

Copyright Information

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 ASUS-TeK COMPUTER INC. (“ASUS”).

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.

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.

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.

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.

Copyright © 2004 ASUSTeK COMPUTER INC. All Rights Reserved.

Limitation of Liability

Circumstances may arise where because of a default on ASUS’ part or other liability, you are entitled to recover damages from ASUS. In each such instance, regardless of the basis on which you are entitled to claim damages from ASUS, ASUS is liable for no more than damages for bodily injury (including death) and damage to real property and tangible personal property; or any other actual and direct damages resulted from omission or failure of performing legal duties under this Warranty Statement, up to the listed contract price of each product.

ASUS will only be responsible for or indemnify you for loss, damages or claims based in contract, tort or infringement under this Warranty Statement.

This limit also applies to ASUS’ suppliers and its reseller. It is the maximum for which ASUS, its suppliers, and your reseller are collectively responsible.

UNDER NO CIRCUMSTANCES IS ASUS LIABLE FOR ANY OF THE FOLLOWING: (1) THIRD-PARTY CLAIMS AGAINST YOU FOR DAMAGES; (2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR (3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF ASUS, ITS SUPPLIERS OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY.



Centralized Network Management

GigaX Management Software

User's Manual

Product Name:	CNM Software
Manual Revision:	1 E1604
Release Date:	May 2004

Table of Contents

1 Introduction	1-3
1.1 GigaX 1024P Features	1-3
1.2 Using this Document	1-5
1.3 ASUS contact information	1-5
2 Getting to Know the GigaX 1024P	1-6
2.1 Parts List	1-6
2.2 Front Panel	1-7
2.3 Rear Panel	1-7
2.4 Technical Specifications	1-8
3 Quick Start Guide	1-9
3.1 Part 1 — Connecting the Hardware	1-9
3.2 Part 2 —Start the Switch	1-11
3.3 Management from CNM.....	1-13
4 Management Functions	1-15
4.1 Start CNM Program	1-15
4.2 Functional Layout	1-16
4.3 General Settings for CNM.....	1-18
4.4 Switch Topology	1-21
4.5 Switch Setup	1-24
4.6 System	1-25
4.7 Configuration	1-31
4.8 Statistics.....	1-38

1 Introduction

Congratulations on your purchase of the ASUS GigaX 1024P. You can now manage your LAN (Local Area Network) through a friendly and powerful user interface, the ASUS CNM. The ASUS CNM runs on Windows OS. Please refer to the CNM installation guide for CM installation details.

This User Guide will show you how to set up the GigaX 1024P through CNM, and how to customize its configuration to get the most out of this product.

1.1 GigaX 1024P Features

- (24) 10/100BASE-TX auto-sensing Fast Ethernet switching ports
- (2) 10/100/1000BASE-T auto-sensing Gigabit Ethernet switching ports
- Auto MDI/MDIX support for 10/100BASE-TX & 10/100/1000BASE-T ports
- 802.3, 802.3u and 802.3ab compliant
- 8.8 Gbps switch capacity and 6.6 Mpps forwarding rate
- 8K MAC address cache with hardware-assisted aging
- 802.3x flow control
- 802.1Q-based tagged VLAN, up to 32 VLANs
- 802.1p CoS (Class of Service), 2 queues per port
- IGMP(v1, v2) snooping support
- 802.3ad link aggregation (trunking), up to 8 trunk groups
- Bandwidth management for each port and Tx/Rx direction
- Broadcast storming filtering
- CNM Windows-based software provides easy management
- LEDs for port link status, speed, duplex mode and collisions

1.2 Using this Document

1.2.1 Notational conventions

- 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 Typographical conventions

- *Italics* are used to present the texts displayed or you type in the CNM user interface.
- **Boldface** type text is used for items you select from menus and drop-down lists

1.2.3 Special messages

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



Note: Provides clarification or nonessential 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.

1.3 ASUS contact information

ASUSTeK COMPUTER INC. (Asia-Pacific)

Web Site Address: www.asus.com.tw
General Email: info@asus.com.tw
General Telephone: +886-2-2894-3447
General Fax: +886-2-2894-7798

Technical Support

Networking (Tel): +886-2-2890-7902 (English)
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)

Web Site Address: usa.asus.com
General Email: tsd@asus.com
General Fax: +1-510-608-4555

Technical Support

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

ASUS COMPUTER GmbH (Germany & Austria)

Web Site Address: www.asuscom.de
Online Contact: www.asuscom.de/sales
General Telephone: +49-2102-95990
General Fax: +49-2102-959911

Technical Support

Online Support: www.asuscom.de/support
Support Fax: +49-2102-959911
Component Support: +49-2102-95990
Notebook Support: +49-2102-959910

ASUS COMPUTER (Middle East and North Africa)

Web Site Address: www.ASUSarabia.com
General Telephone: +9714-283-1774
General Fax: +9714-283-1775

2 Getting to Know the GigaX 1024P

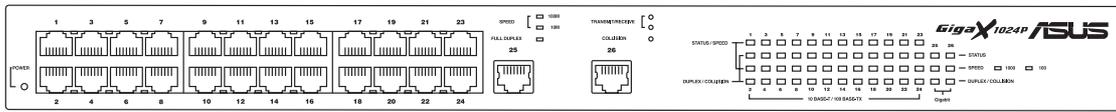
2.1 Parts List

In addition to this document, the switch should come with the following:

- GigaX 1024P managed switch
- AC Power cord
- Rack installation kit (2 brackets with 6 screws (M3 x 6L))
- Installation CD-ROM
- Quick installation guide

2.2 Front Panel

The front panel contains LED indicators that show the status of the unit.



Label	Color	Light	Function
POWER	Green	On	The switch is powered on and operate normally
		Off	The switch is powered off

10/100 ports from 1 to 24

STATUS / SPEED	Green	On	Ethernet link is established in 100 Mbps
		Flashing	Data frames are being transmitted on this port
		Off	No Ethernet link
	Amber	On	Ethernet link is established in 10 Mbps
		Flashing	Data frames are being transmitted on this port
DUPLEX / COLLISION	Amber	On	The port is operating in full duplex mode
		Flashing	The port is operating in half duplex mode and collisions are occurring
		Off	The port is operating in half duplex mode

10/100/1000 Gigabit ports form 25 to 26

STATUS	Green	On	Link is present
		Flashing	Data frames are being transmitted/received on this port
		Off	Link is not present
SPEED	Green	On	1000Mbps
		On	100Mbps
		Off	10Mbps
DUPLEX / COLLISION	Amber	On	The port is operating in full duplex mode
		Flashing	The port is operating in half duplex mode and collisions are occurring
		Off	The port is operating in half duplex mode

2.3 Rear Panel

The rear panel contains the ports for the unit's power connections.



Label	Function
POWER	Connects to the supplied power cord

2.4 Technical Specifications

Physical Dimensions: 43.5mm(H) X 444 mm(W) X 200mm(D)

Environmental Ranges:

Operating temperature:	-10°C to 50°C (14°F to 122°F)
Storage temperature:	-40°C to 70°C (-40°F to 158°F)
Operating humidity:	15% to 90%
Storage humidity:	00% to 95%

Power:

Input:	100-240V AC / 2.5A / 50-60Hz
Power Consumption:	12W

3 Quick Start Guide

This Quick Start Guide provides basic instructions to set up the GigaX environment.

- Part 1 shows you how to install the GigaX on a flat surface or in a rack.
- Part 2 provides instructions to set up the hardware.
- Part 3 shows you how to configure basic settings on the GigaX.

This Quick Start Guide assumes that you have installed ASUS CNM in a Windows PC. Both the switch and the PC are located in the same network. For CNM installation, please refer to the CNM installation guide.

3.1 Part 1 — Connecting the Hardware

In Part 1, you select a proper place to install the switch. Please use the operating environment specifications as references to choose the installation place. The Ethernet cable length from the switch to an attached device cannot exceed 100 meters (328 feet).

3.1.1 Installing the Switch on a Flat Surface

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

3.1.2 Mounting the Switch in a Rack

1. Attach brackets to each side of the switch and make sure that the posts are correctly inserted into the switch. Use the screws provided to fasten the brackets to the switch.
2. Place the switch in the rack, insert and tighten two screws from the brackets on the switch to the nuts on the rack.

3.2 Part 2 —Start the Switch

In Part 2, this guide will show you how to connect the switch to a power outlet, to your computer (with CNM installed), and to the network.

3.2.1 Step 1. Connect to the PC with CNM Installed

The switch can be managed through the ASUS CNM software that is running on a Windows OS computer. Please refer to the CNM installation guide for details. Before starting the CNM application, you have to connect the PC to the same network as the switch is attached to.

3.2.2 Step 2. Connect to 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. Note that both the crossover or straight-through Ethernet cable can be used to connect computers, hubs or switches.



Note: Use twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port. Otherwise, the link speed can not reach 1Gbps.

