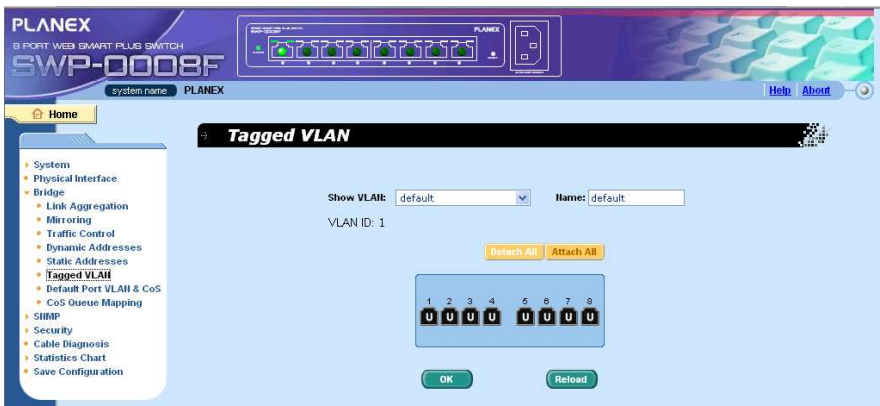


Figure 20. Tagged VLAN

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**.

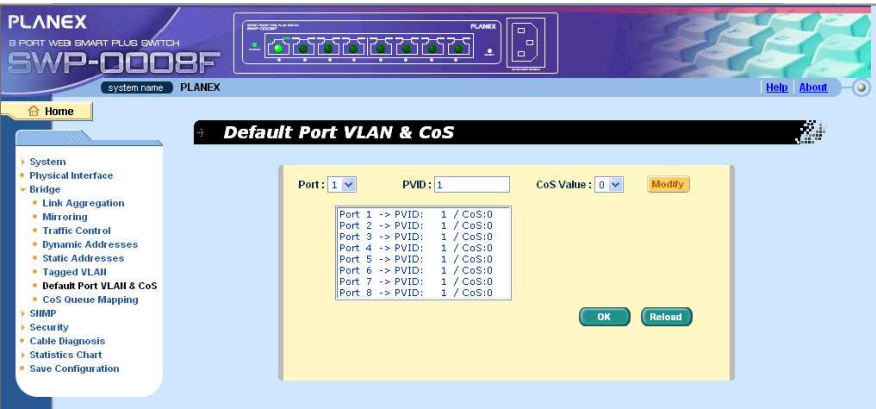


Figure 21. Default Port VLAN and CoS

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 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**

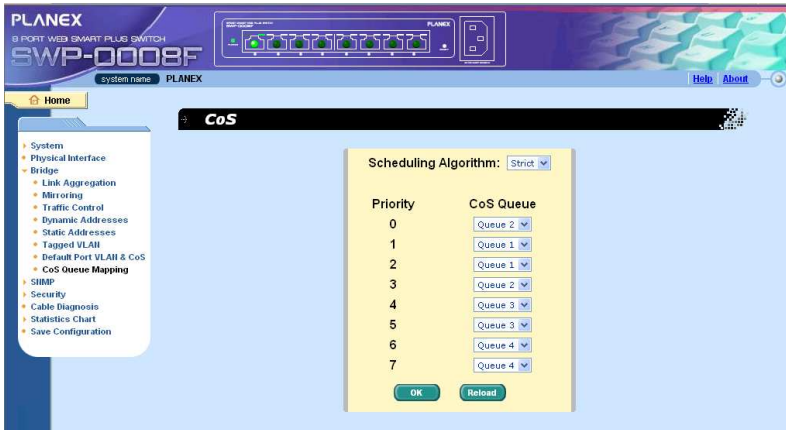


Figure 22. Cos Queue Mapping

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



 to save the configuration permanently or  to refresh the page.



Figure 23. 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.

