NetComm®

Broadband Solutions

User Guide

NP2624M

Stackable 24-Port Switch

Contents

1. Introduction

The NP2624M switch is a high performance web-managed SNMP Layer 2 switch that provides users with 24 x 10/100Mbps Ethernet and 2 x 1000Mbps Gigabit ports. This Switch has SNMP management and remote control capabilities such as "Web Cluster". The Gigabit module, which can be copper or fibre media, supports 1000BASE-SX, 1000BASE-LX or 1000BASE-T, allowing users to increase their network response time at gigabit speeds and with great flexibility. An RS-232 serial port provides an easy way for to install and set-up the Switch.

Non-blocking and maximum wire speed performances are designed on all ports. The Switch not only supports Auto-Negotiation, but also Auto-MDIX function on all switched 24 x 10/100Mbps RJ-45 ports and two Gigabit Copper ports in both half or full duplex mode. The Auto-MDIX function makes it convenient for the user, because it eliminates cabling on straight-line or cross-line issues.

The NP2624M switch provides a convenient way to operate layer 2 management through a web browser. The User-friendly drop-down menus allow the user to easily learn, control and monitor the Switch. It supports not only traditional SNMP function, but also RMON 1,2,3,9 groups for advanced network analysis. A new management tool called "Single IP" provides the administrator an access right to enter the private IP domain through a single real IP. Using this management tool, a network manager can remotely control far-side servers in a private IP domain.

The Switch also supports both Port-based and Tag-based VLANs. To increase bandwidth application, it supports 7 groups with up to 4 ports Trunk, and moreover, these trunk ports offer a fail-over function and provide back up when one or more ports malfunction. A stacking mode is introduced here to enhance the ability of VLAN. An integrated UI not only displays the link status of the stacking sets, but also provides an easy way to set up the VLAN.

Total front access design with full LED status display provide easy installation, inspection and maintenance in rack mount environments. An additional LED display of the fan status allows for quick diagnosis of any over-heating.

1.1 Unpacking

Open the shipping carton of the Switch and carefully unpack its contents, the carton should contain the following items:

- One NP2624M port Fast Ethernet Layer 2 Switch.
- One Mounting Kit including 2 mounting brackets and screws.
- Four rubber feet with adhesive backing.
- One AC power cord.
- One RS-232 cable.
- One CD containing this User Guide.

1.2 Installation

You can use the following guidelines when choosing a place to install the Switch.

- The surface must support at least 3 kg. Do not place heavy objects on the Switch.
- You must be able to visually inspect the power cord and AC power connector.
- Ensure proper heat dissipation by making sure there is adequate ventilation around the Switch.

Desktop or Shelf Installation:

When installing the Switch on a desktop or shelf, the rubber feet included with the device should attached first. Attach these cushioning feet on the bottom at each corner of the device. Allow adequate space for ventilation between the device and the objects around it.

Rack Installation:

The NP2624M switch can be mounted in an ELA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets on the switch side panels (one on each side) and secure them with the screws provided. Then, use the screws provided with the equipment rack to mount the switch on the rack.

Power on:

The NP2624M switch can be used with an AC power supply 100-240V AC, 50-60Hz. The AC power connector is located at the rear of the unit. The switch's power supply will adjust to the local power source automatically and may be turned on with all or none of the LAN segment cables connected.

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink. This blinking of the LED indicators represents a reset of the system.
- The power LED indicator will blink while the Switch loads onboard software and performs a self-test. After approximately 20 seconds, the LED will light again to indicate the switch is in a ready state.
- The Speed, Link/Activity LED indicator may remain ON or OFF depending on every port's situation.
- The fan LED will switch off if the fan is working normally. The LED goes RED if the fan has stopped or failed.

1.3 Initial set up for management

There are two methods of management; one is out-of-band management, where you connect your PC to the switch through an RS232 cable. The other method is in-band-management, where you also connect your PC to the switch, but do so through an Ethernet network either locally or remotely, or simply directly connect your PC and the switch with an Ethernet cable. Before you activate the management function in the Switch, you should read the instructions below carefully to ensure you can access the switch through your PC.

1.3.1 Out-of-band Terminal Mode Management through RS-232

Step 1: Set Hyper Terminal parameters on your PC

Firstly, turn on your PC and execute a terminal mode program. For example, if you are in a Microsoft Window environment, you may choose “Hyper Terminal” from programs that are listed for communication.

Open a New Connection using COM1 (or the port on your computer that you are going to connect the Switch to) and select the following port settings:

Bits Rate per second = 57600

Data Bits = 8

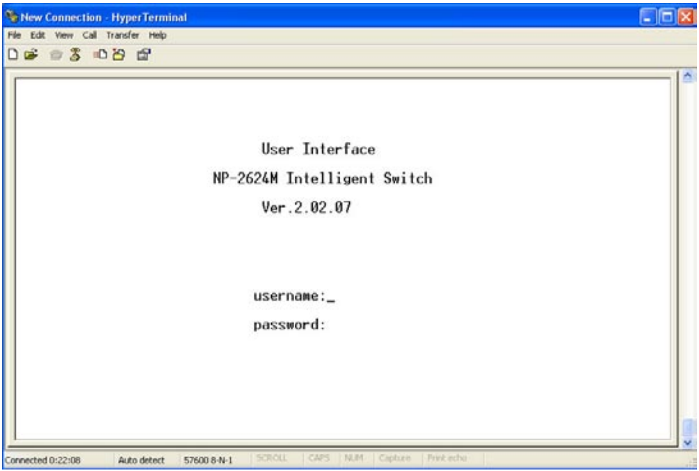
Parity = None

Stop Bit = 1

Flow Control = None

Step 2: Access your Switch

After setting the above parameters on your PC, connect your switch device with the RS-232 cable provided and turn the switch on. After the switch runs its self-test, the device should respond and ask you to enter the username and password. If the switch had already booted, press the enter key to display the login screen. Type the default value for the username and password to proceed, the default username is “**admin**” and default password “**admin**”. To learn more about the operation of the Switch in this mode, refer the instructions in chapter 4 of this manual.


New Connection - HyperTerminal
File Edit View Call Transfer Help

```
           User Interface
    NP-2624M Intelligent Switch
           Ver.2.02.07


          username:_
          password:
```

Connected 0:22:08 Auto detect 57600 8-N-1 SCROLL CAPS NUM Capture Print echo

1.3.2 In-band Management through Ethernet

In addition to terminal mode operation, the NP2624M switch also supports in-band management through a web browser. This function is much more user-friendly than terminal mode and can be performed either locally or remotely through Ethernet.

Before you can access the switch:

1. You have to know the IP Address and Subnet Mask of both your switch and your PC. The default value of the IP Address and Subnet Mask within the switch can be retrieved through terminal mode operation described in chapter 4 and the IP Address and Subnet Mask of your PC can be found in your PC operating system.
2. In general, within a network, the members in the same network domain must have the same Subnet IP unless there are routers between them or members in the same network domain can't talk to each other. Ensure that all users in the same domain have different IP Addresses on the same Subnet Mask.
3. If there is a DHCP server in the network domain, ensure that the DHCP function is enabled in both your PC and the switch, then save the setting and reboot the switch (power-off-and–on once). The DHCP server and its protocol will automatically assign an IP address and related IP Subnet Mask and Default gateway. This allows you to execute your web browser in your PC and simply type "http:// IP-Address-of-switch" to access the switch through Ethernet or over the Internet. If there is no DHCP server in the network, you must follow the steps instructed below:
4. Webpage login will prevent attacks from hackers. If a user fails to correctly login 3 times, http authentication will reject any http request for 3 minutes.

Connecting without a DHCP server

When there is no DHCP server in your network domain, you must ensure that the PC or switch have different IP Addresses and same Subnet Mask. Below, are the steps to modify the IP configuration of the switch to match the domain requirement of the PC:

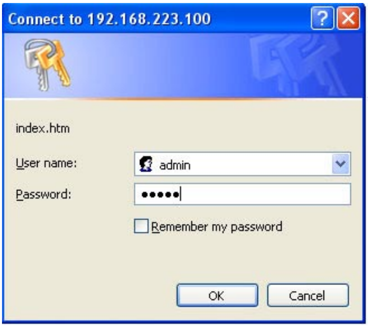
Step 1: Get the IP configuration information in your PC.

Step 2: Get IP configuration value used for switch from your network manager.

Get an IP Address for your switch, the IP Subnet Mask, and the default gateway IP address (if needed) from your network manager.

Step 3: Modify the IP configuration value within the switch to match the rule

In the step 3, you must use the data from step 2 to modify the default values within the switch. To achieve this, use terminal mode operation mentioned as described in 1.3.1 above. After modifying the IP address, Subnet Mask, and Default Gateway in the switch, save the setting and execute the browser program with "http:// IP_Address_ of_ switch". The login dialog box will be displayed. Type in the user name and password to proceed. Refer to the instructions in chapter 3 for more information.



Connect to 192.168.223.100

index.htm

User name: admin

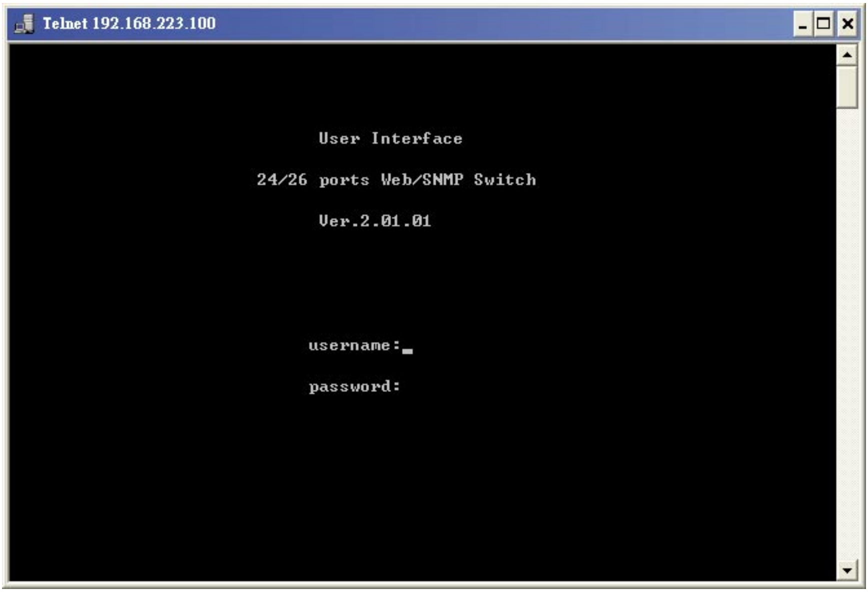
Password: •••••

1.3.3 Telnet management

In addition to local terminal mode operation, the NP2624M switch supports remote management through Telnet over a network or the internet without a web browser. In this mode, the user has to enter the same settings as required in in-band management to the IP Configuration before executing the Telnet program. Again, after properly setting the switch, save the settings and connect your Ethernet cable from your PC to any port of the Switch. Then you simply type the following at the command line to access the switch:

Telnet IP_Address_of_Switch

The following window appears. Follow the prompts and type in the "username" and "password" to proceed. Refer to the instructions in chapter 3 of this manual for more information.



```
          User Interface

    24/26 ports Web/SNMP Switch

          Ver.2.01.01



         username:_

         password:
```

1.4 LED indicators information

There are many LEDs on the front panel of switch. After the initial power on, these LEDs will reflect the current status within the switch as explained below:

There is one power LED on the left side of the front panel. When power is applied, it turns green. Below it is a Diagnostic LED which will blink whilst conducting power-on diagnostics. There are two more FAN status LEDs beside the power LEDs. The upper one indicates the left fan status and the lower one indicates the right fan status. These will turn RED if a fan has stopped or is malfunctioning. Otherwise these LEDs will switch off when the fans are working normally.

Each of the RJ-45 10/100Mbps connectors has two LEDs built-in to its upper corners. The left one indicates the link status and activity, while the right one indicates the speed.

The LEDs for the optional Gigabit module are somewhat different. The upper yellow LED indicates a 10Mbps LINK, the middle green LED indicates a 100Mbps LINK, but for 1000Mbps, or Gigabit, both upper and middle LEDs are lit (i.e. when a Gigabit port is linked with another Gigabit port).

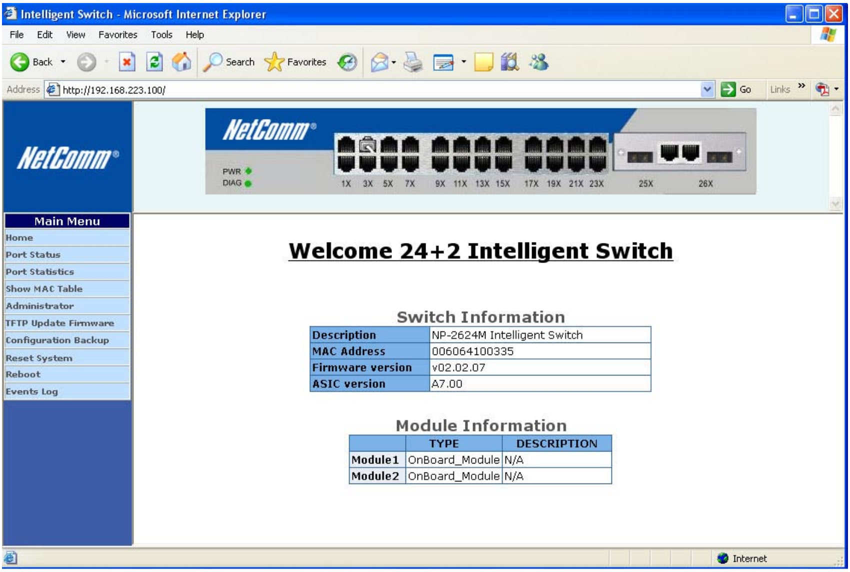
LED	Color	Status	
		Solid	Blinking
Power	Green	Turn solid green when power is applied to this device.	N/A
DIAG	Green	Successful diagnostic.	During power on diagnostics
FAN	Red	Left or Right side fan fail.	N/A
LINK/ACT	Green	Successful connection with Fast Ethernet.	Sending, receiving or collision packets
10/100M	Green	Successful connection with 100Mbps Fast Ethernet.	N/A
	Vanish	Successful connection with 10Mbps Fast Ethernet.	N/A

2. Web Management Function

2.1. Web Management Home Overview

The first page you will see after login to the switch via a web browser is the Web Management page.

This page will display the basic switch and module information. All information displayed in these fields is read-only. That is, the user cannot modify the contents of the fields. The fields are described below:



Welcome 24+2 Intelligent Switch

Switch Information

Description	NP-2624M Intelligent Switch
MAC Address	006064100335
Firmware version	v02.02.07
ASIC version	A7.00

Module Information

	TYPE	DESCRIPTION
Module1	OnBoard_Module	N/A
Module2	OnBoard_Module	N/A

Switch Information

Description: Displays the name of device type.

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

Firmware Version: Displays the switch's firmware version.

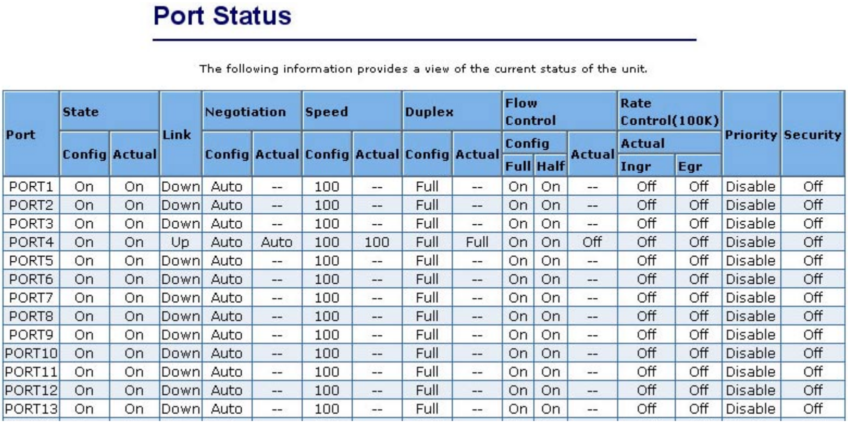
ASIC Version: Displays the switch's ASIC version.

The image of the switch at the top of the page indicates the whether the port is connected. Click on the menu items on the left of the screen to display more information.

The following sections give an explanation of each function.

2.2. Port status

This page provides current status of every port and the negotiation result.



Port Status

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

Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control(100K)		Priority	Security
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config		Actual	Actual			
										Full	Half		Ingr	Egr		
PORT1	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT2	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT3	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT4	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	Off	Off	Off	Disable	Off
PORT5	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT6	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT7	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT8	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT9	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT10	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT11	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT12	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off
PORT13	On	On	Down	Auto	--	100	--	Full	--	On	On	--	Off	Off	Disable	Off

State: Displays the port status: On or Down. "Unlink" will be treated as "off".

Link Status: Displays the link status. Down means "No Link", Up means "Link".

Auto Negotiation: Displays the auto negotiation mode: auto/force/ Nway-force.

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

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

Flow Control: Full: Displays the flow control is enabled or disabled in full mode.

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

Rate Control: Displays the rate control setting.

Ingr: Displays the port effective ingress rate of user setting.

Egr: Displays the port effective egress rate of user setting.

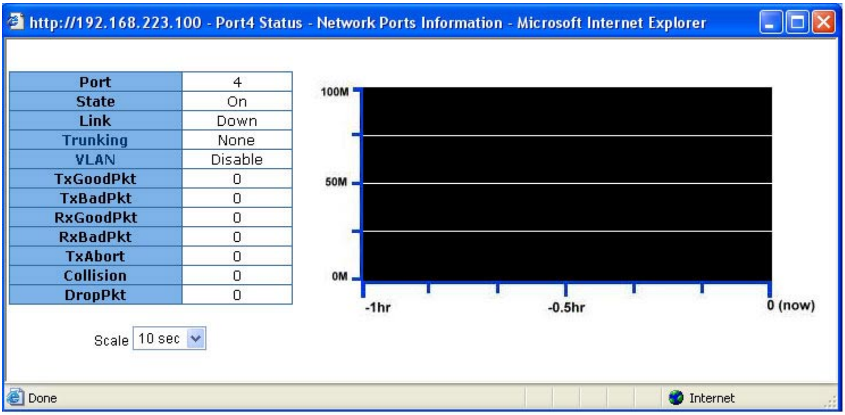
Port Security: Displays the port security is enabled or disabled.

Config: Displays the state of user setting.

Actual: Displays the negotiation result.

2.2.1 Single port counter and status

The user can also click any port directly on the front panel of the Home Page to get single port status which is shown below.


http://192.168.223.100 - Port4 Status - Network Ports Information - Microsoft Internet Explorer
100M
50M
0M
-1hr
-0.5hr
0 (now)
Done
Internet

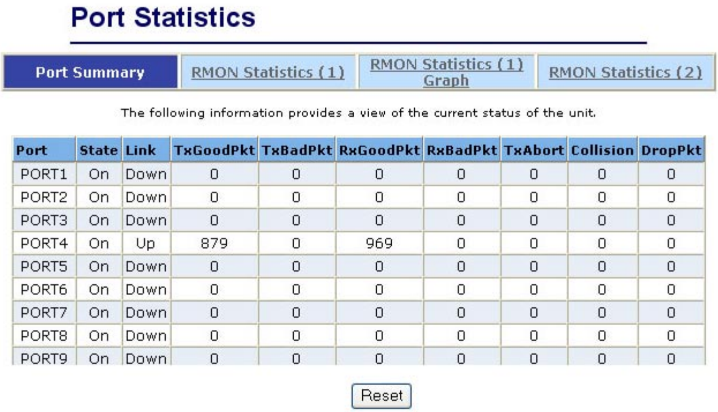
Port	4
State	On
Link	Down
Trunking	None
VLAN	Disable
TxGoodPkt	0
TxBadPkt	0
RxGoodPkt	0
RxBadPkt	0
TxAbort	0
Collision	0
DropPkt	0

Scale 10 sec

There is a flow rate historical chart on the right. The user can track the flow rate of this port for the last 60 hours. Changing the scale will re-calculate the chart.

2.3. Port Statistics

Statistics pages are provided to monitor network traffic. They are: Port Summary, RMON Statistics(1), RMON Statistics(1) Graph, RMON Statistics(2).



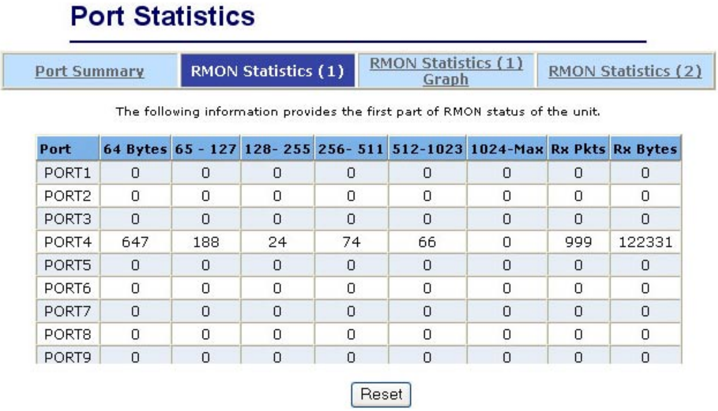
Port Statistics

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

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
PORT1	On	Down	0	0	0	0	0	0	0
PORT2	On	Down	0	0	0	0	0	0	0
PORT3	On	Down	0	0	0	0	0	0	0
PORT4	On	Up	879	0	969	0	0	0	0
PORT5	On	Down	0	0	0	0	0	0	0
PORT6	On	Down	0	0	0	0	0	0	0
PORT7	On	Down	0	0	0	0	0	0	0
PORT8	On	Down	0	0	0	0	0	0	0
PORT9	On	Down	0	0	0	0	0	0	0

The above information provides a summary of the switch's current status, including on/off state, link status, good or bad packets of transmitting and receiving, packets of transmitting abort, packets of collision and drop packets.

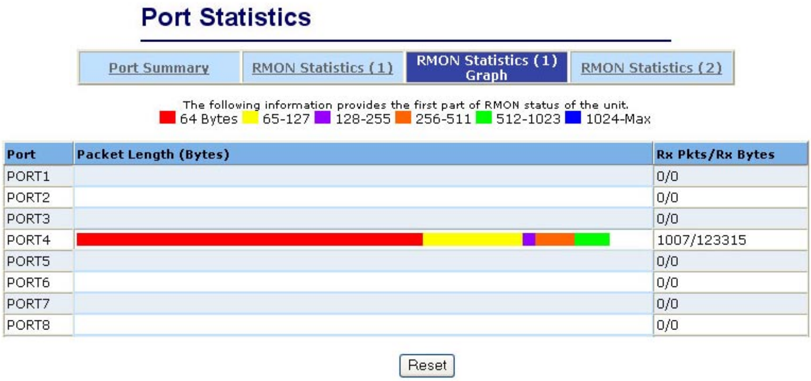
The following pages provide the statistics of RMON 1,2,3,9 groups. The first part collects the information about packets and frame size within the ranges of 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 bytes, the total received packets and the total receives bytes.



Port Statistics

The following information provides the first part of RMON status of the unit.

Port	64 Bytes	65 - 127	128- 255	256- 511	512-1023	1024-Max	Rx Pkts	Rx Bytes
PORT1	0	0	0	0	0	0	0	0
PORT2	0	0	0	0	0	0	0	0
PORT3	0	0	0	0	0	0	0	0
PORT4	647	188	24	74	66	0	999	122331
PORT5	0	0	0	0	0	0	0	0
PORT6	0	0	0	0	0	0	0	0
PORT7	0	0	0	0	0	0	0	0
PORT8	0	0	0	0	0	0	0	0
PORT9	0	0	0	0	0	0	0	0

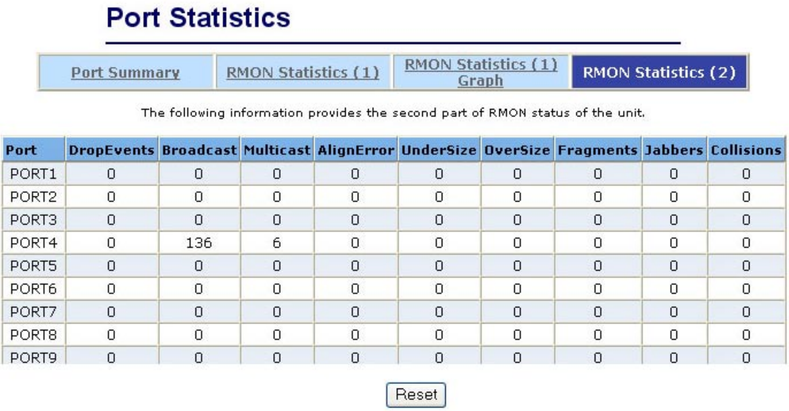


Port Statistics

The following information provides the first part of RMON status of the unit.
🟥 64 Bytes 🟨 65-127 🟪 128-255 🟧 256-511 🟩 512-1023 🟦 1024-Max

Port	Packet Length (Bytes)	Rx Pkts/Rx Bytes
PORT1		0/0
PORT2		0/0
PORT3		0/0
PORT4		1007/123315
PORT5		0/0
PORT6		0/0
PORT7		0/0
PORT8		0/0

The second part collects the information about drop events, broadcast packets, multicast packets, alignment errors, undersize packets, oversize packets, fragments, jabbers and collisions.



Port Statistics

The following information provides the second part of RMON status of the unit.

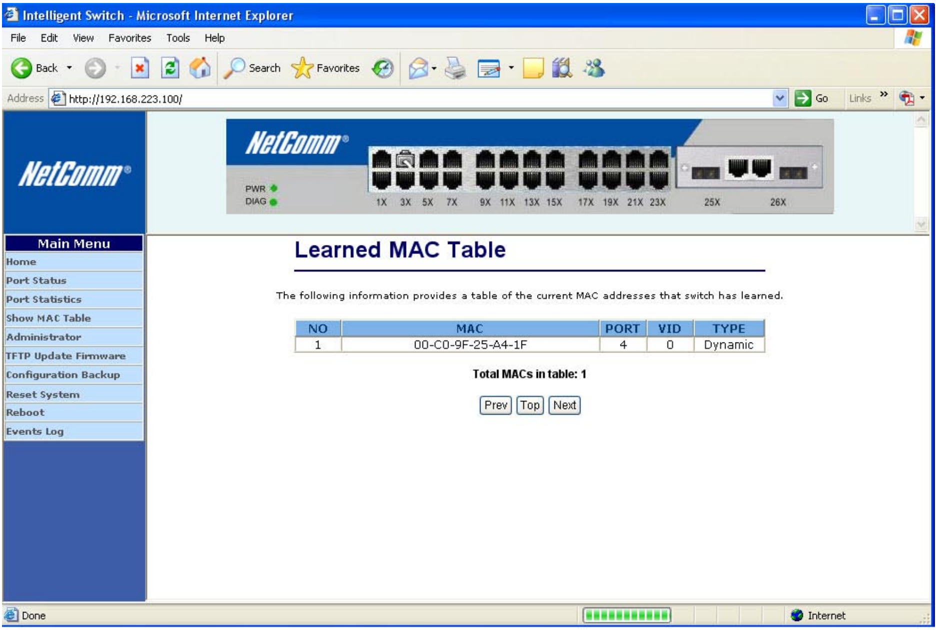
Port	DropEvents	Broadcast	Multicast	AlignError	UnderSize	OverSize	Fragments	Jabbers	Collisions
PORT1	0	0	0	0	0	0	0	0	0
PORT2	0	0	0	0	0	0	0	0	0
PORT3	0	0	0	0	0	0	0	0	0
PORT4	0	136	6	0	0	0	0	0	0
PORT5	0	0	0	0	0	0	0	0	0
PORT6	0	0	0	0	0	0	0	0	0
PORT7	0	0	0	0	0	0	0	0	0
PORT8	0	0	0	0	0	0	0	0	0
PORT9	0	0	0	0	0	0	0	0	0

Press “Reset” button to clear the counter.

2.4. Show MAC Table

The following information provides a table of the current MAC address that the switch has learned.

Press “Prev” or “Next” button to browse previous 50 or next 50 items. The “Top” button will re-list the table from the first MAC.



Learned MAC Table

The following information provides a table of the current MAC addresses that switch has learned.

NO	MAC	PORT	VID	TYPE
1	00-C0-9F-25-A4-1F	4	0	Dynamic

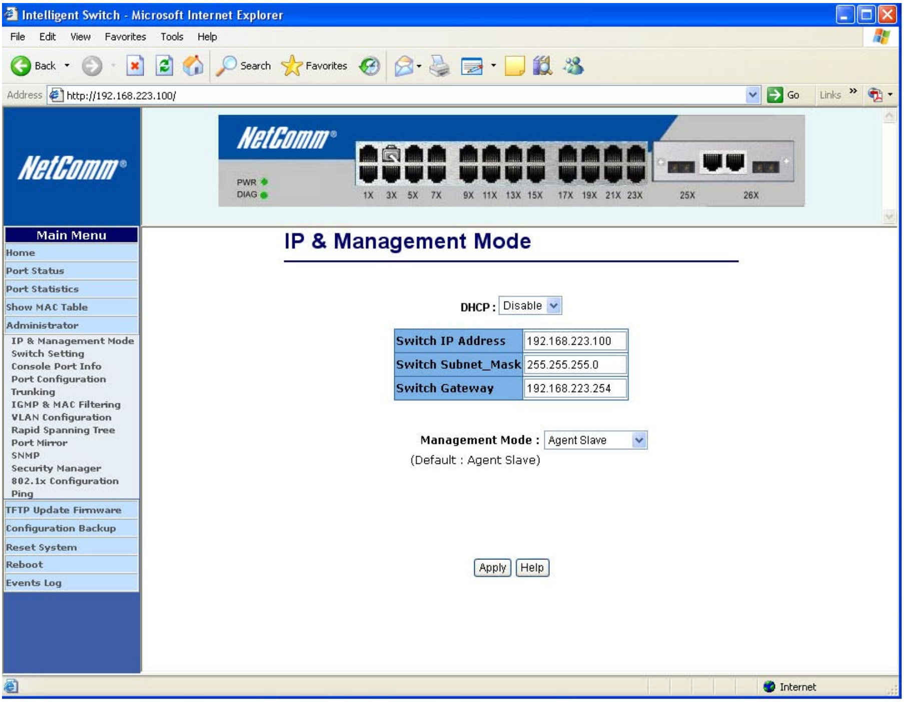
Total MACs in table: 1

The table can be sorted by each of the headings by clicking the header on the top of table. For instance, clicking the “MAC” on the top of table will refresh the table by the index of “MAC”.

2.5. Administrator

There are many management functions that can be set or performed if you click on **Administrator** on Home Page, including:

- IP and Management mode
- Switch settings
- Console port information
- Port configuration
- Trunking
- IGMP and MAC Filter
- VLAN configuration
- Rapid Spanning tree
- Port Mirror
- SNMP
- Security Manager
- 802.1x Configuration
- Ping



IP & Management Mode

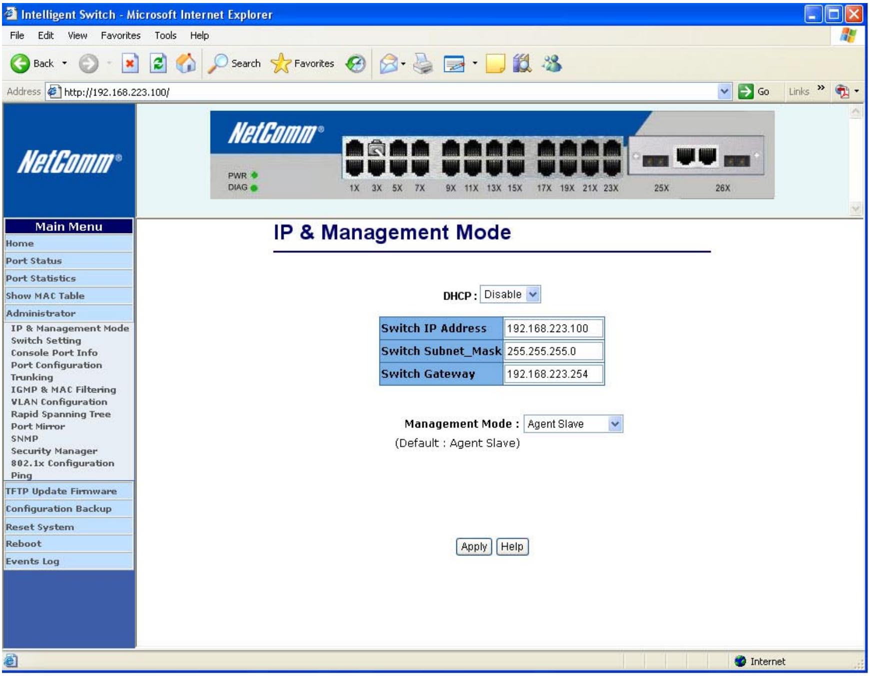
DHCP : Disable

Switch IP Address	192.168.223.100
Switch Subnet_Mask	255.255.255.0
Switch Gateway	192.168.223.254

Management Mode : Agent Slave
(Default : Agent Slave)

2.5.1. IP and Management mode

The user can modify the switch IP Settings by entering the new values and clicking the "apply" button to confirm (save) these settings. Then reboot the switch and the new IP configuration values will be activated.



IP & Management Mode

DHCP : Disable

Switch IP Address	192.168.223.100
Switch Subnet_Mask	255.255.255.0
Switch Gateway	192.168.223.254

Management Mode : Agent Slave
(Default : Agent Slave)

The Management mode indicates which role this switch is currently playing. "Agent Slave" means it is treated as a normal switch. "Agent Master" means the "Single IP" is activated and the switch is treated as agent manager. "Stacking Slave" is used only when this switch is going to be a member of stacking set. This setting will force the switch to activate spanning tree protocol and some VLAN settings in preparation for stacking switches. "Stacking Master" also does the same tasks but it plays the role of manager of the stack. Only the "Stacking Slave" can be added into the members of a stacking set under one "Stacking master". The default management mode is "Agent Slave".

The extra "Agent IP" setting is necessary for the "Single IP" management. It defines the IP and the subnet mask the master switch will be assigned, which are in the same IP domain as the managed hosts' one.

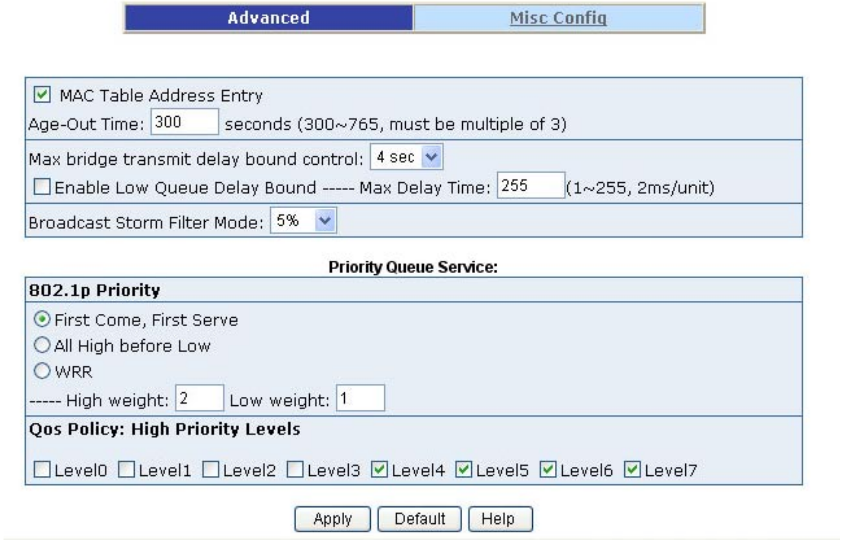
The user can confine the "Single IP" function to local management by assigning the agent IP to the same one as the switch's IP. Different from original IP forwarding method, it will not increase the loading of switch.

"Agent IP" setting and "Agent management" in the main menu will not show up if the agent mode is set as "Slave".

NOTE: If any of the values are changed in this screen, reboot is necessary.

2.5.2 Switch Setting

2.5.2.1 Advanced



☑ MAC Table Address Entry

Age-Out Time: 300 seconds (300~765, must be multiple of 3)

Max bridge transmit delay bound control: 4 sec

□ Enable Low Queue Delay Bound ----- Max Delay Time: 255 (1~255, 2ms/unit)

Broadcast Storm Filter Mode: 5%

Priority Queue Service:

802.1p Priority

● First Come, First Serve

○ All High before Low

○ WRR

----- High weight: 2 Low weight: 1

Qos Policy: High Priority Levels

□ Level0 □ Level1 □ Level2 □ Level3 ☑ Level4 ☑ Level5 ☑ Level6 ☑ Level7

MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.

Max bridge transit delay bound control: Limits the packets queuing time in switch. If enabled, the excess packets will be dropped. These valid values are 1 sec, 2 sec, and 4 sec and off. Default is 1 seconds.

NOTE: Make sure "Max bridge transit delay bound control" is enabled before "Enable Delay Bound", because "Enable Delay Bound" only works under "Max bridge transit delay bound control".

Enable Delay Bound: Limit the low priority packets queuing time in switch. Default Max Delay Time is 255ms. If the amount of time a low priority packet stays in the switch exceeds the Max Delay Time, it will be sent. The valid range is 1-255ms.

Broadcast Storm Filter: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value is 5%, 10%, 15%, 20%, 25% and off.

Priority Queue Service settings:

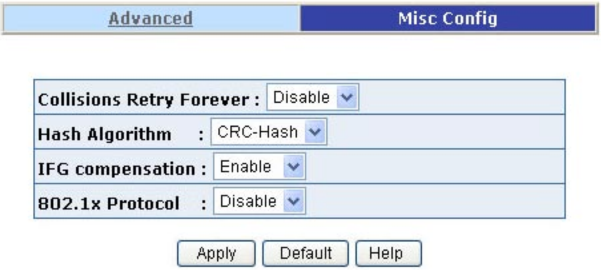
First Come, First Serve: The sequence of packets sent is depending on the arrival order.

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

WRR: (Weighted Round Robin) Select the preference given to packets in the switch's high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, 5 High:2 Low means that the switch sends 5 high-priority packets before sending 2 low- priority packets.

QOS Policy: High Priority Levels: 0~7 priority level can be mapped to a high or low queue.

2.5.2.2 Miscellaneous Configuration



Collisions Retry Forever : Disable

Hash Algorithm : CRC-Hash

IFG compensation : Enable

802.1x Protocol : Disable

Collisions Retry Forever: Disable – In half duplex, the collision-retry maximum is 48 times and packet will be dropped if collisions still happen.

Enable – In half duplex, there is no collision-retry limit. Retry will be attempted indefinitely.

