CTS

CONNECTION TECHNOLOGY SYSTEMS

HET-2106 SERIES

5 ports 10/100Mbps RJ-45 + 1 port 100Mbps fiber optics uplink Managed Ethernet CPE Switch

Network Management

User's Manual

Version 0.97

Trademarks

CTS is a registered trademark of Connection Technology Systems Inc.
Contents subject to revise without prior notice.
All other trademarks remain the property of their owners.

Copyright Statement

Copyright © Connection Technology Systems Inc.
This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from Connection Technology Systems Inc.

FCC Warning

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into a different outlet from that the receiver is connected.
- Consult your local distributors or an experienced radio/TV technician for help.
- Shielded interface cables must be used in order to comply with emission limits.

Changes or modifications to the equipment, which are not approved by the party responsible for compliance, could affect the user's authority to operate the equipment.

Copyright © 2010 All Rights Reserved.

Company has an on-going policy of upgrading its products and it may be possible that information in this document is not up-to-date. Please check with your local distributors for the latest information. No part of this document can be copied or reproduced in any form without written consent from the company.

Trademarks:
All trade names and trademarks are the properties of their respective companies.

Table of Content

1. INTRODUCTION

Thank you for using the 5-Port 10/100TX plus 1-Port 100FX Uplink & 6-Port 10/100Base-TX Fast Ethernet Smart Switch. The built-in management module allows users to configure this Smart Switch and monitor the operation status locally or remotely through network.

The Smart Switch is fully compliant with IEEE 802.3 and 802.3u standards. By employing store and forward switching mechanism, the Smart Switch provides low latency and faster data transmission. Moreover, it also supports more advanced functions such as QoS, Q-in-Q VLAN Tunneling, Rate Limiting, IGMP Snooping, etc. Users can configure the required settings of the Smart Switch and monitor its real-time operational status via Command Line Interface and Web Management. For detailed description on both management methods, please refer to Section 2 and 3 respectively.

1.1 Interfaces

The Smart Switch Series provides two models with different interfaces. Depending on your networking requirements, you can select the most suitable one to apply in your networking environment. Figure 1 below displays the interface with five 10/100 LAN ports; whereas, Figure 2 shows one WAN TP and five 10/100 LAN ports.

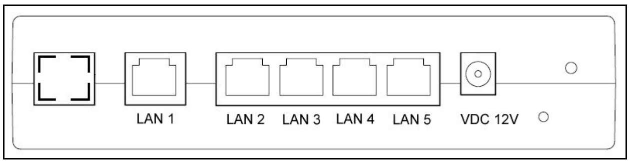


Figure 1. 5 10/100 LAN Ports

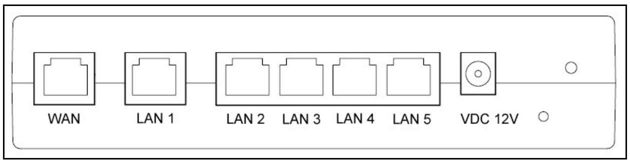


Figure 2. 1 WAN TP Port & 5 10/100 LAN Ports

Both models have the same top panel that displays LED indicators for each LAN connection and link status.

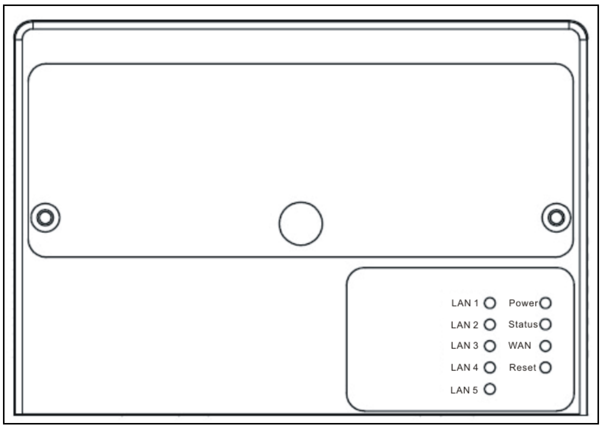


Figure 3. Top Panel with LED Indicators

1.2 Management Preparations

The Smart Switch can be accessed through Telnet connection or a web browser, such as Internet Explorer or Netscape, etc. Before you can access to the Smart Switch to configure it, you need to connect cables properly.

Connecting the Smart Switch

It is extremely important that proper cables are used with correct pin arrangements when connecting Smart Switch to other devices such as switches, hubs, workstations, etc.

100Base-FX Fiber Port

1x100Base-FX fiber port is located inside the Smart Switch. This port is primarily used for up-link connection and will operate at 100M/Full or Half Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with the other Fast Ethernet Fiber port.

Before connecting to other switches, workstation or media converter, make sure both sides of the fiber transfer are with the same media type, for example 100Base-FX Single-mode to 100Base-FX Single-mode, 100Bas-FX Multimode to 100Base-FX Multimode. And check that the fiber-optic cable type matches the fiber transfer model. To connect to 100Base-FX transfer, use the multi-mode fiber cable (one side must be male duplex SC connector type). To connect to 100Base-FX transfer, use the single-mode fiber cable (one side must be male duplex SC connector type).

10/100Base-TX RJ-45 Ports

5 or 6 10/100Base-TX RJ-45 ports are located on the front panel of the Smart Switch depending on the model that you purchased. These RJ-45 ports allow users to connect their traditional copper based Ethernet/Fast Ethernet devices into network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5 cable may be used.

Assigning IP Addresses

IP addresses have the format n.n.n.n, for example 168.168.8.100.

IP addresses are made up of two parts:

- The first part (168.168.XXX.XXX in the example) refers as network address identifies the network on which the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.

- The second part (XXX.XXX.8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult the allocation organization from which your IP addresses were obtained.

Remember that no two devices on a network can have the same address. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not operate.

A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for proper operation of a network with subnets defined.

1.3 LED Definitions

LED	Color	Operation
Power	Off	System is power down.
	Green	System is power up.
Status	Green	System is working normally.
		When the system is set back to default factory setting, the Status LED indicator will blink three times.
WAN	Off	Fiber link is down.
	Green	Fiber link is up.
		Blinking when traffic is present.
LAN1~LAN5	Off	Link is down.
	Green	Link is up.
		Blinking when traffic is present.

2. Command Line Interface (CLI)

This chapter introduces you how to use Command Line Interface (CLI) via Telnet connection, specifically in:

- Configuring the system
- Resetting the system
- Upgrading newly released firmware

2.1 Remote Console Management-Telnet

You can use Command Line Interface to manage the Smart Switch via Telnet session. For first-time users, you must first assign a unique IP address to the Smart Switch before you can manage it remotely. Use any one of the RJ-45 ports on the front panel as the temporary management console port to login to the Smart Switch with the default username & password and then assign the IP address using IP command in Global Configuration mode.

Follow steps described below to access the Smart Switch through Telnet session:

Step 1. Use any one of the RJ-45 ports as a temporary management console port to login to the Smart Switch.

Step 2. Run Telnet client and connect to *192.168.0.1*. For first-time users, make sure the IP address of your PC or workstation is assigned to an IP address between 192.168.0.2 and 192.168.0.254 with subnet mask 255.255.255.0.

Step 3. When asked for a username, enter "***admin***". When asked for a password, *leave the password field blank* and press Enter (by default, no password is required.)

Step 5. If you enter CLI successfully, the prompt display *Switch*> (the model name of your device together with a greater than sign) will appear on the screen.

Step 6. Set up the Smart Switch's IP address, subnet mask and the default gateway using "IP" command in Global Configuration mode.

Step 7. Once you enter new IP address for the Smart Switch, the telnet session will be terminated immediately. Use your new IP address to login to the Smart Switch via Telnet session.

Limitation: Only one active Telnet session can access the Smart Switch at a time.

2.2 Navigating CLI

When you successfully access the Smart Switch, you will be asked for a login username. Enter your authorized username and password, and then you will be directed to User mode. In CLI management, the User mode only provides users basic functions to operate the Smart Switch. If you would like to configure advanced features of the Smart Switch, such as, VLAN, QoS, Rate limit control, you must enter the Configuration mode. The following table provides an overview of modes available in this Smart Switch.

Command Mode	Access Method	Prompt Displayed	Exit Method
User mode	Login username & password	Switch>	logout
Privileged mode	From user mode, enter the *enable* command	Switch#	disable, exit, logout
Configuration mode	From the enable mode, enter the *config* or *configure* command	Switch(config)#	exit

***NOTE:** By default, the model name will be used for the prompt display. You can change the prompt display to the one that is ideal for your network environment using the hostname command. However, for convenience, the prompt display "Switch" will be used throughout this user's manual.*

2.2.1 General Commands

This section introduces you some general commands that you can use in User, Enable, and Configuration mode, including "help", "exit", "history" and "logout".

Entering the command…	To do this…	Available Modes
help	Obtain a list of available commands in the current mode.	User Mode Privileged Mode Configuration Mode
exit	Return to the previous mode or login screen.	User Mode Privileged Mode Configuration Mode
history	List all commands that have been used.	User Mode Privileged Mode Configuration Mode
logout	Logout from the CLI or terminate Telnet session.	User Mode Privileged Mode

2.2.2 Quick Keys

In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

Keys	Purpose
tab	Enter an unfinished command and press "Tab" key to complete the command.
?	Press "?" key in each mode to get available commands.

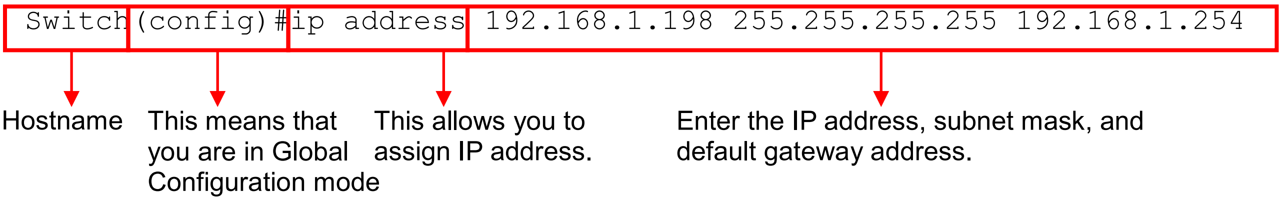
unfinished command followed by ?	Enter an unfinished command or keyword and press "?" key to complete the command and get command syntax help.
	Example 1: List all available commands starting with the characters that you enter.
	`Switch#h?`
	`help                          Show available commands`
	`history                       Show history commands`
	`Switch#he?`
	`<cr>`
	`Switch#help`
	Example 2: Complete a valid command and show the next part of syntax.
	`Switch(config)#sec?`
	`storm-protection              Storm control subcommands`
	`Switch(config)#security`

Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.2.3 Command Format

While in CLI, you will see several symbols very often. As mentioned above, you might already know what ">", "#" and (config)# represent. However, to perform what you intend the device to do, you have to enter a string of complete command correctly. For example, if you want to assign IP address for the Smart Switch, you need to enter the following command with the required parameter and IP, subnet mask and default gateway:

IP command syntax: `Switch(config)#ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]`



```
Switch(config)#ip address 192.168.1.198 255.255.255.255 192.168.1.254
```

Hostname
This means that you are in Global Configuration mode
This allows you to assign IP address.
Enter the IP address, subnet mask, and default gateway address.

The following table lists common symbols and syntax that you will see very frequently in this User's Manual for your reference:

Symbols	Brief Description
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.