The screenshot shows the PLANEX SWP-0008F web interface. The top banner includes the device name and a status bar. The left sidebar contains a navigation menu with options like System, Physical Interface, Bridge, STP, Community Table, Host Table, Trap Setting, Security, Cable Diagnosis, Statistics Chart, and Save Configuration. The main content area is titled 'Host Table' and contains a table with two columns: 'Host IP Address' and 'Community'. The table has 10 rows. The first row has '127.0.0.1' and 'private'. The second row has '0.0.0.0' and 'public'. The remaining 8 rows have empty IP address fields and 'private' in the community dropdown. At the bottom of the table are 'OK' and 'Reload' buttons.

Host IP Address	Community
127.0.0.1	private
0.0.0.0	public
	private
	private
	private
	private
	private
	private
	private
	private

Figure 24. 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 v2c). Click **OK** to save the configuration permanently or **Reload** to refresh the page.

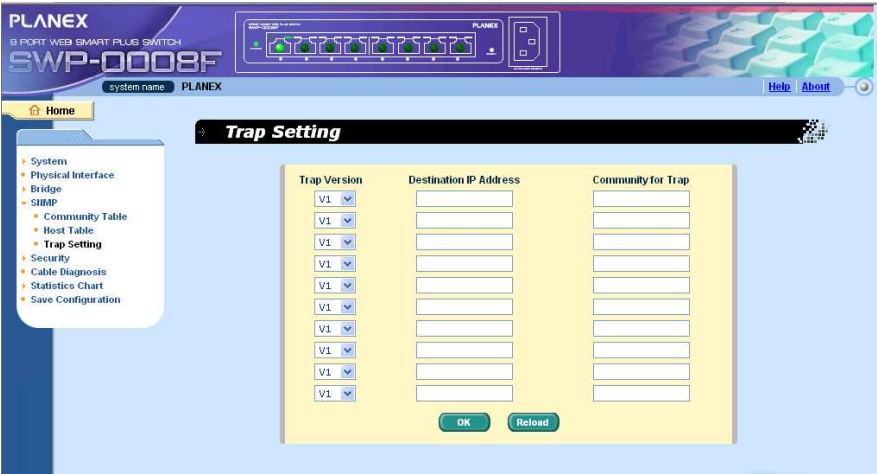


Figure 25. Trap Setting

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 VLAN 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  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.

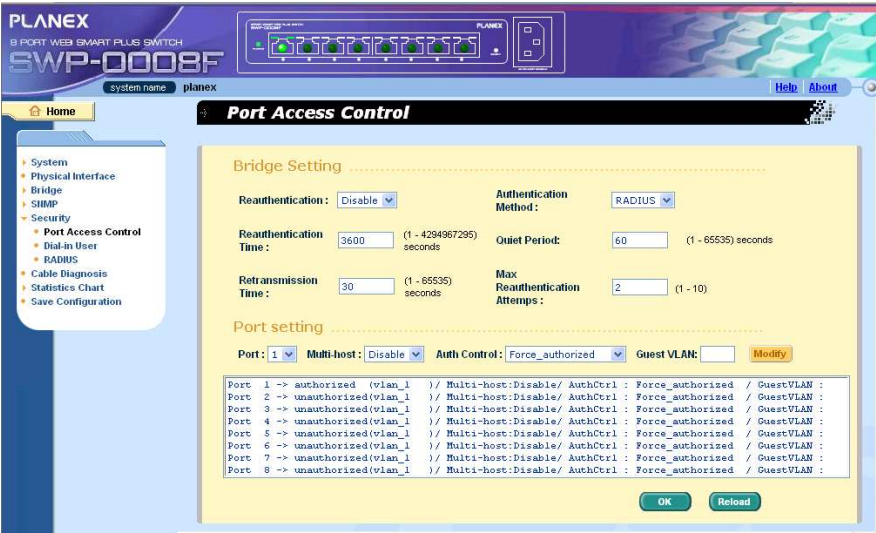


Figure 26. Port Access Control

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.