3.2.3 Step 3. Attach the power cord.

1. Plug the female end of the AC power cord to the POWER receptacle on the back of the switch.
2. Check the front LED indicators with the table 3.1. If the LEDs illuminate as expected, the switch hardware is working properly.
3. Plug the male end of the AC power cord into a wall outlet or a power strip.

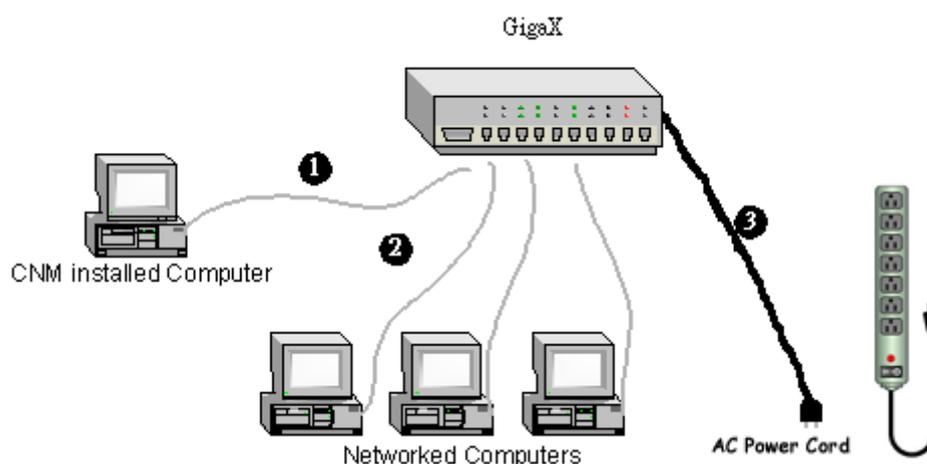


Figure 3.1. Overview of Hardware Connections

LED Indicators

This LED	Should be
POWER	Solid green to indicate that the device is turned on. If this light is not on, check if the power cord is attached to the switch and if it is plugged into a power source.
STATUS of 10/100 ports	Solid green/amber to indicate that the device can communicate with your LAN or flashing when the device is sending or receiving data from your LAN computer.
STATUS of Gigabit ports	Solid green to indicate that the device can communicate with your LAN or flashing when the device is sending or receiving data from your LAN computer.

Table 3.1. LED Indicators

3.3 Management from CNM

In Part 3, start the CNM program and manage the switch to meet your network requirements. Before starting CNM, make sure that your manage station is attached to the same network as the switch is. Otherwise, CNM will not be able to discover the switch.



Note: This version of CNM only manages the switches in the same network.

3.3.1 Switch Discovery and Management

1. Make sure that the switch is powered ON and that the CNM is installed on the management station.
2. Click on the CNM shortcut icon in the desktop of the manage station to start the CNM application. CNM will display a window as shown in Figure 3.2

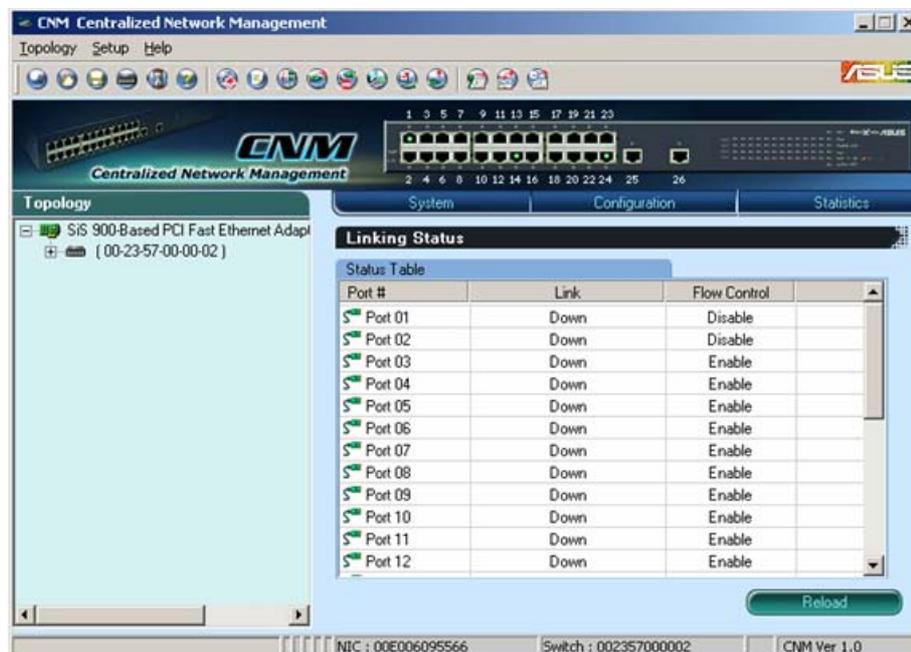


Figure 3.2. CNM Outlook

3. Select the proper NIC at the same network with the switch, then click on the **Discovery** icon in the tool bar. After the discovery is done, the left frame of the window will show the MAC addresses of the switches discovered by the CNM as Figure 3.3.

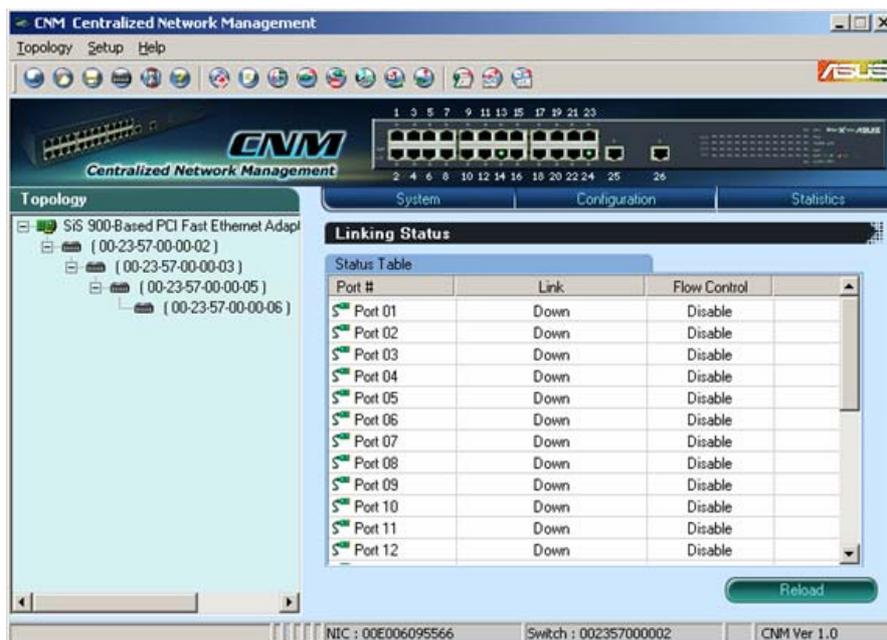


Figure 3.3. Available Switches

4. Select the switch you want to manage by clicking on the MAC address, then you can start to configure the switch by CNM.
5. If the CNM cannot discover the switch you want to manage, please repeat step 1 to 4 again.



Note: The switch must be powered on and connect to your network before starting the CNM.

3.3.2 Password Recovery

The switch is protected by a password. The password is required to make CNM able to manage the switch. Once the password is lost, you need to reset the password back to factory default password, which is **0x2379**. The password is four digit long, could be change through CNM.

1. Prepare one Cat-5 cable and unplug all the cables in the switch ports.
2. Power off the switch, then power it on. Within 20 seconds after power on, plug the Cat-5 cable to port 3 and 4. That is, make a loop by port 3 and 4. The password will reset to default value.
3. Remain the loop about 1 minute to let the password reset happen.
4. Unplug the cable, then power cycle the switch. You can manage the switch by default password.



Note: To reset the password, there must be no connection in the switch except the loop between port 3 and 4.

3.3.3 Factory Default Setting

You can reset the switch configuration back to factory default value by the similar steps as the password recovery. Instead of looping port 3 and 4, use port 1 and 2 to make a loop.

1. Prepare one Cat-5 cable and unplug all the cables in the switch ports.
2. Power off the switch, then power it on. Within 20 seconds after power on, plug the Cat-5 cable to port 1 and 2. That is, make a loop by port 1 and 2. The configuration will reset to factory default value.
3. Remain the loop about 1 minute to let the configuration reset happen.
4. Unplug the cable, then power cycle the switch. You can manage the switch by default password and the switch configuration is back to factory default.

4 Management Functions

ASUS provide a Centralized Network Management (CNM) software to allow users manage the switch in your network. The program is designed to work best with Microsoft Windows operation system.

4.1 Start CNM Program

1. Install CNM in a computer running Windows OS. Refer to CNM installation guide for detail installation steps.
2. The computer with CNM installed must be in the same network as the switches are.
3. Make sure the switches are power on and the network links are good.
4. Click the CNM icon on the PC's desktop. A CNM window comes out as Figure 4.1. This computer becomes the manage station to the switches.
5. Figure 4.1 shows that a password is required to login and control the switch. Use the default password **0x2379**, if it has not been changed.