Syntax	Brief Description
[ ]	Brackets mean that this field is required information.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port-based | 802.1p | dscp]	There are three options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

[0-7] 802.1p_list
[0-63] dscp_list
	Specify one value, more than one value or a range of values.
	For example: specifying one value
	`Switch(config)#qos 802.1p-map 1 0`
	`Switch(config)#qos dscp-map 10 3`
	For example: specifying three values (separating by a comma)
	`Switch(config)#qos 802.1p-map 1,3 0`
	`Switch(config)#qos dscp-map 10,13,15 3`
	For example: specifying a range of values (separating by a hyphen)
	`Switch(config)#qos 802.1p-map 1-3 0`
	`Switch(config)#qos dscp-map 10-15 3`

2.3 User Mode

In User mode, only a limited set of commands are provided. Please note that in Use mode, you have no authority to configure advanced settings. You need to enter Enable mode and Configuration mode to set up advanced functions of a switch feature. For a list of commands available in User mode, enter the question mark (?) or "help" command after the system prompt display Switch>.

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Smart Switch.
enable	Enter the Privileged mode.

2.4 Privileged mode

The only place where you can enter the Privileged (Enable) mode is in User mode. When you successfully enter Enable mode, the prompt will be changed to Switch# (the model name of your device together with a pound sign). Enter the question mark (?) or help command to view a list of commands available for use.

Command	Description
copy-cfg	Restore or backup configuration file via TFTP server.
configure	Enter Global Configuration mode.
disable	Exit Enable mode and return to User Mode.
exit	Exit Enable mode and return to User Mode.
firmware	Upgrade Firmware via TFTP.
help	Display a list of available commands in Enable mode.
history	Show commands that have been used.
logout	Logout from the Managed Switch.
reload	Restart the Managed Switch.
write	Save your configurations to Flash.
show	Show a list of commands or show the current setting of each listed command.

2.4.1 Copy-cfg command

Use "copy-cfg" command to backup a configuration file via TFTP server or restore the Smart Switch back to the defaults or to the defaults but keep IP configurations.

1. Restore a configuration file via TFTP server.

Command	Parameter	Description
Switch# copy-cfg from tftp [A.B.C.D] [file name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file name]	Enter the configuration file name that you want to restore.
Example		
Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. Restore the Smart Switch back to default settings.

Command / Example
Switch# copy-cfg from default

3. Restore the Smart Switch back to default settings but keep IP configurations.

Command / Example
Switch# copy-cfg from default keep-ip

4. Backup a configuration file to TFTP server.

Command	Parameter	Description
Switch# copy-cfg to tftp [A.B.C.D] [file name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file name]	Enter the configuration file name that you want to backup.
Example		
Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf		

2.4.2 Firmware command

Upgrade the latest Firmware version.

Command	Parameter	Description
Switch# firmware upgrade tftp [A.B.C.D] [file name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file name]	Enter the Firmware file name that you want to upgrade.
Example		
Switch# firmware upgrade tftp 192.168.1.198 HS_0600_FW_1.00.00_20110101.bin		

2.4.3 Reload command

To restart the Smart Switch, enter the reload command.

Command / Example
Switch# reload

2.4.4 Write command

To save running configurations to startup configurations, enter the write command. All unsaved configurations will be lost when you restart the Smart Switch.

Command / Example
Switch# write

2.4.5 Configure command

The only place where you can enter Global Configuration mode is in Privileged mode. You can type in “configure” or “config” for short to enter Global Configuration mode. The display prompt will change from “Switch#” to “Switch(config)#” once you successfully enter Global Configuration mode.

Command / Example
Switch#config Switch(config)#
Switch#configure Switch(config)#

2.5 Configuration mode

When you enter “configure” or “config” and press “Enter” in Privileged mode, you will be directed to Global Configuration mode where you can set up advanced switching functions, such as QoS, VLAN and storm control security globally. Any commands entered will apply to running-configuration and the device’s operation. From this level, you can also enter different sub-configuration modes to set up specific configurations for VLAN, QoS, security or interfaces.

Command	Description
exit	Exit the configuration mode.
help	Display a list of available commands in Configuration mode.
history	Show commands that have been used.
ip	Set up the IP address and enable DHCP mode & IGMP snooping.
mac	Set up each port’s MAC learning function.
qos	Set up the priority of packets within the Managed Switch.
security	Configure broadcast, multicast, unknown unicast storm control settings.
snmp-server	Create a new SNMP community and trap destination and specify the trap types.
switch-info	Set up acceptable frame size and address learning, etc.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
no	Disable a command or set it back to its default setting.
interface	Select a single interface or a range of interfaces.
show	Show a list of commands or show the current setting of each listed command.

2.5.1 Entering Interface Numbers

In the Global Configuration mode, you can configure a command that only apply to interfaces specified. For example, you can set up each interface's VLAN assignment, speeds, or duplex modes. To configure, you must first enter the interface number. There are four ways to enter your interface numbers to signify the combination of different interfaces that apply to a command or commands.

Commands	Description
Switch(config)# interface 1 Switch(config-if)#	Enter a single interface. Only interface 1 will apply to commands entered.
Switch(config)# interface 1,3,5 Switch(config-if)#	Enter three discontinuous interfaces, separating by a comma. Interface 1, 3, 5 will apply to commands entered.
Switch(config)# interface 1-3 Switch(config-if)#	Enter three continuous interfaces. Use a hyphen to signify a range of interface numbers. In this example, interface 1, 2, and 3 will apply to commands entered.
Switch(config)# interface 1,3-5 Switch(config-if)#	Enter a single interface number together with a range of interface numbers. Use both comma and hyphen to signify the combination of different interface numbers. In this example, interface 1, 3, 4, 5 will apply to commands entered.

The "interface" command can be used together with "QoS" and "VLAN" commands. For detailed usages, please refer to QoS and VLAN section below.

2.5.2 No command

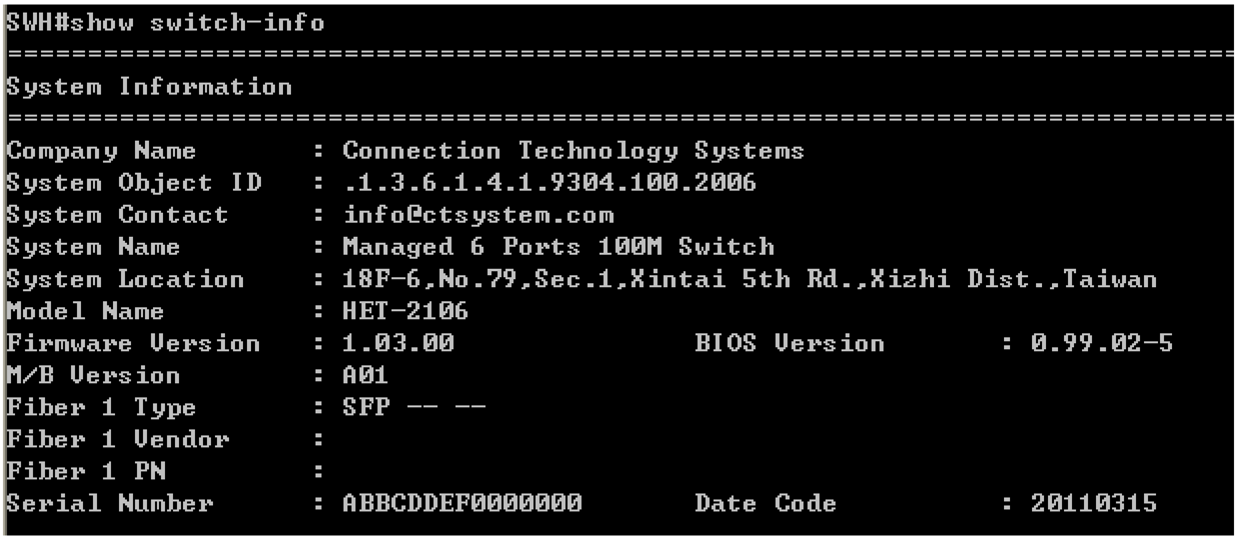
Almost commands that you enter in Configuration mode can be negated using "no" command followed by the original command. The purpose of "no" command is to disable a function, remove a command, or set the setting back to the default value. In each sub-section below, the use of no command to fulfill different purposes will be introduced.

2.5.3 Show command

"show" command is very important for network administrators to get information about the device, receive outputs to verify a command's configurations or troubleshoot a network configuration error. "Show" command can be either used in Privileged or Configuration mode. The following describes different uses of "show" command.

1. Display system information

Enter “show switch-info” command in Privileged or Configuration mode, then the following similar screen page will appear.



```
SWH#show switch-info
=============================================================================
System Information
=============================================================================
Company Name        : Connection Technology Systems
System Object ID    : .1.3.6.1.4.1.9304.100.2006
System Contact      : info@ctsystem.com
System Name         : Managed 6 Ports 100M Switch
System Location     : 18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
Model Name          : HET-2106
Firmware Version    : 1.03.00              BIOS Version       : 0.99.02-5
M/B Version         : A01
Fiber 1 Type        : SFP -- --
Fiber 1 Vendor      :
Fiber 1 PN          :
Serial Number       : ABBCDDEF0000000      Date Code          : 20110315
```

Company Name: Display a company name for this Smart Switch. Use “switch-info company-name [company-name]” command to edit this field.

System Object ID: Display the predefined System OID.

System Contact: Display contact information for this Smart switch. Use “switch-info sys-contact [sys-contact]” command to edit this field.

System Name: Display a descriptive system name for this Smart Switch. Use “switch-info sys-name [sys-name]” command to edit this field.

System Location: Display a brief location description for this Smart Switch. Use “switch-info sys-location [sys-location]” command to edit this field.

Model Name: Display the product’s model name.

Firmware Version: Display the firmware version used in this device.

M/B Version: Display the main board version.

Fiber Type: Display information about the slide-in or fixed fiber type.

Fiber Wavelength: Display the slide-in or fixed fiber’s TX and RX wavelength information.

Serial Number: Display the serial number of this Smart Switch.

Date Code: Display the Smart Switch Firmware date code.

2. Display or verify currently-configured settings

Refer to “Interface command”, “IP command”, “MAC command”, “QoS command”, “Security command”, “SNMP-Server command”, “User command”, “VLAN command” sections.

3. Display interface information or statistics

Refer to “Show interface statistics command” and “Show sfp information command” sections.

2.5.4 Interface command

Use this command to set up various port configurations of discontinuous or a range of ports.

Command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several port numbers separating by a comma or a range of port numbers. For example: 1,3 or 2-4
Switch(config-if)# speed [100 | 10]	[100 | 10]	Set up the selected interfaces’ speed. Speed configuration only works when “no auto-negotiation” command is issued.
Switch(config-if)# auto-negotiation		Set the selected interfaces’ to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
Switch(config-if)# duplex full		Set the selected interfaces’ to full duplex mode.
Switch(config-if)# flowcontrol		Enable the selected interfaces’ flow control function.
Switch(config-if)# shutdown		Administratively disable the selected ports’ status.
No command		
Switch(config-if)# no auto-negotiation		Set auto-negotiation setting to the default setting.
Switch(config-if)# no duplex		Set the selected ports’ duplex mode to the default setting.
Switch(config-if)# no flowcontrol		Set the selected ports’ flow control function to the default setting.
Switch(config-if)# no shutdown		Administratively enable the selected ports’ status.
Switch(config-if)# no speed		Set the selected ports’ speed to the default setting.
Show command		
Switch(config)# show interface status		Show each interface’s port status including media type, forwarding state, speed, duplex mode, flow control and link

	up/down status.
Interface command example	
Switch(config)# interface 1-3	Enter port 1 to port 3’s interface mode.
Switch(config-if)# auto-negotiation	Set the selected interfaces’ to auto-negotiation.
Switch(config-if)# duplex full	Set the selected interfaces’ to full duplex mode.
Switch(config-if)# flowcontrol	Enable the selected interfaces’ flow control function.
Switch(config-if)# speed 100	Set the selected ports’ speed to 100Mbps.
Switch(config-if)# shutdown	Administratively disable the selected ports’ status.