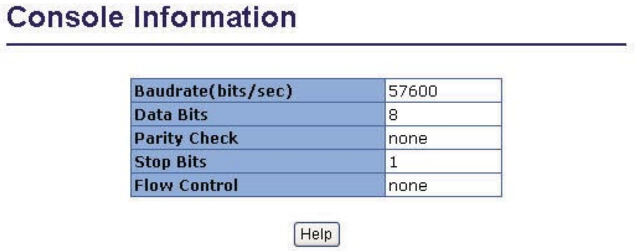
Hash Algorithm: Choose algorithms, CRC-Hash or DirectMap, to maintain MAC address table.

IFG Compensation: Enable or disable inter-frame gap (IFG) compensation.

802.1x Protocol: Enable or disable 802.1x protocol.

2.5.3 Console Port Information

The Console is a standard UART interface which allows you to communicate with the Switch via a Serial Port. The user can use windows HyperTerminal program to link the switch.



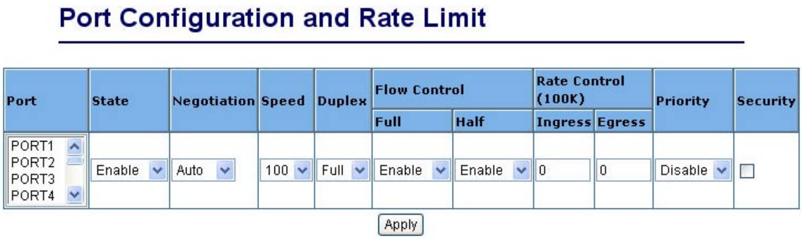
Console Information

Baudrate(bits/sec)	57600
Data Bits	8
Parity Check	none
Stop Bits	1
Flow Control	none

Bits per seconds:	57600
Data bits:	8
Parity:	none
Stop Bits:	1
Flow control:	none

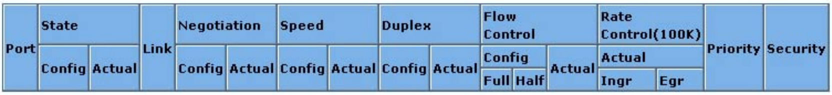
2.5.4 Port Controls

The user may modify or change mode operation in this page.



Port Configuration and Rate Limit

Port	State	Negotiation	Speed	Duplex	Flow Control		Rate Control (100K)		Priority	Security
					Full	Half	Ingress	Egress		
PORT1 PORT2 PORT3 PORT4	Enable	Auto	100	Full	Enable	Enable	0	0	Disable	□



Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control(100K)		Priority	Security
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config		Actual	Actual			
										Full	Half		Ingr	Egr		

Port: Select a port.

State: User can disable or enable this port control.

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

Speed: User can set 100Mbps or 10Mbps speed on Port1~Port24.

User can set 1000Mbps, 100Mbps or 10Mbps speed on Port25~Port26 (depends on module card mode).

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

Flow Control: Full: User can set flow control function to enable or disable in full mode.

Half: User can set backpressure to enable or disable in half mode.

Rate Control: Port1 ~ port 24, supports by-port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate at 1Mbps and ingress rate at 500Kbps. The device will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

Ingress: Type the port effective ingress rate. The valid range is 0 ~ 1000. The unit is 100K.

0: disable rate control.

1 ~ 1000: valid rate value

Egress: Type the port effective egress rate. The valid range is 0~1000. The unit is 100K.

0: disable rate control.

1 ~ 1000: valid rate value.

Priority: Enable or disable the port priority function. There are two priorities (high or low) provided if port priority is enabled.

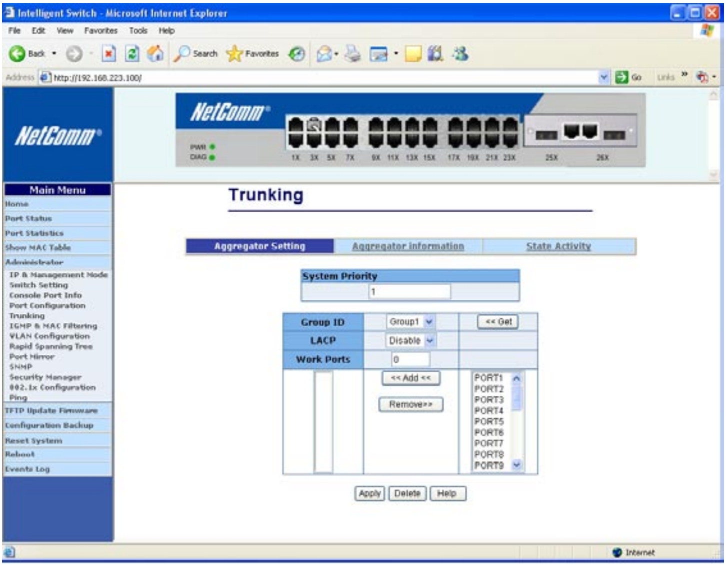
Security: A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. Users can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define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

Enter the settings, then click **Apply** button to change on this page.

2.5.5 Trunking

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

2.5.5.1 Aggregator setting



Trunking

System Priority: 1

Group ID: Group1

LACP: Disable

Work Ports: 0

System Priority: A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP. Valid value is 1~65535.

Group ID: There are seven trunk groups to provide configure. Choose the "group id" and click "Get".

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

Work ports: Allows for a maximum of four ports to be aggregated at the same time. If LACP static trunking group, exceeds ports is standby and able to aggregate if work ports fail. If local static trunking group, the number must be as same as the group member ports.

Select the ports to join the trunking group. Allow a maximum of four ports to be aggregated at the same time.

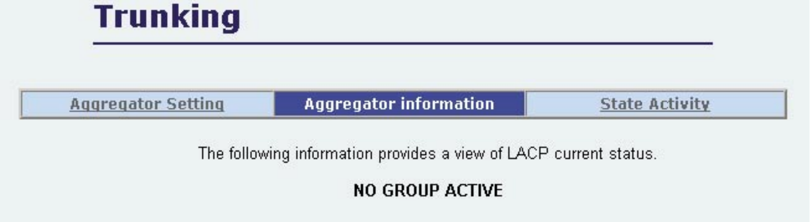
If LACP is enabled, you can configure LACP Active/Passive status in each port on State Activity page.

Click Apply.

2.5.5.2 Aggregator Information

When you are setting LACP aggregator, related information will be displayed.

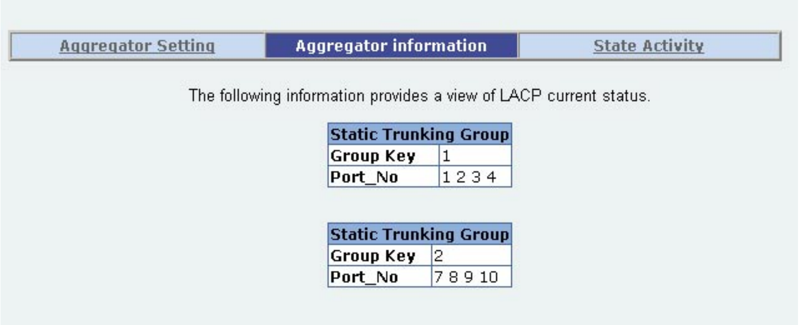
1. This page displays no group active. LACP is not working.



The following information provides a view of LACP current status.

NO GROUP ACTIVE

2. This page displays Static Trunking groups.

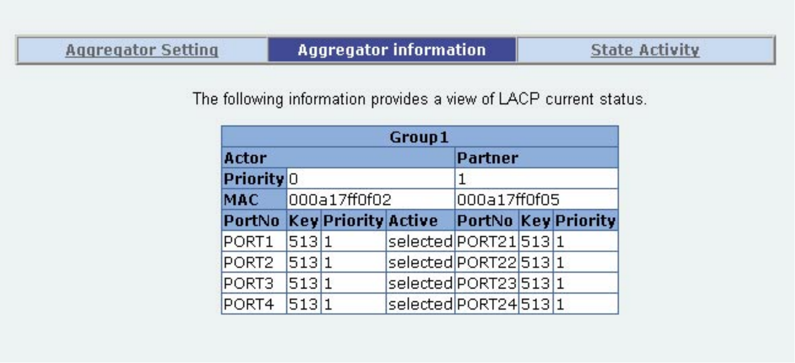


The following information provides a view of LACP current status.

Static Trunking Group	
Group Key	1
Port_No	1 2 3 4

Static Trunking Group	
Group Key	2
Port_No	7 8 9 10

3. This page displays Actor and Partner trunking in one group.



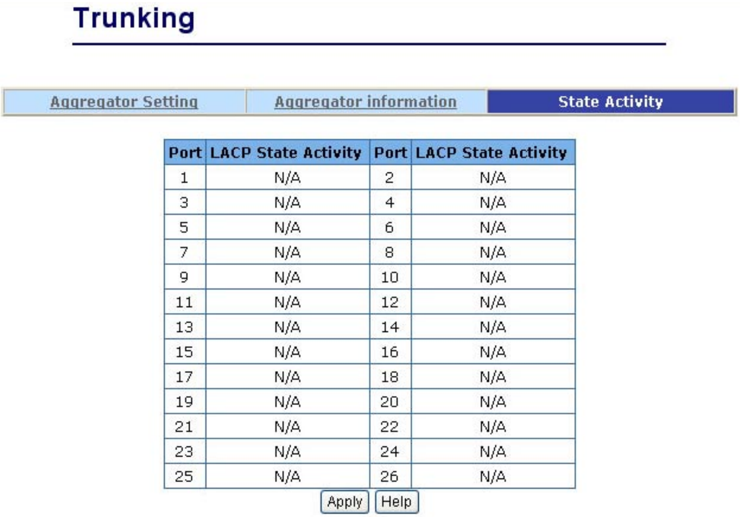
The following information provides a view of LACP current status.

Group1						
Actor				Partner		
Priority	0			1		
MAC	000a17ff0f02			000a17ff0f05		
PortNo	Key	Priority	Active	PortNo	Key	Priority
PORT1	513	1	selected	PORT21	513	1
PORT2	513	1	selected	PORT22	513	1
PORT3	513	1	selected	PORT23	513	1
PORT4	513	1	selected	PORT24	513	1

2.5.5.3 State Activity

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

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



Trunking

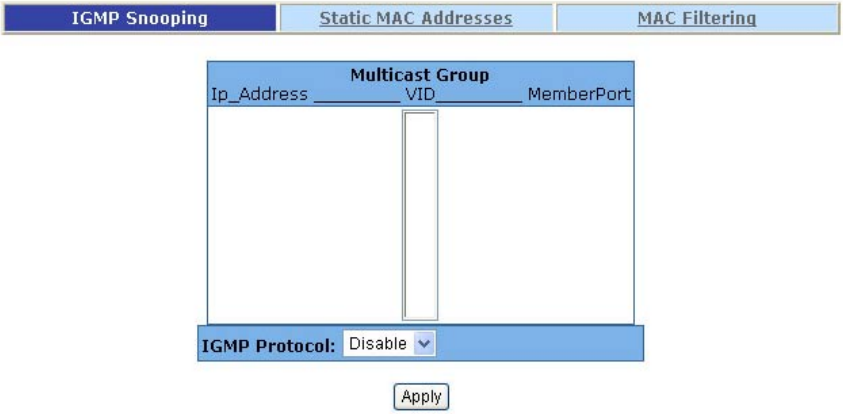
Port	LACP State Activity	Port	LACP State Activity
1	N/A	2	N/A
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

1. A link that has either two active LACP ports or one active port can perform dynamic LACP trunking. A link has two N/A LACP ports will not perform dynamic LACP trunking because both ports are waiting for an LACP protocol packet from the opposite device.
2. If you are active LACP's actor, when you select trunking port, the active status will be created automatically.

2.5.6 Filter Database

2.5.6.1. IGMP Snooping

The NP2624M switch supports multicast IP. IGMP protocol can be enabled on this web page, and IGMP snooping information is displayed on this page. All multicast groups, VIDs and member ports are displayed in the list. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.



IGMP Protocol: Disable

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

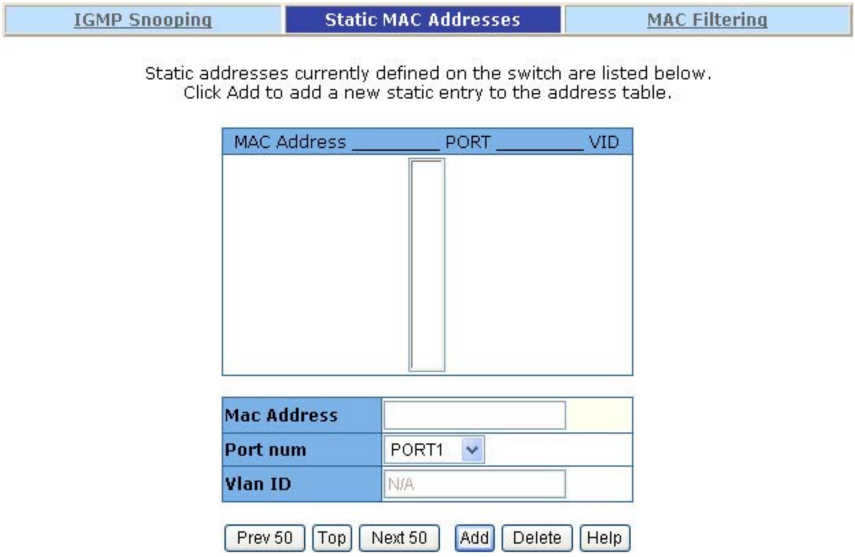
IGMP can manage the multicast traffic if the members (switches, router or other network devices) of groups support IGMP. With IGMP enabled, the member ports will detect IGMP queries, report packets and manage the IP multicast traffic through the switch.

IGMP have three fundamental types of message as follows:

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

2.5.6.2. Static MAC Address

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



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

MAC Address	PORT	VID

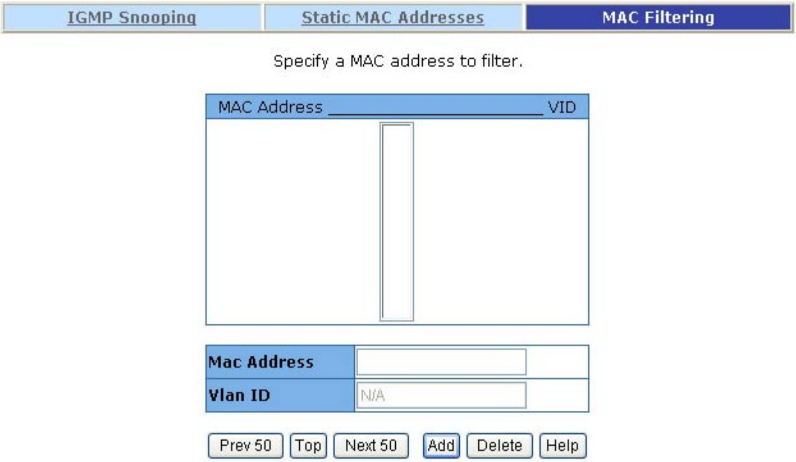
Mac Address	
Port num	PORT1
Vlan ID	N/A

1. At the main menu, click Administrator >Filter Database >Static MAC Address.
2. In the MAC address box, enter the MAC address.
3. In the Port Number box, enter a port number.
4. If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.
5. Click the Add.
6. Click the "Prev 50" will list the previous 50 MAC addresses.
7. Click the "Top" will refresh the list from the first entry.
8. Click the "Next 50" will list the next 50 MAC addresses.

2.5.6.3 MAC filtering

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

1. In the MAC Address box, enter the MAC address that you want to filter.

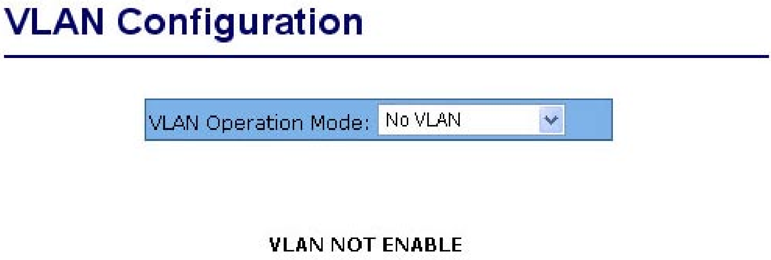


Mac Address	
Vlan ID	N/A

2. If tag-based (802.1Q) VLAN are set up on the switch, in the VLAN ID box, type the VID to associate with the MAC address.
3. Click the Add.
4. Choose the MAC address that you want to delete and then click the Delete.

2.5.7. VLAN configuration

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



VLAN Configuration

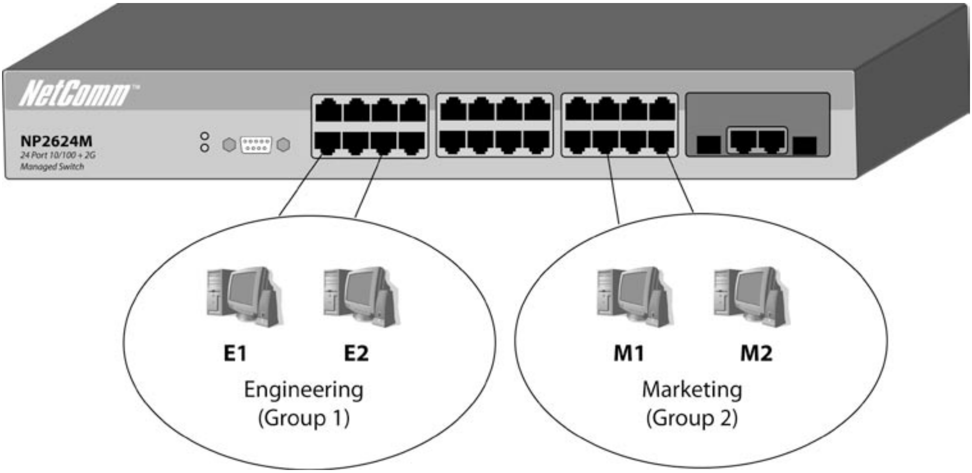
VLAN Operation Mode: No VLAN

VLAN NOT ENABLE

The NP2624M switch supports port-based, 802.1Q (tagged-based) and protocol-base VLAN in web management page. In the default configuration, VLAN support is disabled.

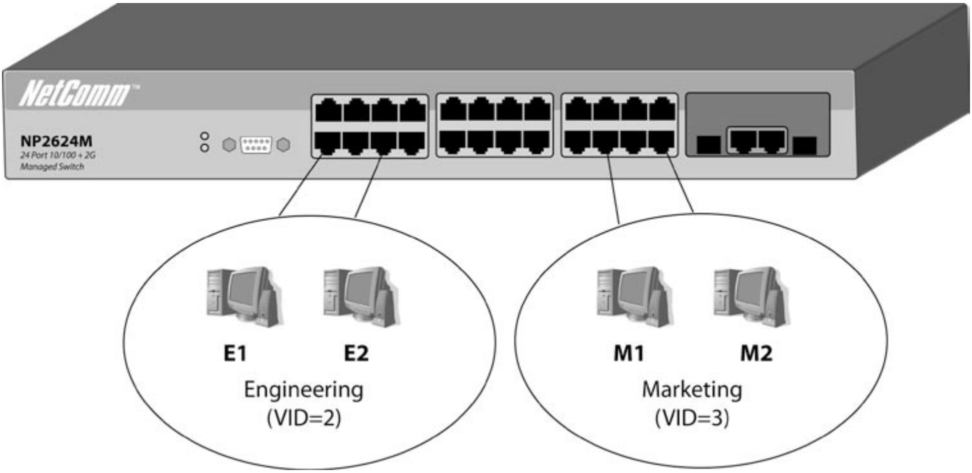
Support Port-based VLAN

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



Support Tag-based VLAN (IEEE 802.1Q VLAN)

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

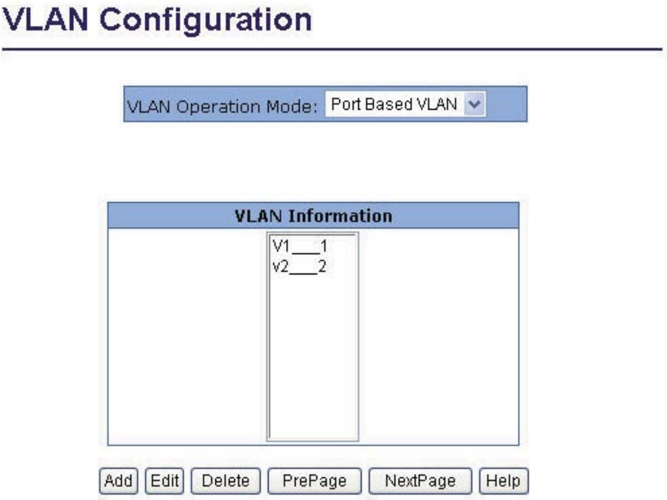


Support Protocol-based VLAN

In order for an end station to send packets to different VLANs, it has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packets with a different VLAN ID based not only on the default PVID but also other information about the packet, such as the protocol.

The NP2624M switch will support protocol-based VLAN classification by means of built-in knowledge of layer 2 packet formats used by selected popular protocols, such as Novell IPX and AppleTalk's Ether Talk, and some degree of programmable protocol matching capability.

2.5.7.1. Port Based VLAN



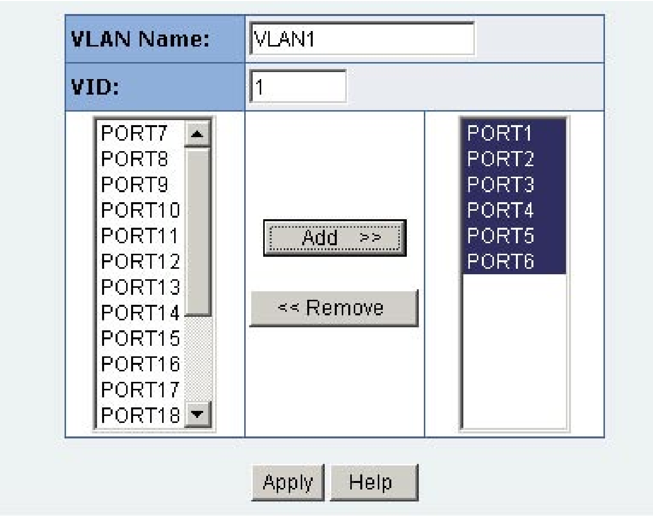
VLAN Configuration

VLAN Operation Mode: Port Based VLAN

VLAN Information

V1___1
v2___2

1. Click Add to create a new VLAN group.
2. Enter the VLAN name, group ID and select the members for the new VLAN.
3. Click Apply.
4. If there are many groups that over the limit of one page, you can click the “Next Page” to view other VLAN groups.



VLAN Name: VLAN1

VID: 1

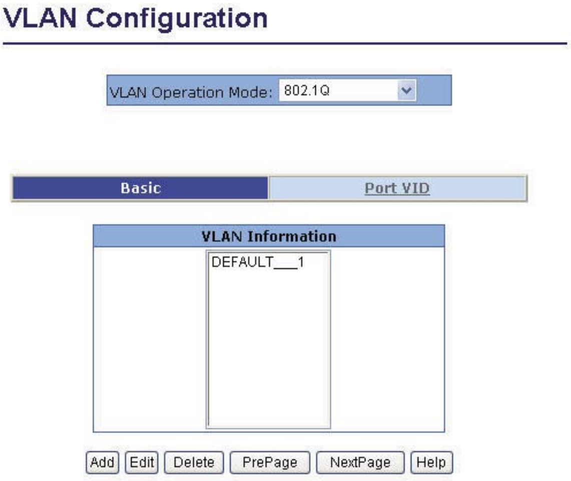
PORT7
PORT8
PORT9
PORT10
PORT11
PORT12
PORT13
PORT14
PORT15
PORT16
PORT17
PORT18

PORT1
PORT2
PORT3
PORT4
PORT5
PORT6

NOTE: If trunk groups exist, they will be displayed (eg: TRK1, TRK2...) in select menu of ports. These can also be configured on the VLAN.

2.5.7.2. 802.1Q VLAN

In this page, the user can create a Tag-based VLAN.



VLAN Configuration

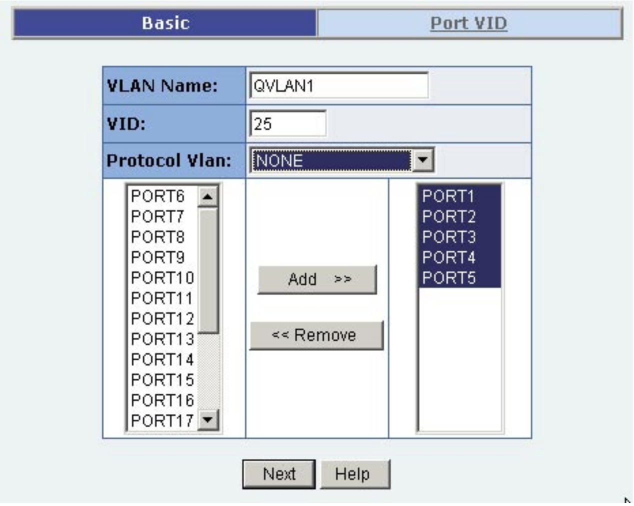
VLAN Operation Mode: 802.1Q

256 VLAN groups can be configured. If 802.1Q VLAN is enabled, then all ports on the switch will belong to the default VLAN (VID is 1). The default VLAN cannot be deleted.

Basic

Create a VLAN and add tagged member ports to it.

1. From the main menu, click Administrator >VLAN configuration, click Add and the following page will be displayed.



VLAN Name: QVLAN1

VID: 25

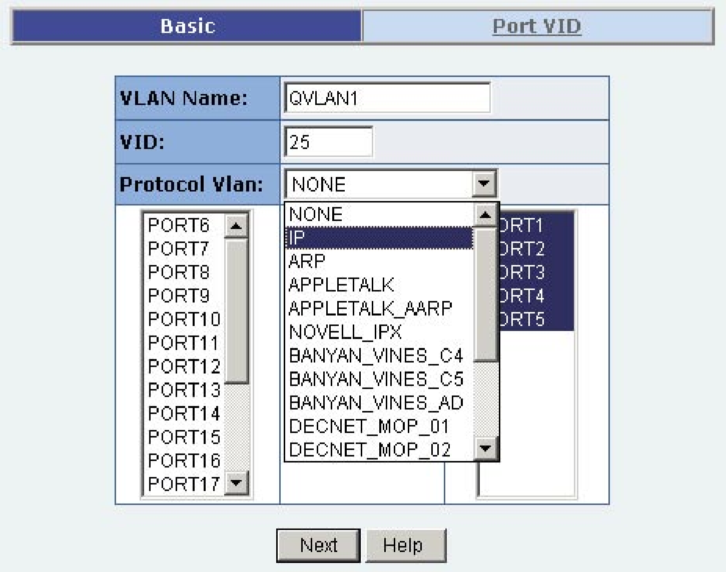
Protocol Vlan: NONE

2. Type a name for the new VLAN.

3. Type a VID (between 2-4094). The default is 1.
4. Choose the protocol type.

   The NP2624M supports 802.1v with the implementation of Port-and-Protocol-based VLAN classification. Users can combine the field “Protocol VLAN” and the field of the port number to form a new VLAN group.

NOTE: IEEE 802.1v allows a user to classify the packets through an untagged port. There are two possible strategies of the 802.1v support: Port-based VLAN and Port-and-Protocol-based VLAN. Both are supported in the NP2624M. Users set the VID to mark the packet from the untagged port and then the packet can be scheduled by the way of the IEEE 802.1q.

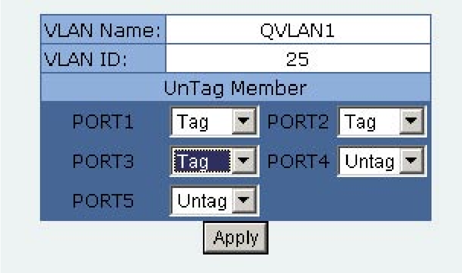


VLAN Name: QVLAN1

VID: 25

Protocol Vlan: NONE

5. From the Available ports box, select ports to add to the switch and click “Add >>”. If the trunk groups exist, they will be displayed here (eg: TRK1, TRK2…) and you can configure it as a member of the VLAN if necessary.
6. Click Next. The following page will be displayed.



VLAN Name:	QVLAN1		
VLAN ID:	25		
UnTag Member			
PORT1	Tag	PORT2	Tag
PORT3	Tag	PORT4	Untag
PORT5	Untag		

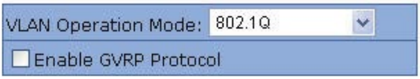
7. Use this page to set whether the outgoing frames are VLAN-Tagged frames or not. Then click Apply.

   Tag: outgoing frames with VLAN-Tagged.

   Untag: outgoing frames without VLAN-Tagged.

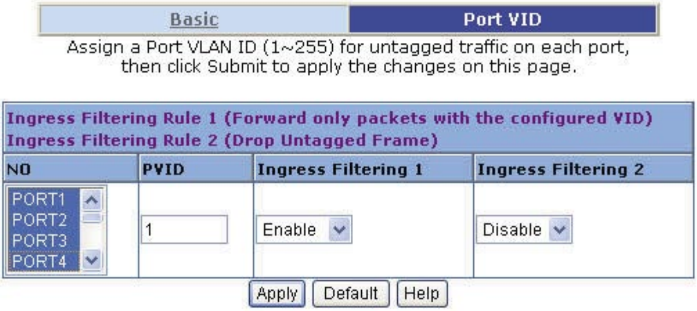
Port VID

From the main Tag-based (IEEE 802.1Q) VLAN page, click Port VID Settings to configure port VID settings.



VLAN Operation Mode: 802.1Q

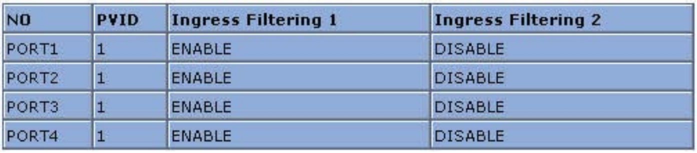
□ Enable GVRP Protocol



Assign a Port VLAN ID (1~255) for untagged traffic on each port, then click Submit to apply the changes on this page.

Ingress Filtering Rule 1 (Forward only packets with the configured VID)
Ingress Filtering Rule 2 (Drop Untagged Frame)

NO	PVID	Ingress Filtering 1	Ingress Filtering 2
PORT1 PORT2 PORT3 PORT4	1	Enable	Disable



NO	PVID	Ingress Filtering 1	Ingress Filtering 2
PORT1	1	ENABLE	DISABLE
PORT2	1	ENABLE	DISABLE
PORT3	1	ENABLE	DISABLE
PORT4	1	ENABLE	DISABLE

Port VID (PVID)

Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but do not support tagging. The NP2624M switch allows each port to set one PVID, the range is 1~255, default PVID is 1. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. The NP2624M switch has two ingress filtering rules as follows:

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

Ingress Filtering Rule 2: Drop Untagged Frame.

2.5.8. Rapid Spanning Tree

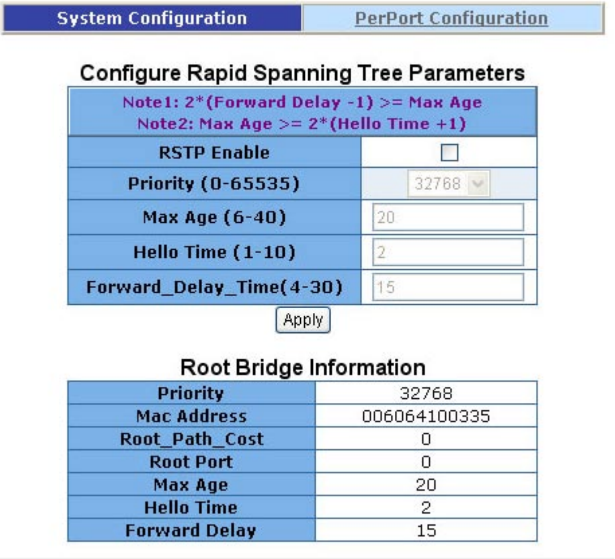
We provide Both Rapid-Spanning-Tree-Protocol (RSTP) and Spanning-Tree Protocol (STP).

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. Enable STP to ensure that only one path at a time is active between any two nodes on the network.

The Rapid-Spanning-Tree-Protocol (RSTP) is a more advanced Protocol than STP. RSTP can shorten spanning tree convergent time if your network topology changes. For the default, the switch will use RSTP. If the switch receives a STP's BPDU, the switch will degrade to STP.

You can enable STP (Spanning-Tree Protocol) using the web management's switch setting advanced item, select enable Spanning-Tree Protocol. We recommend that you enable STP on all switches to ensure a single active path on the network.

1. You can view spanning tree information about the Root Bridge on the following screen:



Configure Rapid Spanning Tree Parameters

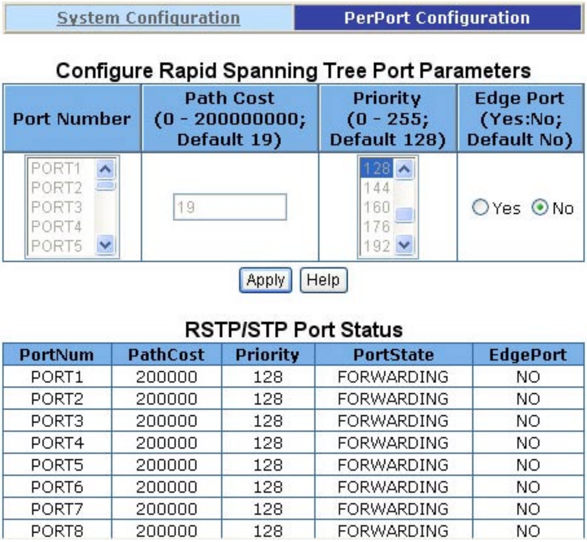
Note1: 2*(Forward Delay -1) >= Max Age
Note2: Max Age >= 2*(Hello Time +1)

RSTP Enable	□
Priority (0-65535)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward_Delay_Time(4-30)	15

Root Bridge Information

Priority	32768
Mac Address	006064100335
Root_Path_Cost	0
Root Port	0
Max Age	20
Hello Time	2
Forward Delay	15

2. You can view spanning tree status about the switch on the following screen:



System Configuration | PerPort Configuration

Configure Rapid Spanning Tree Port Parameters

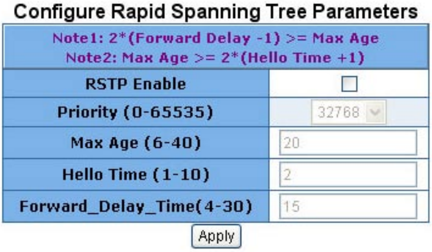
Port Number	Path Cost (0 - 200000000; Default 19)	Priority (0 - 255; Default 128)	Edge Port (Yes:No; Default No)
PORT1 PORT2 PORT3 PORT4 PORT5	19	128 144 160 176 192	○ Yes ● No

Apply Help

RSTP/STP Port Status

PortNum	PathCost	Priority	PortState	EdgePort
PORT1	200000	128	FORWARDING	NO
PORT2	200000	128	FORWARDING	NO
PORT3	200000	128	FORWARDING	NO
PORT4	200000	128	FORWARDING	NO
PORT5	200000	128	FORWARDING	NO
PORT6	200000	128	FORWARDING	NO
PORT7	200000	128	FORWARDING	NO
PORT8	200000	128	FORWARDING	NO

3. You can also set new values for RSTP parameters, then click the Apply button to modify



Configure Rapid Spanning Tree Parameters

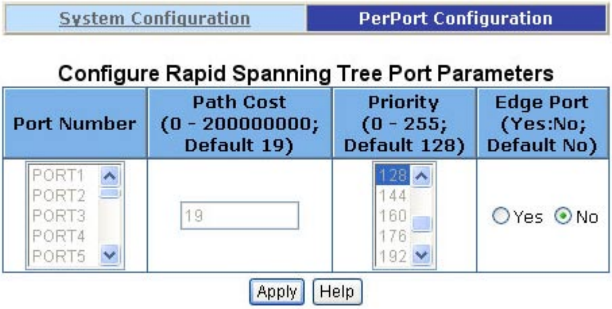
Note1: 2*(Forward Delay -1) >= Max Age
Note2: Max Age >= 2*(Hello Time +1)

RSTP Enable	□
Priority (0-65535)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward_Delay_Time(4-30)	15

Apply

Parameter	Description
Priority	You can change the priority value. A value is used to identify the root bridge. The bridge with lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Max Age	You can change the Max Age value. The number of second bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40.
Hello Time	You can change the Hello time value. The number of seconds among the transmission of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10.
Forward Delay Time	You can change the forward delay time. The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30.

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



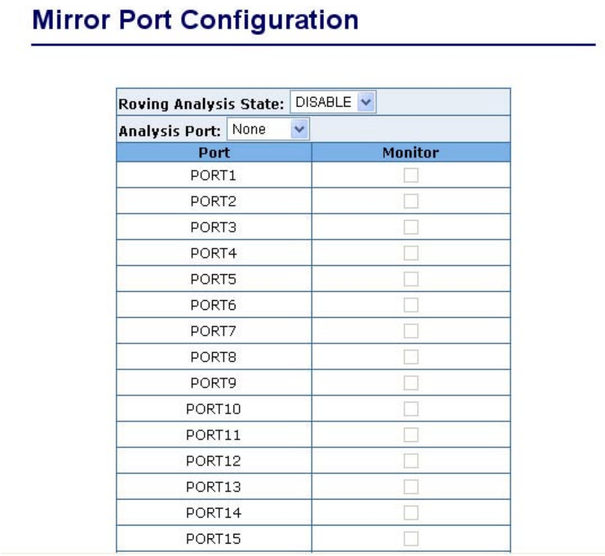
Configure Rapid Spanning Tree Port Parameters

Port Number	Path Cost (0 - 200000000; Default 19)	Priority (0 - 255; Default 128)	Edge Port (Yes:No; Default No)
PORT1 PORT2 PORT3 PORT4 PORT5	19	128 144 160 176 192	○ Yes ● No

Parameter	Description
Port Number	Select the port number.
Path Cost	Specifies the path cost of the port that the switch uses to determine which ports are the forwarding ports. The lowest number is forwarding ports, the range is 1-65535 and default value base on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10
Port Priority	You can make it more or less likely to become the root port, the range is 0-255, and default setting is 128. The lowest number has the highest priority.
Edge Port	Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will keep in forwarding state and skip the listening and learning state. When the link on the edge port is changed, the RSTP topology is not affected.

2.5.9. Port Mirror

The Port Mirror is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic going in or out monitored ports will be duplicated into an Analysis port.



Mirror Port Configuration

Roving Analysis State: DISABLE

Analysis Port: None

Port	Monitor
PORT1	☐
PORT2	☐
PORT3	☐
PORT4	☐
PORT5	☐
PORT6	☐
PORT7	☐
PORT8	☐
PORT9	☐
PORT10	☐
PORT11	☐
PORT12	☐
PORT13	☐
PORT14	☐
PORT15	☐

Roving Analysis Mode: Press Space key to set mirror mode: Disable \Rx \Tx \Both.