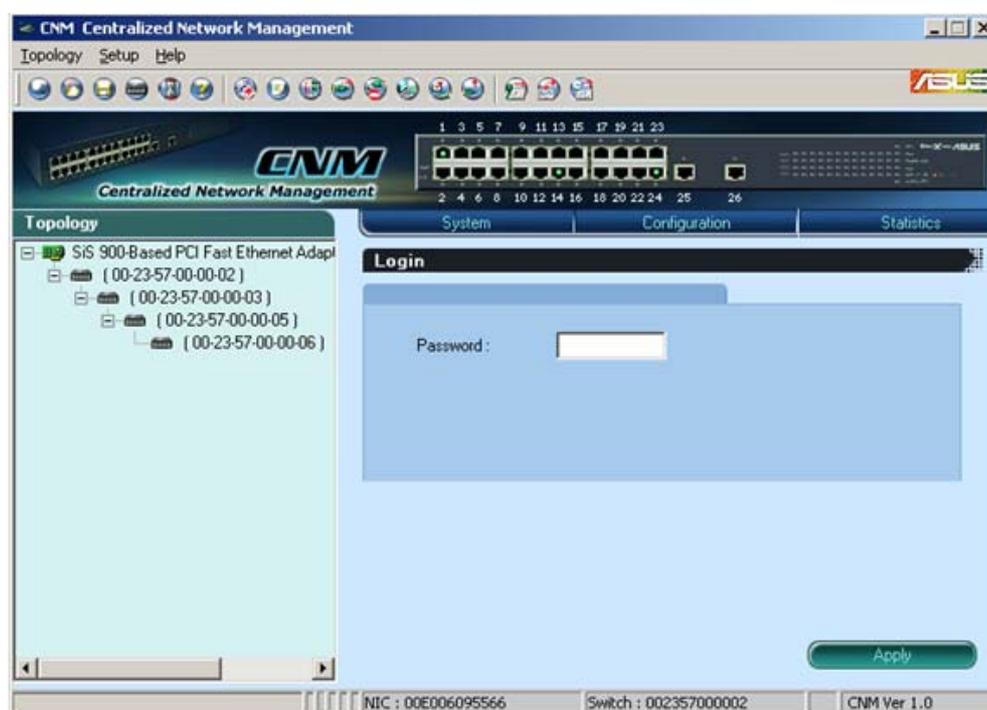


Figure 4.1. CNM window

4.2 Functional Layout

The CNM window consists of three separate frames. The top frame has switch logo and front panel as shown in Figure 4.2. This frame remains on the top of the browser window all the times and updates the LED status periodically. The LED definition has been described as Table 2.1. Each port shows different states by different colors, shown as Table 4.1.



Figure 4.2. Top frame

Green Blinking port	Ethernet link is established
Black	No Ethernet link

Table 4.1. Description of Port Color

The left frame, a topology frame as shown in Figure 4.3, contains all the NICs in the manage station. Each NIC has a tree view to show the switches that are discovered by CNM. You can click on any of these to display a specific configuration of the switch.

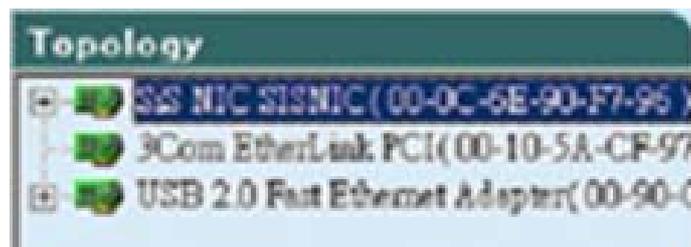


Figure 4.3. A Topology Frame

Click on the NIC, it shows the topology of the switches in the network. If multiple switches are cascaded, the tree view will show the relationship of those switches as Figure 4.4.

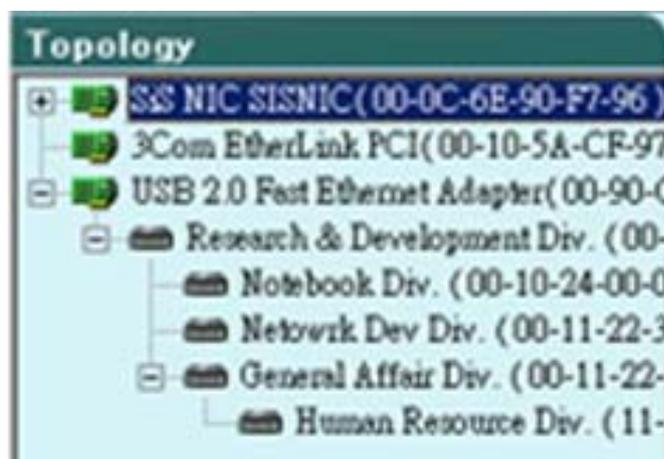


Figure 4.4. Tree view of the network topology

The right frame displays the specified switch configurations or graphics for the statistics. That is, it displays different configuration layout for different model. Section 4.5 will describe 1024P configuration in details. You have to specify a switch by clicking one switch in the topology list.

4.3 General Settings for CNM

There are menu bar and tool bar on the top of the CNM window. They offer general settings for CNM.

The **Topology** item provides the general network discovery, manually add or delete switches, and load or save the current discovered topology.

The **Setup** item provides the update interval and password settings.

The **Help** item provides CNM information and instructions

4.3.1 Topology



Figure 4.5. Topology

Topology is to control the actions of the topology frame. A couple of things you can do to the topology frame are listed as following:

- 3. Discovery:** discover all the 1024Ps in all the networks that your CNM station is connecting to. The discovery result will display in the topology frame. There is a corresponding function icon  in the tool bar.
- 4. Update:** detect if the communications between the CNM station and the discovered switches is good or not. The switch icon will show  to indicate that the communication is broken.

- Add Switch:** add a switch to the topology tree manually. A window pops out for this purpose as Figure 4.6. Select the network adapter you want the switch to attach to, give the switch MAC and name, and an authentication key as the password if you don't use the default one (2379), then click OK to finish the action. However, a manually added switch does not mean it can be configured or discovered by CNM. The function provides a way to add a known switch to topology list once the CNM cannot discover the switch. There is a tool bar button for it..



Figure 4.6. Add Switch

- Remove Switch:** you can remove any switch in the topology list manually through this function. It pops out a switch list and check those switches you want to remove. Please refer to Figure 4.7 for the switch list window.



Figure 4.7. Remove Switch

7. **Load:** load a topology list from a file. There is a tool bar button for it.
8. **Save Topology:** save the current topology list to a file. There is a tool bar button for it.
9. **Save As:** specify a file name to save the topology list
10. **Exit:** exit from CNM program

4.3.2 Setup



Figure 4.8. Setup

CNM polls the switch status periodically, the polling interval can be adjusted.

1. **Auto Update Time Interval:** as Figure 4.9, a proper value can be set. The auto update time interval is used to poll the switch statistics and link status on the top of the window. The interval value could be adjusted from 0 to 300 seconds. 0 means no polling at all. There is a tool bar button for it.

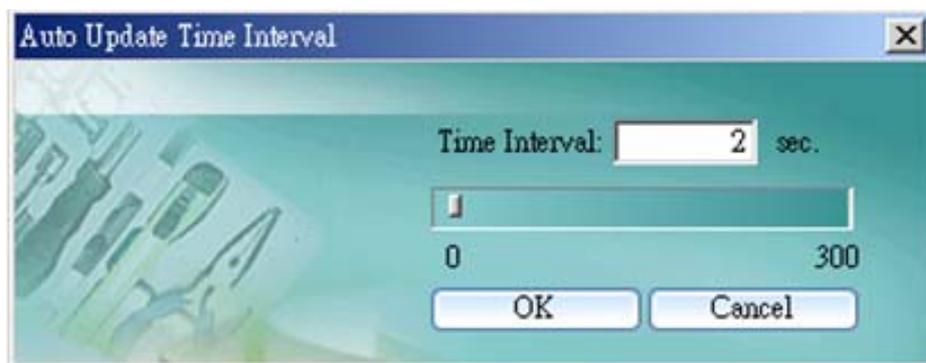


Figure 4.9. Auto Update Time Interval

4.3.3 Help

Help shows you the CNM user guide and current version.

4.4 Switch Topology

The switch topology frame is on the left part of the CNM window. It shows the discovered switches and the relationship among them. Each presents a NIC interface. The interface name and MAC address is shown after the.

The switch topology shows the relationship among the switches in a tree view. That is, if a switch A has connections to switch B and your NIC, then a cascade tree will display as Figure 4.10.