2.5.5 IP command

1. Set up or remove the IP address of the Smart Switch.

IP command	Parameter	Description
Switch(config)# ip address [A.B.C.D] [255.X.X.X] [A.B.C.D]	[A.B.C.D]	Enter the desired IP address for your Smart Switch.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway address.
No command		
Switch(config)# no ip address		Remove the Smart Switch’s IP address.
Show command		
Switch(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
IP command example		
Switch(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the Smart Switch’s IP to 192.168.1.198, subnet mask to 255.255.255.0, and default gateway to 192.168.1.254.

2. Enable the Smart Switch to automatically get IP address from the DHCP server.

Command / Example	Description
Switch(config)# ip address dhcp	Enable DHCP mode.
No command	
Switch(config)# no ip address dhcp	Disable DHCP mode.
Show command	

Switch(config)# show ip address	Show the current IP configurations or verify the configured IP settings.

3. Enable or disable IGMP snooping globally.

IGMP, Internet Group Management Protocol, is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. A switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

Command / Example	**Description**
Switch(config)# ip igmp snooping	Enable IGMP snooping function.
No command	
Switch(config)# no ip igmp snooping	Disable IGMP snooping function.
Show command	
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including immediate leave function.
Switch(config)# show ip igmp snooping groups	Show IGMP group table. When IGMP Snooping is enabled, the Smart Switch is able to read multicast group IP and the corresponding MAC address from IGMP packets that enter the device.

4. Enable IGMP snooping immediate-leave function. This works only when IGMP Snooping is enabled. When Immediate Leave is enabled, the Smart Switch immediately removes the port when it detects IGMPv1 & IGMPv2 leave message on that port.

Command / Example	Description
Switch(config)# ip igmp snooping immediate-leave	Enable IGMP immediate leave function.
No command	
Switch(config)# no ip igmp snooping immediate-leave	Disable IGMP immediate leave function.
Show command	
Switch(config)# show ip igmp snooping	Show current IGMP snooping status including immediate leave function.
Switch(config)# show ip igmp snooping groups	Show IGMP group table.

2.5.6 MAC command

Set up MAC address table aging time. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within aging time.

MAC Command	Parameter	Description
Switch(config)# mac address-table aging time [0-4080]	[0-4080]	Enter the aging time for MAC addresses in seconds.
No command		
Switch(config)# no mac address-table aging-time		Set MAC address table aging time to the default value (300 seconds).
Show command		
Switch(config)# show mac aging-time		Show current MAC address table aging time or verify currently configured aging time.
MAC command example		
Switch(config)# mac address-table aging time 200		Set MAC address aging time to 200 seconds.

2.5.7 QoS command

1. Specify the desired QoS mode.

QoS command	Parameter	Description
Switch(config)# qos [port-based | 802.1p | dscp]	[port-based | 802.1p | dscp]	Specify one QoS mode. **port-based:** Use "*interface*" and "*qos default-class*" command to assign a queue to the selected interfaces. **802.1p:** Use *"qos 802.1p_map"* command to assign priority bits to a queue. **dscp:** Use "*qos dscp-map [0-63] dscp_list [0-7]*" to assign several DSCP values to a priority value.
No command		**Description**
Switch(config)# no qos		Disable QoS function.
Show command		**Description**
Switch(config)# show qos		Show or verify QoS configurations.
QoS command example		
Switch(config)# qos 802.1p		Enable QoS function and use 802.1p mode.
Switch(config)# qos dscp		Enable QoS function and use DSCP mode.
Switch(config)# qos port-based		Enable QoS function and use Port-Based mode.

2. Set up the DSCP and queue mapping.

DSCP-map command	Parameter	Description
Switch(config)# qos dscp-map [0-63] dscp_list [0-3]	[0-63] dscp_list	Specify the corresponding DSCP value or values that you want to map to a priority queue value.
	[0-3]	Specify a queue value from 0 to 3.
No command		
Switch(config)# no qos		Disable QoS function
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
DSCP-map example		
Switch(config)# qos dscp-map 10-50 3		Mapping DSCP values from 10 to 50 to priority queue value 3.

3. Set up QoS queuing mode.

Queuing-mode command	Parameter	Description
Switch(config)# qos queuing-mode [weight]	[weight]	By default, “weight” queuing mode is used. If you want to use “strict” queuing mode, you need to disable “weight” queuing mode. **Strict mode:** This indicates that services to each egress queues are offered based on rates specified. Use *“qos rate-limit egress [0-7] [rate]”* to specify egress rate in Strict mode. **Weight mode**: This mode enables users to assign different weights to 4 queues. Use *“qos queue-weighted [0-4]”* to specify egress rate in Weight mode.
No command		
Switch(config)# no qos queuing-mode		Set the queuing mode to Strict mode.
Show command		
Switch(config)# show qos		Show or verify QoS configurations.
Queuing-mode example		
Switch(config)# qos queuing-mode weight		Change the queuing mode from strict to weight.

4. Assign a tag priority to the specific queue.

<table>
<tr><th>802.1p-map command</th><th>Parameter</th><th>Description</th></tr>
<tr><td rowspan="2">Switch(config)# qos 802.1p-map [0-7] 802.1p_list [0-3]</td><td>[0-7] 802.1p_list</td><td>Assign a 802.1p priority bit or several 802.1p priority bits for mapping.
Set up the corresponding priority value
<table>
<tr><td>Priority Level</td><td>Low</td><td>Low</td><td>Low</td><td>Normal</td><td>Medium</td><td>Medium</td><td>High</td><td>High</td></tr>
<tr><td>802.1p Value</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
</table></td></tr>
<tr><td>[0-3]</td><td>Assign a queue value for mapping.</td></tr>
<tr><th colspan="2">No command</th><th></th></tr>
<tr><td>Switch(config)# no qos 802.1p-map [0-7] 802.1p_list</td><td>[0-7] 802.1p_list</td><td>Assign a 802.1p priority bit or several 802.1p priority bits that you want to delete or remove.</td></tr>
<tr><th colspan="2">Show command</th><th></th></tr>
</table>

Switch(config)# show qos	Show or verify QoS configurations.
802.1p-map example	
Switch(config)# qos 802.1p-map 6-7 3	Map priority bit 6 and 7 to queue 4.
Switch(config)# no qos 802.1p-map 6-7	Delete or remove 802.1p priority bit 6 and 7’s mapping.

5. Use interface command to set up default class, a tag priority to the specific queue and ingress & egress rate limit.

QoS & Interface command	Parameter	Description
Switch(config)# interface [port_list]	[port_list]	Enter several port numbers separating by a comma or a range of port numbers. For example: 1,3 or 2-4
Switch(config-if)# qos default-class [0-3]	[0-3]	Specify the selected interfaces’ default queue.
Switch(config-if)# qos rate-limit ingress [1-1600]	[1-1600]	Specify the ingress rate between 1 and 1600. The actual ingress rate will be the ingress rate specified times 64Kbps.
Switch(config-if)# qos rate-limit egress [0-3] [1-1600]	[0-3]	Specify a queue.
	[1-1600]	Specify a queue rate limit between 1 and 1600. The actual egress rate will be the egress rate specified times 64Kbps.
Switch(config-if)# qos queue-weighted [0-4]	[0-4]	Set up the queue weight of the selected interfaces. **0**: The weighting is 1:1:1:1 **1**: The weighting is 1:2:4:8 **2**: The weighting is 1:3:6:15 **3**: The weighting is 1:4:8:24 **4**: The weighting is 1:5:10:35
No command		
Switch(config-if)# no qos default-class		Set QoS default class setting back to defaults.
Switch(config-if)# no qos rate-limit ingress		Delete QoS ingress rate limit setting.
Switch(config-if)# no qos rate-limit egress [0-4]		Specify the rate limit setting of a certain egress queue that you want to delete or remove.
Switch(config-if)# no qos queue-weighted		Delete QoS queue weighted setting.

Show command	
Switch(config)# show qos	Show or verify QoS configurations.
QoS & Interface example	
Switch(config)# interface 1-3	Enter several discontinuous port numbers separating by a comma or a range of ports with a hyphen. For example:1,3 or 2-4
Switch(config-if)# qos default-class 3	Set the selected ports' default class to 3.
Switch(config-if)# qos rate-limit ingress 1550	Configure the selected interfaces' ingress rate-limit to 1550.
Switch(config-if)# qos rate-limit egress 3 1550	Set the selected interfaces' queue 3 to egress rate 1550.
Switch(config-if)# qos queue-weighted 0	Set the weighting of Weight queuing mode to 1:1:1:1. This setting applies to the Smart Switch only when Weight queuing mode is enabled.

2.5.8 Security command

When a device on the network is malfunctioning or application programs are not well designed or properly configured, broadcast storms may occur, degrade network performance or in the worst situation cause a complete halt. The Smart Switch allows users to set a threshold rate for broadcast traffic on a per switch basis so as to protect network from broadcast/multicast/unknown unicast storms. Any broadcast/multicast/unknown unicast packets exceeding the specified value will then be dropped.

1. Enable or disable broadcast/multicast/unknown unicast storm control.

Security command / example	Description
Switch(config)# security storm-protection broadcast	Enable broadcast storm control.
Switch(config)# security storm-protection multicast	Enable multicast storm control.
Switch(config)# security storm-protection unicast	Enable unicast storm control.
No command	
Switch(config)# no security storm-protection broadcast	Disable broadcast storm control.
Switch(config)# no security storm-protection multicast	Disable multicast storm control.
Switch(config)# no security storm-protection unicast	Disable unicast storm control.
Show command	
Switch(config)# show security storm-protection	Show current security settings including storm control rates.

2. Specify the broadcast, multicast, and unicast storm protection rates per second.

Security command	Parameter	Description
Switch(config)# security storm-protection rates [1-8191]	[1-8191]	Enter the maximum rate per second. (x20 frames/sec) Any broadcast, multicast, and unicast packets exceeding the specified value will be dropped.
Security command example		
Switch(config)# security storm-protection rates 5000		Set broadcast, multicast, and unicast storm protection rates to 5000.
No command		
Switch(config)# no security storm-protection rates		Remove the rate setting. The storm protection rate will be set to the default (8191 x 20 frames/second).
Show command		
Switch(config)# show security storm-protection		Show current security settings including storm control rates.