Analysis Port: This port can be used to see all monitored ports' traffic. You can connect analysis port to LAN analyser or netxray.

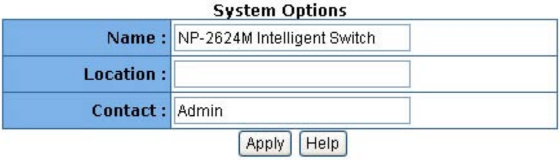
Monitored Port: The ports you want to monitor. All monitored port traffic will be copied to the analysis port. You can select a maximum of 25 monitor ports in the switch. Users can choose which port that they want to monitor in only one mirror mode.

If you want to disable the function, you must deselect monitor port.

2.5.10. SNMP/Trap Manager

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

1. System Options:



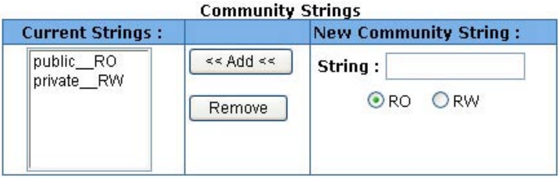
System Options

Name :	NP-2624M Intelligent Switch
Location :	
Contact :	Admin

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

Name:	Enter a name to be used for the switch.
Location:	Enter the location of the switch.
Contact:	Enter the name of a person or organisation.

2. Community Strings



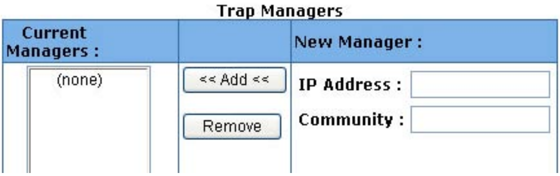
Community Strings

Current Strings :		New Community String :
public__RO private__RW	<< Add << Remove	String : ● RO ○ RW

Community Strings serve as passwords and can be entered as one of the following:

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

3. Trap Manager



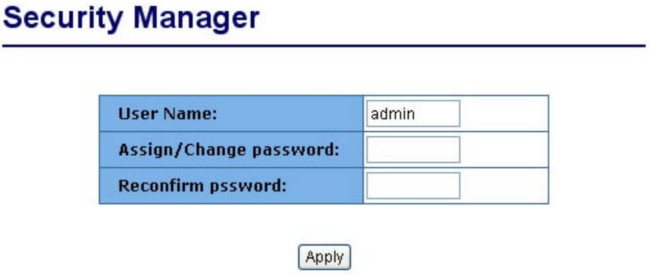
Trap Managers

Current Managers :		New Manager :
(none)	<< Add << Remove	IP Address : Community :

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

2.5.11 Security Manager

On this page, users can change username and password with following steps.



Security Manager

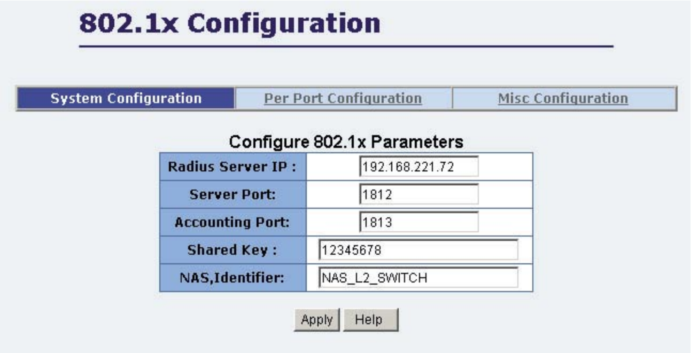
User Name:	admin
Assign/Change password:	
Reconfirm pssword:	

1. In **User Name**: Type the new username.
2. In **Assign/Change password**: Type the new password.
3. In **Reconfirm password**: Retype the new password.
4. Click **Apply**.

2.5.12 802.1x Configuration

System Configuration

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and prevent access to that port in cases where the authentication and authorization process fails.



802.1x Configuration

Configure 802.1x Parameters

Radius Server IP :	192.168.221.72
Server Port:	1812
Accounting Port:	1813
Shared Key :	12345678
NAS,Identifier:	NAS_L2_SWITCH

To enable 802.1x, from Administrator \Switch setting \Advanced then fill in the authentication server information:

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

Server Port: The UDP port number used by the authentication server to authenticate.

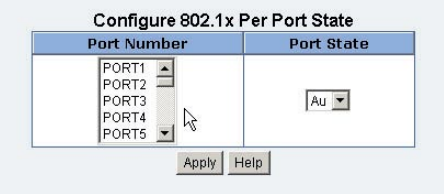
Accounting Port: The UDP port number used by the authentication server to retrieve accounting information.

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

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

Perport Configuration

In this page, users can select the specific port and configure the Authorisation State.



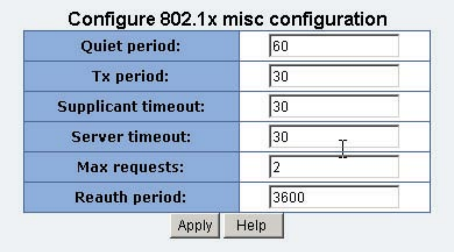
Configure 802.1x Per Port State

Port Number	Port State
PORT1 PORT2 PORT3 PORT4 PORT5	Au

Each port can select four kinds of Authorisation State:

Fu:	Force the specific port to be unauthorised.
Fa:	Force the specific port to be authorised.
Au:	The state of the specific port was determined by the outcome of the authentication.
No:	The specific port didn't support 802.1x function.

Miscellaneous Configuration



Configure 802.1x misc configuration

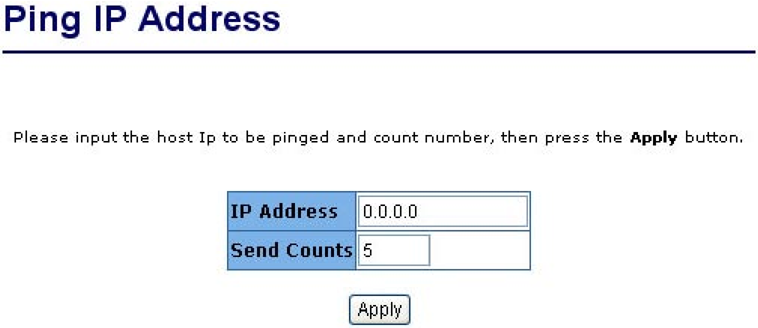
Quiet period:	60
Tx period:	30
Supplicant timeout:	30
Server timeout:	30
Max requests:	2
Reauth period:	3600

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

Quiet Period:	Used to define periods of time during which it will not attempt to acquire a supplicant (Default time is 60 seconds).
Tx Period:	Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
Supplicant Timeout:	Used to determine timeout conditions in the exchanges between the supplicant and authentication server (Default value is 30 seconds).
Server Timeout:	Used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
Max requests:	Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
Reauth Period:	Used to determine a nonzero number of seconds between periodic re-authentication off the supplications (Default value is 3600 seconds).

2.5.13 Ping

The NP2624M switch provides a simplified ping function for users to check whether an IP is online or not.



Ping IP Address

Please input the host Ip to be pinged and count number, then press the **Apply** button.

IP Address	0.0.0.0
Send Counts	5

Enter the IP Address and number of counts for the ping packet to send. Press “Apply” to continue next page.

This page will display the result of the pinging IP. It continues updating the “Reply Counts” to the ping packets that are sent. Users can interrupt the progress by clicking the “Stop” button.

If the reply counts remain zero after the webpage reload stops, it could mean that the pinged host of this IP does not exist.

2.5.14 Single IP

The NP2624M switch provides a new management tool for a user to manage a group of LAN switches by an IP agent method. "Single IP" is the name, meaning that the administrator can access other network devices through one single IP device. There are two management modes: "Agent mode" and "Stacking mode".

Unlike a router's NAT (from virtual IP domain to real IP domain), single IP provides a reverse access (from real IP domain to virtual IP domain) using an IP-forwarding technology. With this IP-agent method, the network administrator can remotely control his far-side hosts without being there, accessing the private domain hosts through the agency of one real IP switch with a "Single IP".

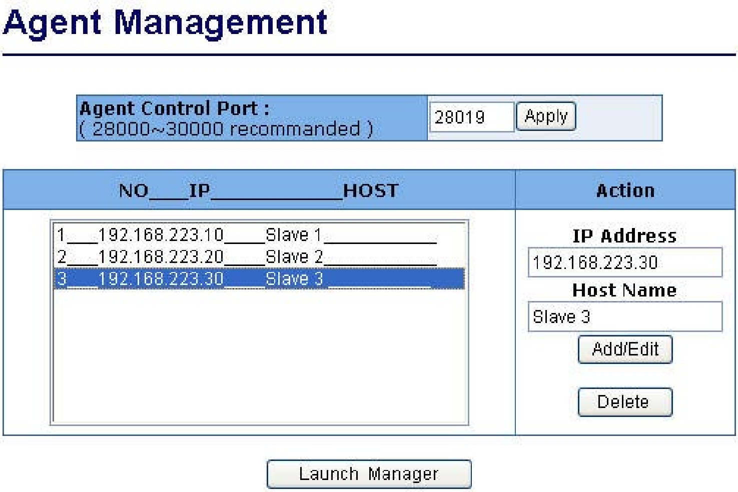
A maximum of 32 sets of information of network devices can be stored in the single IP switch and 16 sets in a stacking switch. Basically these network devices should provide http:// or telnet service for the single IP switch to forward those protocol packets; meanwhile SNMP protocol can be also passed through if they support SNMP service.

Moreover, this single IP switch has no exclusiveness, meaning that administrator can group up network devices of any type (router, switch, server...) or brand without worrying their incompatibility.

However, for stacking switch, only the switches of the same model can detect each other and transfer information to their partner, so it won't support other network devices in this instance. This is the major difference between single IP agent mode and stacking mode. Please read Chapter 5 for more information.

Web UIs of "Agent Management" and "Stacking Management" look similar. In these pages, users can add or delete managed network devices. If the user disables the IP agent function, that is, sets the management mode to "Agent Slave" or "Stacking Slave" in the IP setting webpage, this item will not show up in the main menu.

2.5.14.1 Agent Management



Agent Management

Agent Control Port : (28000~30000 recommanded) 28019 Apply

NO___IP____________HOST

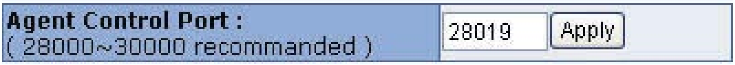
1___192.168.223.10____Slave 1____________
2___192.168.223.20____Slave 2____________
3___192.168.223.30____Slave 3____________

Action

IP Address 192.168.223.30

Host Name Slave 3

Agent Control Port: The control port defines the specific TCP/UDP port the single IP switch is listening, which the agent manager sends its command to. Agent manager use this specific port to tell the single IP switch to change the current forwarding target host. The range of available port number is 28000 ~ 30000. Ignore the default settings of the "Agent Control Port" unless the user has a special need for this protocol port, such as virtual server. The default port number is 28019.



Agent Control Port :
(28000~30000 recommanded)
28019 Apply

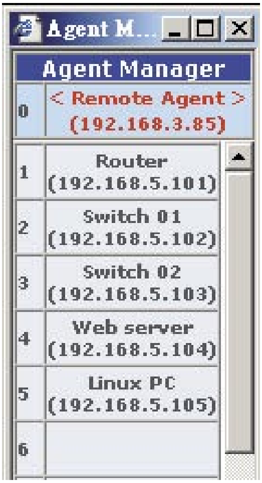
Add/Edit/Delete : To add a member, enter the IP and name in "IP address" and "Host Name", then press "Add/Edit". The new member will be listed on the left. To edit a member's host name, select the member in the list and the IP and name will be shown on the right. Edit the name and then press "Add/Edit" to update the list. To remove a member, just select the member and press "Delete"

Launch Manager : This button launches the Stacking manager.

2.5.14.2 Agent Manager

A floating menu be displayed after clicking "Launch Agent Manager" in the agent management menu.

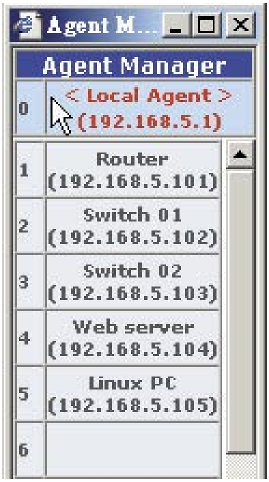
The agent manager holds 32+1 slots in the floating menu. The top slot (zero slot) displays the master switch IP and its relative location. "Remote Agent" means that the user comes from another IP domain than the managed ones, while "Local Agent" means that the user comes from the same IP domain as the managed ones.



Agent M...

Agent Manager

0	< Remote Agent > (192.168.3.85)
1	Router (192.168.5.101)
2	Switch 01 (192.168.5.102)
3	Switch 02 (192.168.5.103)
4	Web server (192.168.5.104)
5	Linux PC (192.168.5.105)
6	



Agent M...

Agent Manager

0	< Local Agent > (192.168.5.1)
1	Router (192.168.5.101)
2	Switch 01 (192.168.5.102)
3	Switch 02 (192.168.5.103)
4	Web server (192.168.5.104)
5	Linux PC (192.168.5.105)
6	

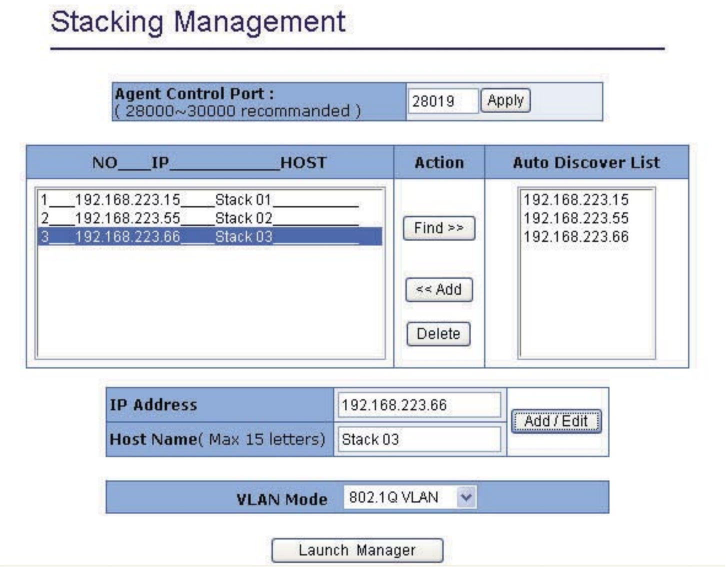
There are differences between "Remote Agent" and "Local Agent". The "Local Agent", referred to as "Local Single IP", uses URL link method and the main browser window will directly jump to the target host. Since the URL of the web browser has changed, authentication will be requested once again when the new host is selected.

Due to switch loading, only one remote user can access the agent manager at a time. Other users will be rejected if someone has launched the agent manager first. The switch will release the control of single IP access in 25 seconds after the previous user closes his agent manager. For "Local Single IP", there is no restriction, but if a remote user has launched the agent manager in the same time, the local user is also denied.

NOTE: Commands from agent manager cannot pass over current management level, meaning that, in cases where a slave host is a single IP switch with its agent function enabled, a user launching the slave host's agent manager will find the agent manager is replaced by the slave's one. Worse still, commands to pick the slave hosts will cause an unexpected forwarding error here.

We strongly recommend that a single IP switch should not activate the IP agent manager when it is a slave host of active master switch.

2.5.14.3 Stacking Management



Stacking Management

Agent Control Port : (28000~30000 recommanded): 28019

NO___IP___________HOST	Auto Discover List
1___192.168.223.15____Stack 01__________	192.168.223.15
2___192.168.223.55____Stack 02__________	192.168.223.55
3___192.168.223.66____Stack 03__________	192.168.223.66

IP Address: 192.168.223.66

Host Name(Max 15 letters): Stack 03

VLAN Mode: 802.1Q VLAN

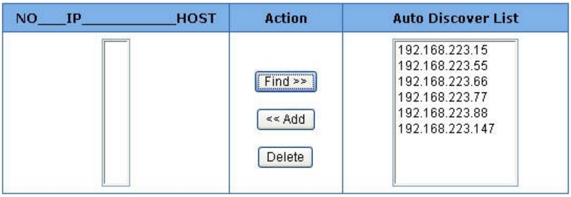
Agent Control Port: The specific TCP/UDP port the single IP switch is listening. See 2.5.14.1 Agent Management for details.

There are two ways to add the members: "Auto-discover" and "Manual".

Auto-discover method:

Press “Find >>” and the found stackable switches will be gathered in “Auto Discover List”. Select these found members and press “ << Add” to add the selected hosts to the list.

The searching range bases on Class C IP domain within Agent IP. Changing the “Agent IP” in “Administrator/IP & Management Mode” will alter the search range. For example, if the Agent IP is set to 192.168.223.100, and then the auto-discover function will search for available switches in the range from 192.168.223.1 to 192.168.223.255.



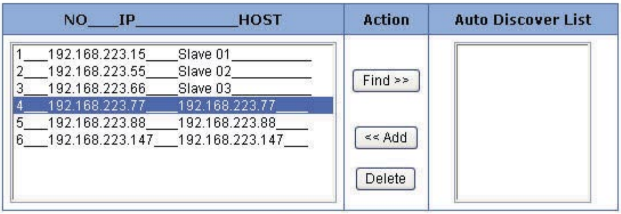
NO___IP___________HOST	Action	Auto Discover List
	Find >> << Add Delete	192.168.223.15 192.168.223.55 192.168.223.66 192.168.223.77 192.168.223.88 192.168.223.147

Manual method:

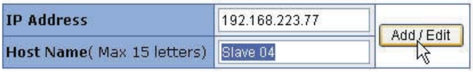
Users can add members manually. Fill up the “IP Address” and “Host Name”, then press “Apply” to complete the a**ddition of a new member**.

Editing an existing member is also easy to do. Simply select the host which needs to edited, the “IP address” and “Host Name” will appear. Then modify the “Host Name” for reference. For any IP that is not within the member list, the modification will assume to add a new member. Press “Apply” to confirm the modification.

To **delete an existing member,** choose the host and press “Delete”. Then the host will be removed from the list.



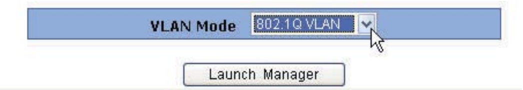
NO___IP___________HOST	Action	Auto Discover List
1___192.168.223.15____Slave 01__________ 2___192.168.223.55____Slave 02__________ 3___192.168.223.66____Slave 03__________ 4___192.168.223.77____192.168.223.77_____ 5___192.168.223.88____192.168.223.88____ 6___192.168.223.147___192.168.223.147___	Find >> << Add Delete	



IP Address	192.168.223.77	Add / Edit
Host Name(Max 15 letters)	Slave 04	

Launch Manager: This button launches the Stacking manager.

For "Stacking mode", there is an extra option "VLAN Mode" for user to choose which type of VLAN the stacking switch will carry on. There are "802.1Q" and "Port-base" VLAN .


VLAN Mode: 802.1Q VLAN

NOTE: In the case of the http:// authentication mechanism, the web browser will always ask the administrator to input username and password when agent manager changes a new host. Typically, the web browser will keep the authentication key of the successful login host and pass it to the other WebPages. The single IP switch remains the URL of the master switch IP no matter how the agent manager has changed the forwarding host, the new host will still receive the same authentication key as the master switch when it requests the login authentication. If the new host has a different username and password from the master switch, authentication failure and hence reentry will be required.

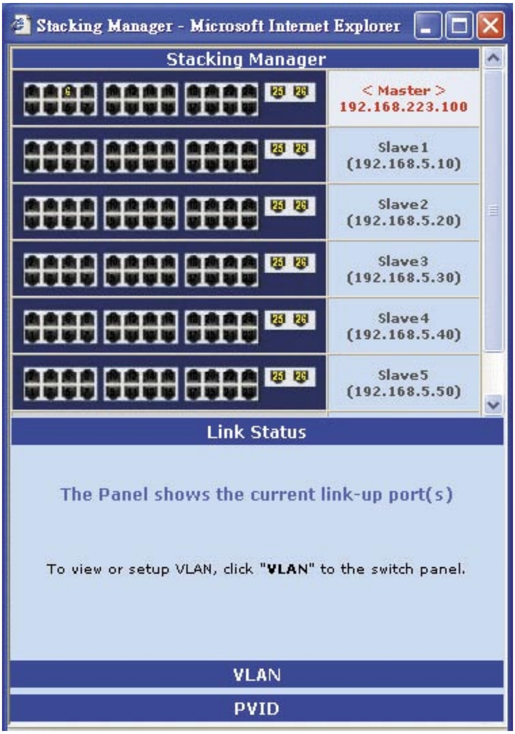
It is strongly recommended that the administrator change the usernames and passwords of the managed hosts to the same ones as the master switch.

2.5.14.4 Stacking Manager

This web UI provides not only the integrated VLAN management, but also a handy IP agent. The administrator can easily access other detail configurations in one individual switch of stacking set by clicking the hostname on the right side of this panel and jumping to its configuration webpage.

Link Status

The first page shows the current link status of all stacking members. Link-up port numbers will be highlighted. An off-line switch will dim to gray if it does not respond to the information request from the stacking master in a period of time. This characteristic provides an easy method of network diagnosis. The network administrator can check backbone connections of stacking switches at a glance from this panel.



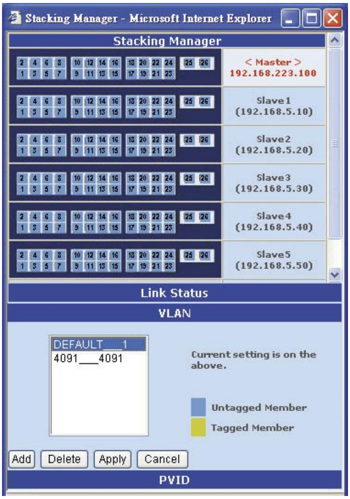
The Panel shows the current link-up port(s)

To view or setup VLAN, click "**VLAN**" to the switch panel.

VLAN SETUP

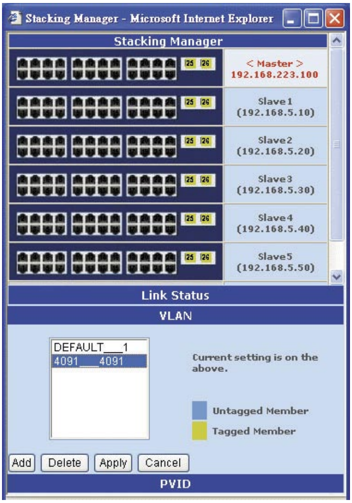
To configure the VLAN setting of the stacking switch, click "VLAN" to bring up the VLAN configuration panel.

There are two default VLANs existing in stacking switches.



DEFAULT___1
4091___4091

Current setting is on the above.



DEFAULT___1
4091___4091

Current setting is on the above.

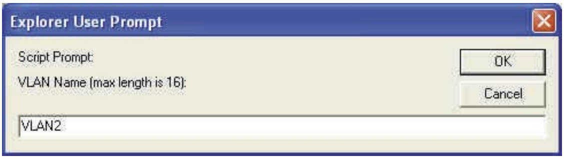
As seen above, the VLAN name " DEFAULT" and VID " 1" is standard setting for general Tag VLAN , and all ports are added as untagged ports; The other VLAN " 4091", also called a "Stacking Tag VLAN", is a unique setting for this type of stacking. All Giga ports are set to tag members to form a VLAN connection channel.

WARNING: Stacking Tag VLAN is highly restricted. Incorrect operation can ruin the connection of stacking switches. Correct use of the Stacking Tag VLAN will be discussed in the next section.

Add a VLAN

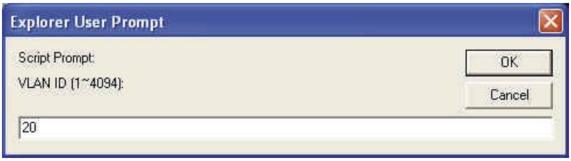
To Add a new VLAN, press " Add" in the VLAN Panel. Two prompts will ask the user to input VLAN name and VLAN ID.

After input, users can choose the VLAN member in the Stacking Manager panel by clicking the designated port. Colour cycling from blue, yellow to black means that the port is set to untagged port, tagged port or no member. When finished, press " Apply" to submit the changes.

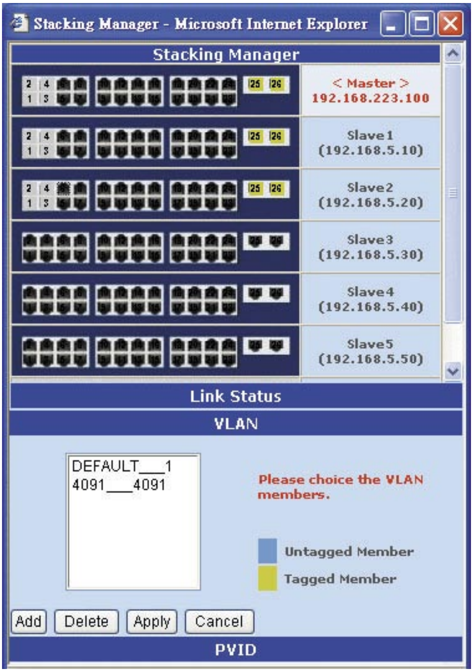


Script Prompt:
VLAN Name (max length is 16):
VLAN2

It is always wise to remember that the Giga ports of each member switch are set to tagged port and keep at least one member port in the master switch.



Script Prompt:
VLAN ID (1~4094):
20



DEFAULT___1
4091___4091

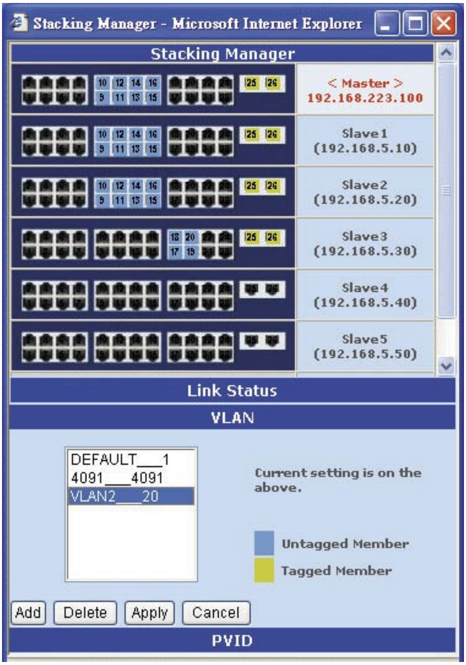
Please choice the VLAN members.

🟦 Untagged Member
🟨 Tagged Member

The stacking switches interchange VLAN information through the Giga ports which are set to tagged members by "Stacking Tag VLAN". New VLANs should keep their Giga ports tagged. Since the master switch holds all VLAN group information, the master switch should have the right to access the new VLAN by adding at least one Giga port to its tagged member. An exclusion of all master switch ports leads to unmanageability on this VLAN, for the master switch has no such VLAN in its internal table.

Edit or Delete a VLAN

To edit an existing VLAN, just select the VLAN from the VLAN panel and modify the members in the Stacking Manager panel. Once done, press " Apply" to submit the setting.



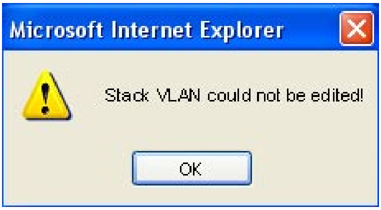
DEFAULT___1
4091___4091
VLAN2___20

Current setting is on the above.

- 🟦 Untagged Member
- 🟨 Tagged Member

To delete a VLAN is also an easy task. Select the unwanted VLAN and press "Delete" to remove it.

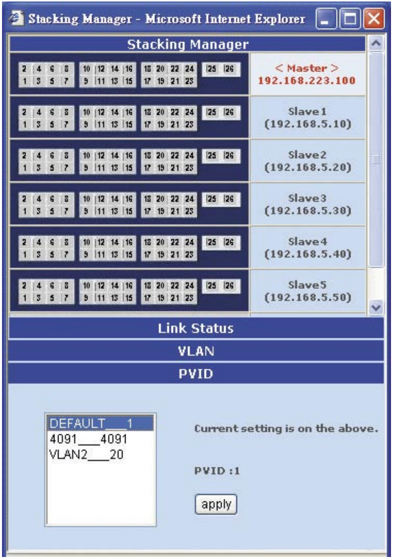
NOTE: The "DEFAULT VLAN" and "Stacking Tag VLAN" are undeletable! A error message will pop up to cancel the task. The Stack VLAN also cannot be edited.



Stack VLAN could not be edited!

PVID SETUP

The default PVID value of all ports of 802.1Q VLAN is 1. Hence only the default VLAN (PVID = 1) has all of its ports as members in the beginning.



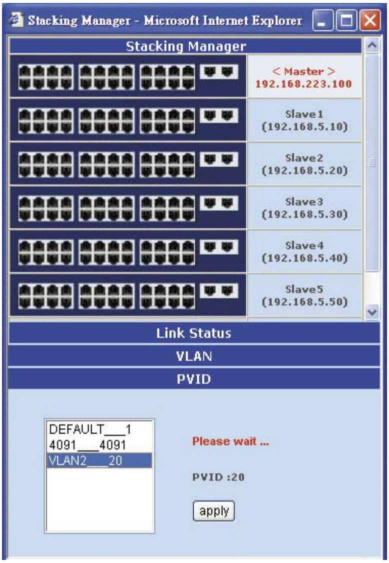
DEFAULT___1
4091___4091
VLAN2___20

Current setting is on the above.

PVID :1

The available PVIDs are based on the VLANs that the user created in the previous “VLAN” page.

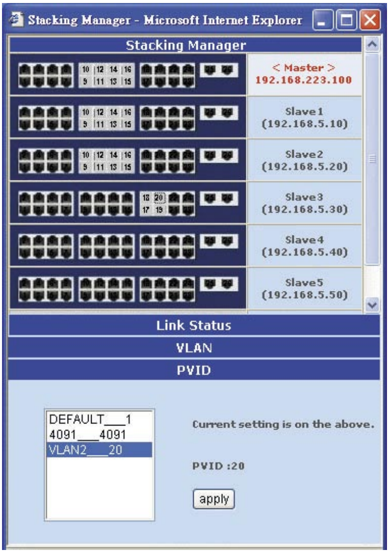
1. Select the PVID to be modified and choose the ports for this PVID value.



DEFAULT___1
4091___4091
VLAN2___20

Please wait ...

PVID :20



DEFAULT___1
4091___4091
VLAN2___20

Current setting is on the above.

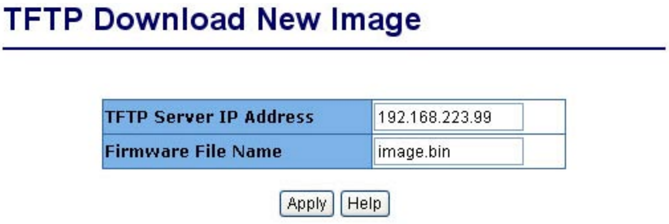
PVID :20

2. Click “Apply” button to submit and a message ”Please wait” will be displayed.
3. When a message advising “Current setting is on …” is displayed, the task is completed.

2.6. TFTP Update Firmware

The following menu options provide some system control functions to allow a user to update firmware and remotely boot the switch system:

1. Install TFTP program (such as Turbo98, or Cisco TFTP) and then execute.
2. Copy the updated firmware image.bin into TFTP server's directory.



TFTP Download New Image

TFTP Server IP Address	192.168.223.99
Firmware File Name	image.bin

3. In web management select administrator—TFTP update firmware.
4. Download the new image.bin file by pressing <update firmware>.

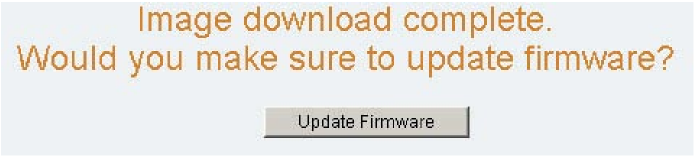
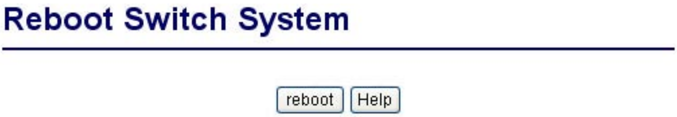


Image download complete.
Would you make sure to update firmware?

5. After the update has completed, press <reboot> to restart the switch.

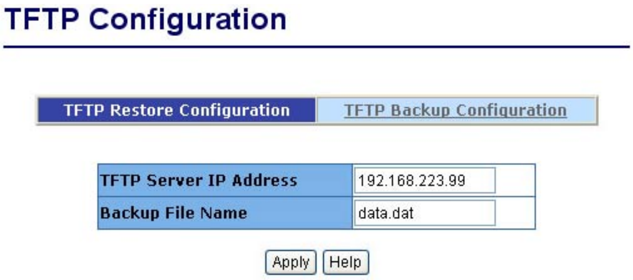


Reboot Switch System

2.7. Configuration Backup

2.7.1. TFTP Restore Configuration

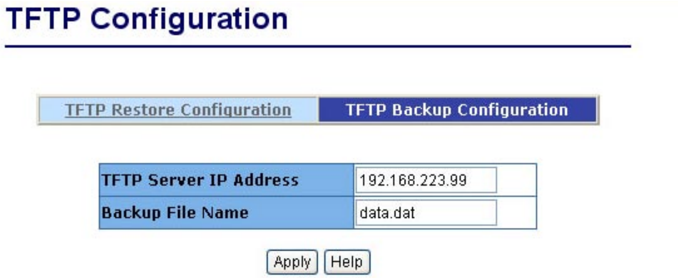
Use this page to set the ftp server address. You can restore the EEPROM value from here, but you must restore the image in the ftp server, the switch will then download the flash image back.



TFTP Server IP Address	192.168.223.99
Backup File Name	data.dat

2.7.2. TFTP Backup Configuration

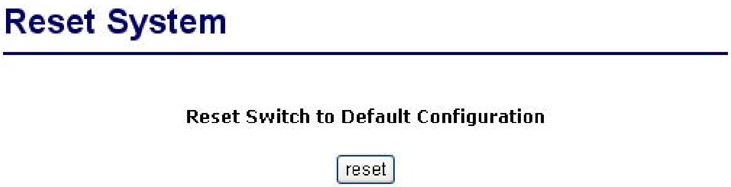
Use this page to set TFTP server IP address. You can save current EEPROM value from here, then go to the TFTP restore configuration page to restore the EEPROM value.



TFTP Server IP Address	192.168.223.99
Backup File Name	data.dat

2.8. Reset System

To Reset the Switch to its default configuration, click on the Reset button.

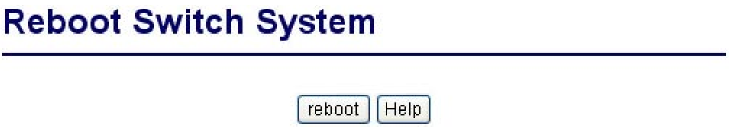


Reset System

Reset Switch to Default Configuration

2.9. Reboot

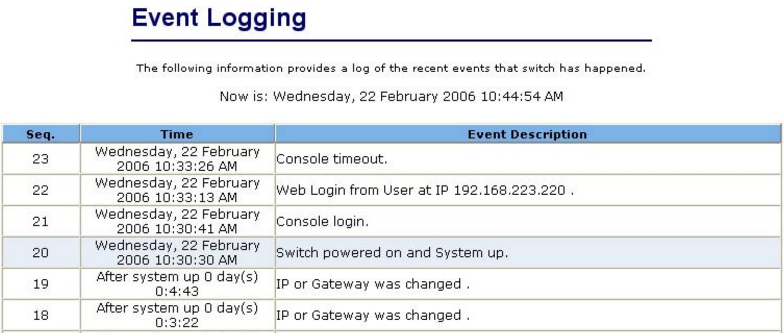
To Reboot the Switch System, click on the Reboot button.



Reboot Switch System

2.10. Event Logging

A history log is provided here to keep track of events occurring on the switch. This logs up to 100 events and then the latest event will overwrite the oldest one.



Event Logging

The following information provides a log of the recent events that switch has happened.

Now is: Wednesday, 22 February 2006 10:44:54 AM

Seq.	Time	Event Description
23	Wednesday, 22 February 2006 10:33:26 AM	Console timeout.
22	Wednesday, 22 February 2006 10:33:13 AM	Web Login from User at IP 192.168.223.220 .
21	Wednesday, 22 February 2006 10:30:41 AM	Console login.
20	Wednesday, 22 February 2006 10:30:30 AM	Switch powered on and System up.
19	After system up 0 day(s) 0:4:43	IP or Gateway was changed .
18	After system up 0 day(s) 0:3:22	IP or Gateway was changed .

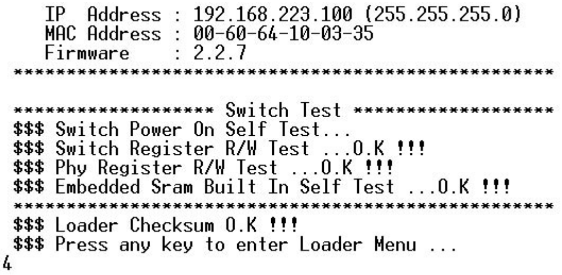
All records will be kept in flash memory even after writing default, unless user clears the event log.

Press “Prev” or “Next” button will browse previous 25 or next 25 sequences. The “Top” button will re-list the table from the latest event. “Clear” button will clear all history.

Event logger displays the real time according to the time zone set by the user.

3. Console – Boot Loader

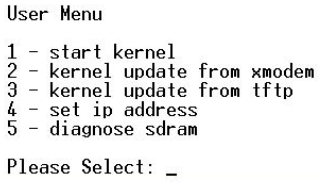
Each time the switch restarts, the user can get some basic information from console (use Hyper terminal 57600 baud rate).



```
    IP  Address : 192.168.223.100 (255.255.255.0)
    MAC Address : 00-60-64-10-03-35
    Firmware    : 2.2.7
***************************************************

******************* Switch Test *******************
$$$ Switch Power On Self Test...
$$$ Switch Register R/W Test ...O.K !!!
$$$ Phy Register R/W Test ...O.K !!!
$$$ Embedded Sram Built In Self Test ...O.K !!!
***************************************************
$$$ Loader Checksum O.K !!!
$$$ Press any key to enter Loader Menu ...
4
```

After switch tests are done, a 5-seconds countdown timer will prompt the user to press any key to enter the "User Menu".