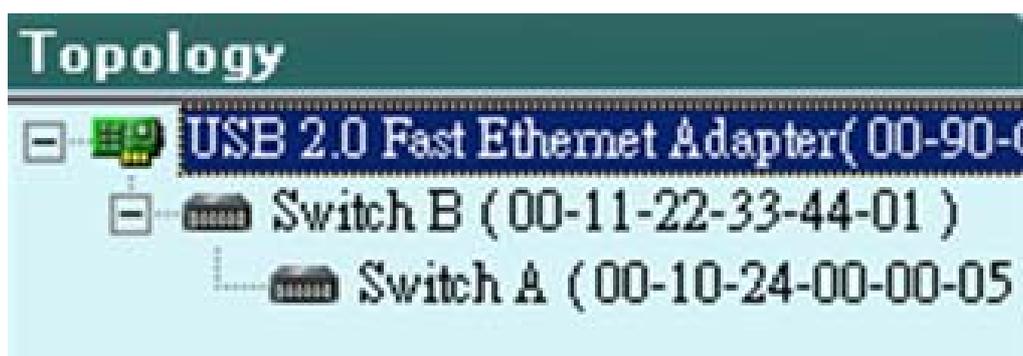


Figure 4.10. Switch Relationship

In this way, you can find the relationship among the switch. It helps design and debug your network. Each is a switch with name and MAC address followed. You can assign a name to the switch by click the right button on the mouse while the mouse is point to the switch MAC address.



Note: All the switch names are kept in CNM file, but not in the switches. So if you use CNM to manage the same switch on another management station, the name may be different because the switch does not keep its name.

4.4.1 Topology Discovery

The topology discovery is done by user's request. That is, no auto update is executed for the topology change. This will reduce the network traffics since the discovery generates some packets to query the switches.

4.4.2 Switch Add and Removal

Discovery action will create the topology tree by all the discovered switches. The default password will be used in the discovery process. Sometimes you may have a switch with another password that is different from the default one. In this case, the switch cannot be discovered by the default password. You need to add a switch to the topology manually.

Figure 4.11 shows the window to add a switch. There are a couple of columns to fill to add a switch successfully.



Figure 4.11. Add Switch

1. **Adapter:** select the corresponding adapter to add a switch under it.
2. **Switch:** check the box if you want the new switch to be added under a specified switch in the topology tree. The manually added switch will be moved to a right place to show the relationships in the topology after a successful discovery.
3. **MAC:** the most important information is the MAC address. If the MAC is wrong, the new added switch can not be accessed by CNM.
4. **Name:** a good name may remind you something about the switch. However, the switch name is good only in the same CNM file. So the name may not be unique when you use different CNM files to do discover.

Once a switch is added to the topology tree, you can find it in the corresponding place. You have to left click the switch symbol to switch the current status/configuration window from other switch to this switch. If the communication is good, you can see the linking status window on the right frame of the CNM window, and the topology tree will display the switch symbol in a correct place to show the relationship. If CNM cannot discover the manually added switch, then a  will attach to the switch to show it is not reachable to the CNM.

Figure 4.12 shows the window to remove switches, just check the box before the switch to select those you want to remove, click the remove icon to start the action. All the corresponding switches will be removed and the tree branch after the removed switches are moved up to under the adapter. A discovery action will update the topology tree for the current network. You may find the removed switches are back to the topology tree because they are discovered again.



Figure 4.12. Remove Switch



Note: The removed switch may be added back to the topology tree because the discovery action finds the switch in the network. This is normal because the switch is still working.

4.4.3 Topology Load and Save

A topology can be saved for later reference. The CNM starts with a default topology file. After the discovery action, it shows the update network topology. You can save it in a good file name and load it when you need it.

4.5 Switch Setup

Before using the configuration windows, it is better to know following buttons or icons because they are used throughout the setup. The following table describes the function for each button or icon.

Table 4.1 2. Description of Commonly Used Buttons and Icons

Button/Icon	Function
	Apply to the selected switch
	Reload the current configuration from the selected switch and display it
	No action is taken and leave the window
	Select all the ports
	Select none of the switch ports



Hint: Clicking the Apply button can only save the configuration temporarily, users need to select “Apply and Save” from “Topology” drop-down menu in order to save the configuration permanently.

Before starting any new configuration, it is always recommended to reload the current switch configuration. This will help you know what you are going to change and the communication between CNM and the switch is good.

There is a message bar on the bottom showing the NIC's MAC and the switch MAC you are working on. Check these information before applying any new configuration to prevent an improper settings.



Note: Check the message bar on the bottom to make sure you are working on the proper switch before any configuration set up.

4.6 System

There are reboot, link status and change password under the system menu.

4.6.1 Reboot

The 1024P provides hardware and software reset as shown in figure 4.13. Hardware reset is to reset the system at a initial state like the process of power on hardware reset.



Note: Hardware reset will clear all current settings if you do not save the configuration.

The software reset will rest the system to the initial state and start the port link negotiations, but the MAC table, VLAN table data, and current configuration will be kept.



Figure 4.13. Reboot

4.6.2 Link Status

Link status table shows the port information including speed, duplex mode and flow control. Click on the **Reload** button will get the update information. Figure 4.14 shows the status table.

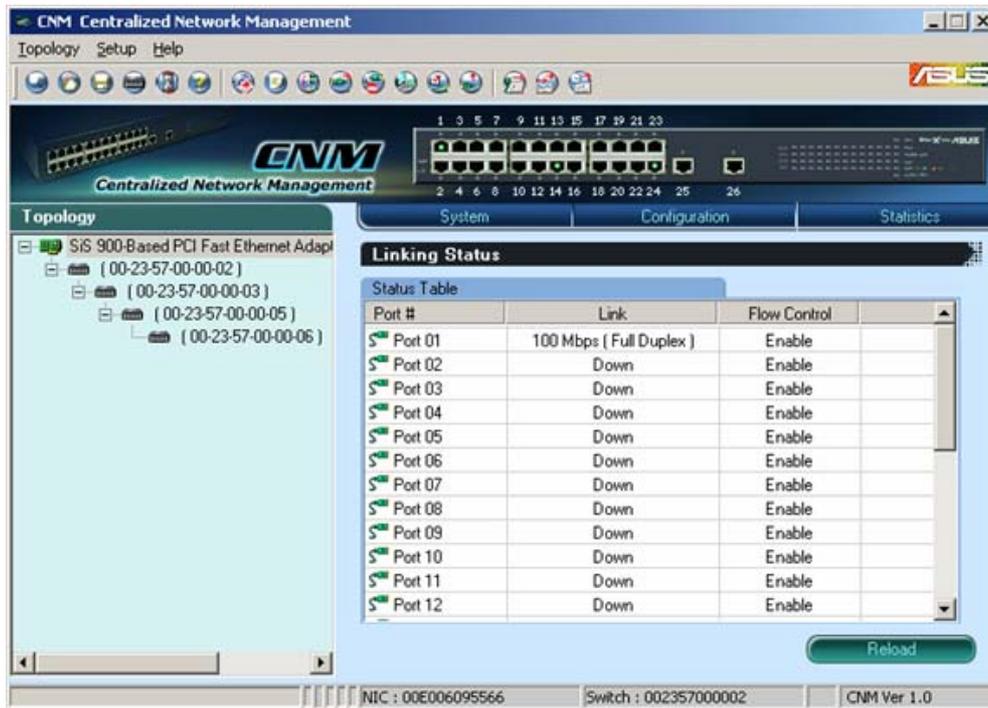


Figure 4.14. Link Status

4.6.3 Change Password

A valid password consists of 4 digits, from 0 to 9, and a to f. The authenticator does not check upper case or lower case. For example, password “12ab” is treated as “12AB”. Once the password gets changed, CNM will use the password to retrieve the information about the switch.

If the password is forgotten, please refer to 3.3.2 to reset the password in the switch. After it, you have to remove the switch from the topology and discover the switch again.

After changing the password, CNM will show a dialog box for administrators to save the topology or not. If not, administrators will have to do two jobs when CNM starts up next time. First, manually add the switch according to section 4.4.2. Second, change password again and replace **0x2379** with correct one.

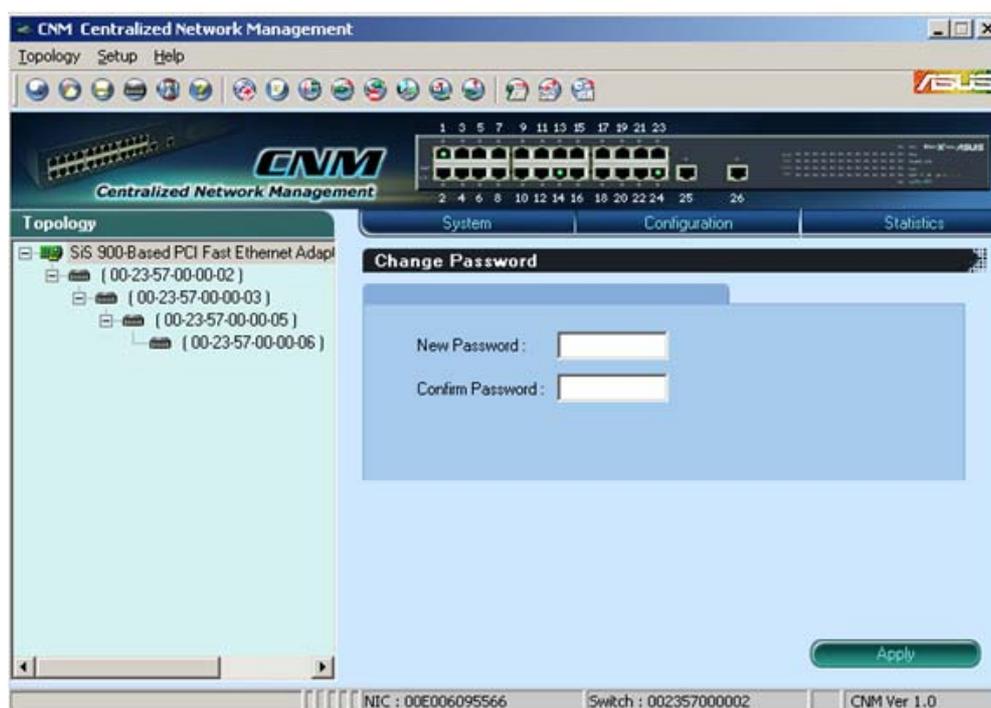


Figure 4.14b. Change Password

Since password was modified, administrators have to login to the switch. Or administrators will not be able to control the switch. The page is shown as Figure 4.14b.