2.5.9 SNMP-Server command

1. Create a SNMP community and set up detailed configurations for this community.

Snmp-server command	Parameter	Description
Switch(config)# snmp-server community [community]	[community]	Specify a SNMP community name of up to 20 alphanumeric characters.
Switch(config-snmp-server)# active		Enable this SNMP community account.
Switch(config-snmp-server)# description [Description]	[Description]	Enter the description for this SNMP community of up to 35 alphanumerical characters.
Switch(config-snmp-server)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. By default, when you create a community, the access privilege for this account is set to “read only”. **admin:** Full access right includes maintaining user account, system information, loading factory settings, etc. **rw:** Read & Write access privilege. Full access right but cannot modify system information, user account, load factory

	settings and upgrade firmware. **ro:** Read Only access privilege. Allow to view only.
No command	
Switch(config)#no snmp-server community mycomm	Delete the community “mycomm”.
Switch(config-snmp-server)#no active	Disable this SNMP community account. In this example “mycomm” community is disabled.
Switch(config-snmp-server)#no description	Remove the entered SNMP community descriptions for “mycomm”.
Switch(config-snmp-server)#no level	Remove the configured level. This will set this community’s level to access_denied.
Show command	
Switch(config)#show snmp-server community mycomm	Show SNMP community account’s information in Global Configuration mode.
Switch(config-snmp-server)#show	View or verify the configured SNMP community account’s information.
Exit command	
Switch(config-snmp-server)#exit	Return to Global Configuration mode.
Snmp-server example	
Switch(config)# snmp-server community mycomm	Create a new community “mycomm” and edit the details of this community account.
Switch(config-snmp-server)#active	Activate the SNMP community “mycomm”.
Switch(config-snmp-server)#description rddeptcomm	Add a description for “mycomm” community.
Switch(config-snmp-server)#level admin	Set “mycomm” community level to admin.

2. Set up a SNMP trap destination.

Trap-dest command	Parameter	Description
Switch(config)# snmp-server trap-destination [1]	[1]	Create a trap destination account.
Switch(config-snmp-server)# active		Enable this SNMP trap destination account.
Switch(config-snmp-server)# community [community]	[community]	Enter the community name of network management system.
Switch(config-snmp-server)# destination [A.B.C.D]	[A.B.C.D]	Enter the trap destination IP address for this trap destination account.
No command		
Switch(config)# no snmp-server trap-destination 1		Delete a trap destination account.
Switch(config-snmp-server)# no active		Disable this SNMP trap destination account.
Switch(config-snmp-server)# no community		Delete the configured community name.
Switch(config-snmp-server)# no description		Delete the configured trap destination description.
Show command		
Switch(config)# show snmp-server trap-destination 1		Show SNMP trap destination information in Global Configuration mode.
Switch(config-snmp-server)# show		View this trap destination account's information.
Exit command		
Switch(config-snmp-server)# exit		Return to Global Configuration mode.
Trap-dest example		
Switch(config)# snmp-server trap-destination 1		Create a trap destination account.
Switch(config-snmp-server)# active		Activate the trap destination account.
Switch(config-snmp-server)# community mycomm		Refer this trap destination account to the community "mycomm".
Switch(config-snmp-server)# description redepttrapdest		Add a description for this trap destination account.
Switch(config-snmp-server)# destination 192.168.1.254		Set trap destination IP address to 192.168.1.254.

3. Set up SNMP trap types that will be sent.

Trap-type command	Parameter	Description
Switch(config)# snmp-server trap-type [all |auth-fail | cold-start | port-link | power-down | warm-start]	all |auth-fail | cold-start | port-link | power-down | warm-start]	Specify the trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down and power is down. **auth-fail:** A trap will be sent when any unauthorized users attempt to login. **cold-start:** A trap will be sent when the device boots up. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device's power is down. **warm-start:** A trap will be sent when the device restarts.
No command		
Switch(config)#no snmp-server trap-type auth-fail		Authentication failure trap will not be sent.
Show command		
Switch(config)#show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
Switch(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

2.5.10 Switch-info command

1. Set up the Smart Switch's basic information including company name, hostname, system name, etc.

Switch-info Command	Parameter	Description
Switch(config)# switch-info company-name [company-name]	[company-name]	Enter a company name for this Smart Switch, up to 55 alphanumeric characters.
Switch(config)# switch-info system-contact [system-contact]	[system-contact]	Enter contact information for this Managed switch, up to 55 alphanumeric characters.
Switch(config)# switch-info system-location [system-location]	[system-location]	Enter a brief description of the Managed Switch location, up to 55 alphanumeric characters. Like the name, the location is for reference only, for example, "13th Floor".
Switch(config)# switch-info system-name [system-name]	[system-name]	Enter a unique name for this Managed Switch, up to 55 alphanumeric characters. Use a descriptive name to identify the Managed Switch in relation to your network, for example, "Backbone 1". This name is mainly used for reference only.
No command		
Switch(config)# no switch-info company-name		Delete the entered company name information.
Switch(config)# no switch-info system-contact		Delete the entered system contact information.
Switch(config)# no switch-info system-location		Delete the entered system location information.
Switch(config)# no switch-info system-name		Delete the entered system name information.
Show command		
Switch(config)# show switch-info		Show switch information including company name, system contact, system location, system name, model name, firmware version and fiber type.
Switch-info example		
Switch(config)# switch-info company-name telecomxyz		Set the company name to "telecomxyz".
Switch(config)# switch-info system-contact info@company.com		Set the system contact field to "info@compnay.com".
Switch(config)# switch-info system-location 13thfloor		Set the system location field to "13thfloor".
Switch(config)# switch-info system-name backbone1		Set the system name field to "backbone1".

2.5.11 User command

1. Create a new login account.

User command	Parameter	Description
Switch(config)# user name [user_name]	[user_name]	Enter the new account's username. The authorized user login name is up to 20 alphanumeric characters. Only 3 login accounts can be registered in this device.
Switch(config-user)# description [description]	[description]	Enter the brief description for this user account.
Switch(config-user)# password [password]	[password]	Enter the password for this user account of up to 20 alphanumeric characters.
No command		
Switch(config)# no user name miseric		Delete "miseric" account.
Switch(config-user)# no description		Remove the configured description.
Switch(config-user)# no password		Remove the configured password value.
Show command		
Switch(config)# show user name		List all user accounts.
Switch(config)# show user name miseric		Show the specific account's information. In this example, information about "miseric" account will be displayed.
Switch(config-user)# show		Show or verify the newly-created user account's information.
User command example		
Switch(config)# user name miseric		Create a new login account "miseric".
Switch(config-user)# description misengineer		Add a description to this new account "miseric".
Switch(config-user)# password mis2256i		Set up a password for this new account "miseric"

2.5.12 VLAN command

1. Create a 802.1q VLAN and management VLAN rule.

<table>
<tr><th>VLAN dot1q command</th><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>Switch(config)# vlan dot1q-vlan</td><td></td><td colspan="2">Globally enable 802.1q VLAN.</td></tr>
<tr><td>Switch(config)# vlan dot1q-vlan [1-4094]</td><td>[1-4094]</td><td colspan="2">Enter a VID number to create a 802.1q VLAN.</td></tr>
<tr><td>Switch(config)# vlan dot1q-vlan isolation</td><td></td><td colspan="2">Enable VLAN isolation mode. When “Isolation” mode is enabled, the device will be forced to follow the port-based VLAN rule shown below.
<table>
<tr><th>Port</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th></tr>
<tr><td>1</td><td>V</td><td></td><td></td><td></td><td></td><td>V</td></tr>
<tr><td>2</td><td></td><td>V</td><td></td><td></td><td></td><td>V</td></tr>
<tr><td>3</td><td></td><td></td><td>V</td><td></td><td></td><td>V</td></tr>
<tr><td>4</td><td></td><td></td><td></td><td>V</td><td></td><td>V</td></tr>
<tr><td>5</td><td></td><td></td><td></td><td></td><td>V</td><td>V</td></tr>
<tr><td>6</td><td>V</td><td>V</td><td>V</td><td>V</td><td>V</td><td>V</td></tr>
</table></td></tr>
<tr><td rowspan="2">Switch(config)# vlan management-vlan [1-4094] management-port [port_list]</td><td>[1-4094]</td><td colspan="2">Enter the management VLAN ID.</td></tr>
<tr><td>[port_list]</td><td colspan="2">Specify the management port number.</td></tr>
<tr><th>VLAN &amp; Interface command</th><th></th><th colspan="2"></th></tr>
<tr><td>Switch(config)# interface [port_list]</td><td>[port_list]</td><td colspan="2">Enter several discontinuous port numbers separating by a comma or a range of ports with a hyphen. For example:1,3 or 2-4</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan access-vlan [1-4094]</td><td>[1-4094]</td><td colspan="2">Set up the selected ports’ PVID.</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan trunk-vlan [1-4094]</td><td>[1-4094]</td><td colspan="2">Assign the selected ports to a specified VLAN.</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan mode access</td><td></td><td>Set the selected ports to access mode (untagged).</td><td rowspan="4">See the table below for ingress/egress port behavior for each mode.</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan mode trunk</td><td></td><td>Set the selected ports to trunk mode (tagged).</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan mode trunk native</td><td></td><td>Set the selected ports to trunk native moe.</td></tr>
<tr><td>Switch(config-if)# vlan dot1q-vlan mode dot1q-tunnel</td><td></td><td>Set the selected ports to dot1q tunnel mode.</td></tr>
<tr><td>Switch(config-if)# vlan port-based [name]</td><td>[name]
The names can be entered are: **port1vlan**, **port2vlan**, **port3vlan**,</td><td colspan="2">Set the selected ports to a specified port-based VLAN. By default, every port is a member port in each port-based VLAN.</td></tr>
</table>

	port4vlan, **port5vlan**, **port6vlan**	
No command		
Switch(config)# no vlan dot1q-vlan		Disable 802.1q VLAN globally.
Switch(config)# no vlan dot1q-vlan [1-4094]	[1-4094]	Delete the specified VID.
Switch(config-if)# no vlan dot1q-vlan access-vlan		Set the selected ports’ PVID to the default setting.
Switch(config-if)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
Switch(config-if)# no vlan dot1q-vlan trunk [1-4094]	[1-4094]	Remove the selected ports’ VLAN 100 port membership. The selected ports are no longer member ports in VLAN 100.
Switch(config-if)# no vlan port-based [name]	[name]	Remove or delete the selected port from the specified port-based VLAN.
Show command		
Switch(config)# show vlan		Display global VLAN information including 802.1q VLAN Enable/Disable status and CPU VLAN ID.
Switch(config)# show vlan interface [port_list]	[port_list]	Show the specified ports’ VLAN assignment and tagging information.
Switch(config)# show vlan dot1q-vlan		Show 802.1q VLAN table.
Switch(config)# show vlan port-based		Show port-based VLAN table.
Switch(config)# show vlan interface		Show each interface’s VLAN assignment and tagging information.
VLAN dot1q & interface example		
Switch(config)# vlan dot1q-vlan		Enable 802.1q VLAN globally.
Switch(config)# vlan dot1q-vlan 100		Create a new VLAN 100.
Switch(config)# vlan management-vlan 1 management-port 1-3		Set port 1~3 to management ports.
Switch(config)# interface 1-3		Enter port 1 to port3’s interface mode.
Switch(config-if)# vlan dot1q-vlan trunk-vlan 100		Assign the selected ports to VLAN 100.
Switch(config-if)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
Switch(config-if)# vlan dot1q-vlan access-vlan 100		Set the selected ports’ PVID to 100.