There are five functions in the menu:



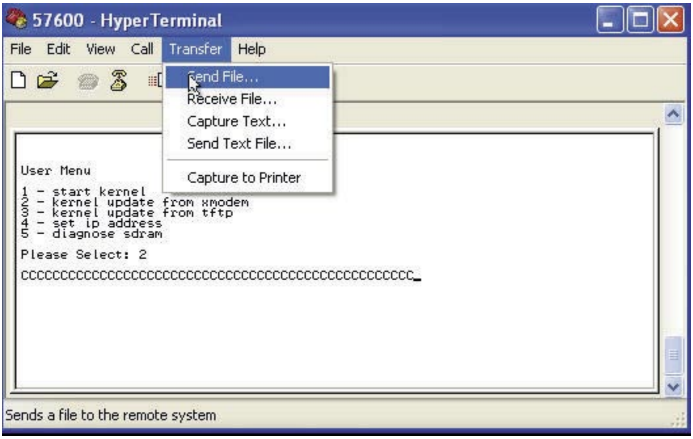
```
User Menu

1 - start kernel
2 - kernel update from xmodem
3 - kernel update from tftp
4 - set ip address
5 - diagnose sdram

Please Select: _
```

1. **start kernel:**	Back to switch system initiation and enter login.
2. **kernel update from xmodem :**	Use 1k X modem to update firmware.
3. **kernel update from tftp:**	Use TFTP to update firmware.
4. **set ip address:**	A shortcut to setup switch IP and gateway.
5. **diagnose sdram:**	A basic SDRAM diagnosis.

3.1 1K X modem Firmware update

We provide the 1k X modem to update firmware from RS232. 1K X modem only works in 57600bps mode. So you must change baud rate to 57600bps to download firmware.

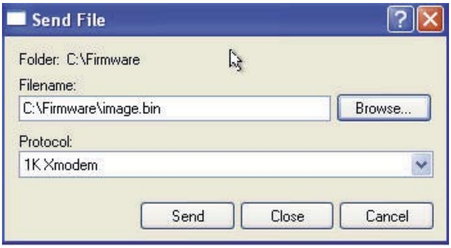
1. Select "2" to start 1K X modem firmware update.
2. When "CCCC…" is displaying on console, select Transfer /Send File.



```
User Menu

1 - start kernel
2 - kernel update from xmodem
3 - kernel update from tftp
4 - set ip address
5 - diagnose sdram

Please Select: 2

CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

Sends a file to the remote system

3. Select the 1K Xmodem in the Protocol item, and browse for the image for updating. Press the Send button.

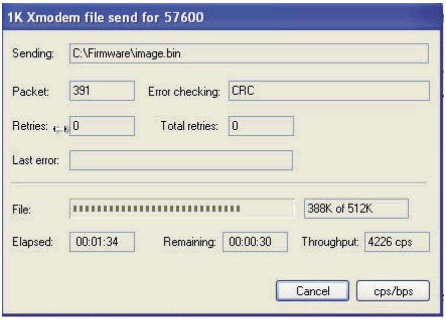


Folder: C:\Firmware

Filename: C:\Firmware\image.bin

Protocol: 1K Xmodem

4. Start downloading the image file.



Sending: C:\Firmware\image.bin

Packet: 391 Error checking: CRC

Retries: 0 Total retries: 0

Last error:

File: 388K of 512K

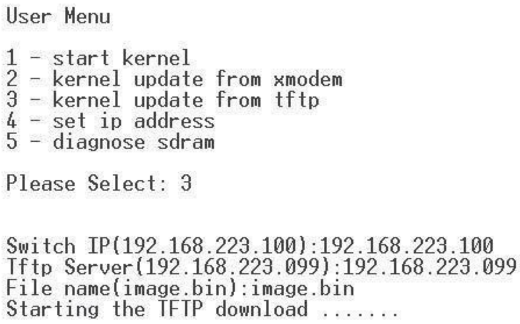
Elapsed: 00:01:34 Remaining: 00:00:30 Throughput: 4226 cps

5. After the firmware has been downloaded, the switch will then automatically update it and then the switch will reboot.

3.2 TFTP Firmware update

We provide the TFTP client to update firmware from Ethernet. The user has to first install TFTP server on their PC and place the image in the download folder.

1. Press "3" to start TFTP update firmware.

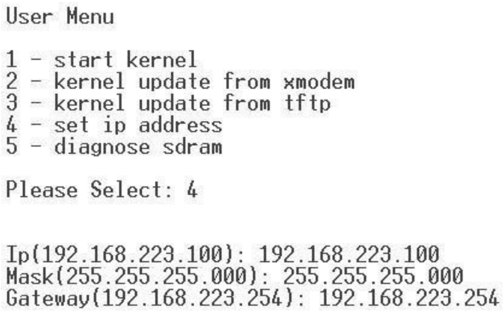


```
User Menu

1 - start kernel
2 - kernel update from xmodem
3 - kernel update from tftp
4 - set ip address
5 - diagnose sdram

Please Select: 3


Switch IP(192.168.223.100):192.168.223.100
Tftp Server(192.168.223.099):192.168.223.099
File name(image.bin):image.bin
Starting the TFTP download .......
```

2. Enter the Switch IP address and press "Enter" to accept default value.
3. Enter the TFTP Server IP address and press "Enter" to accept default value.
4. Enter the File name to download. Press "Enter" to accept default value and the TFTP download will begin and the firmware will be updated.

3.3 Set IP Address

A shortcut to set switch IP address and gateway before switch system initialization has also been provided. This saves time as the switch IP can be changed without the need to wait for the system to boot up and reconfigure.

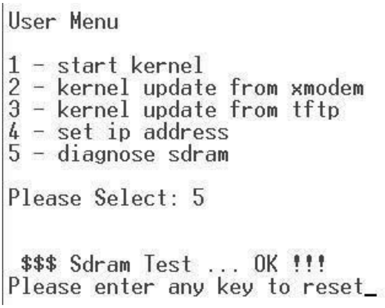


```
User Menu

1 - start kernel
2 - kernel update from xmodem
3 - kernel update from tftp
4 - set ip address
5 - diagnose sdram

Please Select: 4


Ip(192.168.223.100): 192.168.223.100
Mask(255.255.255.000): 255.255.255.000
Gateway(192.168.223.254): 192.168.223.254
```

1. Press "4" to start IP setup.
2. Enter the Switch IP address. Press "Enter" to accept the default value.
3. Enter the Mask. Press "Enter" to accept the default value.
4. Enter the Gateway IP address. Press "Enter" to accept the default value.

3.4 Diagnose Sdram

We provide a basic diagnosis for a SDRAM test. It is important to verify hardware faults when a switch becomes unstable.

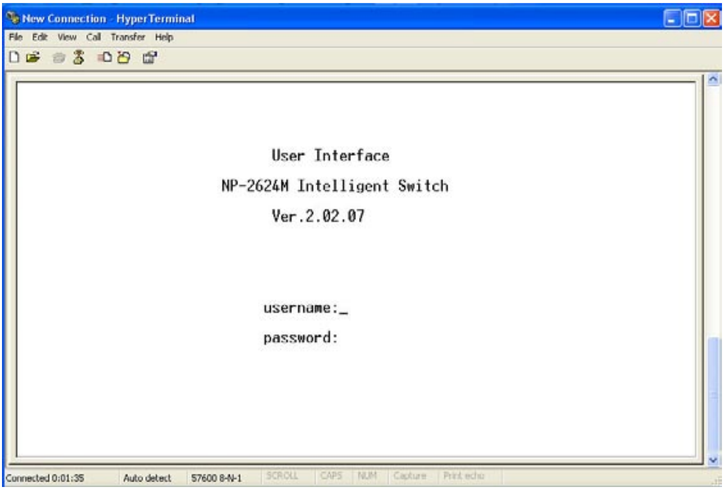


```
User Menu

1 - start kernel
2 - kernel update from xmodem
3 - kernel update from tftp
4 - set ip address
5 - diagnose sdram

Please Select: 5


 $$$ Sdram Test ... OK !!!
Please enter any key to reset_
```

When the test is done, it will display the status and prompt the user to reset the switch.

4. Out-of-band Terminal mode management

The NP2624M switch also provides a serial interface to manage and monitor the switch. Users can follow the Console Port Information provided online to use Windows HyperTerminal program to link to the switch.

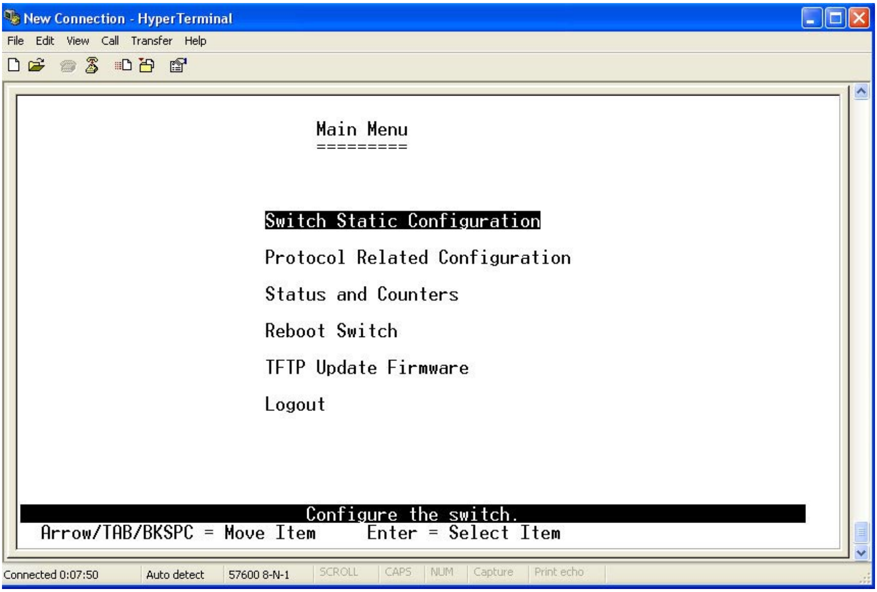

New Connection - HyperTerminal
File Edit View Call Transfer Help

```
User Interface
NP-2624M Intelligent Switch
Ver.2.02.07


username:_
password:
```

Type the username and press enter and then type the password and press enter to login.
The default username is “**admin**”; the default password is “**admin** ”.

4.1 Main Menu

There are six items which can be selected:



```
                 Main Menu
                 =========


           Switch Static Configuration

           Protocol Related Configuration

           Status and Counters

           Reboot Switch

           TFTP Update Firmware

           Logout



                    Configure the switch.
  Arrow/TAB/BKSPC = Move Item     Enter = Select Item
```

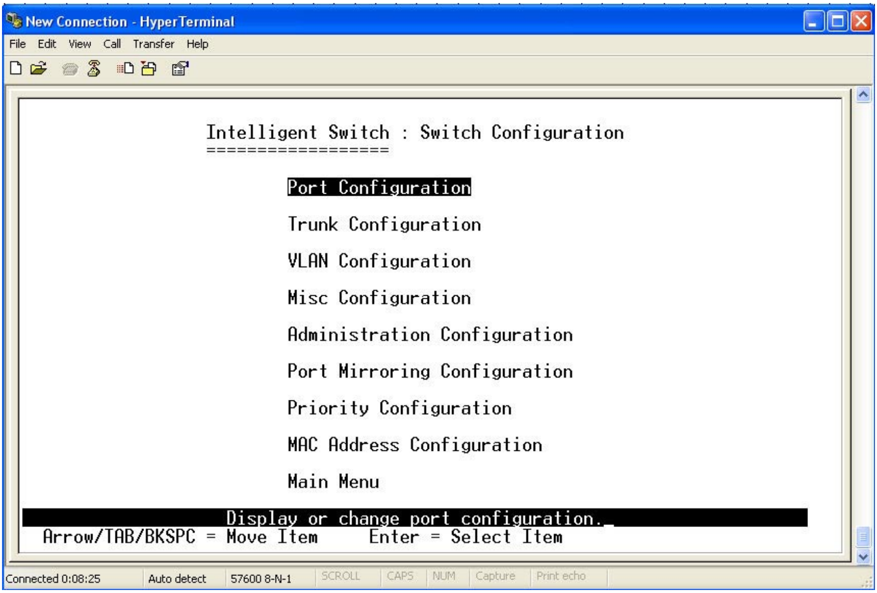
Switch Static Configuration:	Configure the switch.
Protocol Related Configuration:	Configure the protocol function.
Status and Counters:	Show the status of the switch.
Reboot Switch:	Restart the system or reset switch to default configuration.
TFTP Update Firmware:	Use TFTP to download a firmware image.
Logout:	Exit the menu line program.

Control Keys

The following control keys are provided for this mode operation:

Tab:	Move the cursor to next item.
Backspace:	Move the cursor to previous item.
Enter:	Select item.
Space:	Toggle selected item to next configure.

4.2 Switch Static Configuration



```
                    Intelligent Switch : Switch Configuration
                    ==================

                            Port Configuration

                            Trunk Configuration

                            VLAN Configuration

                            Misc Configuration

                            Administration Configuration

                            Port Mirroring Configuration

                            Priority Configuration

                            MAC Address Configuration

                            Main Menu

                      Display or change port configuration._
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

Control Keys

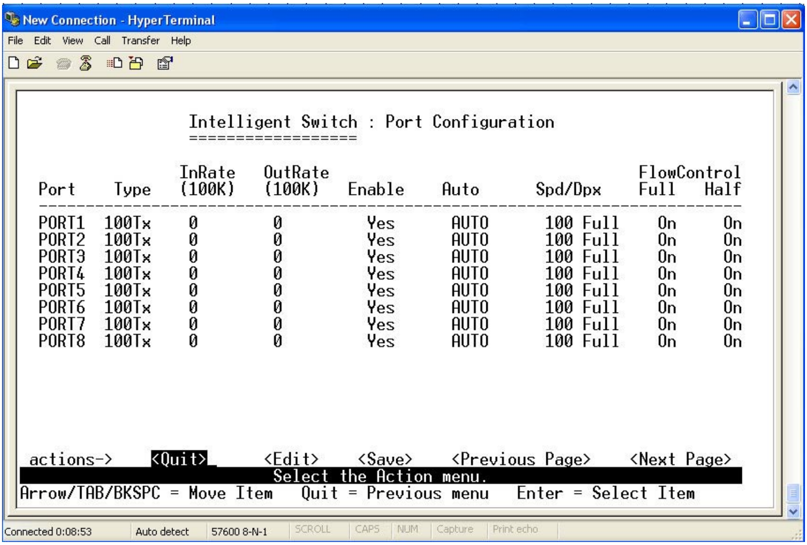
You can press the Tab or Backspace keys to choose an item, and press the Enter key to select an item.

Action Menu Line

<Quit>:	Exit the configuration page and return to the previous menu.
<Edit>:	Configure all items. When you have finished configuring the item, press Ctrl+A to return back to the action menu line.
<Save>:	Save all configured values.
<Previous Page>:	Return to previous page to configure.
<Next page>:	Go to the next page to configure it.

4.2.1. Port Configuration

This page allows you to change the status of every port.



```
                   Intelligent Switch : Port Configuration
                   ==================

                InRate   OutRate                                  FlowControl
Port    Type    (100K)   (100K)   Enable    Auto       Spd/Dpx    Full    Half
-------------------------------------------------------------------------------
PORT1  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT2  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT3  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT4  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT5  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT6  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT7  100Tx    0        0          Yes     AUTO       100 Full   On      On
PORT8  100Tx    0        0          Yes     AUTO       100 Full   On      On




actions->     <Quit>      <Edit>    <Save>    <Previous Page>    <Next Page>
                         Select the Action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

Press the Space key to change the configuration of each item.

InRate (100K/unit): User can set input rate control, which is 100K per unit. The valid range is 0~1000.

0: disable rate control.
1~1000: valid rate value.

OutRate (100K/unit): User can set output rate control, which is 100K per unit. The valid range is 0~1000.

0: disable rate control.
1~1000: valid rate value.

Enabled: User can disable or enable this port control.

"Yes" that mean the port is enabled.
"No" that mean the port is disabled.

Auto: User can set auto negotiation mode to "Auto", "Nway_Force", or "Force" per port.

Spd/Dpx: User can set "100Mbps" or "10Mbps" speed on port 1~port 24.

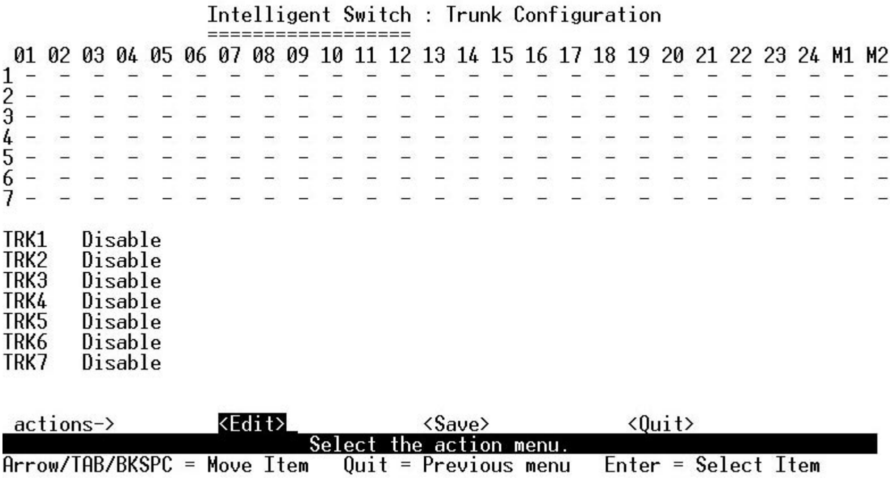
Set "1000Mbps", "100Mbps" or "10Mbps" speed on port25~port26 (dependant on optional Gigabit module card), and set "full-duplex" or "half-duplex" mode.

Flow Control: Full: User can enable or disable full flow control function (pause).
Half: User can enable or disable half flow control function (backpressure).

NOTE: Pressing "Save" will only save one page of configuration. If static trunk groups exist, they will be displayed (eg: TRK1, TRK2...) after port 26, and you can configure them as above.

4.2.2. Trunk Configuration

This page allows the user to create a maximum of seven trunk groups. Users can arbitrarily select up to four ports from port 1~port 26 to build a trunk group.



```
                    Intelligent Switch : Trunk Configuration
                    ==================
 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 M1 M2
1 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
2 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
3 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
4 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
5 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
6 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
7 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -

TRK1   Disable
TRK2   Disable
TRK3   Disable
TRK4   Disable
TRK5   Disable
TRK6   Disable
TRK7   Disable


 actions->          <Edit>             <Save>              <Quit>
                           Select  the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Select <Edit> on the actions menu
2. Press space key to configure the member port of trunk group. You also have to set "Static" or "LACP" for the corresponding trunk group of TRK1~TRK7 item.

   "Static" – the normal trunk.

   "LACP" – this trunk group has link aggregation control protocol.
3. Press Ctrl+A to go back action menu line
4. Select <Save> to save all configure value.
5. If the TRK1~TRK7 are "Disabled", the trunk group is deleted.
6. All ports in the same static trunk group will be treated as a single port. So when setting VLAN members and Port configuration they will be toggled on or off simultaneously.

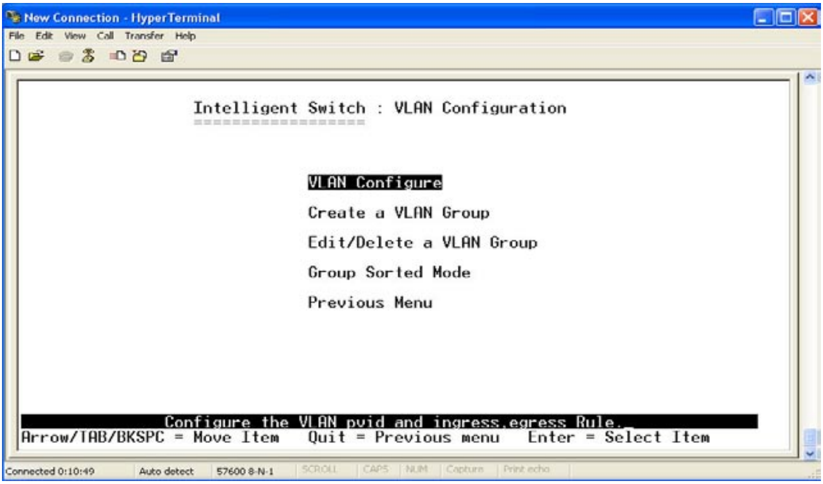
NOTE: If a VLAN group exists, all of the members of static trunk group must be in the same VLAN group.

4.2.3. VLAN Configuration

4.2.3.1. VLAN Configure

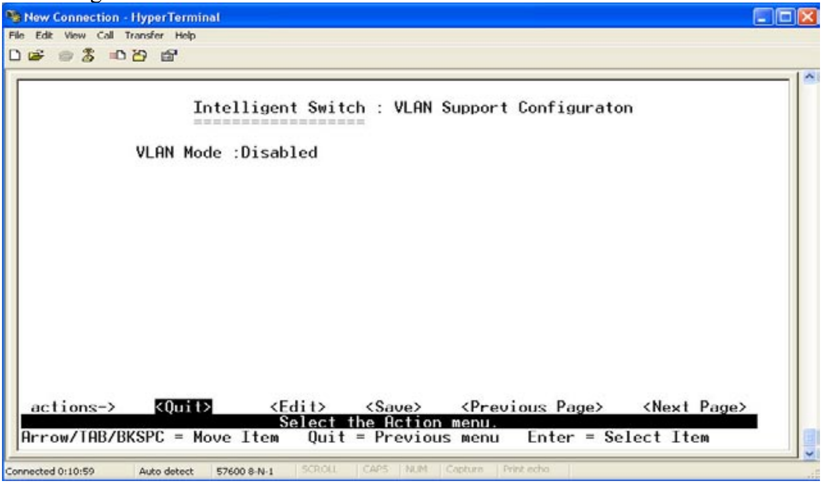
This page allows the user to set VLAN mode to port-based VLAN or 802.1Q VLAN or disable VLAN function.

NOTE: Changing the VLAN mode requires the switch to be restarted.

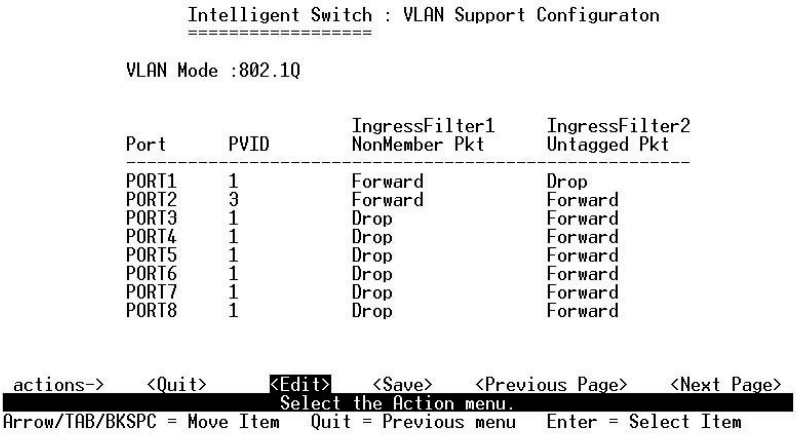

New Connection - HyperTerminal
File Edit View Call Transfer Help
Connected 0:10:49 Auto detect 57600 8-N-1 SCROLL CAPS NUM Capture Print echo

```
                    Intelligent Switch : VLAN Configuration
                    ==================

                                 VLAN Configure

                                 Create a VLAN Group

                                 Edit/Delete a VLAN Group

                                 Group Sorted Mode

                                 Previous Menu

                Configure the VLAN pvid and ingress,egress Rule.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

If the switch is set to 802.1Q VLAN, this page will allow the user to set PVID, ingress filtering 1 and ingress filtering 2.


New Connection - HyperTerminal
File Edit View Call Transfer Help
Connected 0:10:59 Auto detect 57600 8-N-1 SCROLL CAPS NUM Capture Print echo

```
                    Intelligent Switch : VLAN Support Configuraton
                    ==================

              VLAN Mode :Disabled

 actions->     <Quit>       <Edit>     <Save>    <Previous Page>    <Next Page>
                          Select the Action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```



```
              Intelligent Switch : VLAN Support Configuraton
              ==================

         VLAN Mode :802.1Q

                                   IngressFilter1    IngressFilter2
         Port      PVID            NonMember Pkt     Untagged Pkt
         ----------------------------------------------------------
         PORT1     1               Forward           Drop
         PORT2     3               Forward           Forward
         PORT3     1               Drop              Forward
         PORT4     1               Drop              Forward
         PORT5     1               Drop              Forward
         PORT6     1               Drop              Forward
         PORT7     1               Drop              Forward
         PORT8     1               Drop              Forward


 actions->    <Quit>      <Edit>     <Save>    <Previous Page>    <Next Page>
                            Select the Action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

1. **PVID (Port VID: 1~255):** Type the PVID.
2. **Ingress Filter 1 NonMember Pkt:**

   NonMember Pkt works the same as Ingress Filtering Rule 1 on the web interface.

   Forwarding only packets with VID matching this port's configured VID.

   Press Space key to choose "forward" or to "drop" the frame not matching this port's configured VID.
3. **Ingress Filter 2 UnTagged Pkt:**

   UnTagged Pkt works the same as Ingress Filtering Rule 2 on the web interface.

   Drop untagged frame.

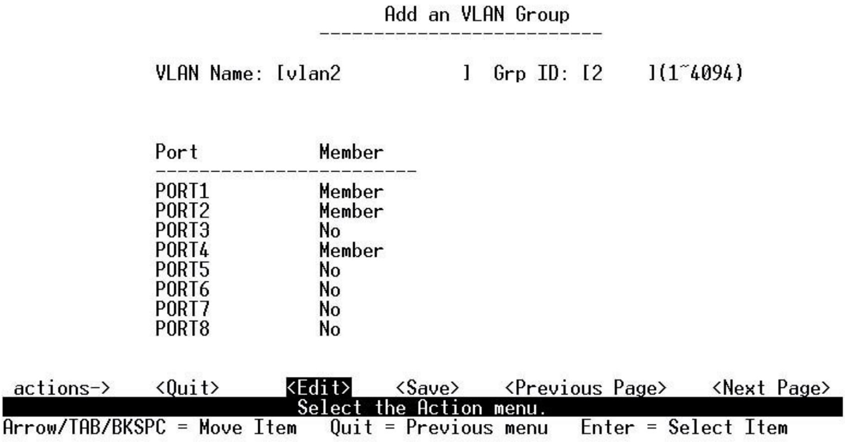
   Press Space key to choose "drop" or "forward" the untagged frame.

4.2.3.2. Create a VLAN Group

Create Port-Based VLAN

Create a port-based VLAN and add member/nonmember ports to it.

1. Select <Edit>.



```
                    Add  an  VLAN  Group
               --------------------------

      VLAN Name: [vlan2          ]  Grp ID: [2    ](1~4094)


      Port             Member
      ------------------------
      PORT1            Member
      PORT2            Member
      PORT3            No
      PORT4            Member
      PORT5            No
      PORT6            No
      PORT7            No
      PORT8            No

 actions->     <Quit>       <Edit>     <Save>     <Previous Page>     <Next Page>
                           Select  the  Action  menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

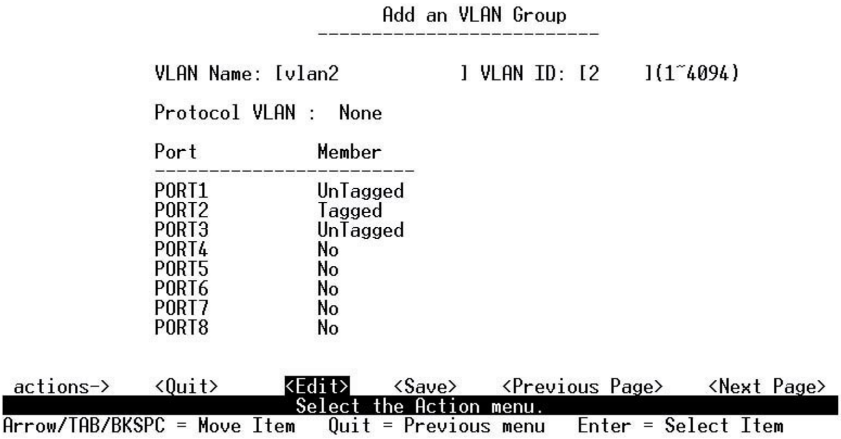
2. VLAN Name: Type a name for the new VLAN.
3. Grp ID: Type the VLAN group ID. The group ID range is 1~4094.
4. Member: Press <Space> key to choose VLAN member. There are two types to select:
   a. Member: the port is member port.
   b. No: the port is NOT member port.
5. Press Ctrl+A go back action menu line.
6. Select <Save> to save all configure value.

NOTE: If trunk groups exist, they will be displayed (eg: TRK1, TRK2...) after port26, and you can configure if necessary.

Create 802.1Q VLAN

Create an 802.1Q VLAN and add tagged /untagged member ports to it.

1. Select <Edit>.



```
                    Add an VLAN Group
                 --------------------------

        VLAN Name: [vlan2          ] VLAN ID: [2    ](1~4094)

        Protocol VLAN :  None

        Port           Member
        ------------------------
        PORT1          UnTagged
        PORT2          Tagged
        PORT3          UnTagged
        PORT4          No
        PORT5          No
        PORT6          No
        PORT7          No
        PORT8          No

 actions->    <Quit>      <Edit>    <Save>    <Previous Page>    <Next Page>
                         Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

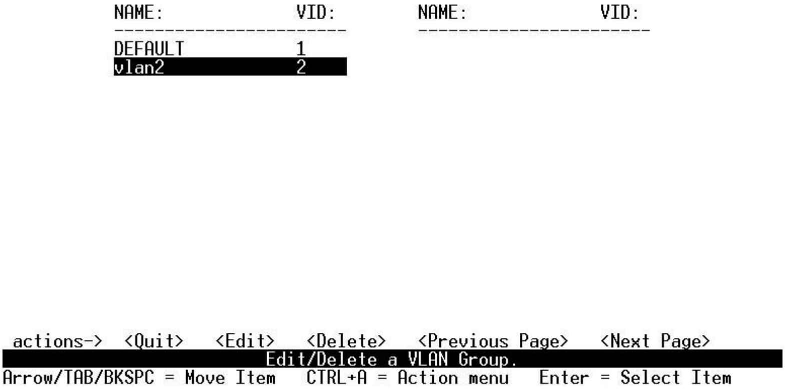
2. VLAN Name: Type a name for the new VLAN.
3. VLAN ID: Type a VID (between 1~4094). The default is 1. There are 256 VLAN groups available.
4. Protocol VLAN: Press the Space key to choose the protocol type.
5. Member: Press the Space key to choose a VLAN member. There are three types to select:
   a. UnTagged: This is the member port of the VLAN group and outgoing frames are NO VLAN-Tagged frames.
   b. Tagged: This is the member port of the VLAN group and outgoing frames are VLAN-Tagged frames.
   c. NO: The port is NOT member of the VLAN group.
6. Press Ctrl+A to go back to the action menu line.
7. Select <Save> to save all configured values.

NOTE: If the trunk groups exist, they will be displayed (ex: TRK1, TRK2...) after port 26, and you can configure them if necessary.

4.2.3.3. Edit / Delete a VLAN Group

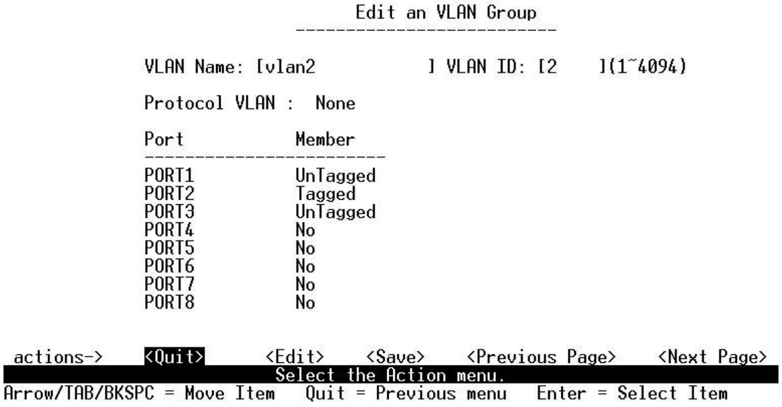
In this page, users can edit or delete a VLAN group.

1. Press <Edit> or <Delete> item.



```
NAME:                VID:        NAME:                VID:
-----------------------        -----------------------
DEFAULT              1
vlan2                2



actions->  <Quit>   <Edit>   <Delete>   <Previous Page>   <Next Page>
                        Edit/Delete a VLAN Group.
Arrow/TAB/BKSPC = Move Item   CTRL+A = Action menu   Enter = Select Item
```

2. Choose the VLAN group that you want to edit or delete and then press enter.
3. Users can modify the protocol VLAN item and the member ports are tagged or untagged and remove some member ports from this VLAN group.



```
                   Edit an VLAN Group
              --------------------------

    VLAN Name: [vlan2           ] VLAN ID: [2    ](1~4094)

    Protocol VLAN :  None

    Port            Member
    ------------------------
    PORT1           UnTagged
    PORT2           Tagged
    PORT3           UnTagged
    PORT4           No
    PORT5           No
    PORT6           No
    PORT7           No
    PORT8           No

actions->    <Quit>     <Edit>    <Save>    <Previous Page>    <Next Page>
                          Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

4. After editing the VLAN, press the <Save> key to save all configuration values.

NOTE:

1. Pressing "Enter" once will complete the deletion when in delete mode.

2. The VLAN Name and VLAN ID cannot be modified.

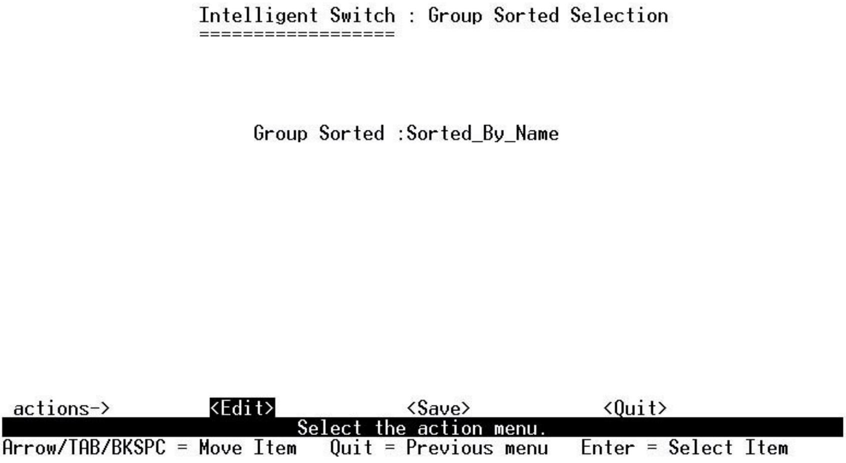
3. The default VLAN cannot be deleted.

4.2.3.4. Groups Sorted Mode

In this page, users can select VLAN groups sorted mode:

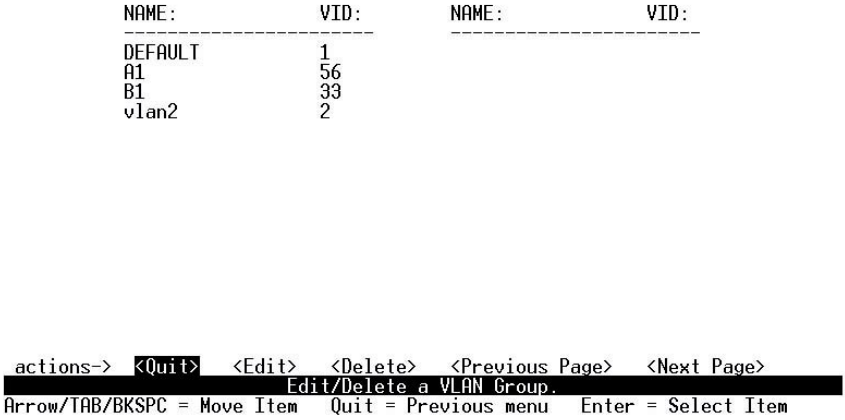
(1) Sorted by Name

(2) Sorted by VID.



```
                         Intelligent Switch : Group Sorted Selection
                         ==================



                              Group Sorted :Sorted_By_Name










 actions->          <Edit>             <Save>             <Quit>
                             Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

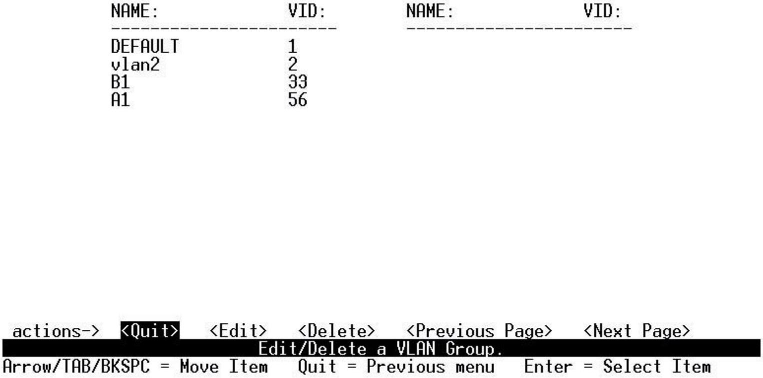
The Edit/Delete a VLAN group page will display the result.



```
            NAME:                VID:         NAME:                VID:
            ------------------------         ------------------------
            DEFAULT              1
            A1                   56
            B1                   33
            vlan2                2









 actions->  <Quit>   <Edit>   <Delete>   <Previous Page>   <Next Page>
                          Edit/Delete a VLAN Group.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

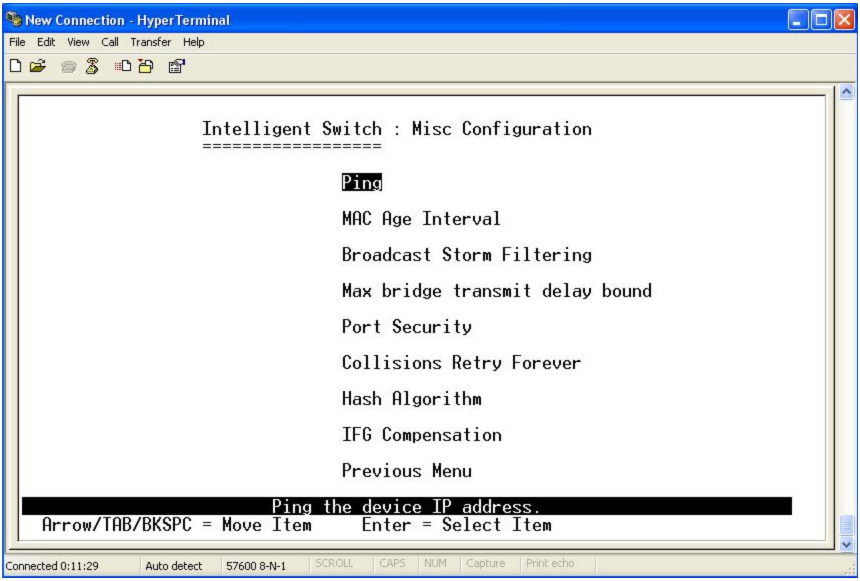
In the Edit/Delete a VLAN Group page, the result of sorted by name.