The screenshot displays the PLANEX SWP-0008F web management interface. The top header includes the device name 'PLANEX SWP-0008F' and a navigation bar with 'Home', 'Help', and 'About'. A left sidebar lists configuration categories: System, Physical Interface, Bridge, SHMP, Security (with sub-items like Port Access Control, **Dial-in User**, and RADIUS), Cable Diagnose, Statistics Chart, and Save Configuration. The main content area is titled 'Dial-in User' and contains a form with the following fields: 'User Name', 'Password', 'Confirm Password', and 'Dynamic VLAN'. To the right of the 'Confirm Password' and 'Dynamic VLAN' fields are buttons for 'Add', 'Modify', and 'Remove'. At the bottom right of the form are 'OK' and 'Reload' buttons. A large empty rectangular box is positioned below the input fields.

Figure 27. 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 SWP-0008F 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.

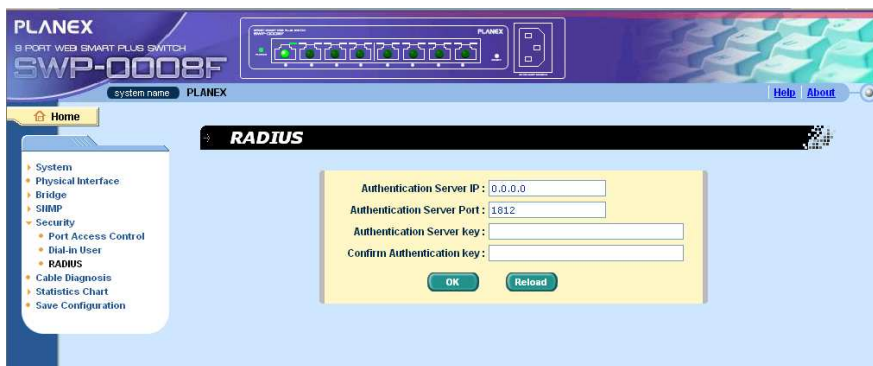


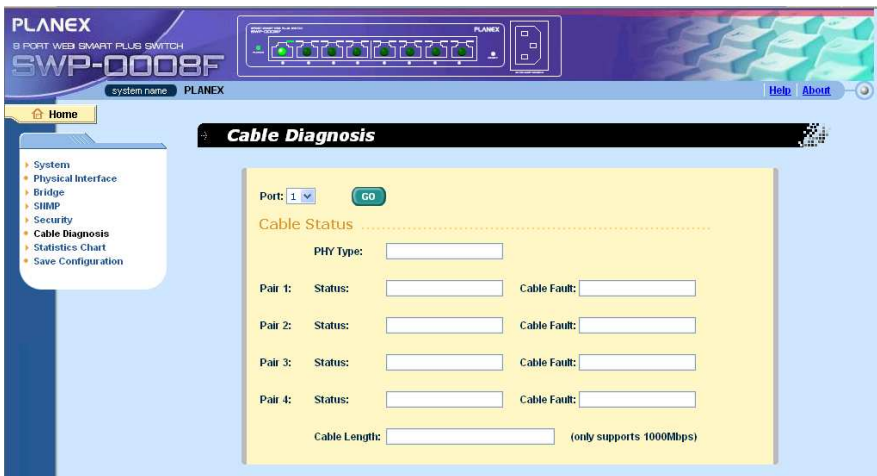
Figure 28. RADIUS

4.8 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 . Test result shall be displayed accordingly.