4.6.4 Load

You can load configuration from the switch or the local file as shown in Figure 4.15. This action will update the current configuration in the CNM. If you want to keep the current configuration, please refer to section 4.6.5.

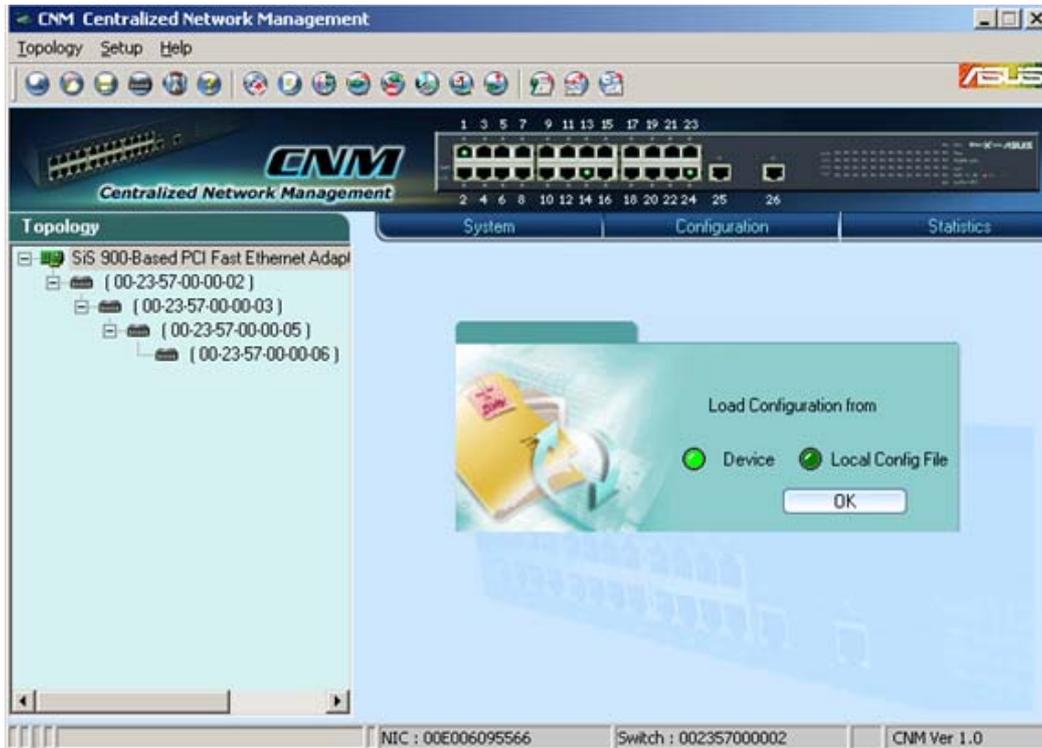


Figure 4.15. Load

4.6.5 Save

Save all the configurations to a local file for future reference. Once you create a configuration file in CNM, you can use it to apply to the other switches to save your time. It is also a backup file for configuration. It is recommended to have a good file name to identify that the configuration is for the certain switch(es).

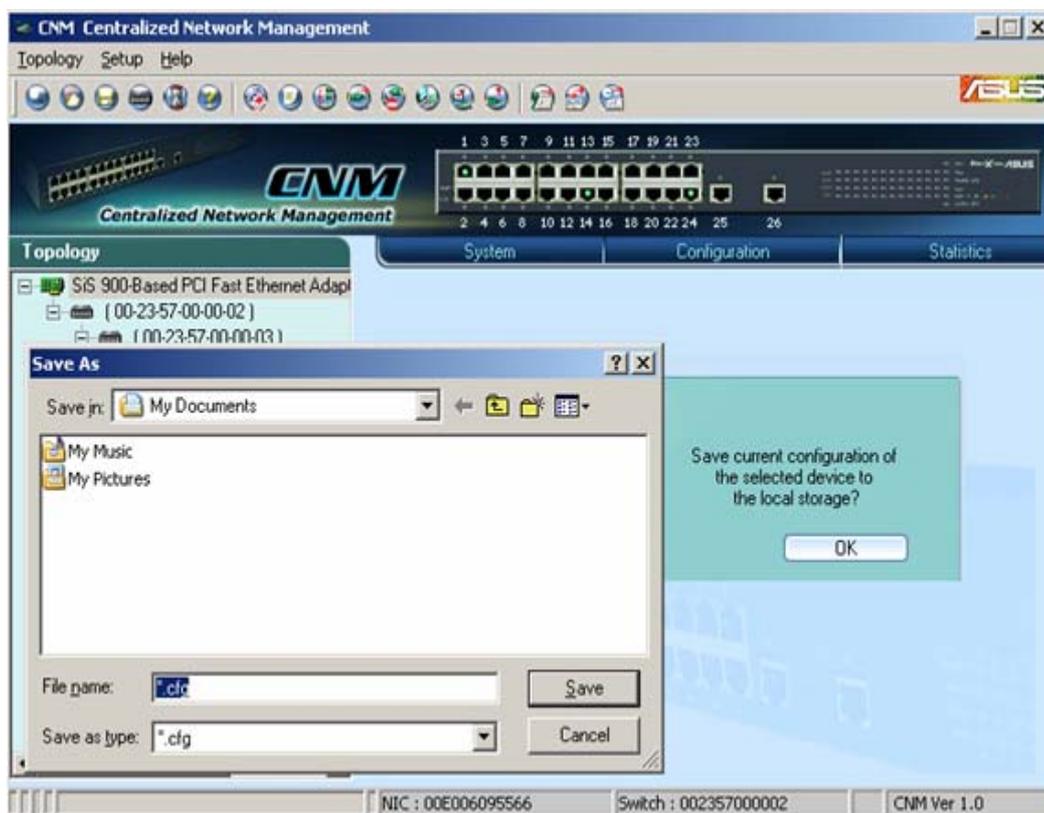


Figure 4.16. Save Configuration

4.6.6 Apply and Save

It applies all the current settings in CNM to the switch and save them in the switch permanently. It is recommended to back up the existed switch configurations before applying a new configuration to the switch.

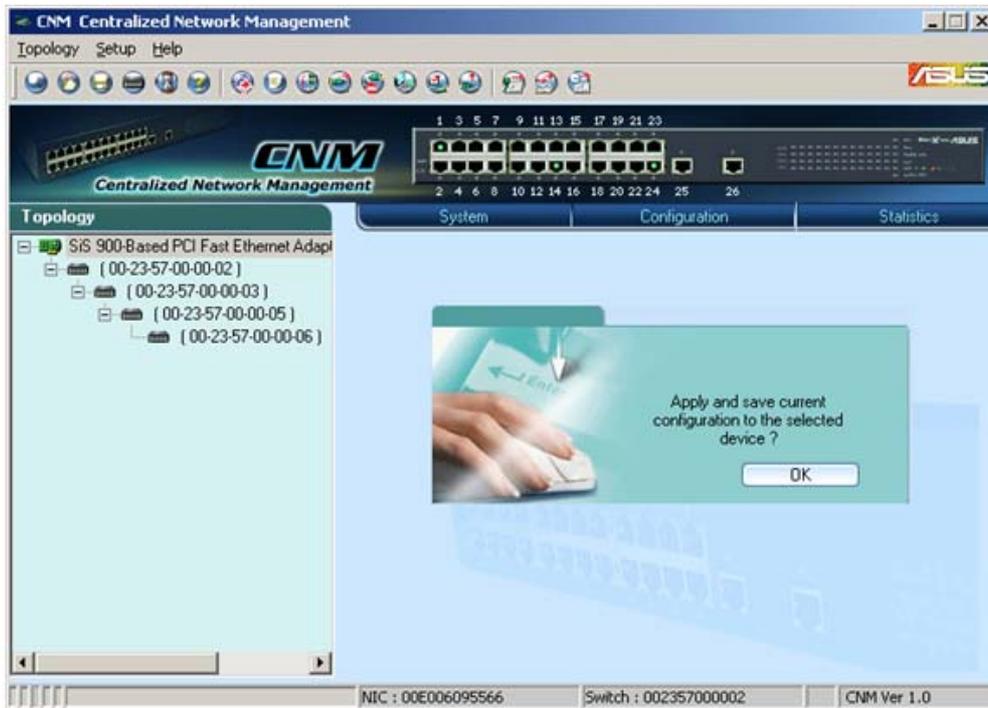


Figure 4.17. Apply Configuration

4.7 Configuration

The Configuration menu provides the configuration for all the functions that the switch can support, like physical interface, link aggregation, bandwidth control, traffic control, VLAN, IGMP snooping and QoS.