In the Edit/Delete a VLAN Group page, the result of sorted by VID.



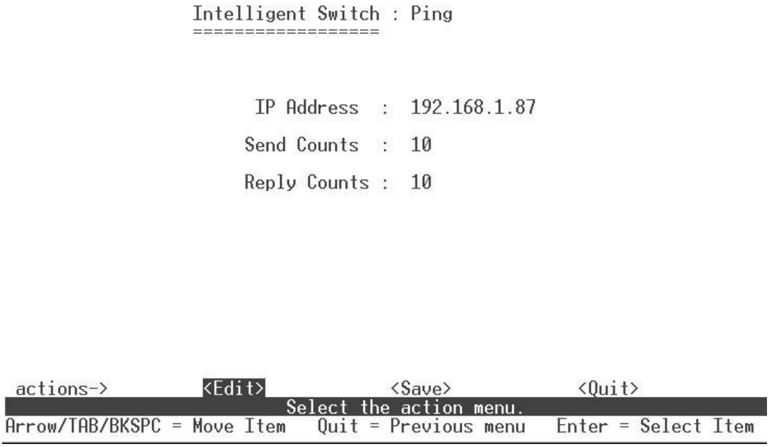
```
NAME:                VID:          NAME:                VID:
-----------------------            -----------------------
DEFAULT              1
vlan2                2
B1                   33
A1                   56





 actions-> <Quit>   <Edit>   <Delete>   <Previous Page>   <Next Page>
                           Edit/Delete a VLAN Group.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

4.2.4. Miscellaneous Configuration



```
                  Intelligent Switch : Misc Configuration
                  ==================

                             Ping

                             MAC Age Interval

                             Broadcast Storm Filtering

                             Max bridge transmit delay bound

                             Port Security

                             Collisions Retry Forever

                             Hash Algorithm

                             IFG Compensation

                             Previous Menu

                         Ping the device IP address.
  Arrow/TAB/BKSPC = Move Item     Enter = Select Item
```

4.2.4.1. Ping

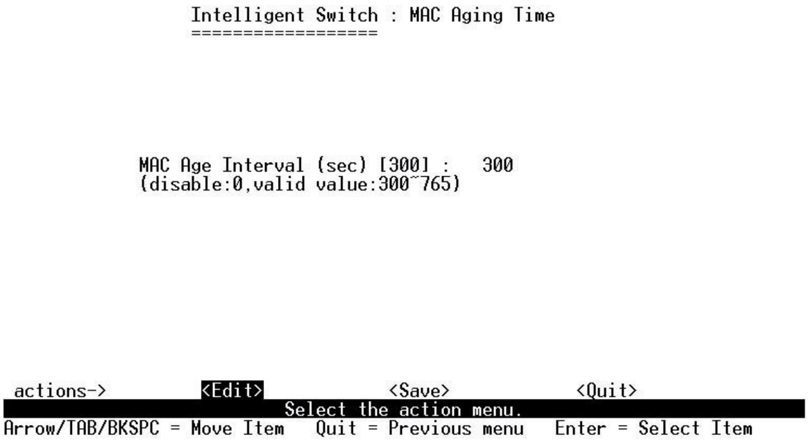


```
                Intelligent Switch : Ping
                ==================


                      IP Address   :  192.168.1.87

                     Send Counts   :  10

                     Reply Counts  :  10




 actions->          <Edit>            <Save>            <Quit>
                         Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

Type the Host IP and the counts for pinging, then go back to action menu and press “Save”. “Reply Counts” will display the result of pinging.

4.2.4.2. MAC Age Interval

Type the number of seconds that an inactive MAC address remains in the switch's address table.

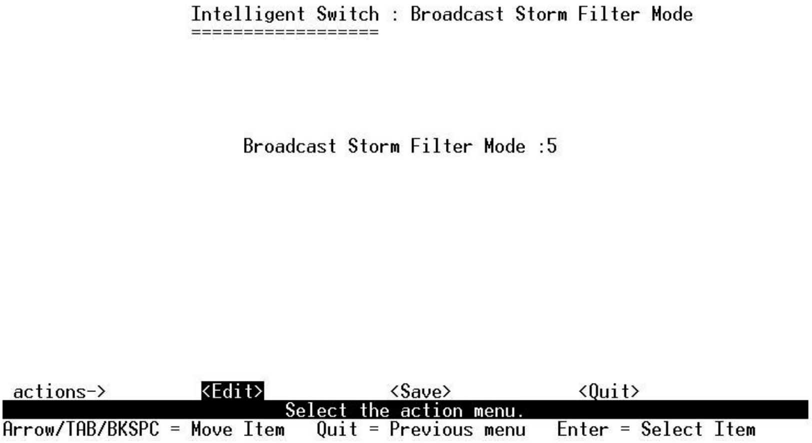


```
                    Intelligent Switch : MAC Aging Time
                    ==================




               MAC Age Interval (sec) [300] :   300
               (disable:0,valid value:300~765)





 actions->            <Edit>             <Save>             <Quit>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

The valid range is 300~765 seconds. Default is 300 seconds.

4.2.4.3. Broadcast Storm Filtering

This page configures the broadcast storm control.

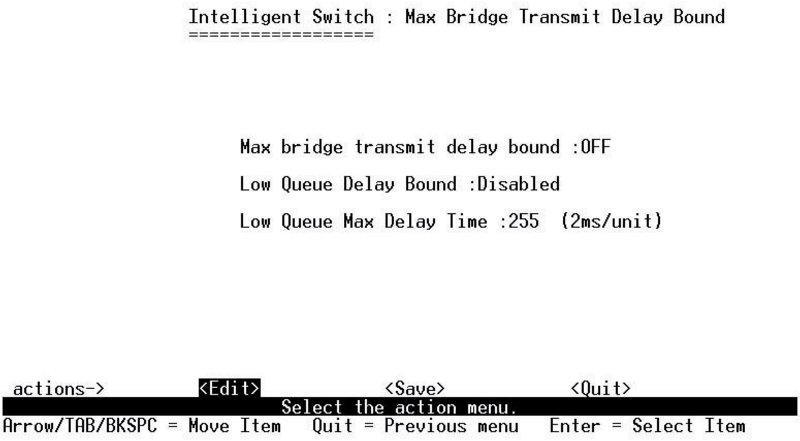


```
                    Intelligent Switch : Broadcast Storm Filter Mode
                    ==================



                         Broadcast Storm Filter Mode :5






 actions->            <Edit>             <Save>             <Quit>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

1. Press <Edit> to configure the broadcast storm filter mode.
2. Press Space key to choose the threshold value.

The valid threshold value is 5%, 10%, 15%, 20%, 25% and NO. Default is 5%.

4.2.4.4. Maximum bridge transmit delay bound



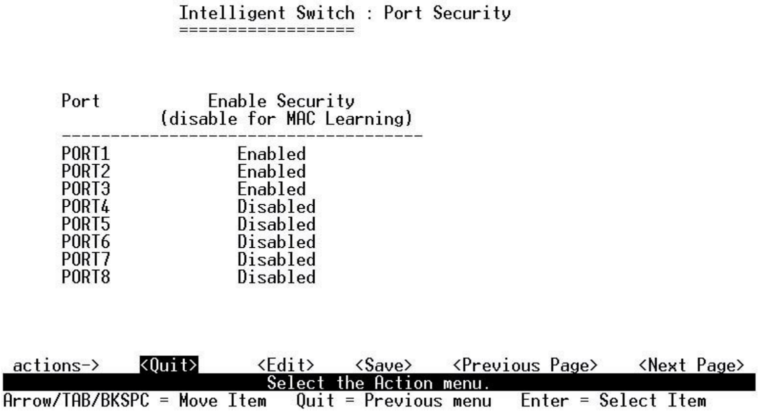
```
                     Intelligent Switch : Max Bridge Transmit Delay Bound
                     ==================



                          Max bridge transmit delay bound :OFF

                          Low Queue Delay Bound :Disabled

                          Low Queue Max Delay Time :255  (2ms/unit)





 actions->          <Edit>           <Save>           <Quit>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. **Max bridge transmit delay bound:** Limits the packets queuing time in switch. If enabled, when the amount of time the packets queued exceeding the maximum they will be dropped. Press the Space key to set the time. Those valid values are 1sec, 2sec, and 4sec and off. Default is off.
2. **Low Queue Delay Bound:** Limits the low priority packets queuing time in switch. If enabled, when the amount of time the low priority packet stays in the switch exceeds Low Queue Max Delay Time, it will be sent. Press the Space key to enable or disable this function. Default is disable.
3. **Low Queue Max Delay Time:** To set the amount of time that low priority packets queuing in switch will be delayed. The valid range is 1~255ms. Default Max Delay Time is 255ms.

NOTE: Make sure “Max bridge transmit delay bound control” is enabled before enabling Low Queue Delay Bound, because Low Queue Delay Bound must be work under “Max bridge transmit delay bound control” is enabled situation.

4.2.4.5. Port Security

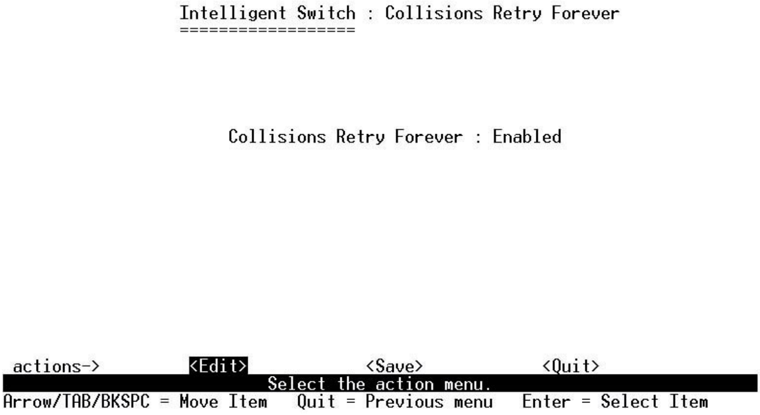
A port in security mode will be "locked" without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. The user can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port.



```
                    Intelligent Switch : Port Security
                    ==================


        Port            Enable Security
                   (disable for MAC Learning)
        ----------------------------------------
        PORT1               Enabled
        PORT2               Enabled
        PORT3               Enabled
        PORT4               Disabled
        PORT5               Disabled
        PORT6               Disabled
        PORT7               Disabled
        PORT8               Disabled



 actions->     <Quit>       <Edit>    <Save>    <Previous Page>    <Next Page>
                           Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Select <Edit>.
2. Press Space key to choose enable / disable item.
3. Press Ctrl+A to go back action menu line.
4. Select <Save> to save all configure value.
5. You can press <Next Page> to configure port9 ~ port26, press <Previous Page> return to last page.

4.2.4.5. Collisions Retry Forever

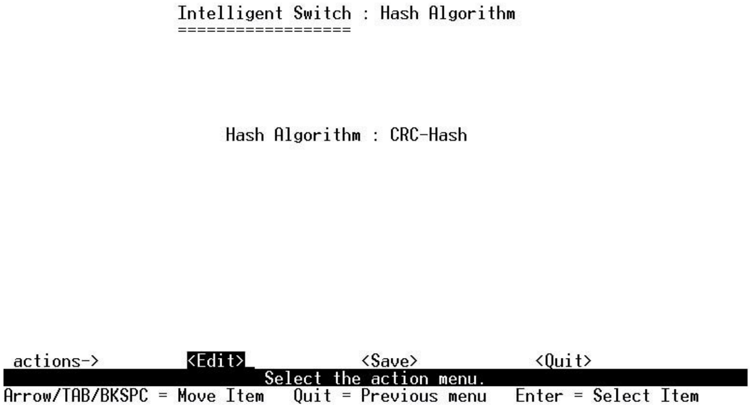


```
                    Intelligent Switch : Collisions Retry Forever
                    ==================



                         Collisions Retry Forever : Enabled







 actions->           <Edit>           <Save>           <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

Collisions Retry Forever:	Disable – In half duplex, in the event of a collision it will retry up to 48 times before dropping the frame. Enable – In half duplex, in the event of a collision it will continue retrying forever (Default).

4.2.4.6. Hash Algorithm

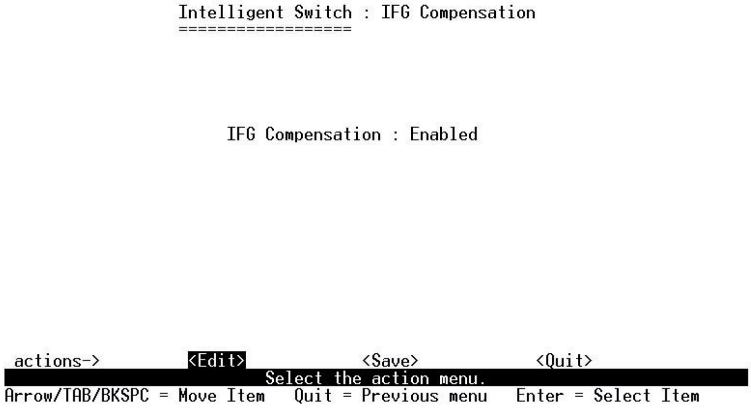
Select CRC-Hash(default) or DirectMap for Hash algorithm.



```
                 Intelligent Switch : Hash Algorithm
                 ==================

                      Hash Algorithm : CRC-Hash

 actions->         <Edit>            <Save>            <Quit>
                          Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

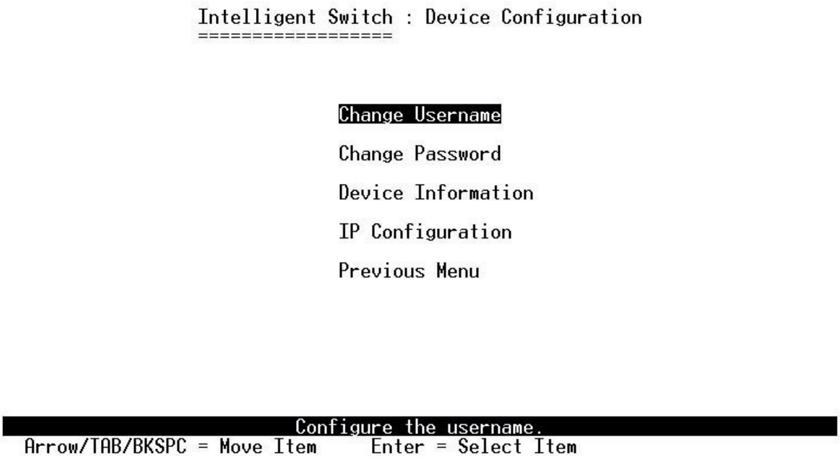
4.2.4.7. IFG Compensation

Enable or disable the inter-frame gap (IFG) compensation function.



```
                 Intelligent Switch : IFG Compensation
                 ==================

                      IFG Compensation : Enabled

 actions->         <Edit>            <Save>            <Quit>
                          Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

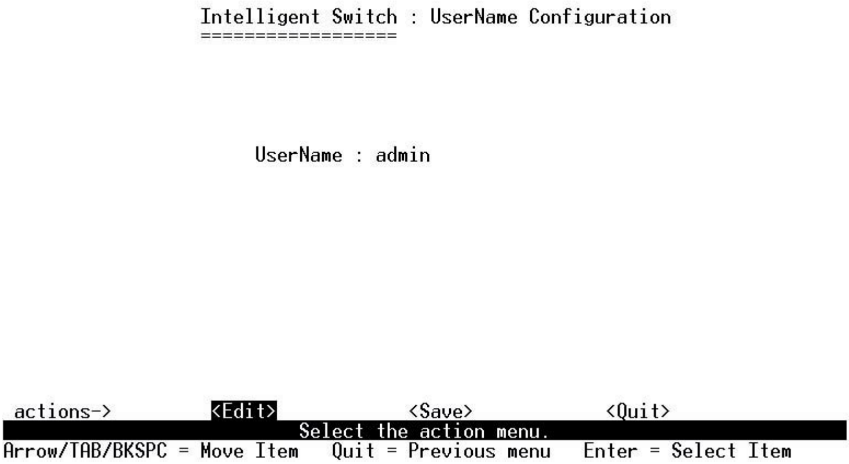
4.2.5. Administration Configuration



```
                    Intelligent Switch : Device Configuration
                    ==================


                                 Change Username

                                 Change Password

                                 Device Information

                                 IP Configuration

                                 Previous Menu




                           Configure the username.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

4.2.5.1. Change Username

This page allows the user to change the web management username.

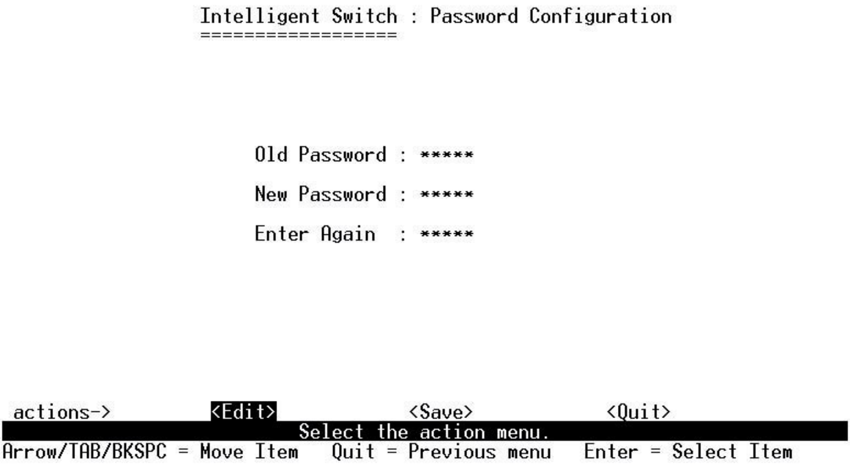


```
                    Intelligent Switch : UserName Configuration
                    ==================



                         UserName : admin








 actions->            <Edit>             <Save>             <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

Type the new username, and then press <Save> item.

4.2.5.2. Change Password

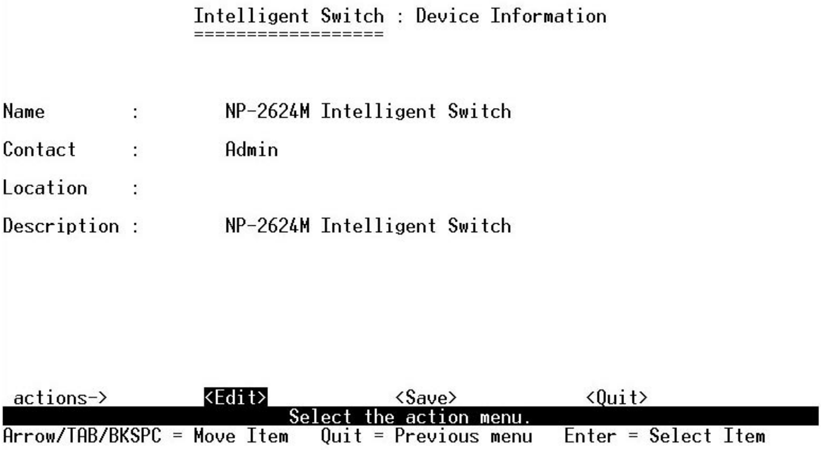
This page allows the user to change the web management login password.



```
                    Intelligent Switch : Password Configuration
                    ==================



                         Old Password : *****

                         New Password : *****

                         Enter Again  : *****




 actions->           <Edit>           <Save>           <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

4.2.5.3. Device Information

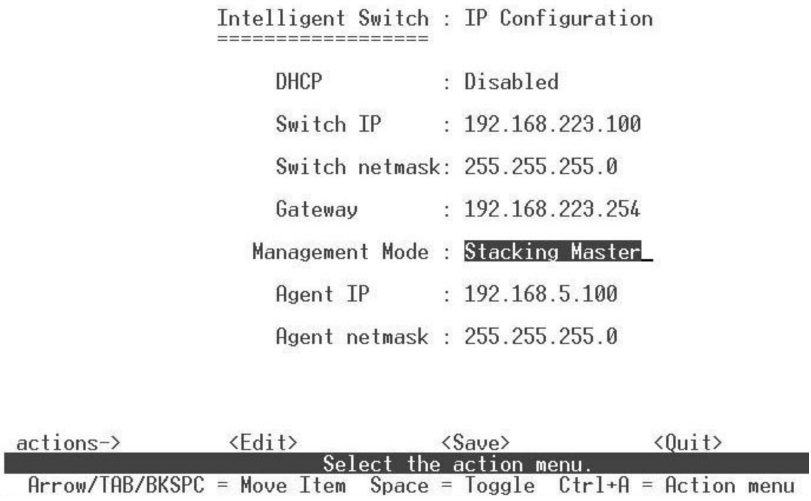
This page allows the user to configure the device information.



```
                    Intelligent Switch : Device Information
                    ==================


Name          :          NP-2624M Intelligent Switch

Contact       :          Admin

Location      :

Description   :          NP-2624M Intelligent Switch




 actions->           <Edit>           <Save>           <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

4.2.5.4. IP Configuration

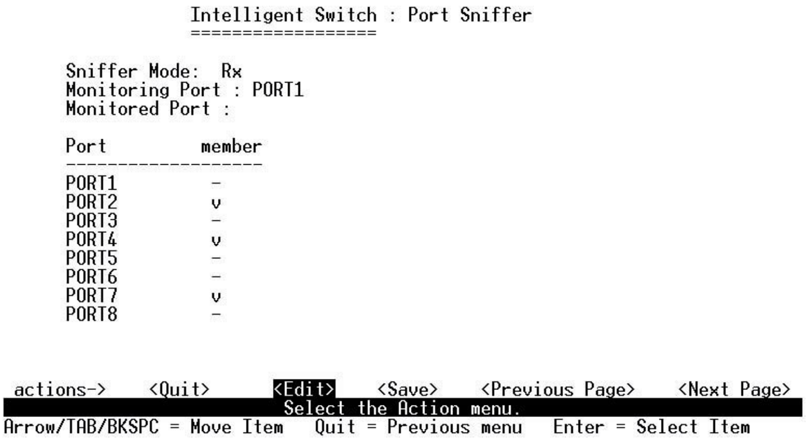
This page allows the user to configure the IP settings and fill in the new values.



```
         Intelligent Switch : IP Configuration
         ==================

              DHCP           : Disabled

              Switch IP      : 192.168.223.100

              Switch netmask: 255.255.255.0

              Gateway        : 192.168.223.254

            Management Mode  : Stacking Master_

              Agent IP       : 192.168.5.100

              Agent netmask  : 255.255.255.0


 actions->          <Edit>            <Save>            <Quit>
                           Select the action menu.
  Arrow/TAB/BKSPC = Move Item   Space = Toggle   Ctrl+A = Action menu
```

4.2.6. Port Mirror Configuration

Port mirroring is a method for monitoring traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic going in or out of monitored ports will be duplicated into the monitoring port.



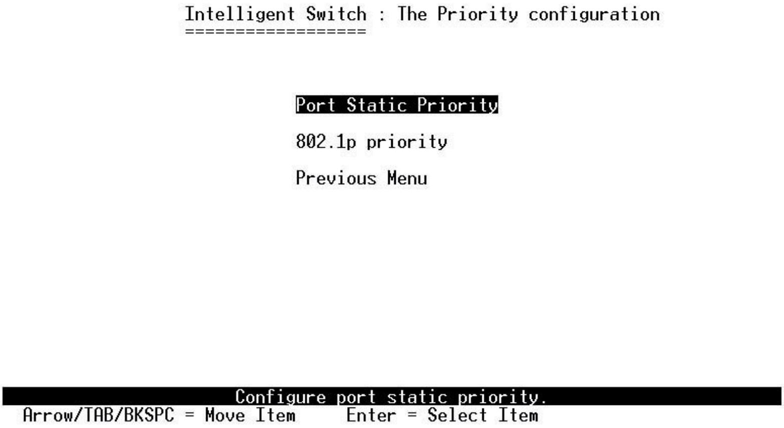
```
                    Intelligent Switch : Port Sniffer
                    ==================

            Sniffer Mode:  Rx
            Monitoring Port : PORT1
            Monitored Port :

            Port          member
            -------------------
            PORT1           -
            PORT2           v
            PORT3           -
            PORT4           v
            PORT5           -
            PORT6           -
            PORT7           v
            PORT8           -


 actions->    <Quit>      <Edit>     <Save>     <Previous Page>     <Next Page>
                           Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

Press the Space key to change configure of per item.

1. Select <Edit>.
2. Sniffer Mode: Press the Space key to set the sniffer mode to Disable,Rx,Tx or Both.
3. Monitoring Port: The sniffer port can be used to see all monitored ports traffic. Press the Space key to choose it.
4. Monitored Port: The ports you want to monitor. All monitored ports traffic will be copied to the sniffer port. You can select a maximum of 25 ports to monitor in the switch. Users can choose which port to monitor in the sniffer mode. Press Space key to choose member port, “V” – denotes a member, “—” – is not a member.
5. Press Ctrl+A to go back to the action menu line
6. Select <Save> to save all configured values.
7. On the action menu line you can press <Next Page> to configure port9 ~ port26, press <Previous Page> return to last page.

NOTE: Only one sniffer mode is active in the switch at a time.

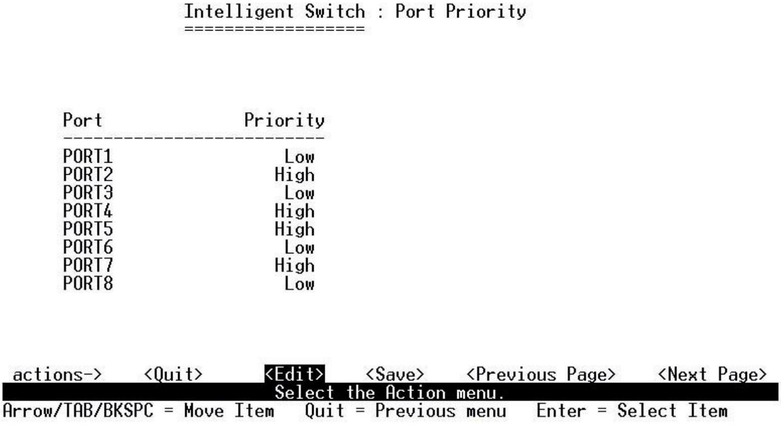
4.2.7. Priority Configuration



```
                        Intelligent Switch : The Priority configuration
                        ==================


                                   Port Static Priority

                                   802.1p priority

                                   Previous Menu








                              Configure port static priority.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

4.2.7.1. Port Static Priority

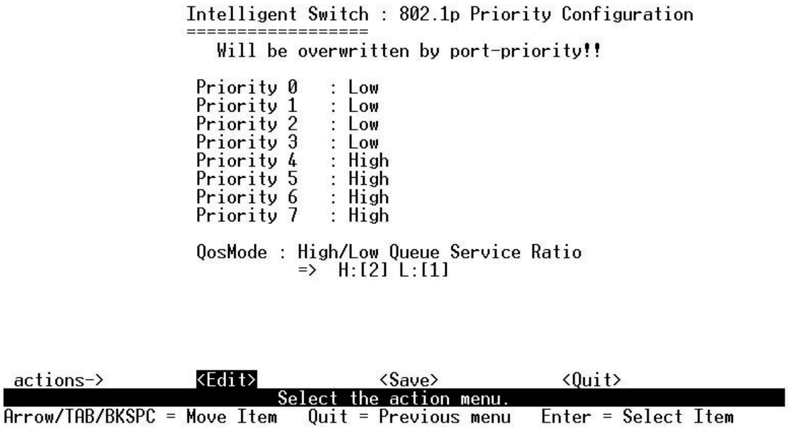
This static priority based on the port, if you set the port to high priority, incoming frames from this port will always be considered to be high priority frames.



```
                        Intelligent Switch : Port Priority
                        ==================



      Port                Priority
      --------------------------
      PORT1                    Low
      PORT2                   High
      PORT3                    Low
      PORT4                   High
      PORT5                   High
      PORT6                    Low
      PORT7                   High
      PORT8                    Low



 actions->    <Quit>      <Edit>    <Save>    <Previous Page>    <Next Page>
                               Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

4.2.7.2. 802.1P Priority Configuration

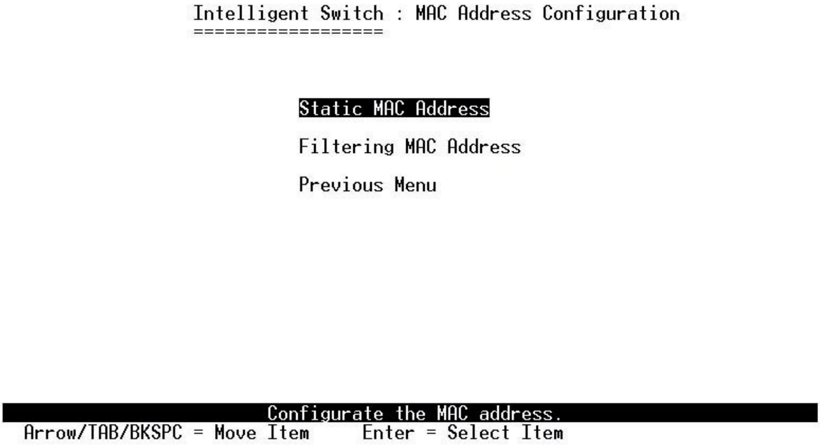
There are 0~7-priority levels that can be mapped to a high or low queue.



```
                      Intelligent Switch : 802.1p Priority Configuration
                      ==================
                         Will be overwritten by port-priority!!

                       Priority 0    : Low
                       Priority 1    : Low
                       Priority 2    : Low
                       Priority 3    : Low
                       Priority 4    : High
                       Priority 5    : High
                       Priority 6    : High
                       Priority 7    : High

                       QosMode : High/Low Queue Service Ratio
                                 =>  H:[2] L:[1]




 actions->           <Edit>             <Save>             <Quit>
                            Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

1. Select <Edit>.
2. Press Space key to select the priority level mapping to high or low queue.
3. High/Low Queue Service Ration H/L: User can select the ratio of high priority packets and low priority packets.
4. Press Ctrl+A to go back action menu line.
5. Select <Save> to save all configured values.

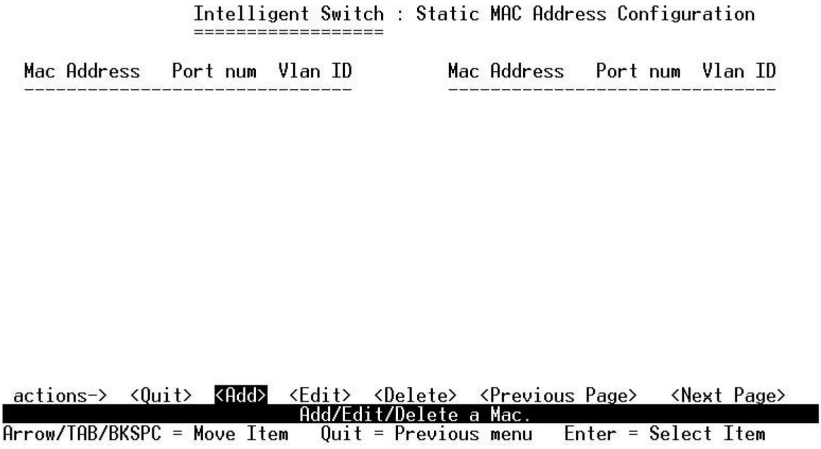
4.2.8. MAC Address Configuration



```
                 Intelligent Switch : MAC Address Configuration
                 ==================


                           Static MAC Address

                           Filtering MAC Address

                           Previous Menu









                    Configurate the MAC address.
   Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

4.2.8.1. Static MAC Address

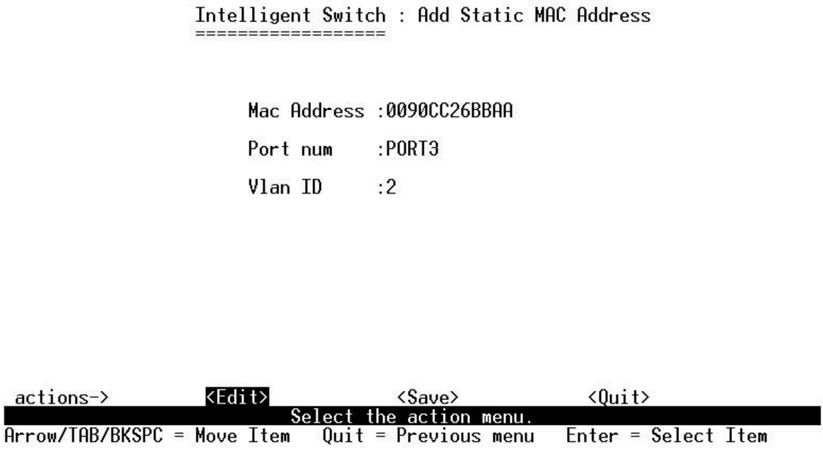
When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when disconnected or powered-off.



```
                 Intelligent Switch : Static MAC Address Configuration
                 ==================

   Mac Address   Port num  Vlan ID        Mac Address   Port num  Vlan ID
   -------------------------------        -------------------------------











  actions-> <Quit> <Add> <Edit> <Delete> <Previous Page>  <Next Page>
                        Add/Edit/Delete a Mac.
 Arrow/TAB/BKSPC = Move Item  Quit = Previous menu  Enter = Select Item
```

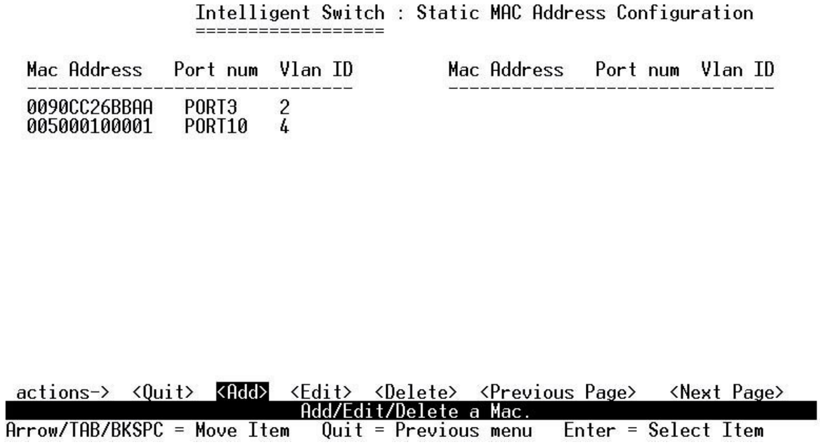
In this page users can add / modify / delete a static MAC address.

Add static MAC address



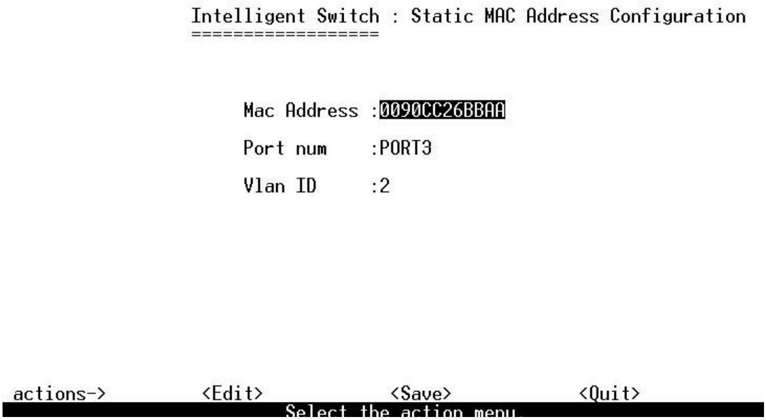
```
                    Intelligent Switch : Add Static MAC Address
                    ===================


                         Mac Address  :0090CC26BBAA

                         Port num     :PORT3

                         Vlan ID      :2



 actions->          <Edit>          <Save>          <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Press <Add> > <Edit> key to add static MAC address.



```
                    Intelligent Switch : Static MAC Address Configuration
                    ===================

  Mac Address   Port num  Vlan ID          Mac Address   Port num  Vlan ID
  -------------------------------          -------------------------------
  0090CC26BBAA   PORT3     2
  005000100001   PORT10    4



 actions->  <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>  <Next Page>
                           Add/Edit/Delete a Mac.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

2. MAC Address: Enter the MAC address which the port should permanently forward traffic, regardless of the device's network activity.



```
Intelligent Switch : Static MAC Address Configuration
==================

Mac Address :0090CC26BBAA
Port num    :PORT3
Vlan ID     :2

actions->          <Edit>          <Save>          <Quit>
                    Select the action menu.
```

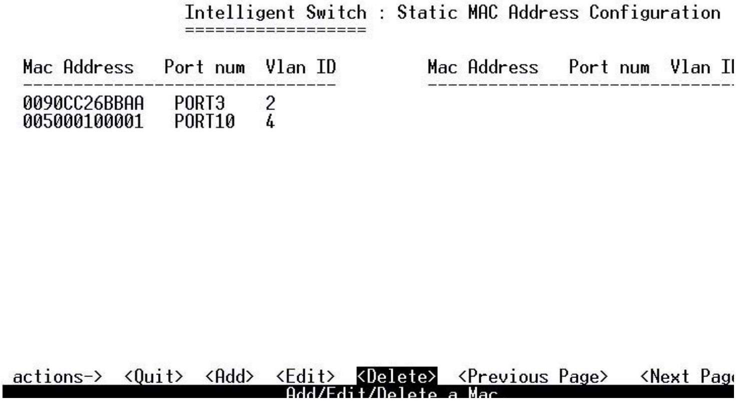
3. Port num: Press the <Space> key to select the port number.
4. Vlan ID: If tag-based (802.1Q) VLAN are set up on the switch, static addresses are associated with individual VLANs. Type the VID to associate with the MAC address.
5. Press Ctrl+A to go back action menu line.
6. Then select <Save> to save all configure value.

Edit static MAC address

1. Press <Edit> key.
2. Choose the MAC address that you want to modify and then press enter.
3. Press <Edit> key to modify all the items.
4. Press Ctrl +A to go back to the action menu line, and then select <Save> to save all configured values.