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



The screenshot displays the web management interface for the PLANEX SWP-0008F 8 PORT WEB SMART PLUS SWITCH. The interface includes a top navigation bar with the device name and a sidebar menu on the left with options like System, Physical Interface, Bridge, Span, Security, Cable Diagnosis, Statistics Chart, and Save Configuration. The main content area is titled "Cable Diagnosis" and contains a form for testing. At the top of the form, there is a "Port:" dropdown menu set to "1" and a green "GO" button. Below this, the "Cable Status" section is divided into two columns. The left column lists "PHY Type:" and "Cable Length:". The right column lists "Status:" and "Cable Fault:" for each of the four port pairs (Pair 1, Pair 2, Pair 3, Pair 4). Each item has an associated input field. A note at the bottom right of the form states "(only supports 1000Mbps)".

Figure 29. Cable Diagnosis

4.9 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.

Select 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.

4.9.1 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.

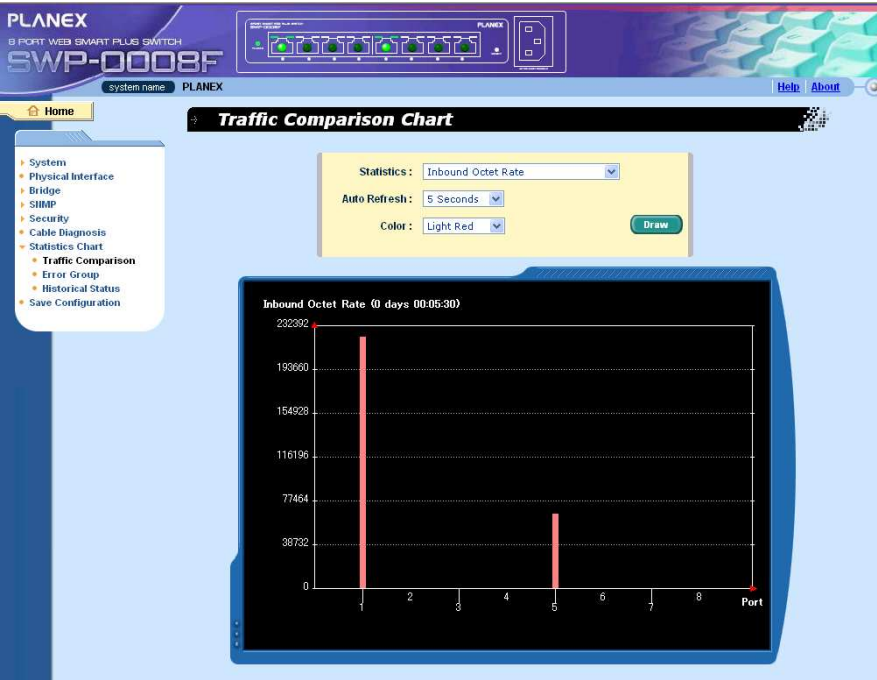


Figure 30. Traffic comparison

4.9.2 Error Group

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

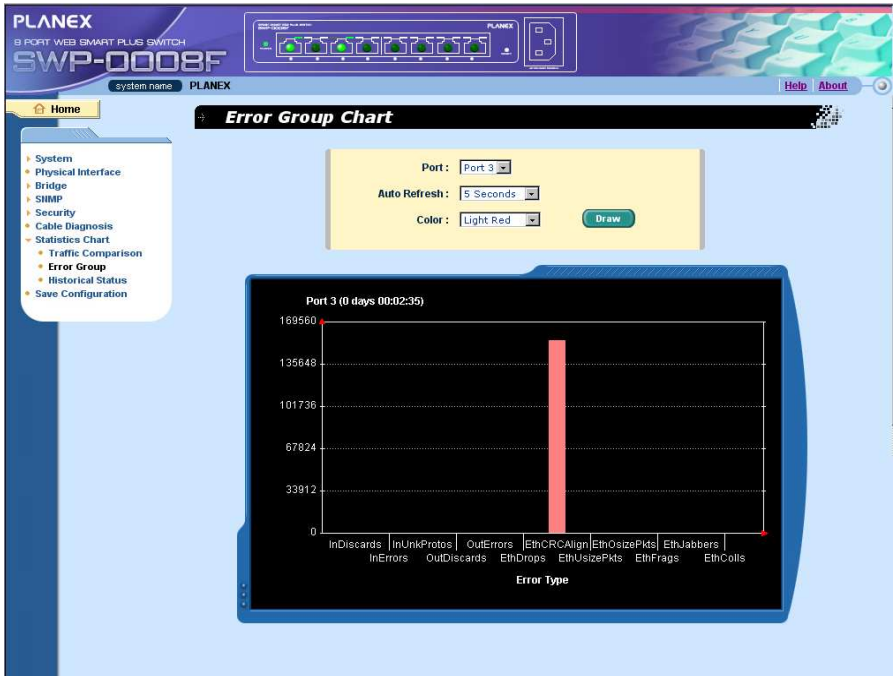


Figure 31. Error group

4.9.3 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.

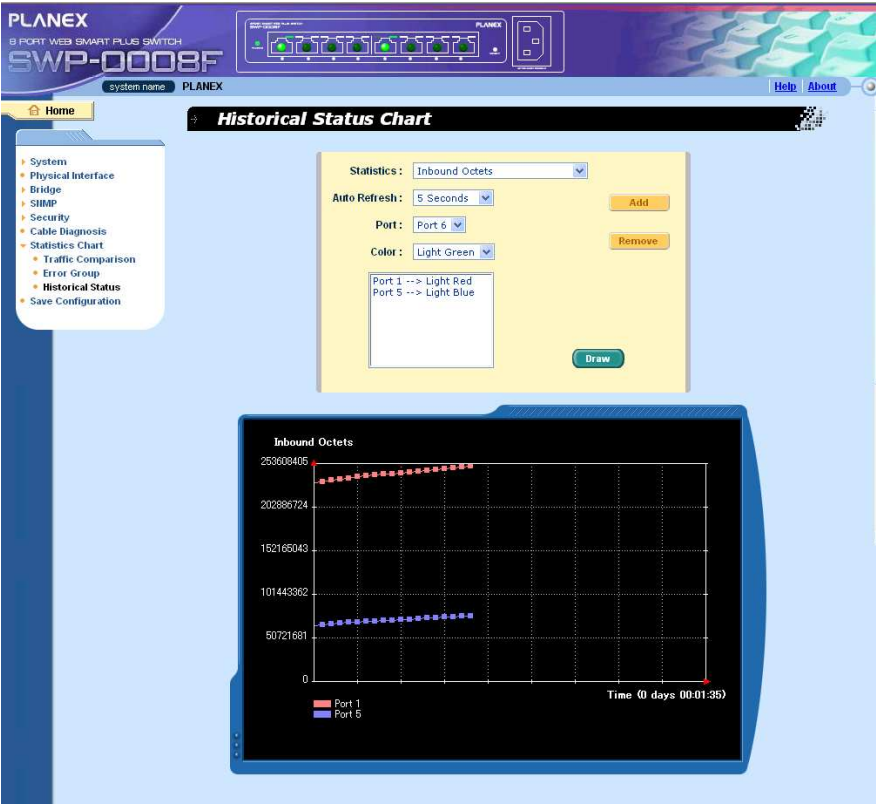




Figure 32. Historical Status

4.10 Save Configuration

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

Sometimes you may want to reset the switch configuration, you can click on  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.