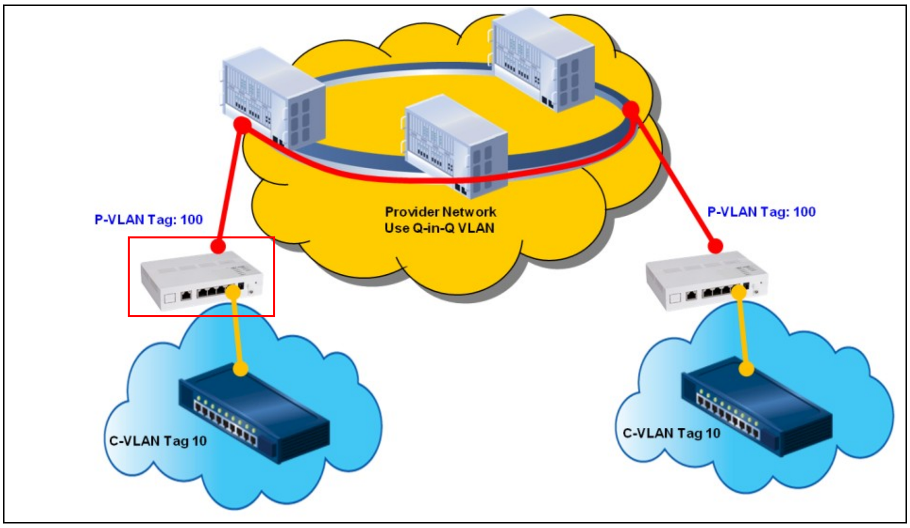
Port Behavior of Each Port Mode:

VLAN Port Mode	Port Behavior	
Access	Receive untagged packets only. Drop tagged packets.	
	Send untagged packets only.	
Trunk	Receive tagged packets only. Drop untagged packets.	
	Send tagged packets only.	
Trunk Native	Receive both untagged and tagged packets.	Untagged packets: PVID is added
		Tagged packets: Stay intact
	When sending packets, PVID and VID will be compared. If PVID and VID are the same, PVID will be removed. If PVID and VID are different, the packets with the original tag will be sent.	
Dot1q Tunnel	Receive both untagged and tagged packets and force to add PVID to both untagged and tagged packets.	
	Remove the outer tag when sending packets.	

Configure Q in Q VLAN

This section provides an example on how to configure Q-in-Q using 802.1q function. Follow the steps described below or use them as reference to set up configurations that are suitable for your networking environment.

Scenario:



CLI Configurations:

Steps	Configurations
Step 1. Enable Dot1q VLAN.	Switch(config)# vlan dot1q-vlan OK!
Step 2. Create a VID 100.	Switch(config)# vlan dot1q-vlan 100 OK!
Step 3. Assign Port 1 & Port 6 to VLAN 100.	Switch(config)# interface 1,6 Switch(config-if)# vlan dot1q-vlan trunk-vlan 100 OK! Switch(config-if)# exit
Step 4. Check both Port 1 & 6 are members in VLAN 100.	Switch(config)#show vlan dot1q-vlan ====================================== IEEE 802.1q Tag VLAN ====================================== VLAN 1 6 CPU ---- ------ --- 1 VVVVVV V 100 V----V - *NOTE: By default, all switch ports are member ports in VLAN 1. This VLAN can be deleted. However, before doing so, make sure you have correct PVID and VLAN mode configurations; otherwise, the connection to the device might be terminated immediately due to inappropriate configurations.*
Step 5. Set Port 1's PVID to 100.	Switch(config)# interface 1 Switch(config-if)# vlan dot1q-vlan access-vlan 100 OK!
Step 6. Set Port 1's VLAN Port mode to dot1q tunnel and Port 6's to trunk.	Switch(config-if)# vlan dot1q-vlan mode dot1q-tunnel OK! Switch(config-if)# exit Switch(config)# interface 6 Switch(config-if)# vlan dot1q-vlan mode trunk OK!
Step 7. Check Port 1's PVID has been changed to 100 and Port 1 & 6's VLAN mode have been changed to dot1q tunnel and trunk mode respectively.	Switch(config)#show vlan interface ====================================== Switch(config)#show vlan ====================================== Port Port VLAN ID Port VLAN Mode ---- ------------ -------------- 1 100 dot1q tunnel 2 1 access 3 1 access 4 1 access 5 1 access 6 1 trunk

2.5.13 Show interface statistics command

“show interface statistics” that can display port traffic statistics, port packet error statistics and port analysis history can be used either in Privileged mode # and Global Configuration mode (config)#. “show interface statistics” is useful for network administrators to diagnose and analyze port traffic real-time conditions.

Command	Description
Switch(config)#show interface statistics analysis	Display packets analysis (events) for each port.
Switch(config)#show interface statistics analysis [port_list]	Display packets analysis for the selected ports.
Switch(config)#show interface statistics analysis rate	Display packets analysis (rates) for each port.
Switch(config)#show interface statistics analysis rate [port_list]	Display packets analysis (rates) for the selected ports.
Switch(config)#show interface statistics error	Display error packets statistics (events) for each port.
Switch(config)#show interface statistics error [port_list]	Display error packets statistics (events) for the selected ports.
Switch(config)#show interface statistics error rate	Display error packets statistics (rates) for each port.
Switch(config)#show interface statistics error rate [port_list]	Display error packets statistics (rates) for the selected ports.
Switch(config)#show interface statistics traffic	Display traffic statistics (events) for each port.
Switch(config)#show interface statistics traffic [port_list]	Display traffic statistics (events) for the selected ports.
Switch(config)#show interface statistics traffic rate	Display traffic statistics (rates) for each port.
Switch(config)#show interface statistics traffic rate [port_list]	Display traffic statistics (rates) for the selected ports.
Switch(config)#show interface statistics clear	Clear all statistics.

2.5.14 Show sfp command

When you slide-in SFP transceiver, detailed information about this module can be viewed by issuing this command.

Command	Description
Switch(config)#show sfp information	Display the slide-in SFP information including speed, distance, vendor name, vendor PN and vendor serial number.
Switch(config)#show sfp state	Display the slide-in SFP information including temperature, voltage, TX bias, TX power, RX power.

3. WEB MANAGEMENT

The Smart Switch can be managed via a Web browser. However, you must first assign a unique IP address to the Smart Switch before doing so. Use a RJ45 LAN cable and one of the 10/100Base-TX RJ-45 ports of the Smart Switch (as the temporary RJ-45 Management console port) to login to the Switch and set up the IP address for the first time. (The default IP of the Smart Switch can be reached at **"http://192.168.0.1"**. You can change the Switch's IP address to the needed one later in its **Network Management** menu.)

Follow these steps to manage the Smart Switch through a Web browser:

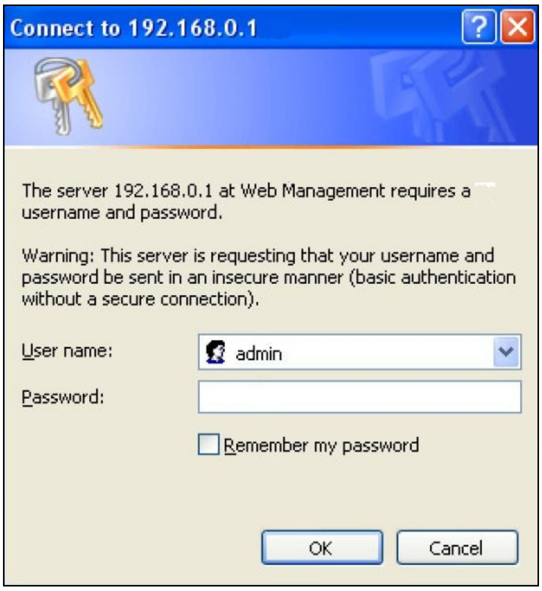
1. Use one of the 10/100Base-TX RJ-45 ports (as the temporary RJ-45 Management console port) to set up the assigned IP parameters of the Smart Switch including the following:

   - IP address
   - Subnet Mask
   - Default Switch IP address, if required

2. Run a Web browser and specify the Smart Switch's IP address to reach it. (The default IP address for the Smart Switch can be reached at **"http://192.168.0.1"** before any changes.)

3. Login to the Smart Switch to reach the Main menu.

Once you gain the access, a Login windows shows up like this,



Connect to 192.168.0.1

The server 192.168.0.1 at Web Management requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

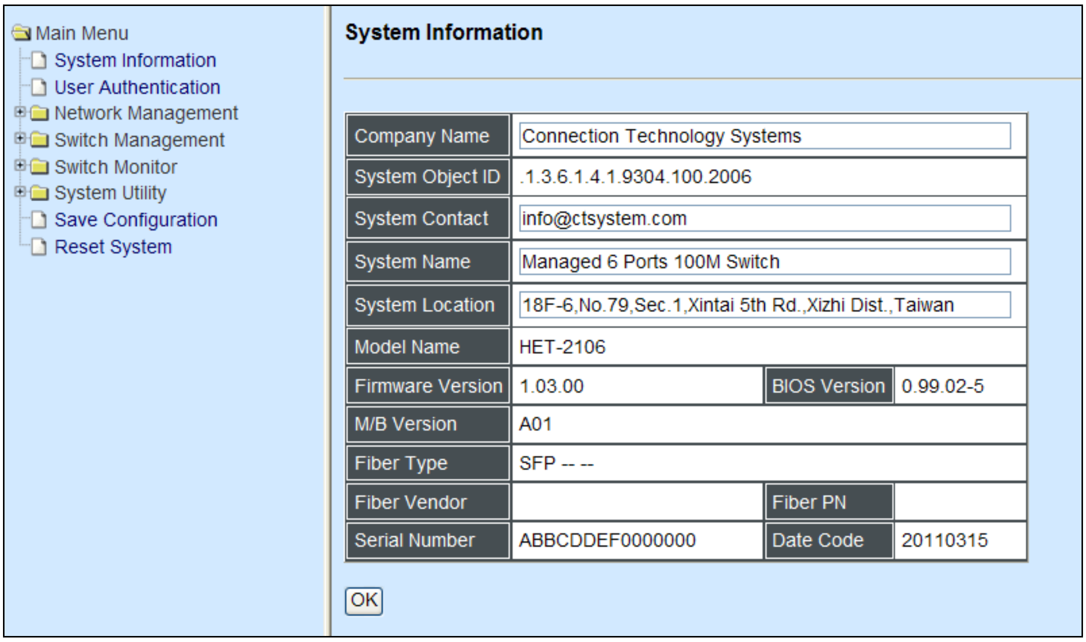
User name: admin

Password:

□ Remember my password

Enter the default user name and password for the initial login then select "OK" to login to the main screen page. The default user name is ***admin*** and without password (leave the password field empty).

After a successful login, the Main Menu screen appears as below.



System Information

Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.2006		
System Contact	info@ctsystem.com		
System Name	Managed 6 Ports 100M Switch		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
Model Name	HET-2106		
Firmware Version	1.03.00	BIOS Version	0.99.02-5
M/B Version	A01		
Fiber Type	SFP -- --		
Fiber Vendor		Fiber PN	
Serial Number	ABBCDDEF0000000	Date Code	20110315

1. **System Information:** Name the Smart Switch, specify the location and check the current version of information.

2. **User Authentication:** Create and view the registered user list.

3. **Network Management:** Set up or view the IP address and related information about the Smart Switch required for network management applications.

4. **Switch Management:** Set up switch or port configuration, VLAN configuration, QoS and other functions.

5. **Switch Monitor:** View the operation status and traffic statistics of the ports.