Delete static MAC address

1. Press <Delete> key.

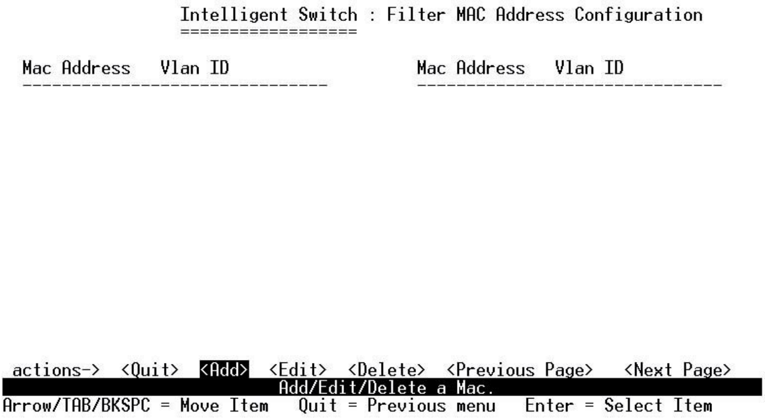


```
Intelligent Switch : Static MAC Address Configuration
==================

Mac Address    Port num   Vlan ID        Mac Address    Port num   Vlan II
------------------------------           ------------------------------
0090CC26BBAA    PORT3     2
005000100001    PORT10    4

actions->  <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>   <Next Pag
                    Add/Edit/Delete a Mac
```

2. Choose the MAC address that you want to delete and then press enter.
3. Pressing <Enter> once will complete deletion in delete mode.

4.2.8.2. Filtering MAC Address

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

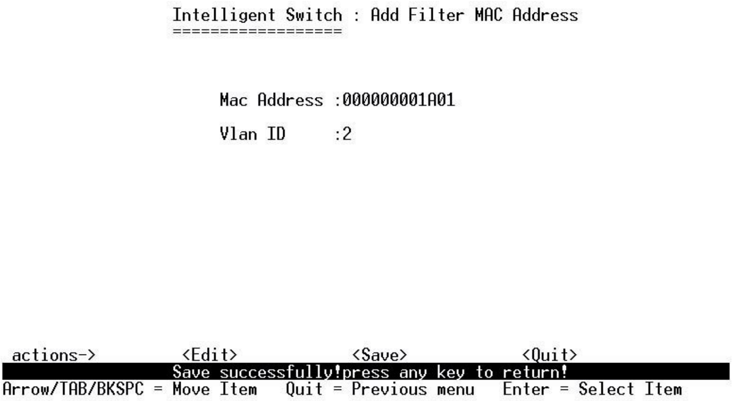


```
                    Intelligent Switch : Filter MAC Address Configuration
                    ==================

      Mac Address   Vlan ID                         Mac Address   Vlan ID
      --------------------------------              --------------------------------









 actions->  <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>   <Next Page>
                                  Add/Edit/Delete a Mac.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

In this page users can add /modify /delete a MAC address filter.

Add filter MAC address

1. Press <Add> > <Edit> key to add a MAC address filter.

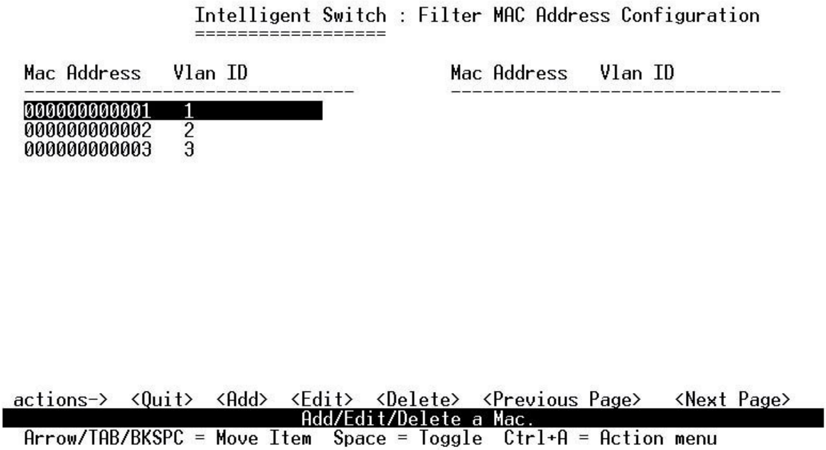


```
                  Intelligent Switch : Add Filter MAC Address
                  ==================


                       Mac Address :000000001A01

                       Vlan ID     :2








 actions->          <Edit>            <Save>            <Quit>
                  Save successfully!press any key to return!
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

2. MAC Address: Type the MAC address to filter.
3. Vlan ID: If tag-based (802.1Q) VLAN are set up on the switch, type the VID to associate with the MAC address.
4. Press Ctrl+A to go back to the action menu line, and then select <Save> to save all configured values.

Edit filter MAC address

1. Press <Edit> key.

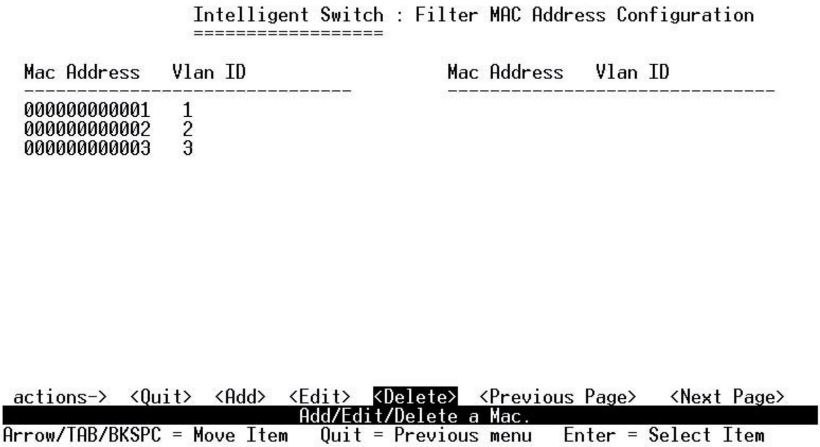


```
                 Intelligent Switch : Filter MAC Address Configuration
                 ==================

 Mac Address   Vlan ID                       Mac Address   Vlan ID
 -------------------------------             -------------------------------
 000000000001    1
 000000000002    2
 000000000003    3




actions-> <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>   <Next Page>
                            Add/Edit/Delete a Mac.
 Arrow/TAB/BKSPC = Move Item  Space = Toggle  Ctrl+A = Action menu
```

2. Choose the MAC address that you want to modify and then press enter.
3. Press <Edit> key to modify all the items.
4. Press Ctrl+A to go back to the action menu line, and then select <Save> to save all configured values.

Delete filter MAC address

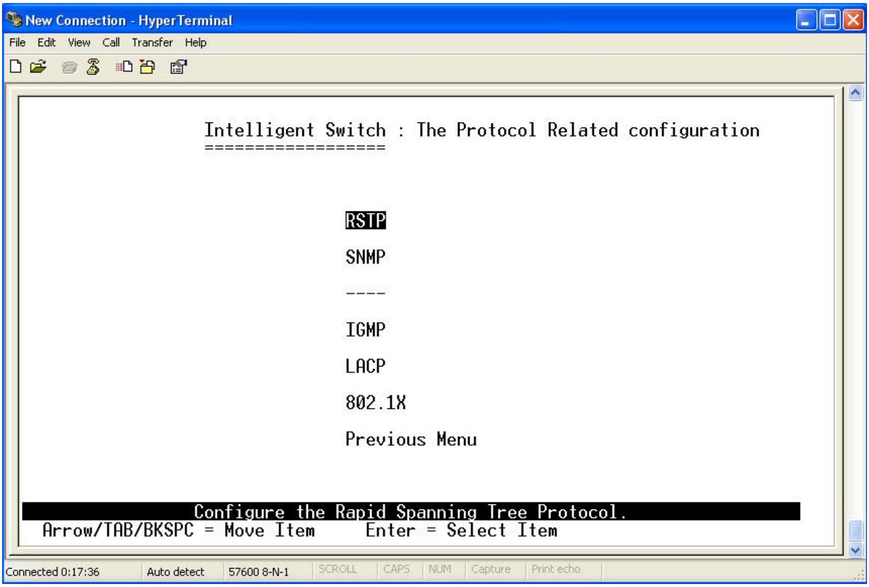
1. Press <Delete> key to delete a filter MAC address.



```
                 Intelligent Switch : Filter MAC Address Configuration
                 ==================

 Mac Address   Vlan ID                       Mac Address   Vlan ID
 -------------------------------             -------------------------------
 000000000001    1
 000000000002    2
 000000000003    3




actions-> <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>   <Next Page>
                            Add/Edit/Delete a Mac.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

2. Choose the MAC address that you want to delete and then press enter.
3. Pressing <Enter> once will complete the deletion when in delete mode.

4.3. Protocol Related Configuration

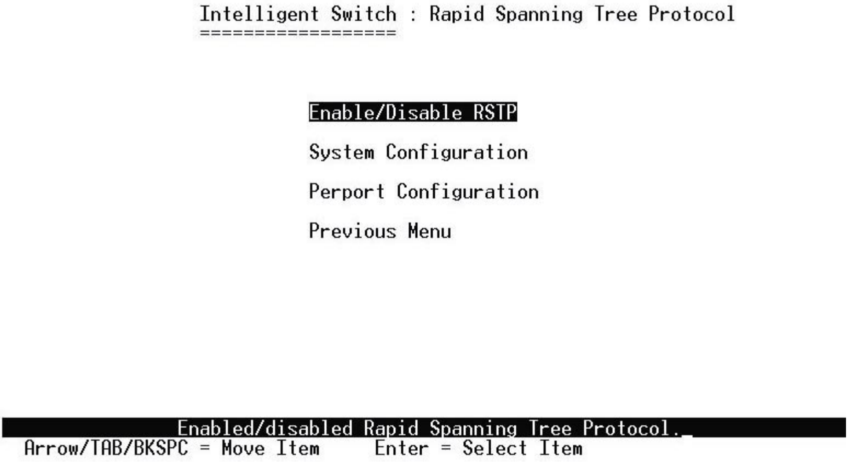

New Connection - HyperTerminal
File Edit View Call Transfer Help

```
                Intelligent Switch : The Protocol Related configuration
                ==================

                            RSTP

                            SNMP

                            ----

                            IGMP

                            LACP

                            802.1X

                            Previous Menu


                 Configure the Rapid Spanning Tree Protocol.
  Arrow/TAB/BKSPC = Move Item       Enter = Select Item
```

4.3.1. RSTP

The Rapid-Spanning-Tree Protocol (RSTP) is a standardized method (IEEE 802.1w) for avoiding loops in switched networks. RSTP is enabled, to ensure that only one path at a time is active between any two nodes on the network.

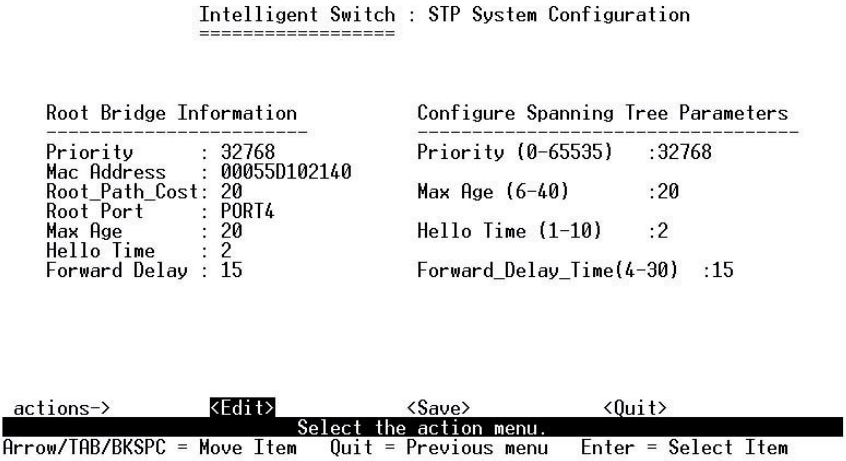
4.3.1.1. Enable/Disable RSTP



```
                    Intelligent Switch : Rapid Spanning Tree Protocol
                    ==================


                              Enable/Disable RSTP

                              System Configuration

                              Perport Configuration

                              Previous Menu




                    Enabled/disabled Rapid Spanning Tree Protocol._
  Arrow/TAB/BKSPC = Move Item     Enter = Select Item
```

This page allows the user to enable or disable the Spanning Tree function. Press the Space key to select enable or disable.

4.3.1.2. RSTP System Configuration

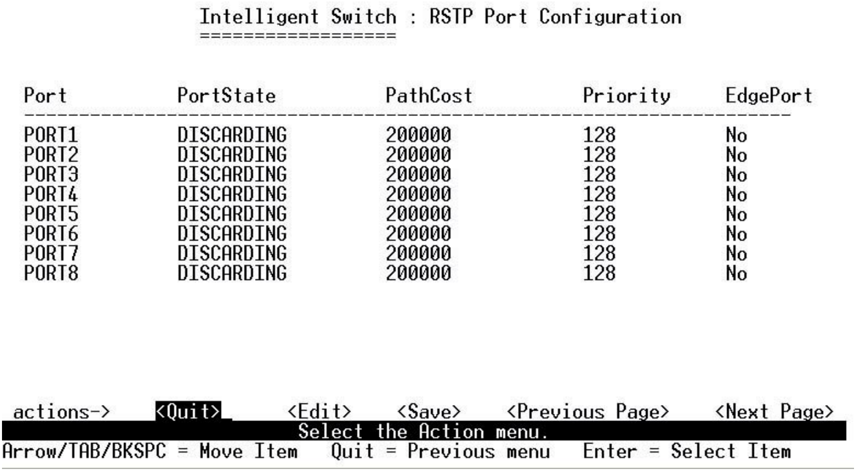


```
                    Intelligent Switch : STP System Configuration
                    ==================


     Root Bridge Information              Configure Spanning Tree Parameters
     ------------------------             -----------------------------------
     Priority       : 32768               Priority (0-65535)   :32768
     Mac Address    : 00055D102140
     Root_Path_Cost: 20                   Max Age (6-40)       :20
     Root Port      : PORT4
     Max Age        : 20                  Hello Time (1-10)    :2
     Hello Time     : 2
     Forward Delay  : 15                  Forward_Delay_Time(4-30)  :15



 actions->           <Edit>            <Save>            <Quit>
                        Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. You can view spanning tree information about the Root Bridge on the left.
2. On the right, users can set new values for the RSTP parameter.

NOTE: For more information on parameter descriptions please see section 2-4-8.

4.3.1.3. Per port Configuration



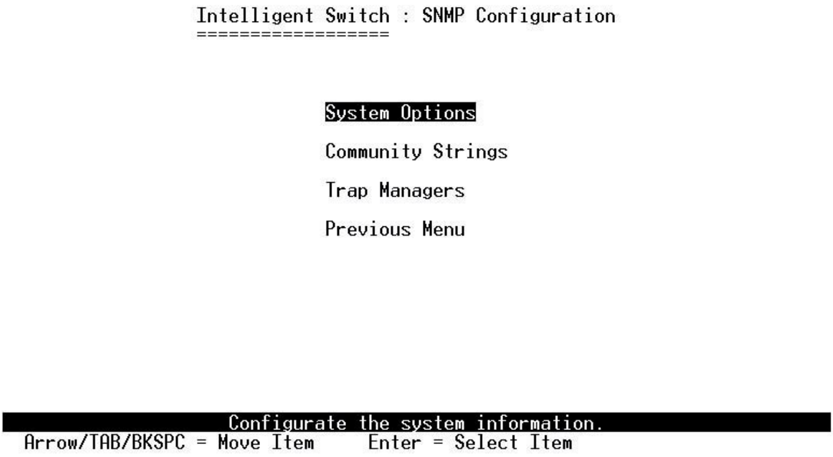
```
                 Intelligent Switch : RSTP Port Configuration
                 ===================

  Port          PortState          PathCost          Priority      EdgePort
  ----------------------------------------------------------------------
  PORT1         DISCARDING         200000            128           No
  PORT2         DISCARDING         200000            128           No
  PORT3         DISCARDING         200000            128           No
  PORT4         DISCARDING         200000            128           No
  PORT5         DISCARDING         200000            128           No
  PORT6         DISCARDING         200000            128           No
  PORT7         DISCARDING         200000            128           No
  PORT8         DISCARDING         200000            128           No




 actions->     <Quit>_      <Edit>    <Save>    <Previous Page>    <Next Page>
                            Select the Action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. PortState: Displays spanning tree status about the switch which per port is forwarding or blocking.
2. Select <Edit>.
3. PathCost: Specifies the path cost of the port that the switch uses to determine which ports are the forwarding ports.
4. Priority: The Priority Port allows you to make it more or less likely to become the root port.
5. EdgePort: If the port connected to a device does not understand STP or RSTP, you can set as “No”. This means the switch will stay in the forwarding state.
6. Press Ctrl +A to go back to the action menu line.
7. Select <Save> to save all configured values.
8. On the action menu line you can press <Next Page> to configure port9 ~ port26, press <Previous Page> return to last page.

NOTE: For more information on parameter descriptions please see section 2-4-8.

4.3.2. SNMP

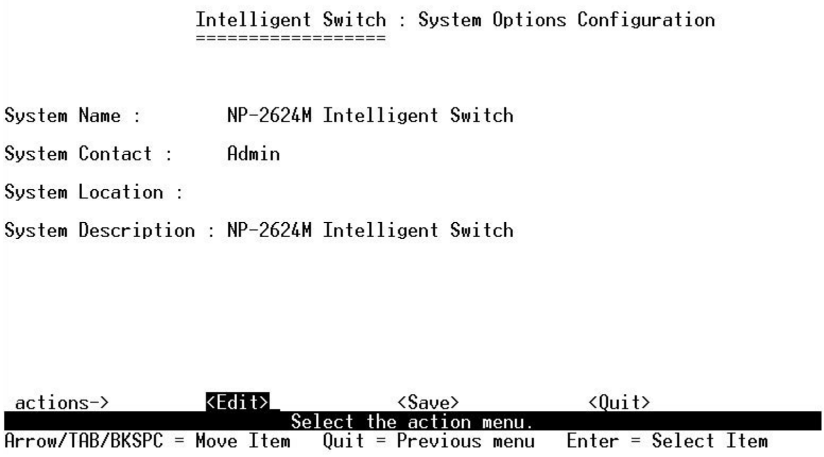
Any Network Management running the simple Network Management Protocol (SNMP) can be managed by the switch.



```
                        Intelligent Switch : SNMP Configuration
                        ==================


                                 System Options

                                 Community Strings

                                 Trap Managers

                                 Previous Menu








                      Configurate the system information.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

Use this page to define management stations as trap managers and to enter SNMP community strings. Users can also define a name, location, and contact person for the switch.

4.3.2.1. System Options



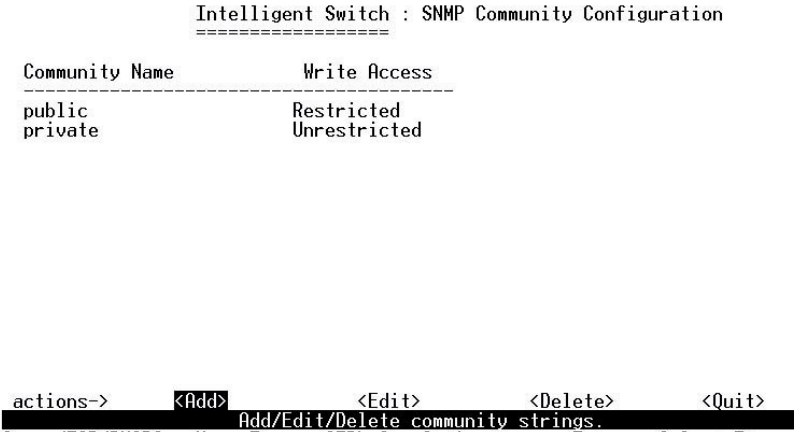
```
                 Intelligent Switch : System Options Configuration
                 ==================


System Name :         NP-2624M Intelligent Switch

System Contact :      Admin

System Location :

System Description : NP-2624M Intelligent Switch






 actions->          <Edit>          <Save>          <Quit>
                          Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Press <Edit>.
2. System Name: Type a name to be used for the switch.
3. System Contact: Type the name of contact person or organization.
4. System Location: Type the location of the switch.
5. System Description: Type the description of the switch.
6. Press Ctrl+A to go back to the action menu line.
7. Press <Save> to save the configured values.

4.3.2.2. Community Strings

Use this page to Add/ Edit/ Delete SNMP community strings.

1. Community Name: The name of current strings.
2. Write Access: Enable the rights as read only or read-write.



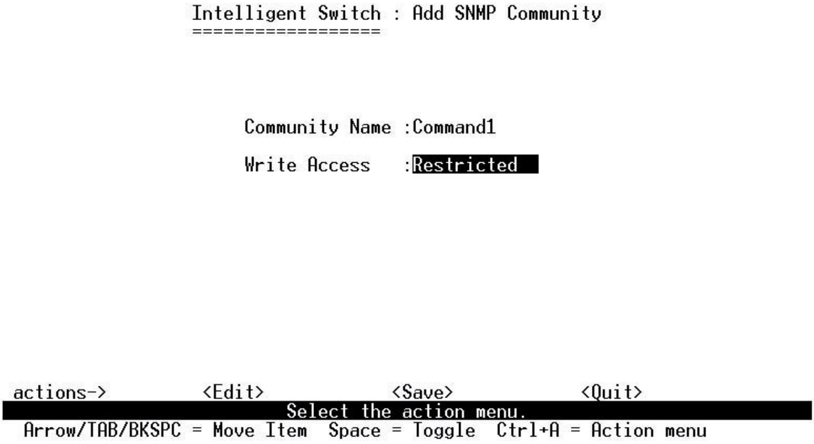
```
                Intelligent Switch : SNMP Community Configuration
                ==================

  Community Name              Write Access
  ----------------------------------------
  public                     Restricted
  private                    Unrestricted




actions->       <Add>          <Edit>          <Delete>         <Quit>
                    Add/Edit/Delete community strings.
```

Restricted: Read only, enables requests accompanied by this string to display MIB-object information.

Unrestricted: Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.

Add Community Name

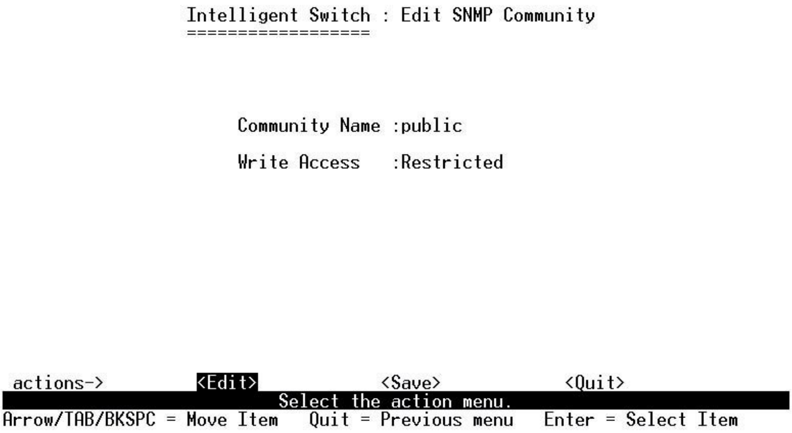
1. Press <Add> > <Edit> key.



```
               Intelligent Switch : Add SNMP Community
               ==================


                    Community Name  :Command1

                    Write Access    :Restricted




actions->        <Edit>           <Save>           <Quit>
                        Select the action menu.
  Arrow/TAB/BKSPC = Move Item  Space = Toggle  Ctrl+A = Action menu
```

2. Community Name: Type the community name.
3. Write Access: Press the Space key to toggle between restricted or unrestricted.

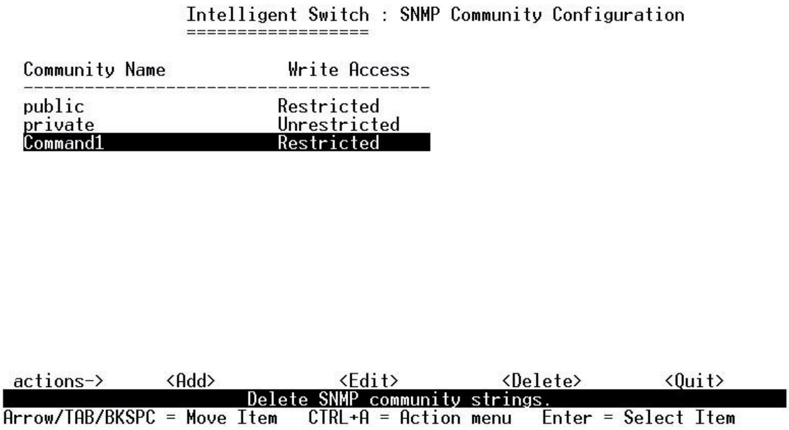
Edit Community Name



```
                  Intelligent Switch : Edit SNMP Community
                  ==================



                       Community Name :public

                       Write Access   :Restricted










 actions->           <Edit>            <Save>             <Quit>
                          Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Press the <Edit> key, choose the item that you want to modify and then press Enter.
2. Community Name: Type the new name.
3. Write Access: Press the <Space> key to toggle between restricted or unrestricted.

Delete Community Name

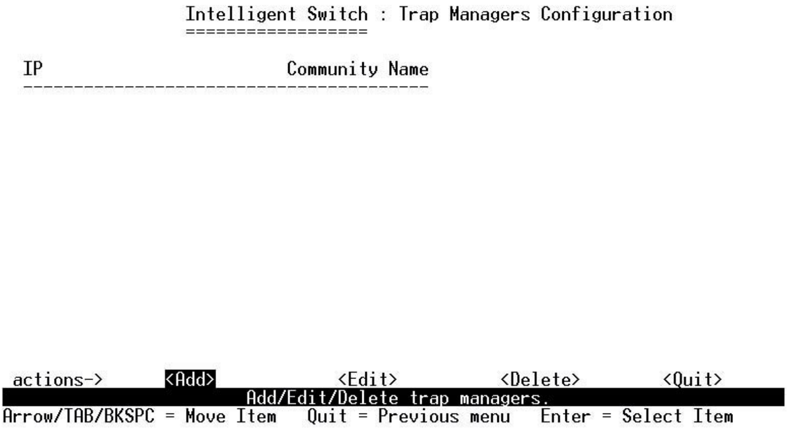


```
                  Intelligent Switch : SNMP Community Configuration
                  ==================

  Community Name             Write Access
  -----------------------------------------
  public                    Restricted
  private                   Unrestricted
  Command1                  Restricted









 actions->      <Add>            <Edit>          <Delete>         <Quit>
                         Delete SNMP community strings.
Arrow/TAB/BKSPC = Move Item   CTRL+A = Action menu   Enter = Select Item
```

1. Press the <Delete> key.
2. Choose the community name that you want to delete and then press enter.
3. Pressing <Enter> once will complete the deletion when in delete mode.

4.3.2.3. Trap Managers

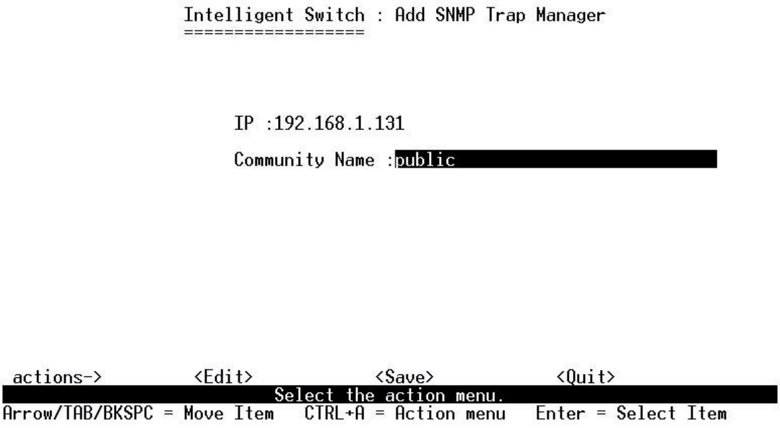
A Trap Manager is a management station that receives traps; the system alerts generated by the switch. If no trap manager is defined, no traps are issued. Create a trap manager by entering the IP address of the station and a community string.



```
                    Intelligent Switch : Trap Managers Configuration
                    ==================

 IP                          Community Name
 ------------------------------------------










actions->        <Add>            <Edit>           <Delete>          <Quit>
                         Add/Edit/Delete trap managers.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

Add SNMP trap manager

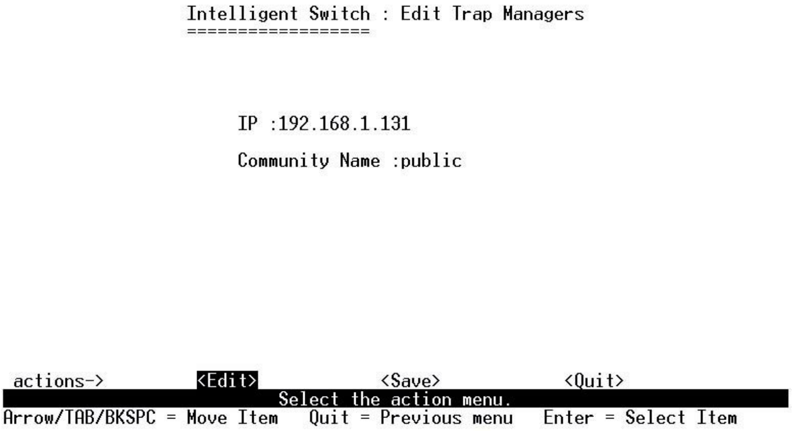
1. Press <Add> > <Edit> to add the trap manager.



```
                    Intelligent Switch : Add SNMP Trap Manager
                    ==================



                         IP :192.168.1.131

                         Community Name :public









actions->          <Edit>             <Save>             <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   CTRL+A = Action menu   Enter = Select Item
```

2. IP: Type the IP address.
3. Community Name: Type the community name.
4. Press Ctrl +A to go back to the action line menu and press <Save> key to save the configuration.

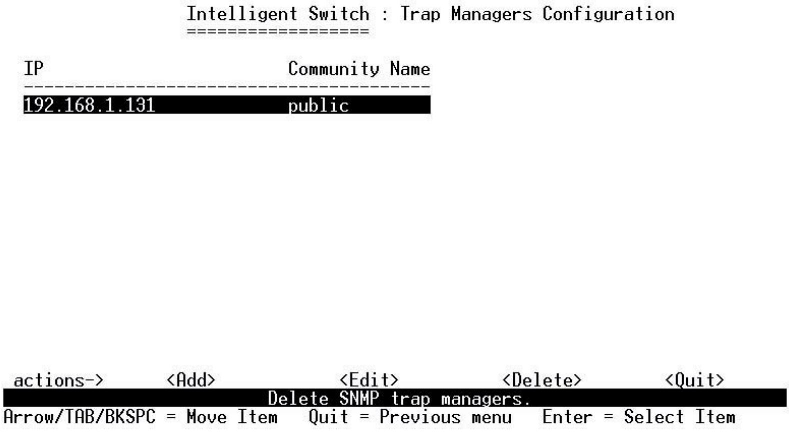
Edit trap managers



```
                   Intelligent Switch : Edit Trap Managers
                   ==================


                        IP :192.168.1.131

                        Community Name :public




 actions->          <Edit>            <Save>            <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Press the <Edit> key, and then choose the item that you want to modify.
2. IP: Type the new IP address
3. Community Name: Type the community name.
4. Press Ctrl +A to go back to the action line menu and press <Save> key to save configuration.

Delete trap manager

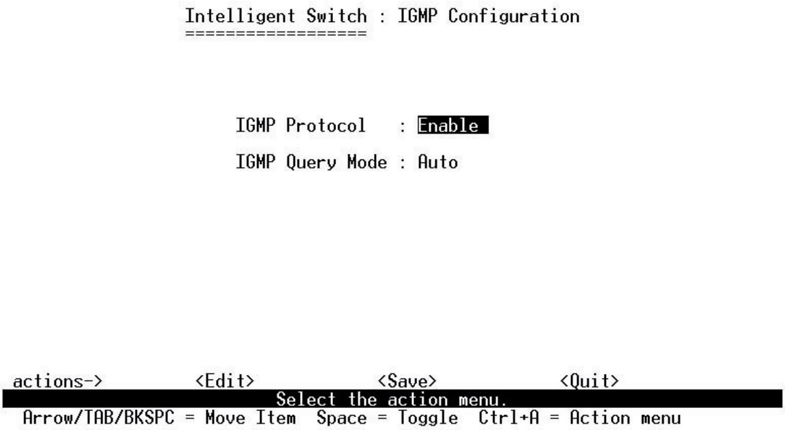


```
                   Intelligent Switch : Trap Managers Configuration
                   ==================

 IP                           Community Name
 ----------------------------------------------
 192.168.1.131                public




 actions->     <Add>            <Edit>           <Delete>          <Quit>
                          Delete SNMP trap managers.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Press the <Delete> key.
2. Choose the trap manager that you want to delete and then press enter.
3. Pressing <Enter> once will complete deletion when in delete mode.

4.3.3. IGMP

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



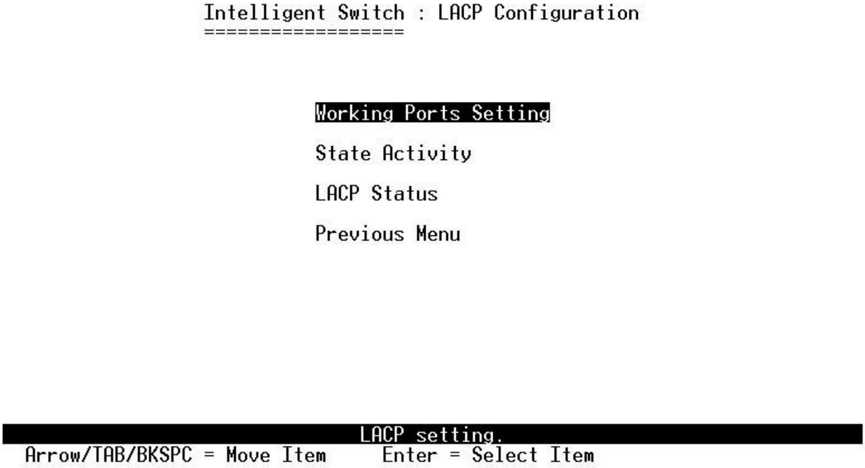
```
                    Intelligent Switch : IGMP Configuration
                    ==================

                         IGMP Protocol    : Enable
                         IGMP Query Mode  : Auto



 actions->          <Edit>           <Save>           <Quit>
                         Select the action menu.
  Arrow/TAB/BKSPC = Move Item  Space = Toggle  Ctrl+A = Action menu
```

This page allows you to enable / disable the IGMP support.

1. Select <Edit>.
2. IGMP Protocol: Press Space key to choose Enable / Disable.
3. IGMP Query Mode: Press Space key to choose Auto / Enable /Disable.
4. Press Ctrl+A to go back to the action menu line.
5. Select <Save> to save configured values.

4.3.4. LACP (Link Aggregation Control Protocol)

This page allows you to configure and view the LACP status.

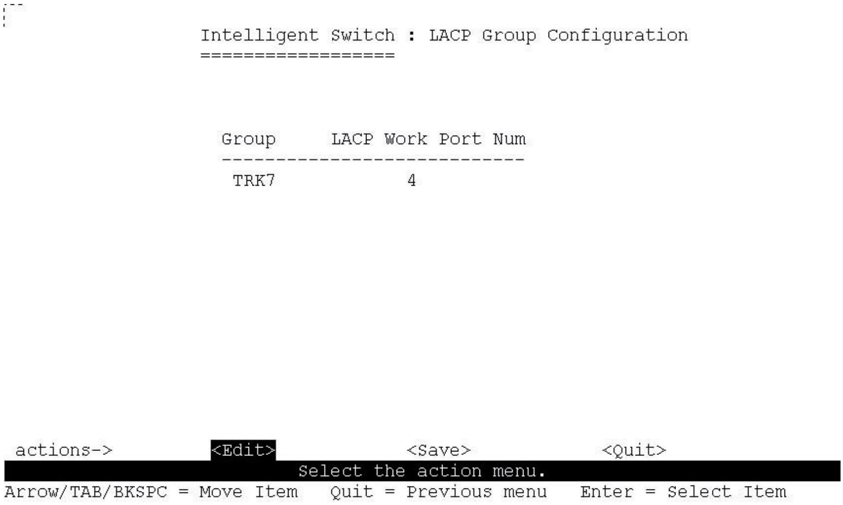


```
                    Intelligent Switch : LACP Configuration
                    ==================


                              Working Ports Setting

                              State Activity

                              LACP Status

                              Previous Menu






                                 LACP setting.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

NOTE: All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.

4.3.4.1. Working Port Setting

This page allows you to set work ports in trunk groups.



```
                   Intelligent Switch : LACP Group Configuration
                   ==================


                     Group      LACP Work Port Num
                     ----------------------------
                      TRK7             4






 actions->             <Edit>            <Save>            <Quit>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

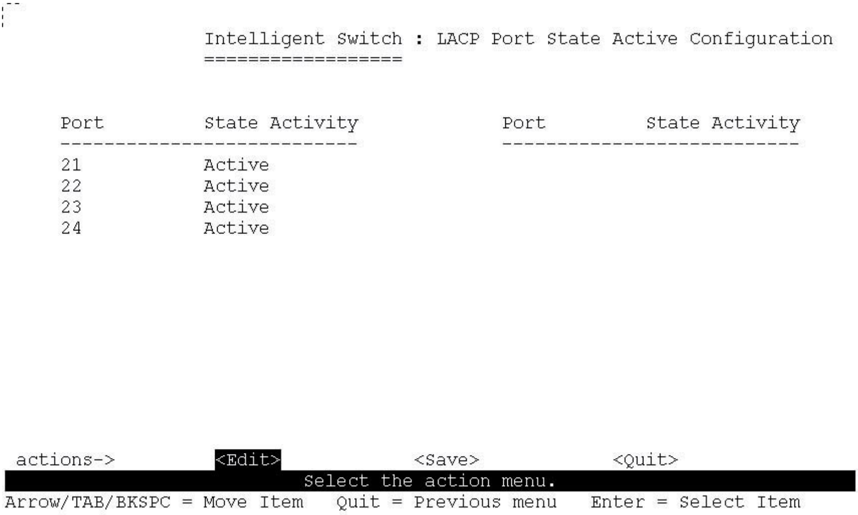
1. Select <Edit>.
2. Group: Displays the trunk group ID.
3. LACP: Displays the trunk group's LACP status.

4. LACP Work Port Num: Defines the maximum number of ports that can be aggregated at the same time. If local static trunk group, the number must be the same as group member ports.

NOTE: Before changing settings on this page, you have to set trunk group on the page of Trunk Configuration first.

4.3.4.2. State Activity

1. Select <Edit>.