To keep all the new configurations and save the bandwidth for communications, each configuration page will not retrieve information from switch until you click the **Reload** button. In some configuration pages, you can select the ports to reload the information from the switch.

4.7.1 Physical Interface

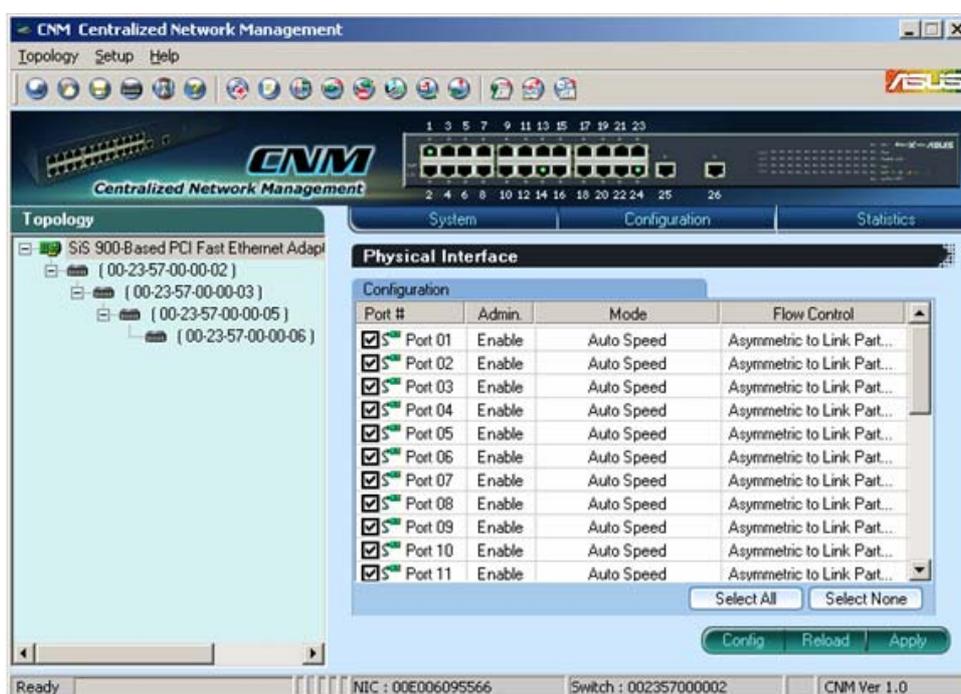


Figure 4.18. Physical Interface

Figure 4.18 shows the configuration for each port. Select the ports you want to configure or reload information from the switch by clicking on the check boxes in front of the ports, then click on **Config** to set the configuration for the ports, or click on **Reload** to retrieve configuration from the switch, or click on **Apply** to apply the new settings to the switch. Some settings you can do to the physical interface

1. Enable or disable a port
2. Speed and duplex mode. Select 1000 full-duplex on the Fast Ethernet ports (from 1 to 24) will set the ports to 100 full-duplex mode.
3. Flow control - Back pressure flow control is used in half and full duplex modes to prevent packet loss.

A software reset will be triggered after the configuration is apply. The purpose of software reset is to restart link negotiations.

4.7.2 Link Aggregation

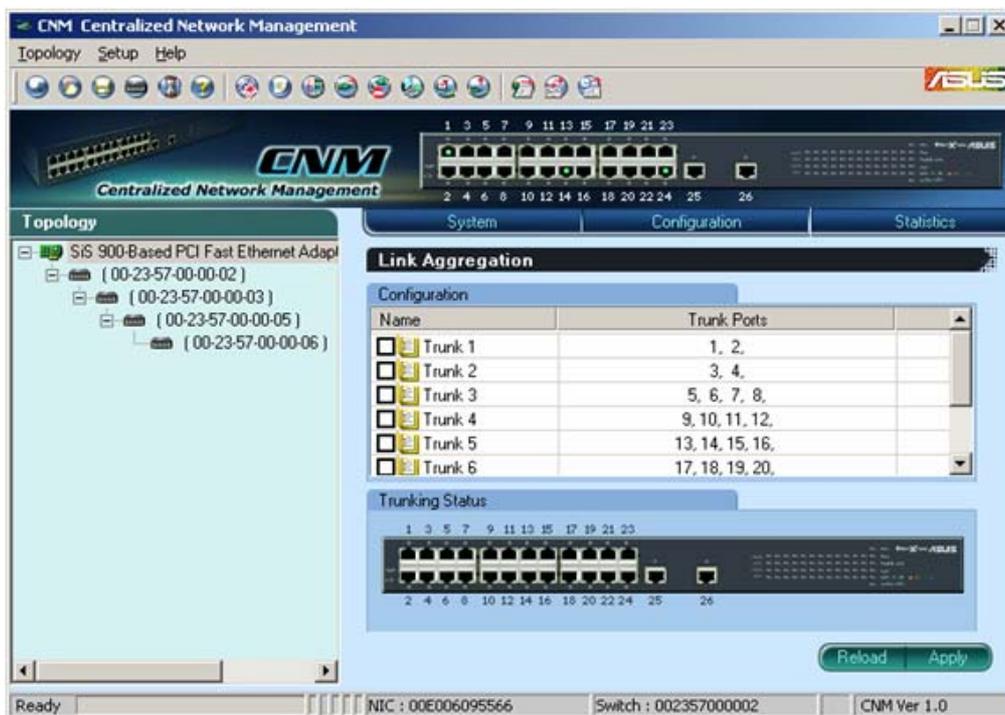


Figure 4.19. Link Aggregation

Link aggregation creates new virtual links with more bandwidth. For example, port 1 and 2 can work together as one link to another device. The new virtual link has 200Mbps bandwidth. The switch provides 8 groups of link aggregations shown on the top of figure 4.19.

Click on the **Reload** button to retrieve the configuration from switch. The checked trunk group means this group has been activated. You can check the trunk group to enable new trunk or uncheck the trunk group to disable the trunks. Click on **Apply** to make them effective in the switch.

The **Trunking Status** shows the ports work as trunk ports currently. A green light in the port means the port is working as trunk port properly, otherwise it shows no light.

4.7.3 Bandwidth

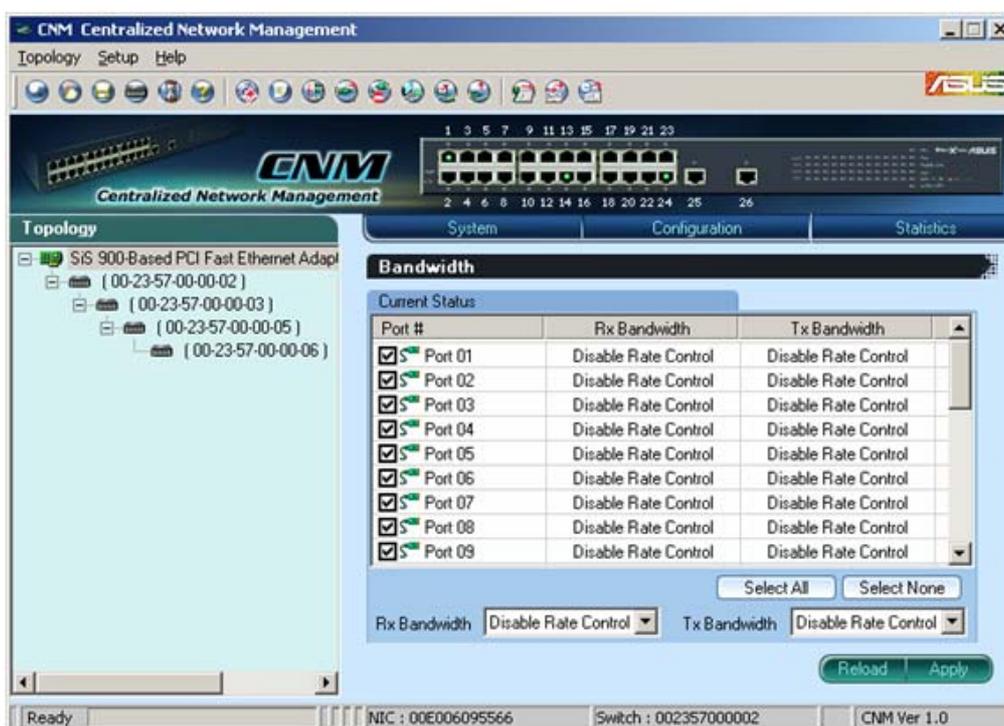


Figure 4.20. Bandwidth Configuration

1024P provides TX/RX bandwidth control for each port. Please reload the configuration before you start to set up new configuration. The page is shown as figure 4.20.