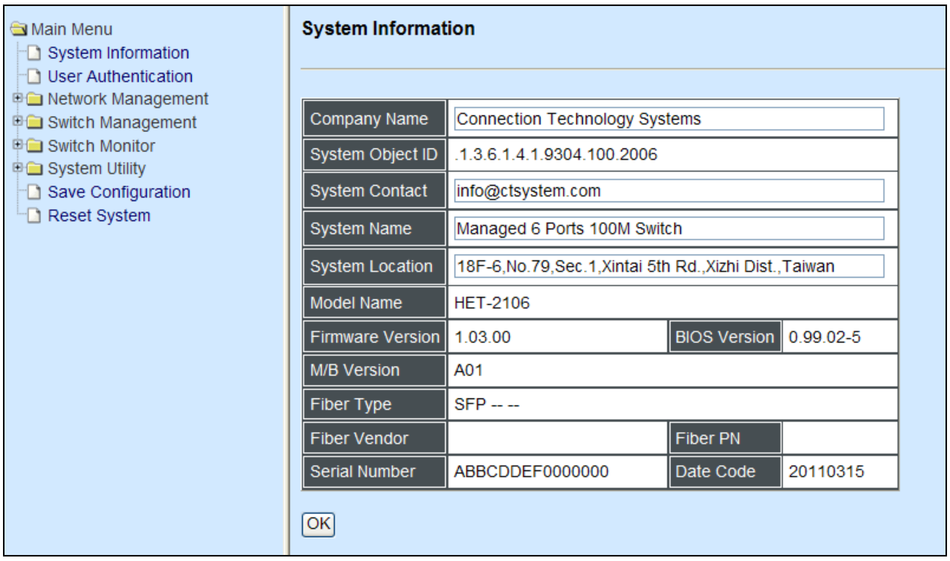
6. **System Utility:** Upgrade Firmware and Load Factory Settings.

7. **Save Configuration:** Save all changes to the system.

8. **Reset System:** Reset the Smart Switch.

3.1 System Information

Select **System Information** from the **Main Menu** and then the following screen shows up.



System Information

Company Name	Connection Technology Systems		
System Object ID	.1.3.6.1.4.1.9304.100.2006		
System Contact	info@ctsystem.com		
System Name	Managed 6 Ports 100M Switch		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
Model Name	HET-2106		
Firmware Version	1.03.00	BIOS Version	0.99.02-5
M/B Version	A01		
Fiber Type	SFP -- --		
Fiber Vendor		Fiber PN	
Serial Number	ABBCDDEF0000000	Date Code	20110315

Company Name: Enter a company name for this Smart Switch, up to 55 alphanumeric characters.

System Object ID: View-only field that shows the predefined System OID.

System Contact: Enter contact information for this Smart switch, up to 55 alphanumeric characters.

System Name: Enter a unique name for this Smart Switch, up to 55 alphanumeric characters. Use a descriptive name to identify the Smart Switch in relation to your network, for example, “Backbone 1”. This name is mainly used for reference.

System Location: Enter a brief description of the Smart Switch location, up to 55 alphanumeric characters. The location is for reference only.

Model Name: View-only field that shows the product’s model name.

Firmware Version: View-only field that shows the product’s firmware version.

M/B Version: View-only field that shows the main board version.

Fiber Type: View-only field that shows information about the slide-in or fixed fiber type.

Fiber Wavelength: View-only field that shows the slide-in or fixed fiber’s TX and RX wavelength information.

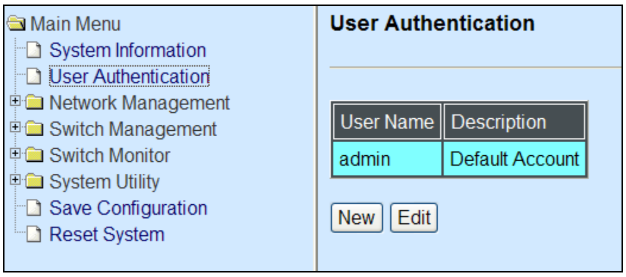
Serial Number: View-only field that shows the serial number of this switch.

Date Code: View-only field that shows the Smart Switch Firmware date code.

3.2 User Authentication

To prevent any un-authorized operations, only registered users are allowed to operate the Smart Switch. Any users who want to operate the Smart Switch need to register into the user's list first.

To view or change current registered users, select **User Authentication** from the **Main Menu** and then the following screen page shows up.

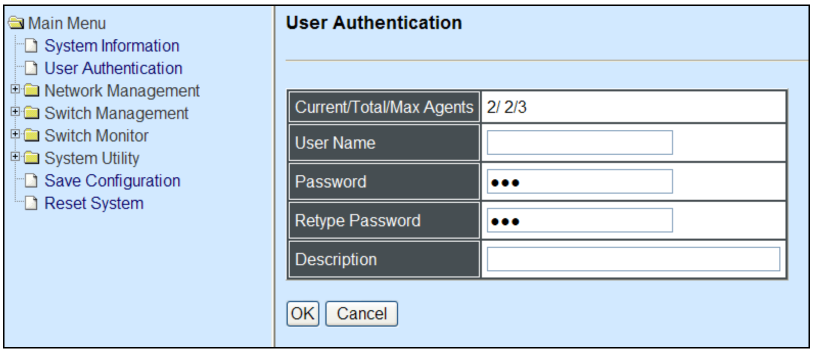


User Name	Description
admin	Default Account

Click **New** to add a new user account, then the following screen page appears.

Click **Edit** to view and edit a registered user setting.

Click **Delete** to remove a registered user setting.



Current/Total/Max Agents	2/ 2/3
User Name	
Password	•••
Retype Password	•••
Description	

Current/Total/Max Users: View-only field.

Current: This shows the number of current registered users.

Total: This shows the total number of users who have registered.

Max: This shows the maximum number available for registration. The maximum number is 3.

User Name: Specify the authorized user login name, up to 20 alphanumeric characters.

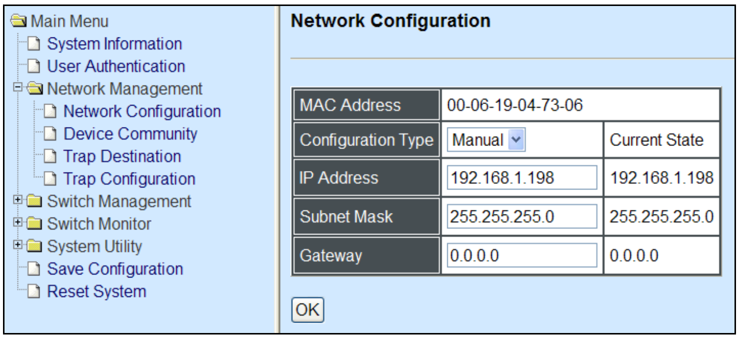
Password: Enter the desired user password, up to 20 alphanumeric characters.

Retype Password: Enter the password again to confirm.

Description: Enter a unique description for this user, up to 35 alphanumeric characters. This is mainly for reference only.

3.3 Network Management

In order to enable network management of the Smart Switch, proper network configuration is required. To do this, click the folder **Network Management** from the **Main Menu** and then the following screen page appears.



MAC Address	00-06-19-04-73-06	
Configuration Type	Manual	Current State
IP Address	192.168.1.198	192.168.1.198
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0

1. **Network Configuration:** Set up the required IP configuration of the Managed Switch.

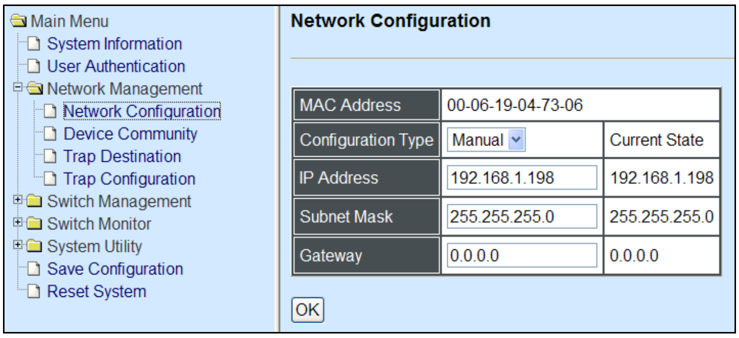
2. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.

3. **Trap Destination:** View the registered SNMP trap destination list.

4. **Trap Configuration:** Set up which type of trap is sent when a certain situation occurs.

3.3.1 Network Configuration

Click the option **Network Configuration** from the **Network Management** menu and then the following screen page appears.



MAC Address	00-06-19-04-73-06	
Configuration Type	Manual	Current State
IP Address	192.168.1.198	192.168.1.198
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	0.0.0.0	0.0.0.0

MAC Address: This view-only field shows the unique and permanent MAC address pre-assigned to the Smart switch. You cannot change the Smart Switch’s MAC address.

Configuration Type: There are two configuration types that users can select from the pull-down menu; these are **“DHCP”** and **“Manual”**. When **“DHCP”** is selected and a DHCP server is also available on the network, the Smart Switch will automatically get the IP address from the DHCP server. If "**Manual"** is selected, users need to specify the IP address, Subnet Mask and Gateway.

NOTE: *This Smart Switch supports auto-provisioning function that enables DHCP clients to automatically download the latest Firmware and configuration image from the server. For information about how to set up a DHCP server, please refer to APPENDIX A.*

IP Address: Enter the unique IP address for this Smart Switch. You can use the default IP address or specify a new one when the situation of address duplication occurs or the address does not match up with your network. (The default factory setting is 192.168.0.1.)

Subnet Mask: Specify the subnet mask. The default subnet mask values for the three Internet address classes are as follows:

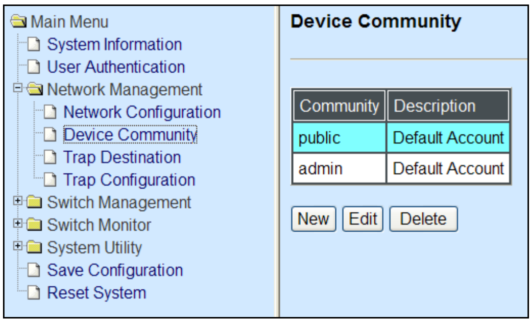
- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Smart Switch. This address is required when the Smart Switch and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and Smart Switch are on the same network.

Current State: These View-only fields show manually assigned IP address, Subnet Mask and Gateway of the Smart Switch.

3.3.2 Device Community

Click the option **Device Community** from the **Network Management** menu and then the following screen page appears.



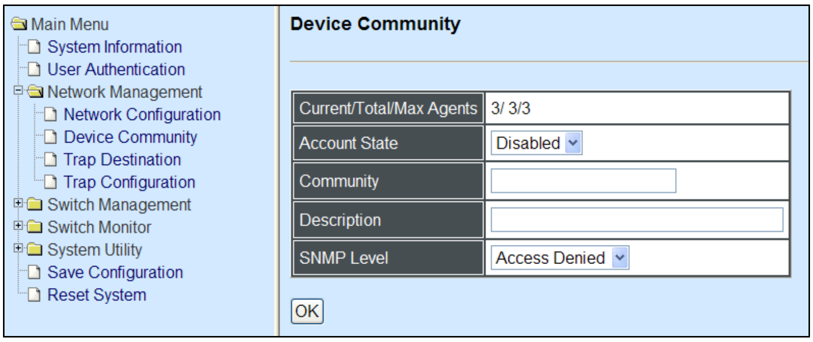
Device Community

Community	Description
public	Default Account
admin	Default Account

Click **New** to add a new SNMP community name list and then the following screen page appears.

Click **Edit** to view the current community settings.

Click **Delete** to remove a registered community.



Device Community

Current/Total/Max Agents	3/ 3/3
Account State	Disabled
Community	
Description	
SNMP Level	Access Denied

Current/Total/Max Agents: View-only field.

Current: This shows the number of currently registered communities.

Total: This shows the number of total registered community users.

Max Agents: This shows the number of maximum number available for registration. The default maximum number is 3.

Account State: Enable or disable this Community Account.

Community: Specify the authorized SNMP community name, up to 20 alphanumeric characters.

Description: Enter a unique description for this community name, up to 35 alphanumeric characters. This is mainly for reference only.