```
                    Intelligent Switch : LACP Port State Active Configuration
                    ==================


      Port          State Activity               Port          State Activity
      ----------------------------               ----------------------------
      21            Active
      22            Active
      23            Active
      24            Active







  actions->          <Edit>              <Save>              <Quit>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

2. Press the Space key to choose the item.

   Active: The port automatically sends LACP protocol packets.

   Passive: The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

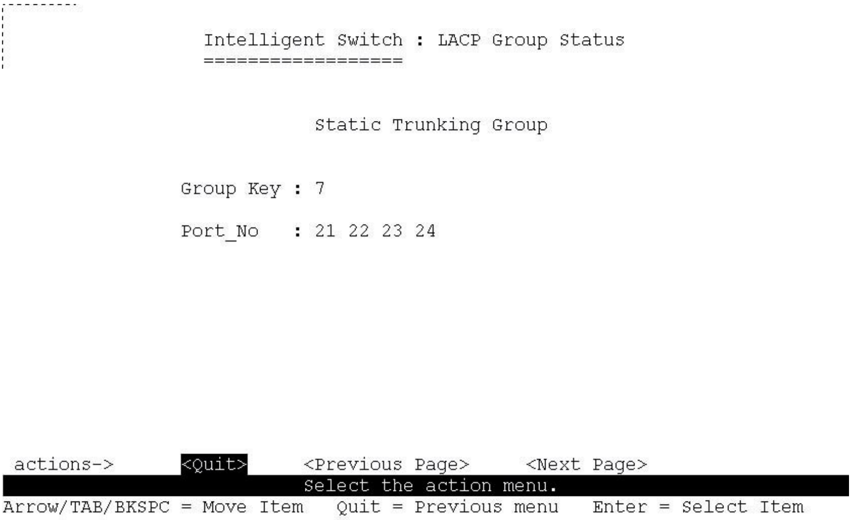
3. Press Ctrl+A go back action menu line.
4. Select <Save> to save configured values.

NOTE: If a user sets LACP mode in the trunk group, all of the member ports of this trunk group will set “Active” automatic.

4.3.4.3. LACP Status

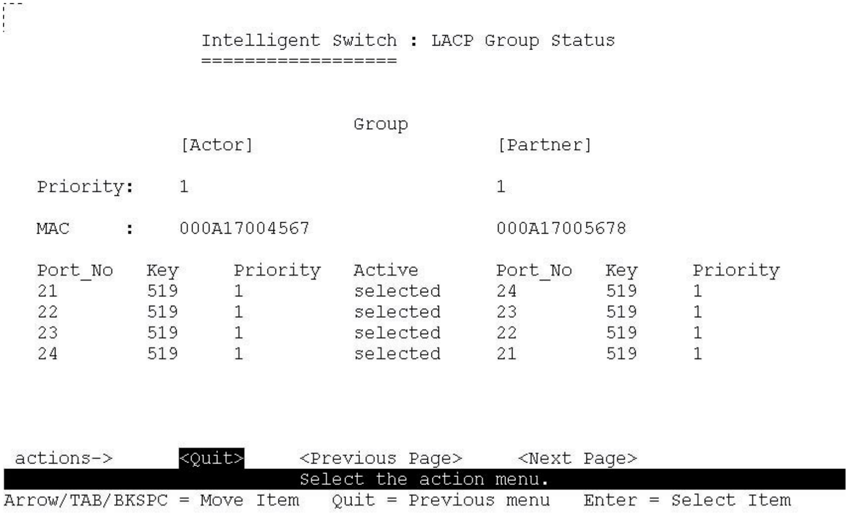
Relational Information for trunk groups can be found on this page.

Static trunk group



```
                    Intelligent Switch : LACP Group Status
                    ==================

                              Static Trunking Group

                  Group Key : 7

                  Port_No   : 21 22 23 24






 actions->        <Quit>     <Previous Page>     <Next Page>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

LACP trunk group

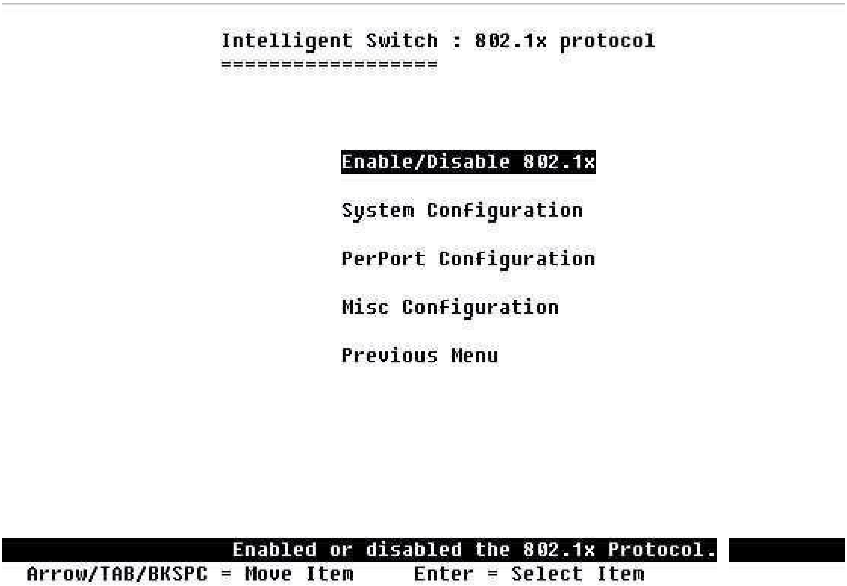


```
                    Intelligent Switch : LACP Group Status
                    ==================

                                Group
                  [Actor]                      [Partner]

    Priority:     1                            1

    MAC      :    000A17004567                 000A17005678

    Port_No    Key      Priority   Active      Port_No    Key      Priority
    21         519      1          selected    24         519      1
    22         519      1          selected    23         519      1
    23         519      1          selected    22         519      1
    24         519      1          selected    21         519      1


 actions->        <Quit>     <Previous Page>     <Next Page>
                           Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

<Quit>:	Exit this page and return to previous menu.
<Previous Page>:	Return to previous page to view.
<Next page>:	Go to the next page to view.

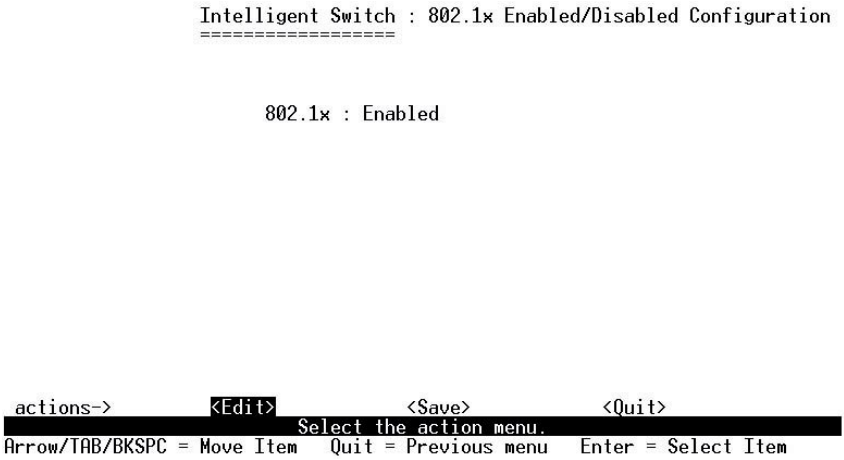
4.3.5. 802.1x Protocol

In this page the user can configure and view all the 802.1x status.



```
                 Intelligent Switch : 802.1x protocol
                 ==================


                      Enable/Disable 802.1x

                      System Configuration

                      PerPort Configuration

                      Misc Configuration

                      Previous Menu



                    Enabled or disabled the 802.1x Protocol.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

4.3.5.1. Enable/Disable 802.1x

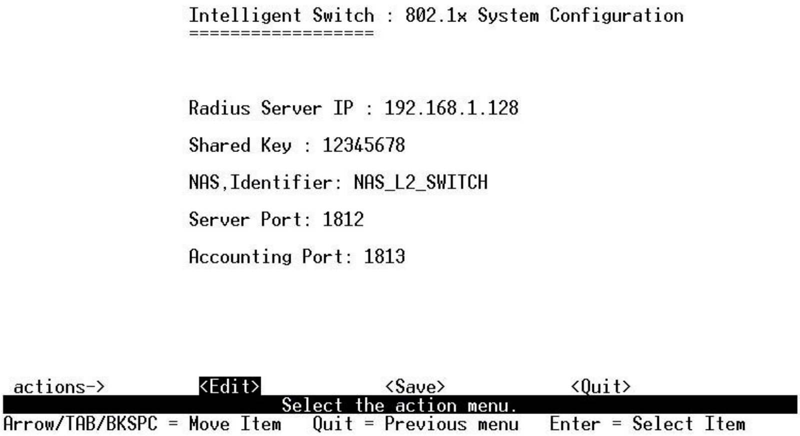


```
                 Intelligent Switch : 802.1x Enabled/Disabled Configuration
                 ==================


                    802.1x : Enabled



 actions->           <Edit>            <Save>            <Quit>
                             Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

1. Select <Edit>.
2. Press the Space key to choose Enabled / Disabled.
3. Press Ctrl+A to go back to the action line menu.
4. Select <Save> to save configured values.

4.3.5.2. 802.1x System Configuration

1. Press <Edit>.



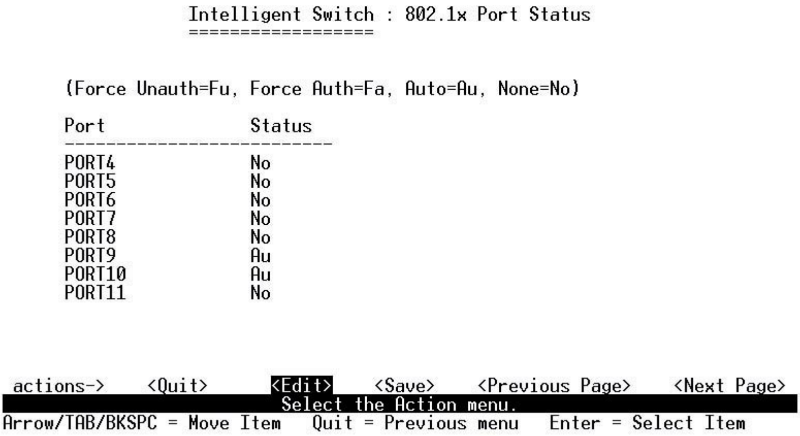
```
                    Intelligent Switch : 802.1x System Configuration
                    ==================


                    Radius Server IP : 192.168.1.128

                    Shared Key : 12345678

                    NAS,Identifier: NAS_L2_SWITCH

                    Server Port: 1812

                    Accounting Port: 1813



 actions->          <Edit>             <Save>             <Quit>
                         Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

2. Radius Server IP Address: the IP address of the authentication server.
3. Shared Key: A key shared between this switch and authentication server.
4. NAS, Identifier: A string used to identify this switch.
5. Server Port: The UDP port number used by the authentication server to authenticate.
6. Accounting Port: The UDP port number used by the authentication server to retrieve accounting information.
7. Press Ctrl+A go back action menu line.
8. Press <Save> to save configured values.

4.3.5.3. 802.1x PerPort Configuration

In this page, set the authorisation status to activate 802.1x function by port

1. Select <Edit>.



```
                    Intelligent Switch : 802.1x Port Status
                    ==================


          (Force Unauth=Fu, Force Auth=Fa, Auto=Au, None=No)

          Port                Status
          --------------------------
          PORT4               No
          PORT5               No
          PORT6               No
          PORT7               No
          PORT8               No
          PORT9               Au
          PORT10              Au
          PORT11              No


 actions->    <Quit>      <Edit>    <Save>    <Previous Page>    <Next Page>
                         Select the Action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

2. Status: Press <Space> key to choose Fu / Fa / Au / No authorization status.
3. Press Ctrl+A to go back to the action line menu.
4. Select <Save> to save all configured values.

Note: Fu: Force the specific port to be unauthorized.

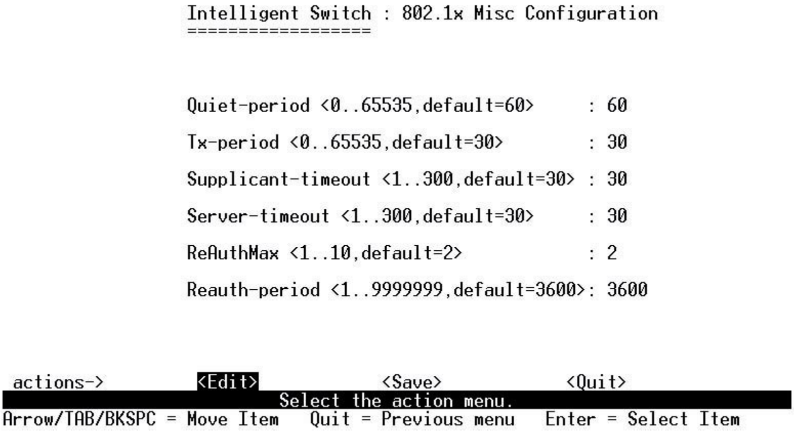
Fa: Force the specific port to be authorized.

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

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

4.3.5.4. 802.1x Miscellaneous Configuration

1. Press <Edit>.

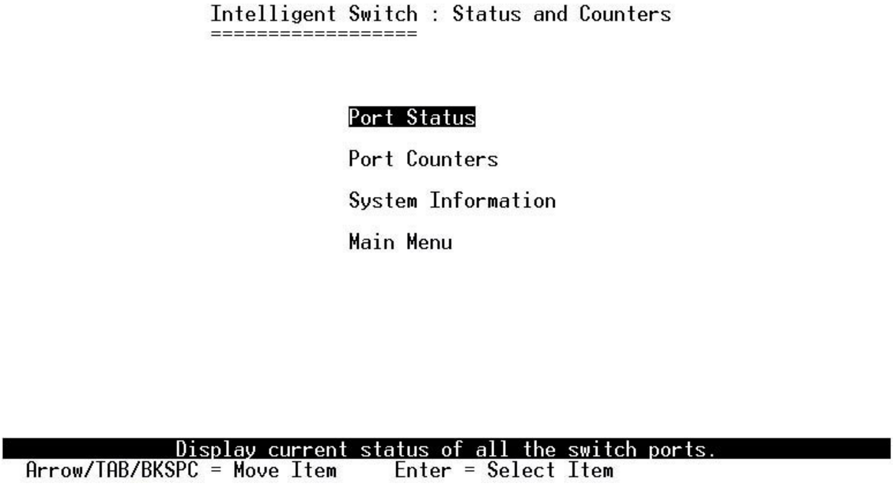


```
                    Intelligent Switch : 802.1x Misc Configuration
                    ==================


                    Quiet-period <0..65535,default=60>      : 60

                    Tx-period <0..65535,default=30>         : 30

                    Supplicant-timeout <1..300,default=30>  : 30

                    Server-timeout <1..300,default=30>      : 30

                    ReAuthMax <1..10,default=2>             : 2

                    Reauth-period <1..9999999,default=3600>: 3600


 actions->           <Edit>            <Save>           <Quit>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

2. Quiet Period: Used to define periods of time during which it will not attempt to acquire a supplicant (Default time is 60 seconds).
3. Tx Period: Used to determine when an EAPOL PDU is to be transmitted (Default value is 30 seconds).
4. Supplicant Timeout: Used to determine timeout conditions in the exchanges between the supplicant and authentication server (Default value is 30 seconds).
5. Server Timeout: Used to determine timeout conditions in the exchanges between the authenticator and authentication server (Default value is 30 seconds).
6. ReAuthMax: Used to determine the number of re-authentication attempts that are permitted before the specific port becomes unauthorized (Default value is 2 times).
7. Reauth Period: Used to determine a nonzero number of seconds between periodic re-authentication of the supplications (Default value is 3600 seconds).
8. Press Ctrl+A to go back to the action line menu.
9. Press <Save> to save configured values.

4.4. Status and Counters

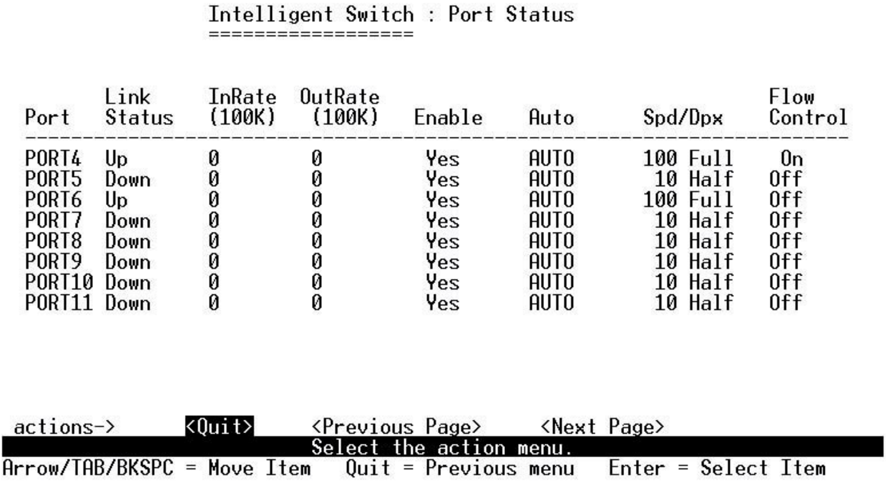
You can press the Tab or Backspace keys to choose items, and press the Enter key to select an item.



```
                     Intelligent Switch : Status and Counters
                     ==================


                               Port Status

                               Port Counters

                               System Information

                               Main Menu




              Display current status of all the switch ports.
  Arrow/TAB/BKSPC = Move Item       Enter = Select Item
```

4.4.1. Port Status

This page display every ports status



```
                     Intelligent Switch : Port Status
                     ==================


 Port     Link     InRate   OutRate                                Flow
          Status   (100K)   (100K)   Enable    Auto      Spd/Dpx    Control
 -------------------------------------------------------------------------
 PORT4    Up       0        0          Yes     AUTO      100 Full    On
 PORT5    Down     0        0          Yes     AUTO       10 Half   Off
 PORT6    Up       0        0          Yes     AUTO      100 Full   Off
 PORT7    Down     0        0          Yes     AUTO       10 Half   Off
 PORT8    Down     0        0          Yes     AUTO       10 Half   Off
 PORT9    Down     0        0          Yes     AUTO       10 Half   Off
 PORT10   Down     0        0          Yes     AUTO       10 Half   Off
 PORT11   Down     0        0          Yes     AUTO       10 Half   Off



 actions->       <Quit>      <Previous Page>      <Next Page>
                              Select the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

Link Status:	Displays the ports as linked or not linked.
InRate:	Displays the input rate control (100K/unit) setting value.
OutRate:	Displays the output rate control (100K/unit) setting value.

Enabled: Displays whether the port is enabled or disable depending on user settings. Enabled will display "Yes", disabled will display "No". If the port is unlinked, it will be treated as "No".

Auto: Displays which Nway mode the port is linked on: Auto, Nway_Force, and Force.

Spd/Dpx: Displays the port speed and duplex.

FlowCtrl: In Auto / Nway force mode, displays whether the flow control status is enabled or not after negotiation.

In force mode, displays whether the flow control status is enabled or disabled depending on user settings.

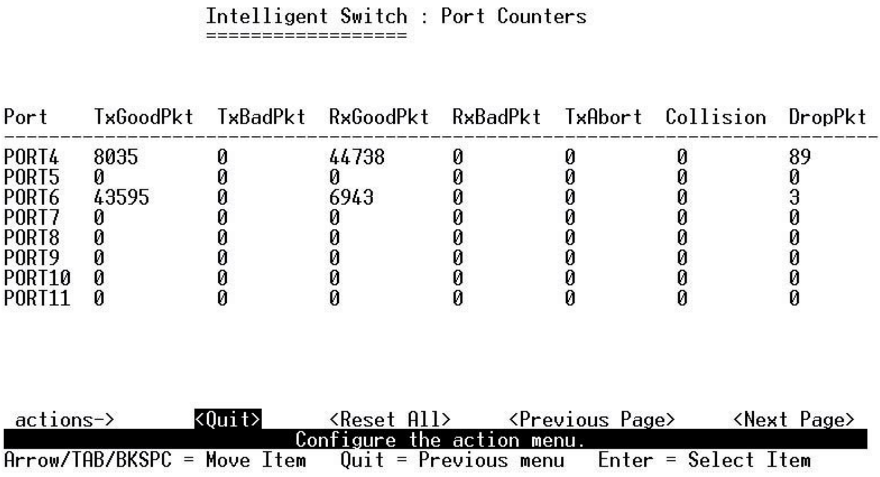
<Quit>: Exit the port status page and return to previous menu.

<Previous Page>: Display previous page.

<Next page>: Display next page.

4.4.2. Port Counters

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



```
                    Intelligent Switch : Port Counters
                    ==================


Port     TxGoodPkt  TxBadPkt  RxGoodPkt  RxBadPkt  TxAbort  Collision  DropPkt
-------------------------------------------------------------------------------
PORT4    8035       0         44738      0         0        0          89
PORT5    0          0         0          0         0        0          0
PORT6    43595      0         6943       0         0        0          3
PORT7    0          0         0          0         0        0          0
PORT8    0          0         0          0         0        0          0
PORT9    0          0         0          0         0        0          0
PORT10   0          0         0          0         0        0          0
PORT11   0          0         0          0         0        0          0



 actions->        <Quit>      <Reset All>     <Previous Page>      <Next Page>
                        Configure the action menu.
Arrow/TAB/BKSPC = Move Item    Quit = Previous menu    Enter = Select Item
```

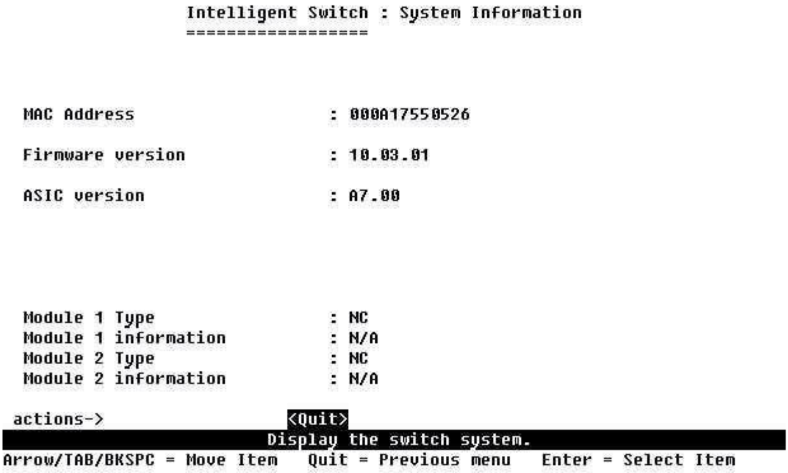
<Quit>: Exit the port status page and return to previous menu.

<Reset All>: Set all count to 0.

<Previous Page>: Display previous page.

<Next page>: Display next page.

4.4.3. System Information



```
                    Intelligent Switch : System Information
                    ==================


    MAC Address                     : 000A17550526

    Firmware version                : 10.03.01

    ASIC version                    : A7.00




    Module 1 Type                   : NC
    Module 1 information            : N/A
    Module 2 Type                   : NC
    Module 2 information            : N/A

  actions->                   <Quit>
                          Display the switch system.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

MAC Address: The unique hardware address assigned by a manufacturer.

Firmware Version: Displays the switch's firmware version.

ASIC Version: Displays the switch's Hardware version.

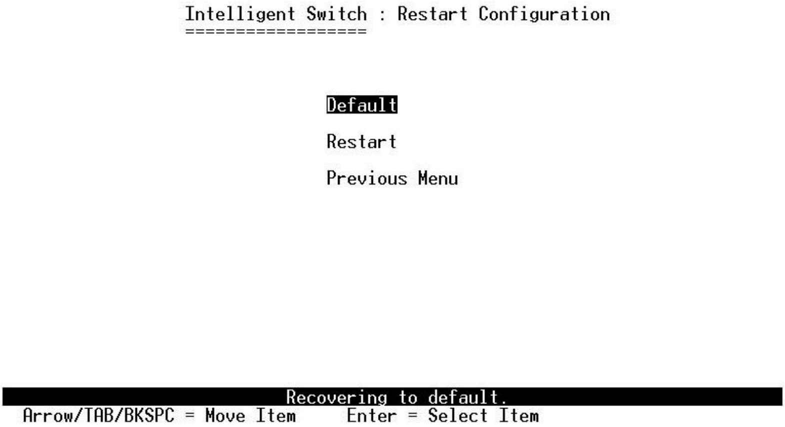
Module 1 Type: Displays the module 1 Type: 1000Tx or 100Fx ext. Depends on module card mode.

Module 1 information: Displays the information saved in EEPROM of module1.

Module 2 Type: Displays the module 2 Type: 1000Tx or 100Fx ext. Depends on module card mode.

Module 2 information: Displays the information saved in EEPROM of module2.

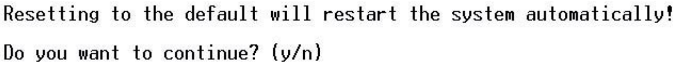
4.5. Reboot Switch



```
                Intelligent Switch : Restart Configuration
                ==================

                           Default

                           Restart

                           Previous Menu



                        Recovering to default.
  Arrow/TAB/BKSPC = Move Item      Enter = Select Item
```

4.5.1. Default

To reset the switch to its default configuration, please refer to section 2-4-14.



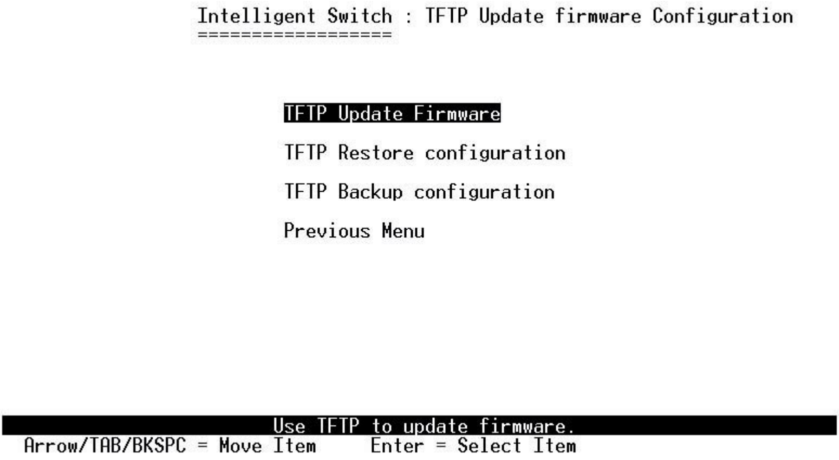
```
Resetting to the default will restart the system automatically!

Do you want to continue? (y/n)
```

4.5.2. Restart

Reboots the switch.

4.6. TFTP Update Firmware

This page allows the user to update the firmware or restore the EEPROM value or upload the current EEPROM value.

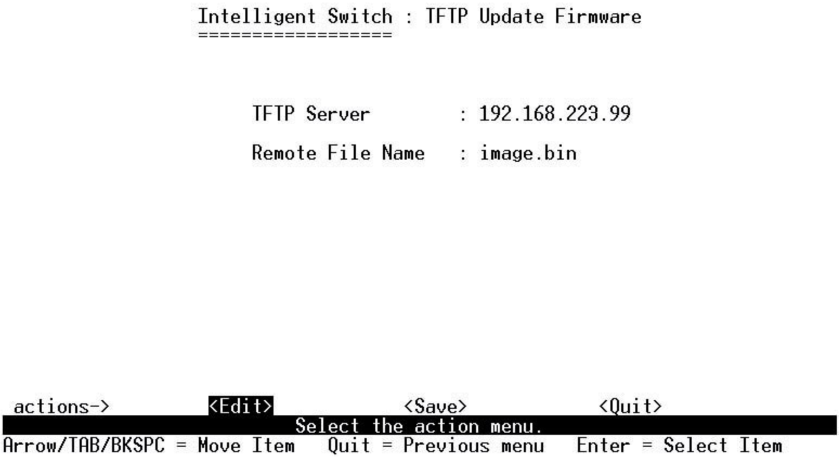


```
Intelligent Switch : TFTP Update firmware Configuration
==================

                TFTP Update Firmware

                TFTP Restore configuration

                TFTP Backup configuration

                Previous Menu

                    Use TFTP to update firmware.
 Arrow/TAB/BKSPC = Move Item     Enter = Select Item
```

4.6.1. TFTP Update Firmware

This page allows the user to use TFTP to update the firmware.

1. Start the TFTP server, and copy firmware update version image file to TFTP server.
2. Press <Edit> on this page.



```
Intelligent Switch : TFTP Update Firmware
==================

          TFTP Server          : 192.168.223.99

          Remote File Name     : image.bin

 actions->         <Edit>          <Save>          <Quit>
                    Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

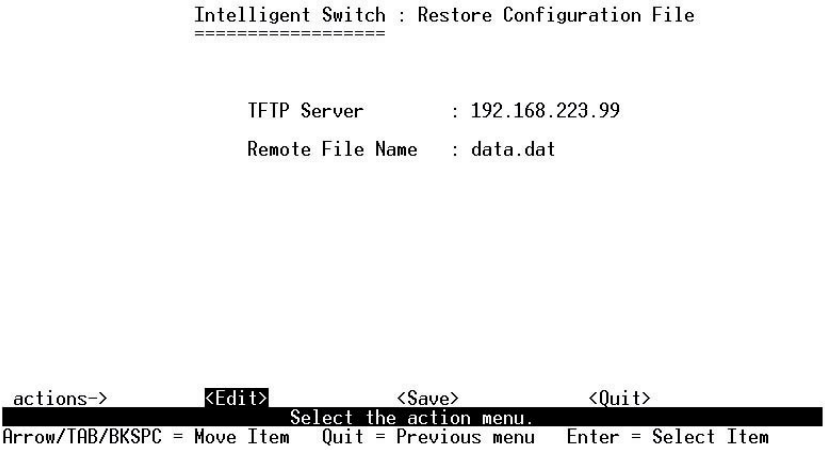
3. TFTP Server: Type the IP of TFTP server.
4. Remote File Name: Type the image file name.
5. Press Ctrl+A go to action line.
6. Press <Save> key, it will start to download the image file.

7. Once saved, the image file will automatically update.
8. Restart switch.

4.6.2. Restore Configure File

This page allows the user to restore EEPROM value, save previous image file, from TFTP server.

1. Start the TFTP server.
2. Press <Edit> on this page.



```
Intelligent Switch : Restore Configuration File
==================


TFTP Server          : 192.168.223.99

Remote File Name     : data.dat







actions->           <Edit>           <Save>           <Quit>
                     Select the action menu.
Arrow/TAB/BKSPC = Move Item   Quit = Previous menu   Enter = Select Item
```

3. TFTP Server: Type the IP of TFTP server.
4. Remote File Name: Type the image file name.
5. Press Ctrl+A go to action line.
6. Press <Save> key, it will start to download the image file.
7. Once saved, the image file will automatically update.
8. Restart switch.

4.6.3. Backup Configure File

This page allows the user to save the current EEPROM value to an image file. Then restore the EEPROM value from the update configuration page.

1. Start the TFTP server.
2. Press <Edit> on this page.
3. TFTP Server: Type the IP of TFTP server.
4. Remote File Name: Type the image file name.
5. Press Ctrl+A go to action line.
6. Press <Save> key, it will start to upload the image file.
7. Once saved, the image file will automatically update.
8. Restart switch.

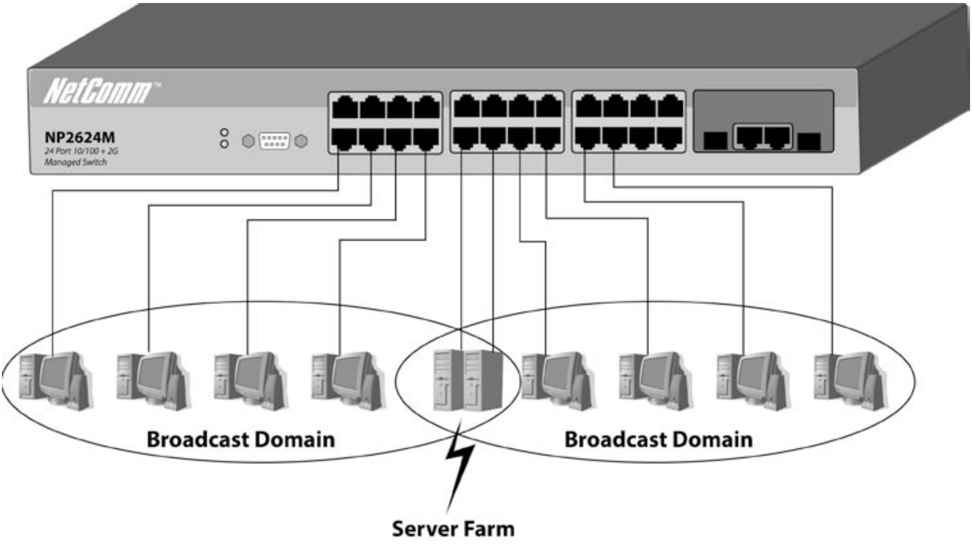
5. Application Examples

5.1. VLAN application used with switch

VLAN is a simple solution to protect your network against broadcast storming by creating segments based on Layer2 Ethernet information and avoiding the complexity and the heavy processing requirements of Layer3 IP based routers.

As a result, each group of stations connect to separate Segmented Ports to form different isolated Broadcast Domains. The Broadcast Sharing Ports should be used to connect servers and other common services, such as Internet access, that are used by all the stations connected to the different Segmented Ports.

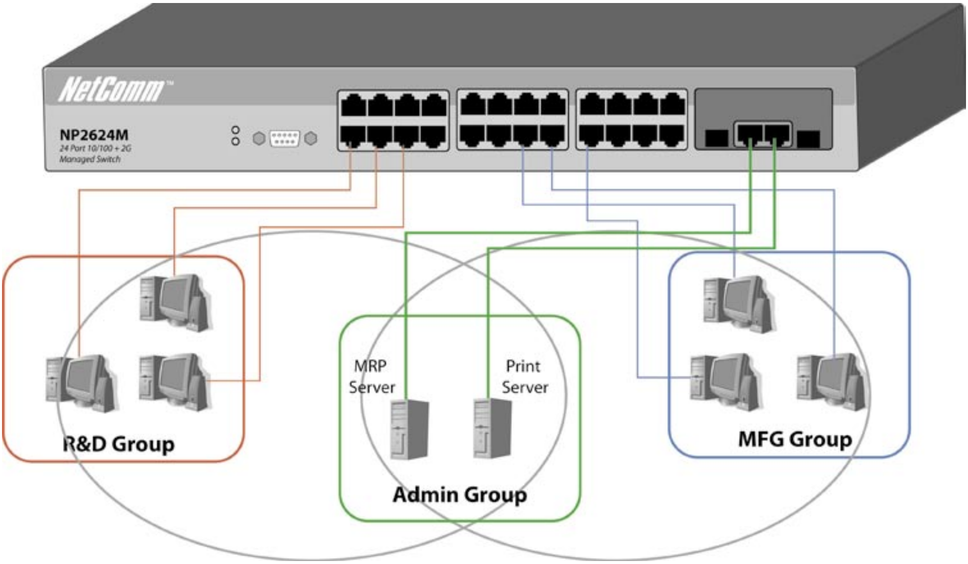
Virtual LAN, or VLAN, is generally defined as broadcast domain. It can be viewed as a group of end nodes, possibly on different physical network segments, which can communicate with each other.



Benefits of VLANs

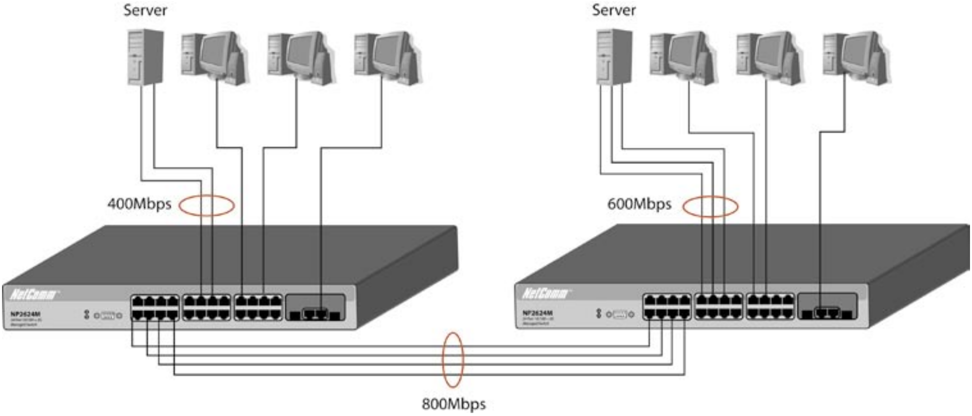
- Groups users into logical networks for performance enhancement.
- Provides effective broadcast containment between Segmented Ports, which prevents flooding of a network.
- Offers security by completely isolating the different Broadcast Domains connected on separate Segmented Ports.
- Preserves current investment in equipment and cabling.
- Provides an easy, flexible, economic way to modify logical groups when needed.
- Network administrators can easily “fine tune” the network.
- Keeps the network structure separate to the physical topology of the cabling.
- Makes large networks more manageable.

You can group users according to some shared characteristic, such as a common business function or a common protocol. A single switch may have several independent VLANs within it. Below is a example that R&D, Manufacturing and Administration group can be partitioned into different VLAN groups, members in different groups can't talk directly, but they still share the same server, such as MRP server, printer server in Administration group…etc.



5.2. Trunking Application used with switch

Trunking allows you to increase the available bandwidth between switches by grouping ports into a trunk. Trunking can also be used to connect servers to switches when higher bandwidth services are required. You can use trunking to improve the throughput between segments. Moreover, this switch also provides trunking with a fail-over function, that is, when one of the links of the trunk fails or is broken, the traffic going through that link will automatically be re-directed to other links of the trunk. This redundancy greatly increases the value of trunking.



5.3. "Single IP – Agent mode" application used with switch

Single IP is a management utility of network devices for administrators to access private IP devices through a single IP (real IP or private IP). By this utility, an administrator can manage many more network devices and reduce the demand of real IPs, because every real IP switch can be an agent host for any network devices in their private IP domain.

There are some defects in the current solutions of network management. For example, switches with legacy "stack" capability have to stack together due to their special limited-length cables, and have the limitation of stacking quantities and brand compatibility due to hardware specification. Moreover, the administrator always has trouble in finding out the target window among those multi-display interfaces. Although there are expert network management utilities like HP OpenView, available in the current market, they are too expensive to purchase and too difficult to implement into embedded systems for their practical application.