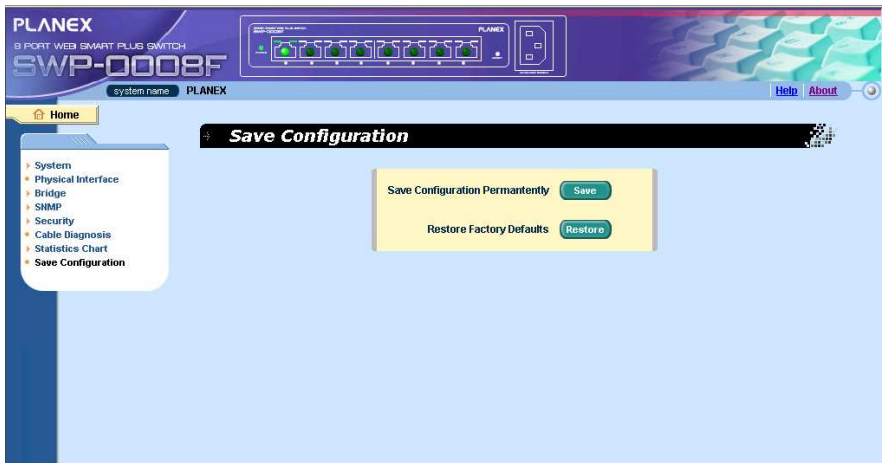


Figure 33. Save Configuration

5 The configuration backup and restore

5.1 The configuration backup method

Use MS-DOS prompt, 192.168.1.1 is SWP-0008F's IP-address.

C:\>ftp 192.168.1.1

Connected to 192.168.1.1.

220 PLANEX SWP-0008F FTP version 1.0 ready

User (192.168.1.1:(none)): admin

331 Enter PASS command

Password:

230 Logged in

ftp> get backup -----> configuration backup
command (file name is backup)

200 Port command okay

150 Opening data connection for RETR backup

226 File received OK

ftp: 48972 bytes received in 0.64Seconds 76.52Kbytes/sec.

ftp>bye

Backup file is made as file-name backup.

5.2 The configuration restore method

Use MS-DOS prompt, 192.168.1.1 is SWP-0008F's IP-address.

If there is backup file in C:\ ,

C:\>ftp 192.168.1.1

Connected to 192.168.1.1.

220 PLANEX SWP-0008F FTP version 1.0 ready

User (192.168.1.1:(none)): admin

331 Enter PASS command

Password:

230 Logged in

ftp> put backup

→ configuration restore command (file name is backup)

200 Port command okay

150 Opening data connection for RETR backup

226 File sent OK

ftp: 48972 bytes sent in 0.00Seconds 48972000.00Kbytes/sec.

ftp> bye

221 System is rebooting, bye

→system will reboot after configuration restore command

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 6 shows the structure of an IP address.

Table 6. IP address structure

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

Following are examples of valid IP addresses:

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

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

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

6.1.2 Network classes

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

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

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

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

Some important notes regarding IP addresses:

The class can be determined easily from field1:

field1 = 1-126: Class A

field1 = 128-191: Class B

field1 = 192-223: Class C

(field1 values not shown are reserved for special uses)

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

6.2 Subnet masks



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

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

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

255.255.255.128

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

11111111. 11111111. 11111111.10000000

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

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

255.255.255.192 or 11111111. 11111111. 11111111.11000000

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

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



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

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

7 Troubleshooting

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

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


7.1 Diagnosing problems using IP utilities

7.1.1 Ping

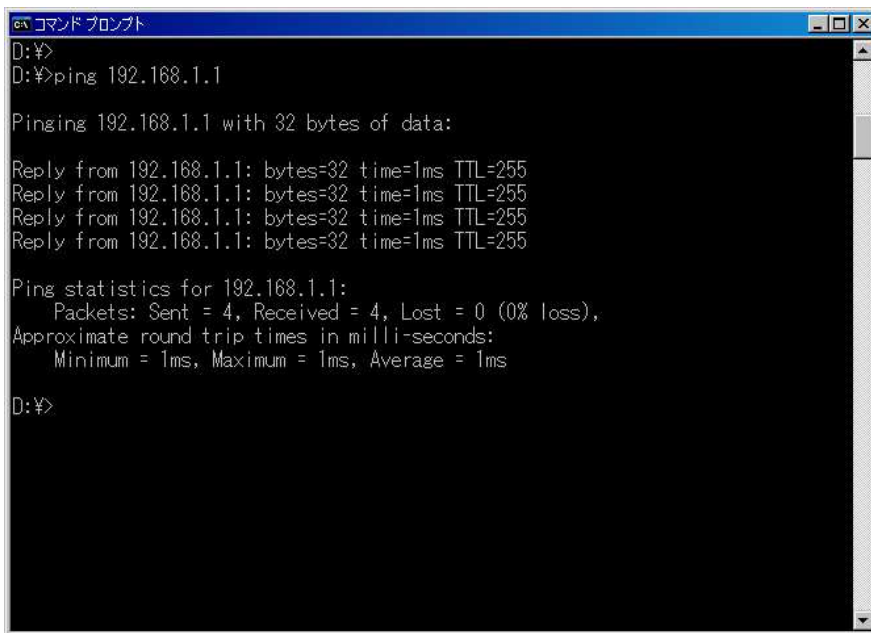
Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer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