SNMP Level: Select the preferred SNMP level for this newly created community.

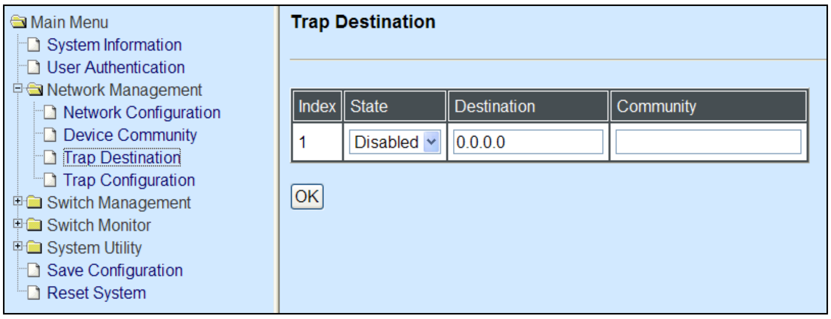
Administrator: Full access right includes maintaining user account, system information, loading factory settings, etc.

Read & Write: Full access right but cannot modify system information, user account, load factory settings and upgrade firmware.

Read Only: Read Only access privilege. Allow to view only.

3.3.3 Trap Destination

Click the option **Trap Destination** from the **Network Management** menu and then the following screen page appears.



Trap Destination

Index	State	Destination	Community
1	Disabled	0.0.0.0	

OK

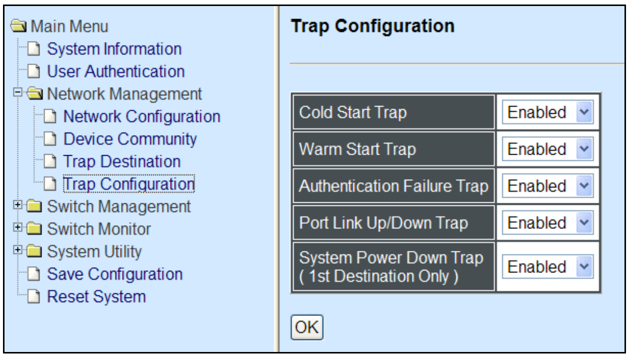
State: Enable or disable the function of sending traps to the specified destination. Please note that only power down trap will be sent.

Destination: Enter the specific IP address of the network management system that will receive traps.

Community: Enter the community name of the network management system.

3.3.4 Trap Configuration

Click the option **Trap Configuration** from the **Network Management** menu and then the following screen page appears.



Trap Configuration

Cold Start Trap	Enabled
Warm Start Trap	Enabled
Authentication Failure Trap	Enabled
Port Link Up/Down Trap	Enabled
System Power Down Trap (1st Destination Only)	Enabled

OK

Cold Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch cold starts.

Warm Start Trap: Enable or disable the Managed Switch to send a trap when the Managed Switch warm starts.

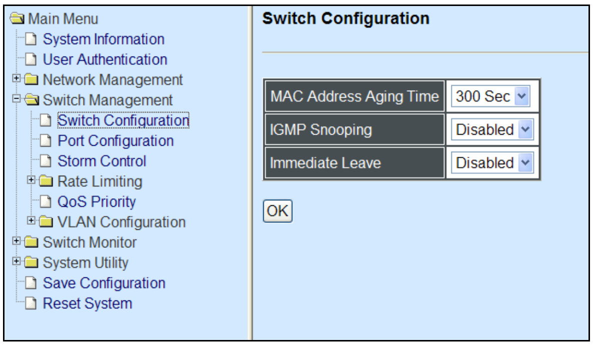
Authentication Failure Trap: Enable or disable the Managed Switch to send authentication failure trap after any unauthorized users attempt to login.

Port Link Up/Down Trap: Enable or disable the Managed Switch to send the port link up/link down trap when the selected port(s) is link up or down.

System Power Down Trap: Send a trap notice while the Managed Switch is power down.

3.4 Switch Management

In order to manage the Smart switch and set up required switching functions, click the folder **Switch Management** from the **Main Menu** and then several options and folders will be displayed for your selection.



MAC Address Aging Time	300 Sec
IGMP Snooping	Disabled
Immediate Leave	Disabled

1. **Switch Configuration:** Set up address learning aging time and enable or disable IGMP Snooping and Immediate Leave.

2. **Port Configuration:** Enable or disable port speed, flow control, etc.

3. **Storm Control:** Enable or disable multicast, broadcast, and unicast storm control.

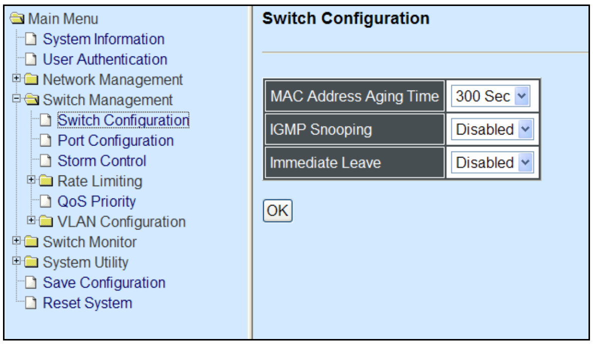
4. **Rate Limiting:** Enable or disable Port priority and setup Port Rate limit, etc.

5. **QoS Priority:** Set up QoS Priority based on Port-based, IEEE 802.1p and ToS/DSCP Qos mode.

6. **VLAN Configuration:** Set up Port-based and IEEE 802.1q Tag VLAN configuration.

3.4.1 Switch Configuration

Click the option **Switch Configuration** from the **Switch Management** menu and then the following screen page appears.



Switch Configuration

MAC Address Aging Time	300 Sec
IGMP Snooping	Disabled
Immediate Leave	Disabled

MAC Address Aging Time: Select MAC Address aging time from the pull-down menu. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within aging time.

IGMP Snooping: Enable or disable IGMP Snooping.

IGMP, Internet Group Management Protocol, is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It can be used for online streaming video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

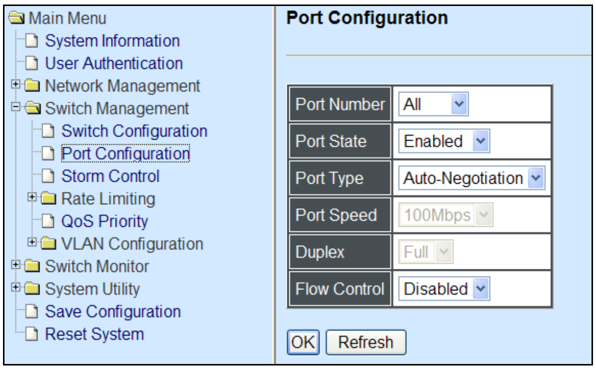
When IGMP snooping is enabled in a switch it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast list for that group. And, when the switch hears an IGMP Leave, it removes the host's port from the table entry.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. A switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

Immediate Leave: Enable or disable Immediate Leave function. This works only when IGMP Snooping is enabled. When Immediate Leave is enabled, the Smart Switch immediately removes the port when it detects IGMPv1 & IGMPv2 leave message on that port.

3.4.2 Port Configuration

Click the option **Port Configuration** from the **Switch Management** menu and then the following screen page appears.



Port Configuration

Port Number	All
Port State	Enabled
Port Type	Auto-Negotiation
Port Speed	100Mbps
Duplex	Full
Flow Control	Disabled

Port Number: Click the pull-down menu to select the port number for configuration.

Port State: Enable or disable the current port state.

Port Type: Select Auto-Negotiation or Manual mode as the port type.

Port Speed: When you select Manual port type, you can further specify the transmission speed (10Mbps/100Mbps) of the port(s).

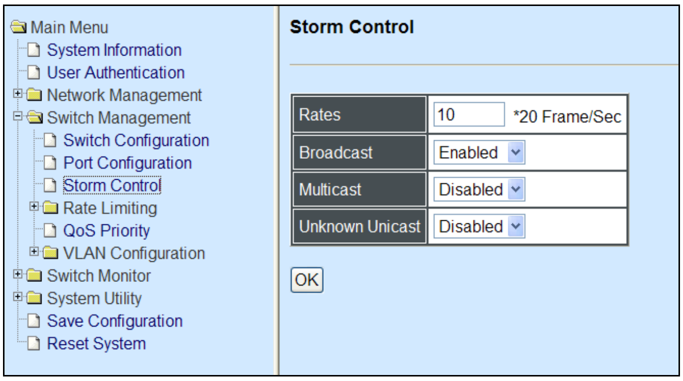
Duplex: When you select Manual port type, you can further specify the current operation Duplex mode (full or half duplex) of the port(s).

Flow Control: Enable or disable the flow control.

Description: Enter the unique description for this port. This is used for reference only.

3.4.3 Storm Control

Click the option **Storm Control** from the **Switch Management** menu and then the following screen page appears.



Storm Control

Rates	10 *20 Frame/Sec
Broadcast	Enabled
Multicast	Disabled
Unknown Unicast	Disabled

Per Unit: Specify the number of rates (One unit equals 20 packets per second).

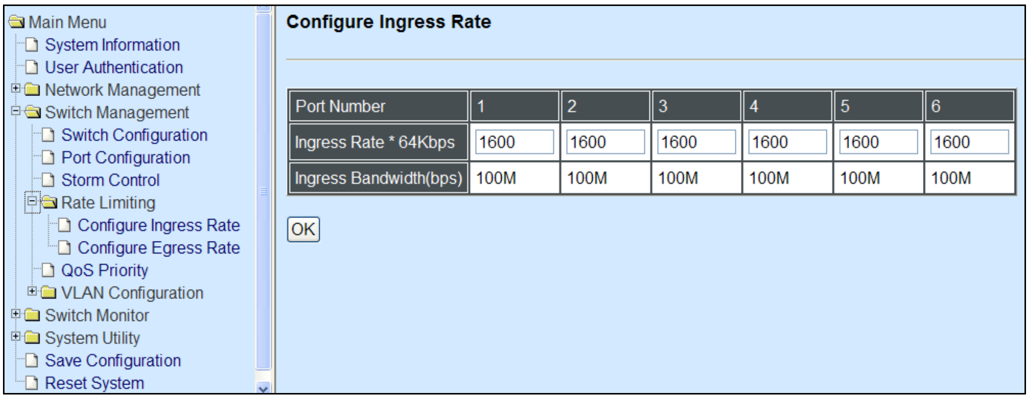
Broadcast: To enable or disable broadcast storm control. Broadcast storms may occur and degrade network performance even to a complete halt when a device on the network is malfunctioning, or if application programs are not well designed or properly configured. The network can be protected from broadcast storms by setting a threshold rate for broadcast traffic on a per switch basis. Any broadcast packets exceeding the specified value will then be dropped.

Multicast: To enable or disable multicast storm control. When enabled, the multicast frames can not exceed the rate specified. Any multicast packets exceeding the specified value will then be dropped.

Unicast: To enable or disable unicast storm control. When enabled, the unicast frames can not exceed the rate specified. Any unicast packets exceeding the specified value will then be dropped.

3.4.4 Rate Limiting

Click the folder **Rate Limiting** from the **Main Menu** and then the following screen page appears.