Select the ports you want to configure, then select proper bandwidth for TX/RX directions. Click on **Apply** to apply to the switch.

4.7.4 Traffic Control

Traffic control is to set the following items

1. Broadcast storm filtering control: if enabled, each port start to drop broadcast packets after a continuous received broadcast packets count up to 64. It will be back to normal if no more broadcast packet is received in 800ms or any non-broadcast packet is received.
2. IP multicast packet flow control: if enabled, the system will drop IP multicast packets under a congestion condition. Otherwise, the packet will be forwarded to non-congested ports.
3. Broadcast packet flow control: if enable, the system will drop broadcast packets under a congestion condition. Otherwise, the broadcast packet will be forwarded to non-congested ports.

Again, please reload the settings from the switch before starting to do new configurations.

4.7.5 VLAN Setup

A VLAN is simply a configured broadcast domain. An administrator applies VLAN to separate a network. VLAN Setup provides administrators abilities to set up port-based and tag-based Vlan. The page is shown as figure 4.21.

An administrator could refer the following to add a VLAN

1. Choose VLAN type, port-based or tag-based VLAN.
2. Assign VLAN id, if you choose tag-based VLAN.
3. Click  or  to assign port members.
4. Click **Add Vlan** to add a Vlan, and then Vlan Table will show it.
5. Repeat step 1 through 4, if need to create another Vlan.
6. Click **Apply** and then Vlan configuration will take effect.

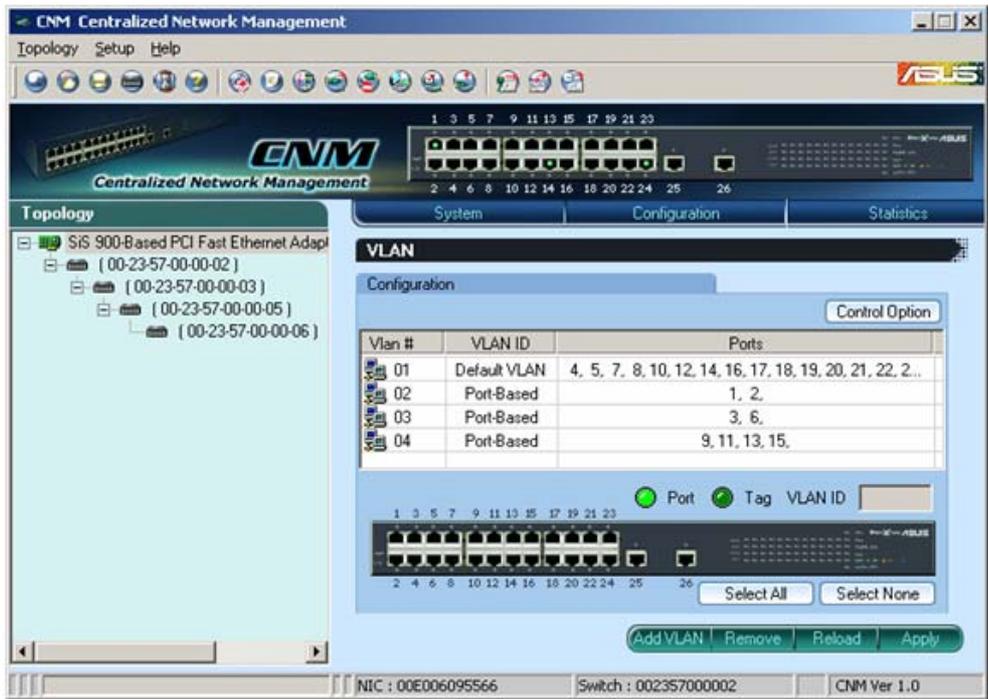


Figure 4.21. VLAN

All VLAN behavior will be influenced by VLAN control option. Click **Control Option** and a window will pop out as Figure 4.22. Enable or disable these options carefully, these options are global setting for VLAN



Figure 4.22. VLAN Control Options

7. VLAN function: enable or disable the VLAN function.
8. Unicast packet inter-VLAN leaky: to enable the packet to be forwarded to a destination port (L2 table hit) at different VLAN.
9. ARP broadcast packet inter-VLAN leaky: to enable ARP frame to broadcast to all switch ports.
10. IP multicast packet inter-VLAN leaky: to enable IP multicast packet to be flooded to all the multicast address group member set ignore the VLAN member set domain limitation.
11. 802.1Q VLAN tag aware: to enable tag-based VLAN function.
12. Ingress rule for acceptable frame types: to admit all frames or to admit only VLAN-tagged frames.
13. Ingress rule for ingress filtering: to enable filter the frame received from a port which port is not included in the classified VLAN group member.

4.7.6 IGMP Snooping

Enable the IGMP snooping will let the switch learn the multicast router port and group address member ports into the multicast address table. The table is combined with L2 MAC table, so the maximum entry is 8K. The valid port member will auto aging out after about 5 minute idle. Figure 4.23 shows the page.

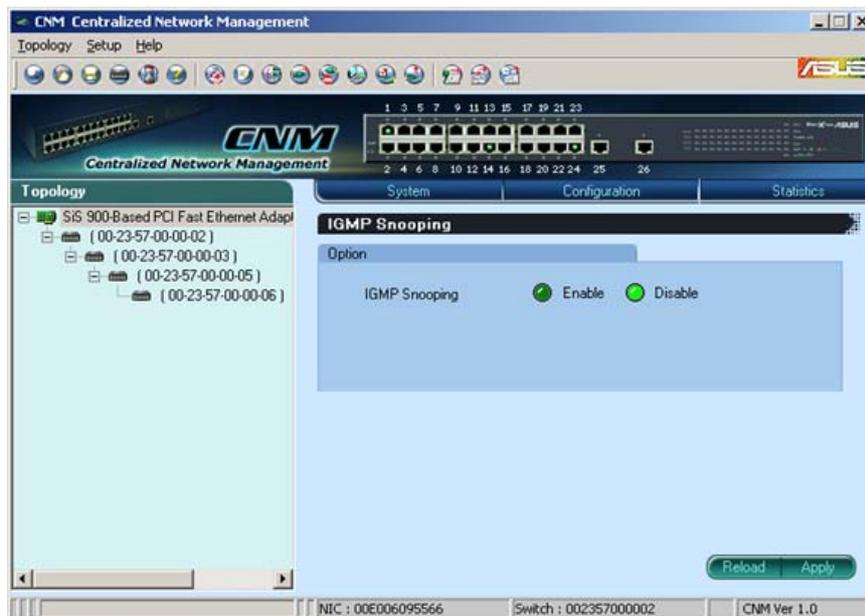


Figure 4.23. IGMP Snoop

4.7.7 QoS Setup

The system support 2 level priority queues. The queue service rate is based on the packet-based Weighted Round Robin algorithm. The ratio can be set as 4:1, 8:1, 16:1, or strictly high priority first.

The port-based priority is to decide the packet priority by the receiving ports. You can select the high priority ports from the switch graphic.

If TOS/DSCP based priority is enabled, it will be assigned to high priority queue if the field value is:

```

expected forwarding: 0b101110;
assured forwarding: 0b001010, 0b010010, 0b011010, 0b100010
network control: 0b11x000
  
```

If 802.1p based priority is enabled, the packet forward priority is decided by the CoS value. The high priority packets have the CoS value from 4 to 7.

In some situations, you may want the high priority packets to get forwarded even the 802.3x flow control stop transmitting packets. In this case, enable **Adapted Flow Control** will turn off 802.3x flow control for a short time to let the high priority packets get forwarded. The 802.3x is re-enable when no high priority frames are received for 1 to 2 seconds.

The Quality of Service page is shown as figure 4.24

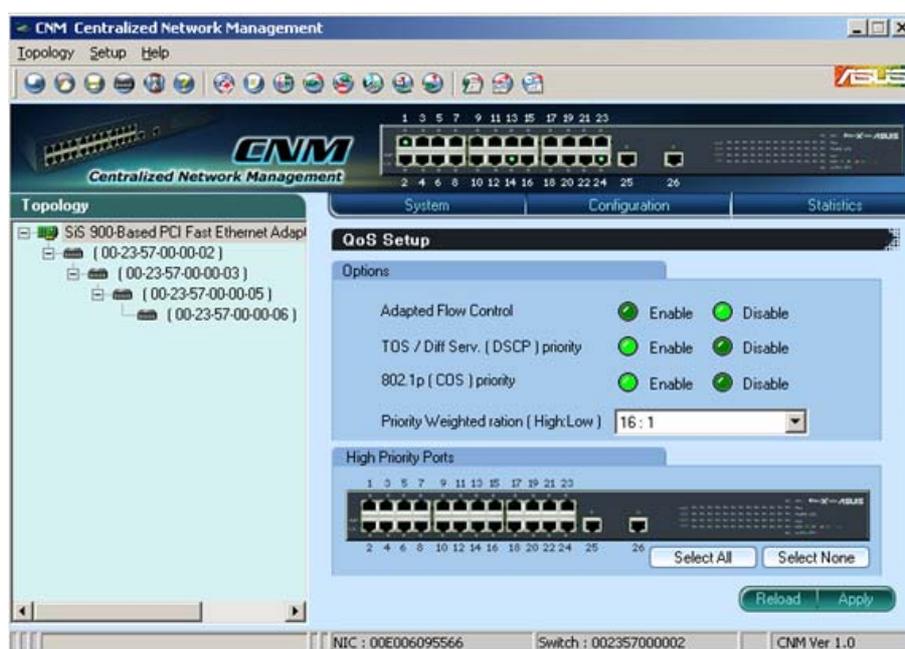


Figure 4.24. QoS Setup

4.8 Statistics

Statistics offer **Port Traffic**, **Traffic History** and **Comparison** charts. The switch has 3 counters for 8 kinds of statistics. So you cannot see all the statistics at the same time. That is, the old statistics data will be gone if you start to use the counter for another statistics.