On Windows-based computers, you can execute a ping command from the Start menu. Click the Start button, and then click Run. In the Open text box, type a statement such as the following: ping 192.168.1.1

ping 192.168.1.1

Click . 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 34.



```
コマンド プロンプト
D:\>
D:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

D:\>
```

Figure 34. Using the ping utility

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

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

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


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

7.1.2 nslookup

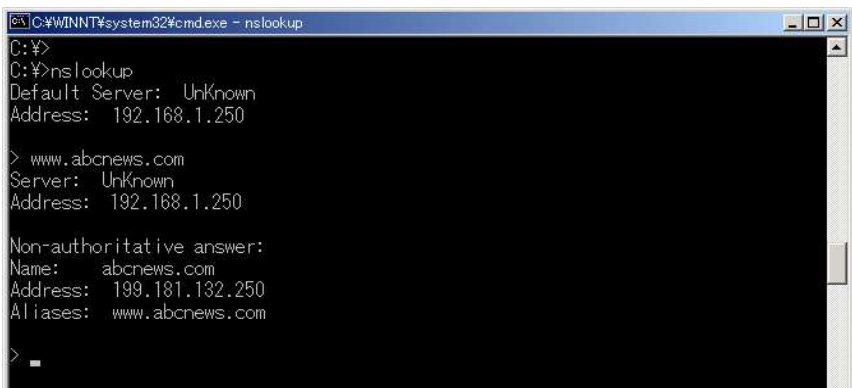
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred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

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

nslookup

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

The window displays the associate IP address you know. See Figure 35.



```
C:\WINNT\system32\cmd.exe - nslookup
C:\>
C:\>nslookup
Default Server: Unknown
Address: 192.168.1.250

> www.abcnews.com
Server: Unknown
Address: 192.168.1.250

Non-authoritative answer:
Name:      abcnews.com
Address: 199.181.132.250
Aliases:   www.abcnews.com

> _
```


Figure 35. Using the nslookup utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information. To exit from the nslookup utility, type **exit** and press <Enter> at the command prompt.

7.2 Simple fixes

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

Table 7. Troubleshooting

Problem	Suggested Action
LEDs	
SYSTEM LED does not light up after the switch is turned on.	Verify if the power cord is securely connected to the switch and a wall socket/power strip.
Network Access	
PC cannot access another host in the same network	<ol style="list-style-type: none">1. Check the Ethernet cabling is good and the LED is green.2. If the port LED is amber, check if this port is disabled. .
PCs cannot display web configuration pages.	<ol style="list-style-type: none">1. The switch is powered up and the connecting port is enabled. The factory default IP for the switch is 192.168.1.1.2. Verify your network setup in your PC for this information. If your PC does not have a valid route to access the switch, change the switch IP to an appropriate IP that your PC can access.3. Ping "switch IP" from the PC, if it still fails, repeat step 2.
Web Configuration Interface	
You forgot/lost your WEB Configuration Interface user ID	If you have not changed the password from the default, try using "admin" as the user ID.
Some pages do not display completely	<ol style="list-style-type: none">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.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.
Changes to Configuration are not being retained.	Be sure to click on  button in the Save Configuration page to save any changes.
Setting Factory default	
Setting Factory default.	You can press the reset button about 3 ~ 5 seconds, then the switch will reboot and reset the configurations to the factory default.