Because of the rapid development of Ethernet, the scare of real IP shortage becomes a serious issue when an enterprise continues its IA growth. It is a waste of money and resources for every individual host to have its own real IP inside the enterprise's network. Privates IPs and NAT function (provided by router, gateway or IP sharing) provide a solution to the shortage of real IP, but gives rise to new issue that remote users from the internet have no access permission into the private IP domain. Thus an administrator until now had no choice but to assess private IP devices from the very location of the local area network to trouble shoot any problems that network clients report. The "Single IP-Agent mode", one of this switch special features, provides a new solution for the issues above.

There are benefits of "Single IP-Agent mode":

1. Reduce the demand of real IP (public IP).

Since there are up to 32 devices which have a IP agent as "Single IP" switch, meaning that the switch becomes a network agent and handles all functions of these devices, MIS can reduce the number of hosts that are directly connected to internet, and make use of real IPs more efficiently.

2. Integrate network devices without modifying hardware or software.

"Single IP" is a technique mainly based on application layer in OSI standard. The connection between master and slave hosts is linked by Ethernet protocol and has little to do with the hardware. Modifications of hardware or software of the slave hosts is not necessary. Thanks to its characteristics, the single IP switch gives the best compatibility with other network devices, router, gateway, web server and even another brand switch.

3. Handy User interface without learning complex setting or changing user's habit of operation.

A floating menu gives a comprehensive user interface for the administrator to pick and manage devices. It provides host IP and host name, saving the administrator the need to remember which IPs those slave hosts are assigned to. Since there is only one browser windows displaying on the screen at any point in time, the agent manager plays a similar role to a TV channel controller. The administrators can easily switch to a device and enter the setting webpage as needed.

4. Totally remote control of network devices in private IP domain.

It is not necessary for MIS to put all devices together in one place. Single IP function will operate normally no matter how far the distance is between the master and the slave hosts if their packets can reach each other in local area network. Moreover, a remote administrator can access the far-side servers in the private domain through the intermediary of single IP switch which is directly connected to internet.

5. No up-link limitation through Gigabit port.

Unlike stacking mode, up-link in agent mode can be achieved through any port rather than Gigabit port only. This provides greater flexibility and allows Gigabit ports to be saved for other applications.

5.3.1 Typical setup of “Single IP-Agent mode” network:

The basic rules to set up “Single IP”:

1. The “Agent IP” of master switch should be within the IP domain of the managed hosts. (slave switches)
2. The “Agent IP” should be the same as “Switch IP” if administrator is within the IP domain of slaves; On other hand, the “Agent IP” should be different from “Switch IP” if the administrator wants to manage the slaves across the IP domain.

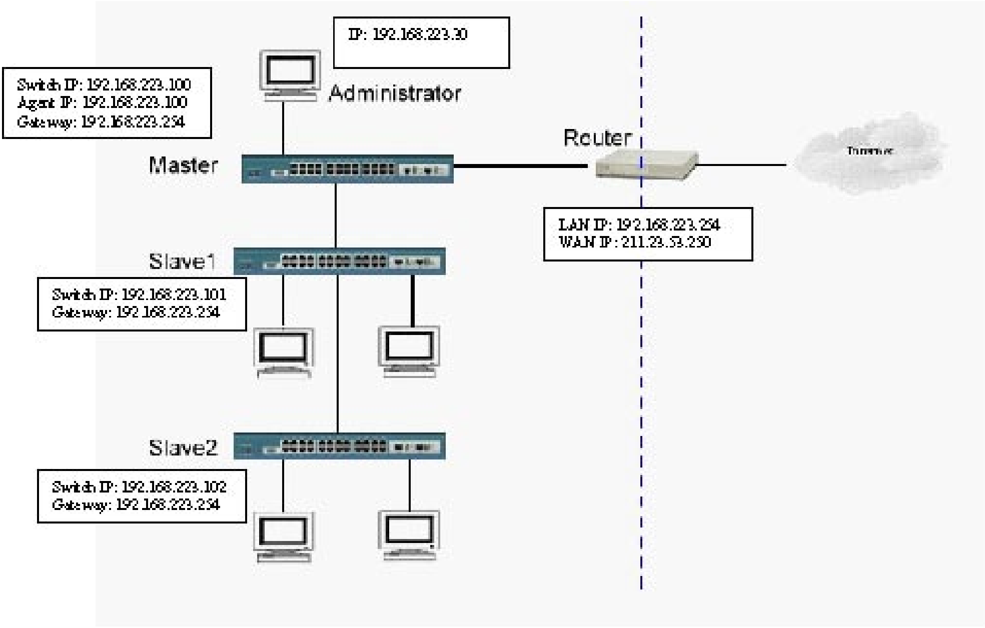
There are three typical examples to demonstrate the usage of “Single IP-Agent mode”.

1. **Master and slave switches in the same LAN domain.**

   In this example, the master switch will manage 2 slave switches and 1 router.

   Switch IP of master is 192.168.223.100. Set its management mode to “Agent Master”. Since the IP domain of slaves and router are in the IP domain 192.168.223.0, Agent IP of master should be set as same as switch IP (192.168.223.100).

   Add slave1 and slave2 into agent list using auto-discover or manually. Routers can only be added by manually. Administrator (192.168.223.30) can access those slaves through the master.



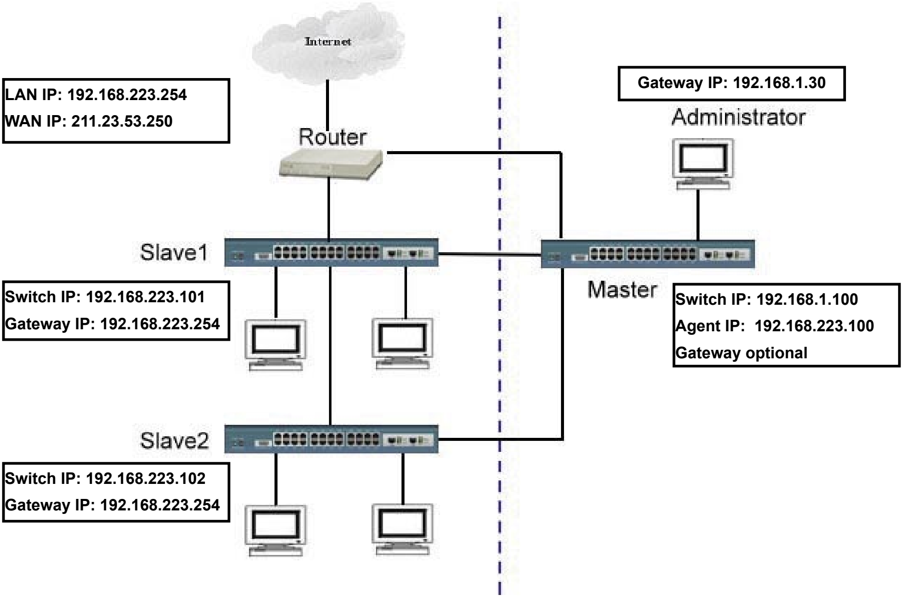
2. **Master and slave switches in different LAN domain.**

   In this example, master will manage 2 slave switches and 1 router in other IP domain.

   The difference between the examples is that the administrator and master switch IP is in the other IP domain (192.168.1.0). Switch IP of master is 192.168.1.100. Set its management mode to "Agent Master". According to the basic rule 1, the agent IP should be set in the same domain as slaves, that is, 192.168.223.100. The other procedures are the same as example 1. Now the administrator (192.168.1.30) can access the slaves in the other domain (192.168.223.0).

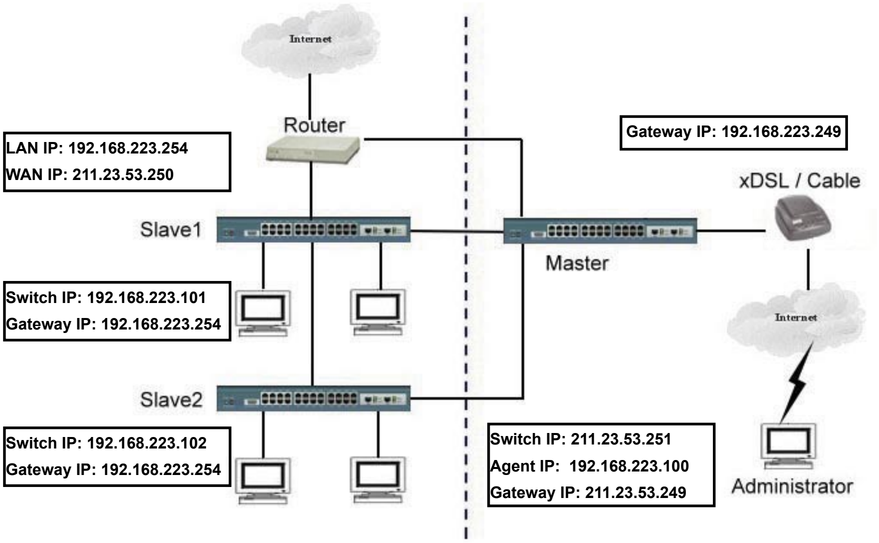
3. **Master in WAN domain and slaves in LAN domain.**

   This example gives a practical application for remote management.



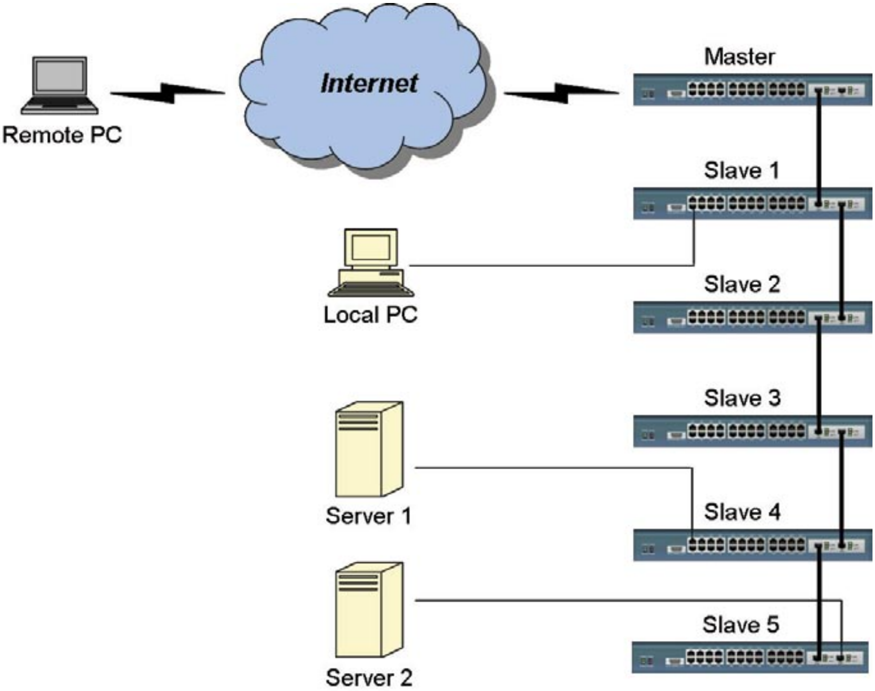
The difference from example 2 is that the master switch links directly to internet and administrator from the WWW and can access it through internet. Set the Switch IP and gateway of master switch to real IP (211.23.53.251 and 211.23.53.249) and make sure the administrator can access the master switch from internet. The other procedures are the same as example 1.

Now the administrator from the internet can access the slaves in the other domain (192.168.223.0). We can somewhat imagine that the master is playing a role of tiny virtual server for these slaves.


Internet
Router
LAN IP: 192.168.223.254
WAN IP: 211.23.53.250
Gateway IP: 192.168.223.249
xDSL / Cable
Slave1
Master
Switch IP: 192.168.223.101
Gateway IP: 192.168.223.254
Internet
Slave2
Switch IP: 192.168.223.102
Gateway IP: 192.168.223.254
Switch IP: 211.23.53.251
Agent IP: 192.168.223.100
Gateway IP: 211.23.53.249
Administrator

5.4. "Single IP - Stacking mode" application used with switch

This switch provides traditional stacking mode to stack a maximum of 16 switches by cascading their Gigabit ports. This feature helps network administrators use one switch assigned as the master to manage the other stacked switches through the browser. That is, the master can bring a "global view" showing all stacked devices to network administrator as long as he/she has access to the master switch by using its IP (this IP should be public for remote access through the internet). This will easily let the network administrator know the group settings (e.g. tag-based VLAN groups) and link status among all stacked units. A typical arrangement of network connection of "Single IP – Stacking mode" is shown below:



Typical connections for switch management by stacking

The significant characteristics of this switch are:

1. **No redundant hardware required:**

   Unlike special requirement of connecting cable among "hardware stacking" switches, this switch provides the least demand as a Gigabit module to build up a stacking set. The Gigabit module give the best performance for inter-communication between stacking switches and the administrator can spare one port of Gigabit module in the top switch or the bottom one in the stack for flexible usage.

2. **Well integrated UI to view status of stacking switches:**

   An user-friendly Web UI provides the user a total view of the port link status and VLAN group settings for all stacked switches at a glance.

3. **Easy adding or removal stacking member:**

   All Stacking members can be easily added or removed through the network. By clicking on the UI, the administrator can quickly determinate which switch will join the stack, without adjusting the network connection in front of those switches. It saves time when trouble-shooting any network abnormality.

5.4.1 A guide to build up "Stacking Switches"

Follow these steps to build up a set of "Stacking Switches":

1. **Connect switches with Giga port in serial sequence.**

   By reference to the picture of typical network connection of "Single IP – Stacking mode", the user can connect these stacking switches with Giga port in serial sequence.

   A connection check by pinging these switches' IP will help to avoid network failure.

2. **Make sure the master switch is set to "Stacking Master" and slaves to "Stacking Slave".**

   In the Main Menu "Administrator/IP & Management Mode", the user has to set the management mode to "Stacking Master" and slave switches to "Stacking Slave".

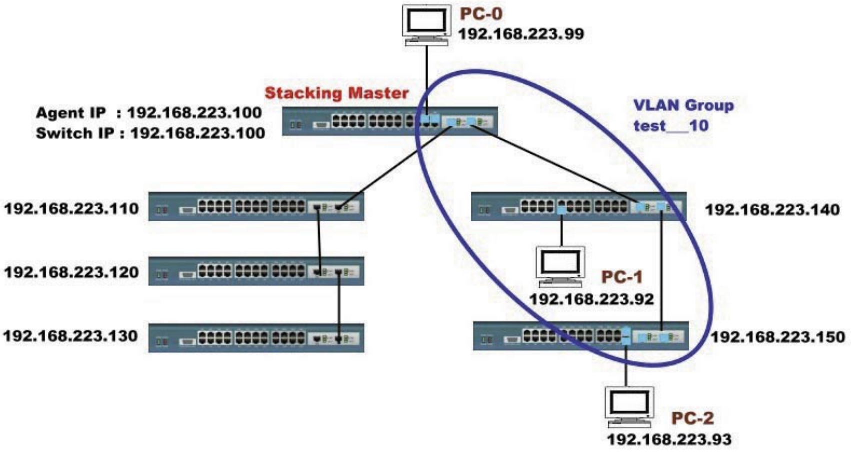
   Users wishing to access the stacking switches from remote IP, should fill up the switch IP with a real IP and the agent IP with the alternative LAN IP; On other hand, for local area network access only, the switch IP and agent IP should be kept exactly the same as the LAN IP.

3. **Add stacking members in the Stacking management.**

   Please refer to section 2-4-14 for detailed information on configuration.

4. **Launch the Stack manager.**

5.4.2 An Example of Port-Base Stacking VLAN



Port-Base Stacking VLAN setting:

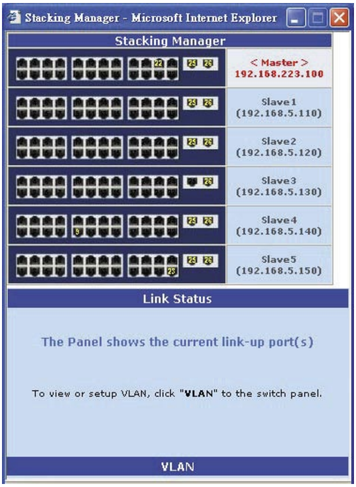
Switch:	Master	(192.168.223.100)
	Slaves	(192.168.223.110, 192.168.223.120, 192.168.223.130, 192.168.223.140, 192.168.223.150)
	PC:	PC-0(192.168.223.99) on port 22 of Master (192.168.223.100)
		PC-1(192.168.223.92) on port 9 of Slave 4(192.168.223.140)
		PC-2(192.168.223.93) on port 23 of Slave 5(192.168.223.150)

Port-Base VLAN Group:

VLAN name :	test
VLAN ID :	10
Members:	Port 22, 24 of Master (192.168.223.100)
	Port 9 of Slave4 (192.168.223.140)
	Port 23, 24 of Slave5 (192.168.223.150)

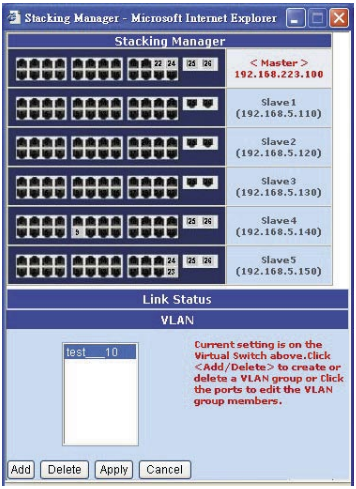
Test case:

1. PC-0 ping or trace PC-01 and PC-02 (The same VLAN)
2. Remove port 9 of Slave4 from VLAN test, and process test1 again.



The Panel shows the current link-up port(s)

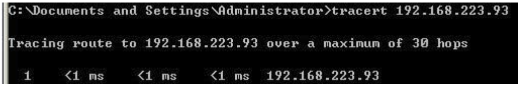
To view or setup VLAN, click "VLAN" to the switch panel.



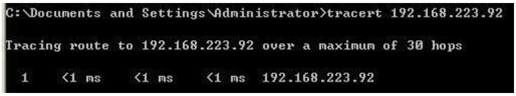
Current setting is on the Virtual Switch above.Click <Add/Delete> to create or delete a VLAN group or Click the ports to edit the VLAN group members.

Result:

1. PC-0 can access both PC-01 and PC-02.

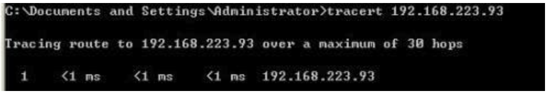


```
C:\Documents and Settings\Administrator>tracert 192.168.223.93

Tracing route to 192.168.223.93 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.223.93
```

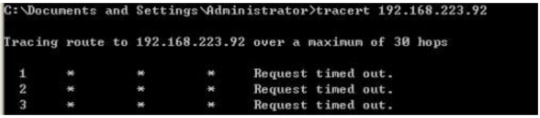


```
C:\Documents and Settings\Administrator>tracert 192.168.223.92

Tracing route to 192.168.223.92 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.223.92
```

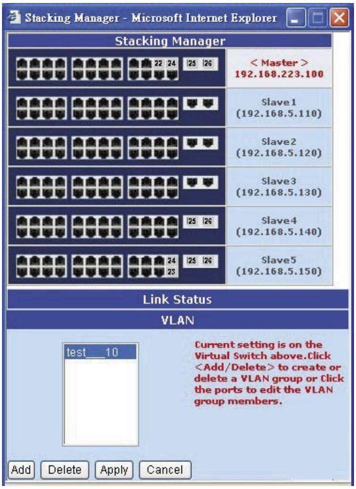
2. PC-0 can only access PC-02 only. PC-01 will not reply.



```
C:\Documents and Settings\Administrator>tracert 192.168.223.93

Tracing route to 192.168.223.93 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.223.93
```



```
C:\Documents and Settings\Administrator>tracert 192.168.223.92

Tracing route to 192.168.223.92 over a maximum of 30 hops

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
```

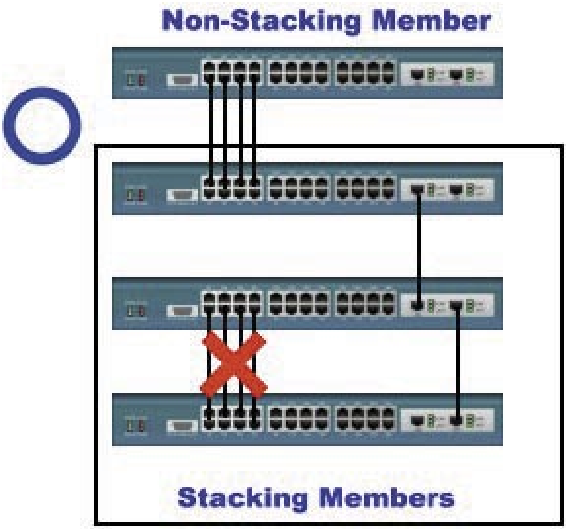


Current setting is on the Virtual Switch above.Click <Add/Delete> to create or delete a VLAN group or Click the ports to edit the VLAN group members.

5.4.3 Issue on Trunk and Stacking mode

There are Two basic rules here:

1. Stacking members cannot and should not truck each other.
2. Stacking members can trunk with non-stacking members.



The packet traffic between stacking members are transferred only through Giga module. Trunking between stacking members may cause the spanning tree protocol (STP) to alter the topology and change the routed ports. If this happens, Giga port traffic may break and the stacking mechanism will fail.

For non-stacking member, there is no such limitation.

5.5 Compatibility on Virtual Server and "Single IP"

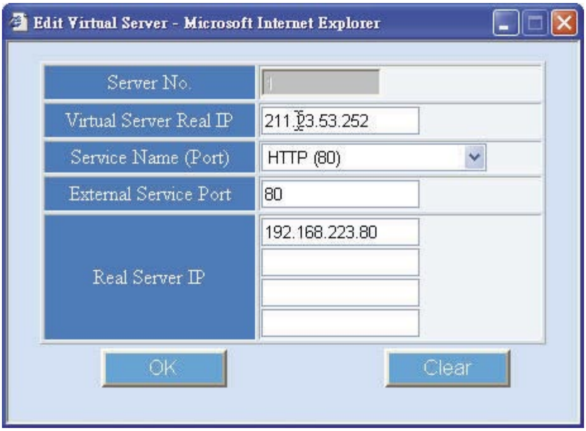
There are practical applications on combinations of virtual server and single IP. The network administrator generally prefers a router to have a unique gateway to Internet and a "Single IP" to manage his network hosts both from LAN and WAN. This example offers an example of how to setup a virtual server with an agent/stacking switch.

Example target:

1. Any client with port 80 (http) go to company's default web server (example 192.168.223.80)
2. Any client with port 28010 go to agent/stacking switch.(example 192.168.223.90).
3. Any client can use the agent/stacking function through virtual server.

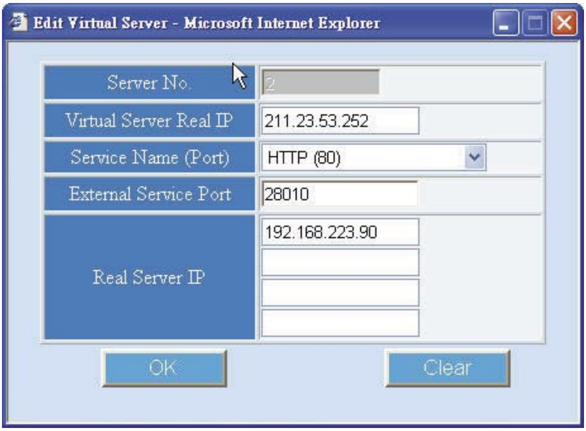
The instructive pictures may vary depending on the router the user sets up.

Step 1: Set up web server mapping port (211.23.53.252:80 --> 192.168.223.80:80)



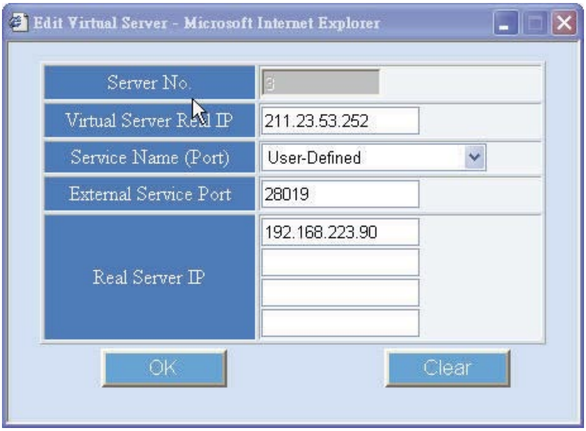
Server No.	1
Virtual Server Real IP	211.23.53.252
Service Name (Port)	HTTP (80)
External Service Port	80
Real Server IP	192.168.223.80

Step 2. Set up an agent/stacking switch mapping port (211.23.53.252:28010->192.168.223.90:80)



Server No.	2
Virtual Server Real IP	211.23.53.252
Service Name (Port)	HTTP (80)
External Service Port	28010
Real Server IP	192.168.223.90

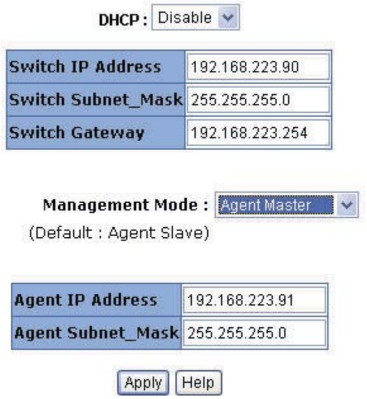
Step 3: Set up an agent function mapping port (211.23.53.252:28019->192.168.223.90:28019)



Edit Virtual Server - Microsoft Internet Explorer

Server No.	3
Virtual Server Real IP	211.23.53.252
Service Name (Port)	User-Defined
External Service Port	28019
Real Server IP	192.168.223.90

Step 4: Modify Master's "Agent IP" to new IP other than its "Switch IP" (Important)



DHCP : Disable

Switch IP Address	192.168.223.90
Switch Subnet_Mask	255.255.255.0
Switch Gateway	192.168.223.254

Management Mode : Agent Master
(Default : Agent Slave)

Agent IP Address	192.168.223.91
Agent Subnet_Mask	255.255.255.0

According to the basic rule 2 of "Single IP", if the administrator accesses the slaves from the Internet the master's Switch IP should differ from its Agent IP.

In this case, change Agent IP to 192.168.223.91 to meet the rule, even thought Switch IP and Agent IP are still within the same IP domain.

NOTE: If the administrator wishes to access the slaves from LAN, the Agent IP should be changed back to the Switch IP before launching the Agent/Stacking Manager.

Appendix A: Glossary of Terms

NUMBERS

10BASE-T 10BASE-T is Ethernet over UTP Category III,IV, or V unshielded twisted-pair media.

100BASE-TX The two-pair twisted-media implementation of 100BASE-T is called 100BASE-TX.

802.11g An IEEE standard for wireless local area networks. It offers transmissions speeds at up to 54 Mbps in the 2.4-GHz band.

A

Access point It is the hardware interface between a wireless LAN and a wired LAN. The access point attaches to the wired LAN through an Ethernet connection.

Applet Applets are small Java programs that can be embedded in an HTML page. The rule at the moment is that an applet can only make an Internet connection to the computer form that the applet was sent.

ASCII American Standard Code For Information Interchange, it is the standard method for encoding characters as 8-bit sequences of binary numbers, allowing a maximum of 256 characters.

ARP Address Resolution Protocol. ARP is a protocol that resides at the TCP/IP Internet layer that delivers data on the same network by translating an IP address to a physical address.

AVI Audio Video Interleave, it is a Windows platform audio and video file type, a common format for small movies and videos.

B

BOOTP Bootstrap Protocol is an Internet protocol that can automatically configure a network device in a diskless workstation to give its own IP address.

C

Communication Communication has four components: sender, receiver, message, and medium. In networks, devices and application tasks and processes communicate messages to each other over media. They represent the sender and receivers. The data they send is the message. The cabling or transmission method they use is the medium.

Connection In networking, two devices establish a connection to communicate with each other.

D

DHCP

Dynamic Host Configuration Protocol was developed by Microsoft a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. This simplifies the task for network administrators because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means a new computer can be added to a network without the hassle of manually assigning it a unique IP address. DHCP allows the specification for the service provided by a router, gateway, or other network device that automatically assigns an IP address to any device that requests one

DNS

Domain Name System is an Internet service that translates domain names into IP addresses. Since domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses every time you use a domain name the DNS will translate the name into the corresponding IP address. For example, the domain name *www.network_camera.com* might translate to *192.167.222.8*.

E

Enterprise network

An enterprise network consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and operates the company's mission-critical applications.

Ethernet

The most popular LAN communication technology. There are a variety of types of Ethernet, including 10 Mbps (traditional Ethernet), 100 Mbps (Fast Ethernet), and 1,000 Mbps (Gigabit Ethernet). Most Ethernet networks use Category 5 cabling to carry information, in the form of electrical signals, between devices. Ethernet is an implementation of CSMA/CD that operates in a bus or star topology.

F

Fast Ethernet

Fast Ethernet, also called 100BASE-T, operates at 10 or 100Mbps per second over UTP, STP, or fiber-optic media.

Firewall

Firewall is considered the first line of defense in protecting private information. For better security, data can be encrypted. A system designed to prevent unauthorized access to or from a private network. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially Intranets all messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

G

Gateway A gateway links computers that use different data formats together.

Group Groups consist of several user machines that have similar characteristics such as being in the same department.

H

HEX Short for hexadecimal refers to the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9 and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (8 bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

I

IEEE Institute of Electrical and Electronic Engineers.

Intranet This is a private network, inside an organization or company, that uses the same software you will find on the public Internet. The only difference is that an Intranet is used for internal usage only.

Internet The Internet is a globally linked system of computers that are logically connected based on the Internet Protocol (IP). The Internet provides different ways to access private and public information worldwide.

Internet address To participate in Internet communications and on Internet Protocol-based networks, a node must have an Internet address that identifies it to the other nodes. All Internet addresses are IP addresses

IP Internet Protocol is the standard that describes the layout of the basic unit of information on the Internet (the *packet*) and also details the numerical addressing format used to route the information. Your Internet service provider controls the IP address of any device it connects to the Internet. The IP addresses in your network must conform to IP addressing rules. In smaller LANs, most people will allow the DHCP function of a router or gateway to assign the IP addresses on internal networks.

IP address IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packets across the Internet. For example 80.80.80.69 is an IP address, it is the closet thing the Internet has to telephone numbers. When you “call” that number, using any connection methods, you get connected to the computer that “owns” that IP address.

ISP Internet Service Provider, is a company that maintains a network that is linked to the Internet by way of a dedicated communication line. An ISP offers the use of its dedicated communication lines to companies or individuals who can’t afford the high monthly cost for a direct connection.

J

JAVA

Java is a programming language that is specially designed for writing programs that can be safely downloaded to your computer through the Internet without the fear of viruses. It is an object-oriented multi-thread programming best for creating applets and applications for the Internet, Intranet and other complex, distributed network.

L

LAN

Local Area Network a computer network that spans a relatively small area sharing common resources. Most LANs are confined to a single building or group of buildings.

N

NAT

Network Address Translator generally applied by a router, that makes many different IP addresses on an internal network appear to the Internet as a single address. For routing messages properly within your network, each device requires a unique IP address. But the addresses may not be valid outside your network. NAT solves the problem. When devices within your network request information from the Internet, the requests are forwarded to the Internet under the router's IP address. NAT distributes the responses to the proper IP addresses within your network.

Network

A network consists of a collection of two or more devices, people, or components that communicate with each other over physical or virtual media. The most common types of network are:

LAN – (local area network): Computers are in close distance to one another. They are usually in the same office space, room, or building.

WAN – (wide area network): The computers are in different geographic locations and are connected by telephone lines or radio waves.

NWay Protocol

A network protocol that can automatically negotiate the highest possible transmission speed between two devices.

P

PING

Packet Internet Groper, a utility used to determine whether a specific IP address is accessible. It functions by sending a packet to the specified address and waits for a reply. It is primarily used to troubleshoot Internet connections.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as DSL or cable modem. All the users over the Ethernet share a common connection.

Protocol Communication on the network is governed by sets of rules called protocols. Protocols provide the guidelines devices use to communicate with each other, and thus they have different functions. Some protocols are responsible for formatting and presenting and presenting data that will be transferred from file server memory to the file server's net work adapter Others are responsible for filtering information between networks and forwarding data to its destination. Still other protocols dictate how data is transferred across the medium, and how servers respond to workstation requests and vice versa. Common network protocols responsible for the presentation and formatting of data for a network operating system are the Internetwork Packet Exchange (IPX) protocol or the Internet Protocol (IP). Protocols that dictate the format of data for transferors the medium include token-passing and Carrier Sense Multiple Access with Collision Detection (CSMA/CD),implemented as token-ring, ARCNET, FDDI, or Ethernet. The Router Information Protocol (RIP),a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, forwards packets from one network to another using the same network protocol.

R

RARP Reverse Address Resolution Protocol, a TCP/IP protocol that allows a physical address, such as an Ethernet address, to be translated into an IP address.

RJ-45 RJ-45 connector is used for Ethernet cable connections.

Router A router is the network software or hardware entity charged with routing packets between networks.

S

Server It is a simple computer that provides resources, such as files or other information.

SMTP The Simple Mail Transfer Protocol is used for Internet mail.

SNMP Simple Network Management Protocol. SNMP was designed to provide a common foundation for managing network devices.

Station In LANs, a station consists of a device that can communicate data on the network. In FDDI, a station includes both physical nodes and addressable logical devices. Workstations, single-attach stations, dual-attach stations, and concentrators are FDDI stations.

Subnet mask In TCP/IP, the bits used to create the subnet are called the subnet mask.

T

(TCP/IP) Transmission Control Protocol/Internet Protocol is a widely used transport protocol that connects diverse computers of various transmission methods. It was developed y the Department of Defense to connect different computer types and led to the development of the Internet.

Transceiver A transceiver joins two network segments together. Transceivers can also be used to join a segment that uses one medium to a segment that uses a different medium. On a 10BASE-5 network, the transceiver connects the network adapter or other network device to the medium. Transceivers also can be used on 10BASE-2 or 10BASE-T networks to attach devices with AUI ports.

U

UDP The User Datagram Protocol is a connectionless protocol that resides above IP in the TCP/IP suite

ULP The upper-layer protocol refers to Application Layer protocols such as FTP,SNMP, and SMTP.

User Name The USERNAME is the unique name assigned to each person who has access to the LAN.

Utility It is a program that performs a specific task.

UTP Unshielded twisted-pair. UTP is a form of cable used by all access methods. It consists of several pairs of wires enclosed in an unshielded sheath.

W

WAN Wide-Area Network. A wide-area network consists of groups of interconnected computers that are separated by a wide distance and communicate with each other via common carrier telecommunication techniques.

Windows Windows is a graphical user interface for workstations that use DOS.

Workgroup A workgroup is a group of users who are physically located together and connected to the same LAN, or a group of users who are scattered throughout an organization but are logically connected by work and are connected to the same network group.

Workstations Workstation refers to the intelligent computer on the user's desktop. This computer may be an Intel-based PC, a Macintosh, or a UNIX-based workstation. The workstation is any intelligent device a user works from.

Appendix B: Cable Information

This cable information is provided for your reference only. Please ensure you only connect the appropriate cable into the correct socket on either this product or your computer.

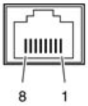
If you are unsure about which cable to use or which socket to connect it to, please refer to the hardware installation section in this manual. If you are still not sure about cable connections, please contact a professional computer technician or NetComm for further advice.

RJ-45 Network Ports

RJ-45 Network Ports can connect any networking devices that use a standard LAN interface, such as a Hub/Switch Hub or Router. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable to connect the networking device to the RJ-45 Ethernet port. Depending on the type of connection, 10Mbps or 100Mbps, use the following Ethernet cable, as prescribed.

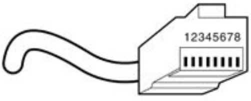
10Mbps:	Use EIA/TIA-568-100-Category 3, 4 or 5 cable.
100Mbps:	Use EIA/TIA-568-100-Category 5 cable.

Note: To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.



RJ-45 Connector Pin Assignment	Normal Assignment
1	Input Receive Data +
2	Input Receive Data -
3	Output Transmit Data +
6	Output Transmit Data -
4,5,7,8	Not used

Figure 1



RJ-45 plug attached to cable

Figure 2

Straight and crossover cable configuration

There are two types of the wiring: Straight-Through Cables and Crossover Cables. Category 5 UTP/STP cable has eight wires inside the sheath. The wires form four pairs. Straight-Through Cables has same pinouts at both ends while Crossover Cables has a different pin arrangement at each end.

In a straight-through cable, wires 1,2,3,4,5,6,7 and 8 at one end of the cable are still wires 1~8 at the other end. In a crossover cable, the wires of 1,2,3,6 are reversed so that wire 1 become 3 at the other end of the cable, 2 becomes 6, and so forth.

To determine which wire is wire 1, hold the RJ-45 cable tip with the spring clip facing towards the ground and the end pointing away from you. The copper wires exposed upwards to your view. The first wire on the far left is wire 1. You can also refer to the illustrations and charts of the internal wiring on the following page.

Straight-Through Cabling

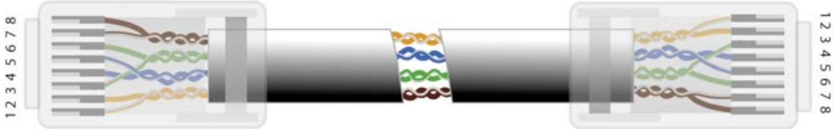


Figure 3

Wire	Becomes
1	1
2	2
3	3
6	6

Cross-Over Cabling

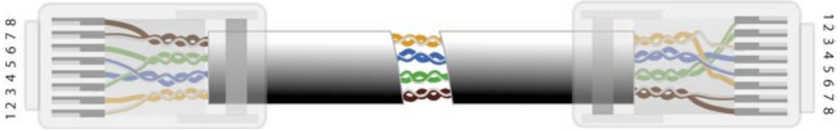


Figure 4

Wire	Becomes
1	3
2	6
3	1
6	2

Note: To prevent loss of signal, make sure that the length of any twisted-pair connection does not exceed 100 metres.

Appendix C: Registration and Warranty Information

All NetComm Limited ("NetComm") products have a standard 12 month warranty from date of purchase against defects in manufacturing and that the products will operate in accordance with the specifications outlined in the User Guide. However some products have an extended warranty option (please refer to your packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at:

www.netcomm.com.au

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email:	support@netcomm.com.au
Fax:	(+612) 9424-2010
Web:	www.netcomm.com.au

Copyright Information

NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product. Please note that the images used in this document may vary slightly from those of the actual product. Specifications are accurate at the time of the preparation of this document but are subject to change without notice.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice. NetComm is a registered trademark of NetComm Limited. All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

(1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.

(2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:

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

(3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

NetComm®
Broadband Solutions

NETCOMM LIMITED ABN 85 002 490 486
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: sales@netcomm.com.au **W:** www.netcomm.com.au