4.8.1 Port Traffic

Select port number, the statistics item and color to draw the traffic chart. The chart will be auto updated in the time interval you set in **Setup** menu. Refer to 4.3.2 for time interval setup.

Press the **Draw Traffic Chart** button to start drawing.

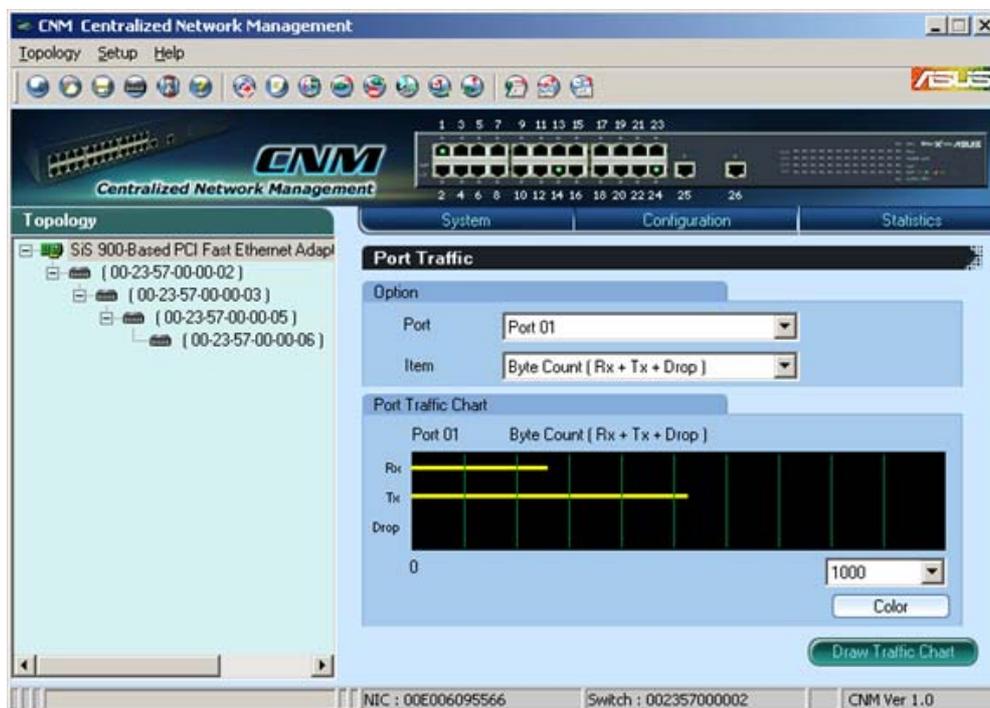


Figure 4.25. Port Traffic

4.8.2 Traffic History

Select the statistics item, ports and colors you want to see in the chart, then press the **Draw Traffic Chart** button to start the drawing. The chart will be auto updated in the time interval you set in **Setup** menu. Refer to 4.3.2 for time interval setup.

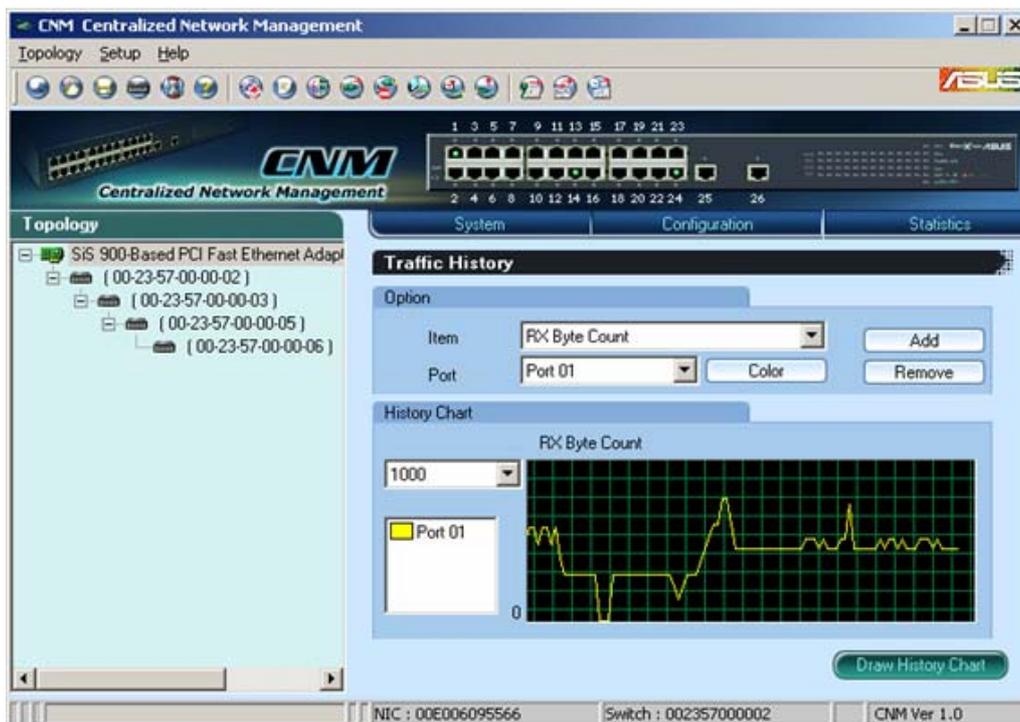


Figure 4.26. Traffic History

4.8.3 Comparison

Select the statistics item to do comparison for port 1 to 26. Press the **Draw Traffic Chart** button to start the drawing. The chart will be auto updated in the time interval you set in **Setup** menu.

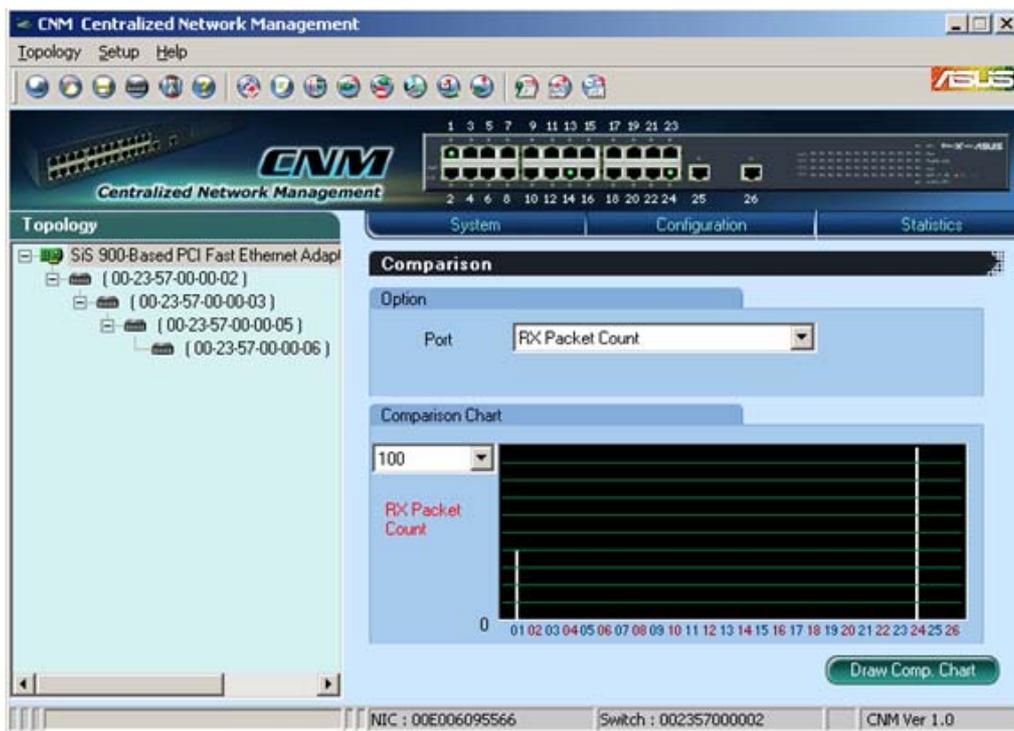


Figure 4.27. Port Comparison