8 Glossary

10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. <i>See also data rate, Ethernet.</i>
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. <i>See also data rate, Ethernet.</i>
1000BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 1000 Mbps.
binary	The "base two" system of numbers, that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. <i>See also bit, IP address, network mask.</i>
bit	Short for "binary digit," a bit is a number that can have two values, 0 or 1. <i>See also binary.</i>
bps	bits per second
CoS	Class of Service. Defined in 802.1Q, the value range is from 0 to 7.

broadcast	To send data to all computers on a network.
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. <i>See also 10BASE-T, 100BASE-T, twisted pair.</i>
FTP	<p>File Transfer Protocol</p> <p>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.</p>
host	A device (usually a computer) connected to a network.
ICMP	<p>Internet Control Message Protocol</p> <p>An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.</p>
IGMP	<p>Internet Group Management Protocol</p> <p>An Internet protocol that enables a computer to share information about its membership in multicast groups with adjacent routers.</p> <p>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.</p>
IGMP Snooping	Snoop the IGMP packets on each port and associate the port with a layer 2 muticast group.

mask	<i>See network mask.</i>
Multicast	To send data to a group of network devices.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
Monitor	Also called " <i>Roving Analysis</i> ", allow you to attach a network analyzer to one port and use it to monitor the traffics of other ports on the switch.
network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. <i>See also binary, IP address, subnet, "IP Addresses Explained" section.</i>
NIC	<p>Network Interface Card</p> <p>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. <i>See Ethernet, RJ-45.</i></p>
packet	<p>Data transmitted on a network consists of units called packets.</p> <p>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).</p>

ping	<p>Packet Internet (or Inter-Network) Groper</p> <p>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.</p>
port	<p>A physical access point to a device such as a computer or router, through which data flows into and out of the device.</p>
protocol	<p>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.</p>
remote	<p>In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.</p>
RJ-45	<p>Registered Jack Standard-45</p> <p>The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.</p>
RMON	<p>Remote Monitoring</p> <p>Extensions to SNMP, provide comprehensive network monitoring capabilities.</p>
routing	<p>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.</p>

SNMP	<p>Simple Network Management Protocol</p> <p>The TCP/IP protocol used for network management.</p>
STP	<p>Spanning Tree Protocol</p> <p>The bridge protocol to avoid packet looping in a complicate network.</p>
subnet	<p>A subnet is a portion of a network. The subnet is distinguished from the larger network by a <i>subnet mask</i> 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. <i>See also network mask.</i></p>
subnet mask	<p>A mask that defines a subnet. <i>See also network mask.</i></p>
TCP	<p><i>See TCP/IP.</i></p>
TCP/IP	<p>Transmission Control Protocol/Internet Protocol</p> <p>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.</p>

Telnet/SSH	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.
TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
Trunk	Two or more ports are combined as one virtual port, also called as Link Aggregation.
TTL	Time To Live A field in an IP packet that limits the life span of that packet. Originally meant as a time duration, the TTL is usually represented instead as a maximum hop count; each router that receives a packet decrements this field by one. When the TTL reaches zero, the packet is discarded.
twisted pair	The ordinary copper telephone wiring long used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. <i>See also 10BASE-T, 100BASE-T, Ethernet.</i>

upstream	The direction of data transmission from the user to the Internet.
VLAN	Virtual Local Area Network
WAN	<p>Wide Area Network</p> <p>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.</p>
Web browser	<p>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. <i>See also HTTP, web site, WWW.</i></p>
Web page	<p>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 <i>home page</i>. <i>See also hyperlink, web site.</i></p>
Web site	<p>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. <i>See also hyperlink, web page.</i></p>