Configure Ingress Rate

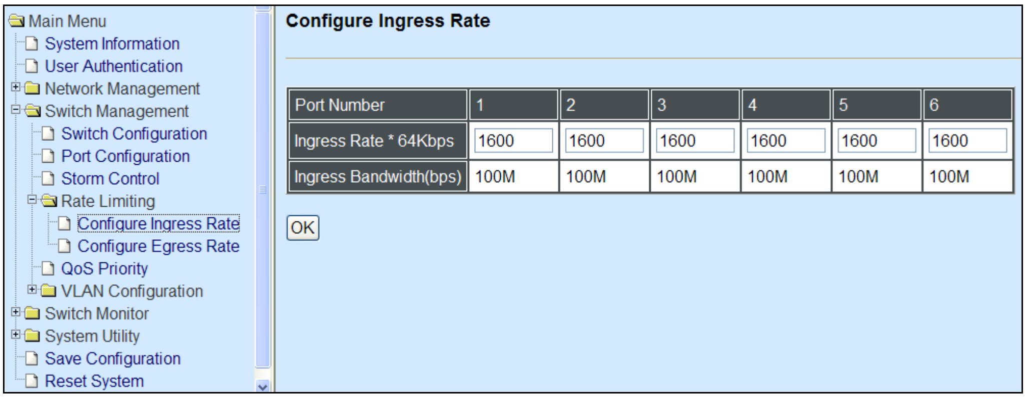
Port Number	1	2	3	4	5	6
Ingress Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Ingress Bandwidth(bps)	100M	100M	100M	100M	100M	100M

1. **Configure Ingress Rate:** Set up ingress rate.

2. **Configure Egress Rate:** Set up egress rate.

3.4.4.1 Configure Ingress Rate

Click the option **Configure Ingress Rate** from the **Rate Limiting** menu and then the following screen page appears.



Configure Ingress Rate

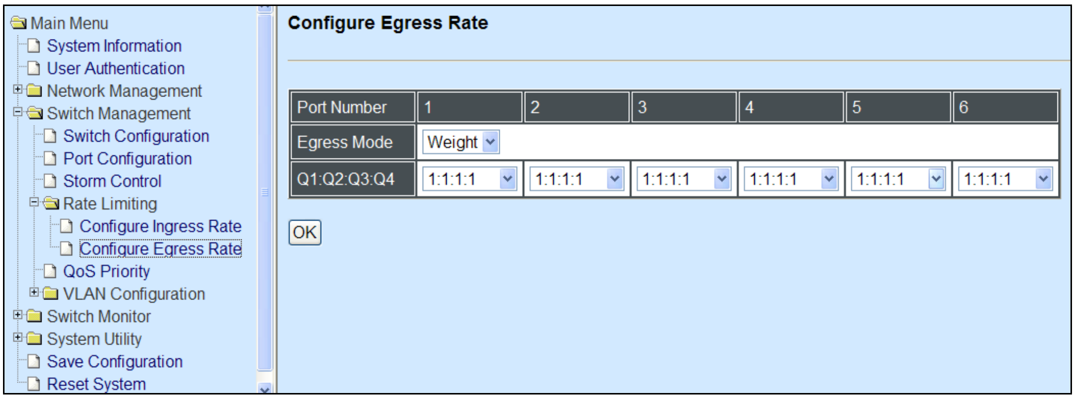
Port Number	1	2	3	4	5	6
Ingress Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Ingress Bandwidth(bps)	100M	100M	100M	100M	100M	100M

Ingress Rate: Specify the ingress rate between 1 to 1600. The actual ingress rate will be the ingress rate that you specify times 64Kbps.

Ingress Bandwidth: Each ingress bandwidth will be changed automatically based on ingress rates specified.

3.4.4.2 Configure Egress Rate

Click the option **Configure Egress Rate** from the **Rate Limiting** menu and then the following screen page appears.



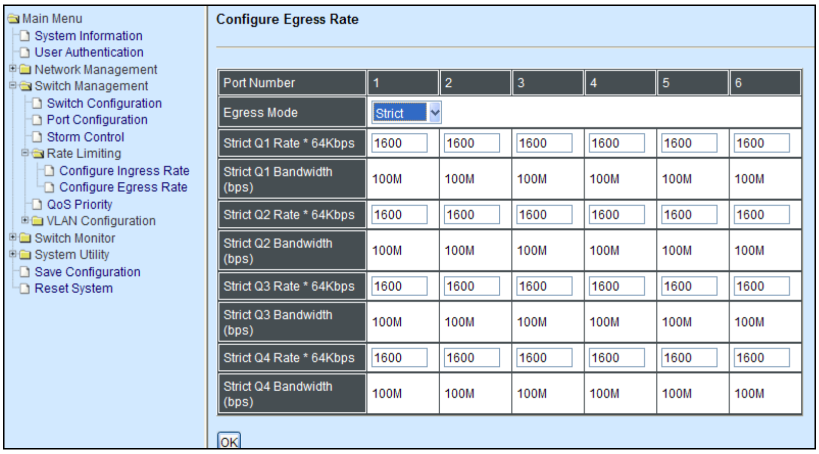
Configure Egress Rate

Port Number	1	2	3	4	5	6
Egress Mode	Weight					
Q1:Q2:Q3:Q4	1:1:1:1	1:1:1:1	1:1:1:1	1:1:1:1	1:1:1:1	1:1:1:1

Egress Mode: There are two egress modes available for your selection, these are Weight and Strict.

Weight Mode: This mode enables users to assign different weights to 4 queues.

Q1:Q2:Q3:Q4: Select one weighting option from the pull-down menu that is suitable for your networking environment.



Configure Egress Rate

Port Number	1	2	3	4	5	6
Egress Mode	Strict					
Strict Q1 Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Strict Q1 Bandwidth (bps)	100M	100M	100M	100M	100M	100M
Strict Q2 Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Strict Q2 Bandwidth (bps)	100M	100M	100M	100M	100M	100M
Strict Q3 Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Strict Q3 Bandwidth (bps)	100M	100M	100M	100M	100M	100M
Strict Q4 Rate * 64Kbps	1600	1600	1600	1600	1600	1600
Strict Q4 Bandwidth (bps)	100M	100M	100M	100M	100M	100M

Strict: This indicates that services to each egress queues are offered based on rates specified.

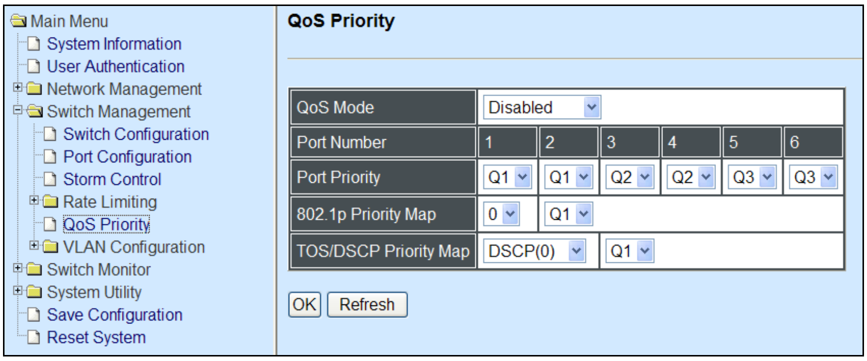
Strict Q1~Q4 Rate: Specify each outbound queue's rate.

Strict Q1~Q4 Bandwidth: Each queue's bandwidth will be changed automatically based on the rate specified.

3.4.5 QoS Priority

Network traffic is always unpredictable and the only basic assurance that can be offered is the best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria and receives preferential treatments.

QoS enables users to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. Click the option **QoS Priority** from the **Switch Management** menu and then the following screen page appears.



QoS Priority

QoS Mode	Disabled					
Port Number	1	2	3	4	5	6
Port Priority	Q1	Q1	Q2	Q2	Q3	Q3
802.1p Priority Map	0	Q1				
TOS/DSCP Priority Map	DSCP(0)	Q1				

QoS Mode: Four options are available; these are Disabled, Port-based, IEEE 802.1p, TOS/DSCP.

Port Priority: Assign a port priority (Q0~Q3) to each port.

802.1p Priority Map: Assign a tag priority to the specific queue.

There are eight priority levels that you can choose to classify data packets. Choose one of the listed options from the pull-down menu for CoS (Class of Service) priority tag values. The default value is "0".

The default 802.1p settings are shown in the following table:

Priority Level	Low	Low	Low	Normal	Medium	Medium	High	High
802.1p Value	0	1	2	3	4	5	6	7

TOS/DSCP Priority Map: Select priority queue mapping for the DSCP field of every IP packet from the pull-down menu. The DSCP includes DSCP (0) to DSCP (63), and the priority queue includes Q0, Q1, Q2 and Q3.

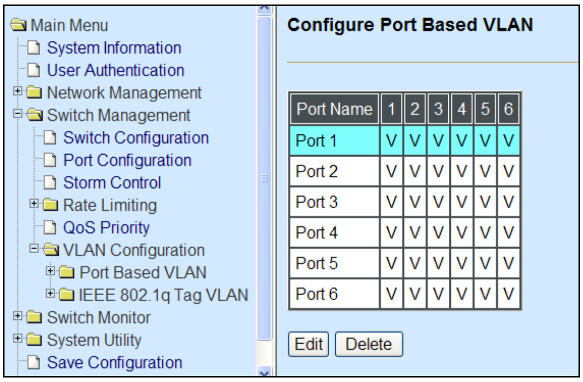
3.4.6 VLAN Configuration

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logics instead of physical locations. End nodes that frequently communicate with each other are assigned to the same VLAN, no matter where they are physically located on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be ‘moved’ to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another. This allows VLAN to accommodate network moves, changes and additions with the greatest flexibility.

The Smart Switch supports two types of VLAN, these are: **Port-Based VLAN** and **IEEE 802.1Q Tag VLAN**.

Click the option **VLAN Configuration** from the **Switch Management** menu and then the following screen page appears.



Configure Port Based VLAN

Port Name	1	2	3	4	5	6
Port 1	V	V	V	V	V	V
Port 2	V	V	V	V	V	V
Port 3	V	V	V	V	V	V
Port 4	V	V	V	V	V	V
Port 5	V	V	V	V	V	V
Port 6	V	V	V	V	V	V

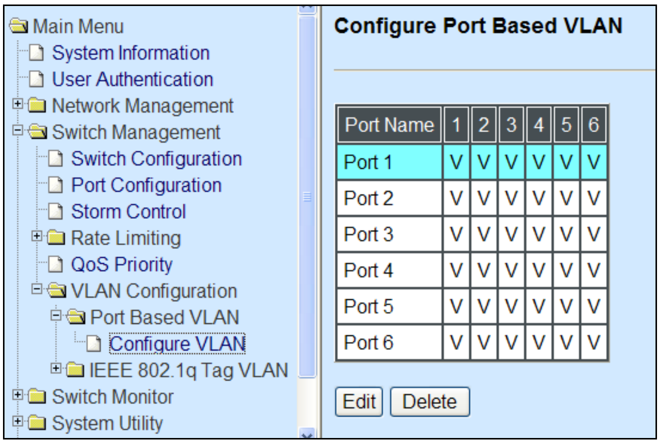
1. **Port-Based VLAN:** Set up Port-Based VLAN configurations.

2. **IEEE 802.1q Tag VLAN:** Set up 802.1q Tag VLAN configurations.

3.4.6.1 Port-Based VLAN

Port-based VLAN can effectively segment one network into several broadcast domains, Broadcast/Multicast and unknown packets will be limited to within the VLAN. Port-Based VLAN is uncomplicated and fairly rigid in implementation and is useful for network administrators who wish to quickly and easily set up VLAN so as to isolate the effect of broadcast packets on their network.

Click the option **Configure VLAN** from the **Port-Based VLAN** menu and then the following screen page appears.

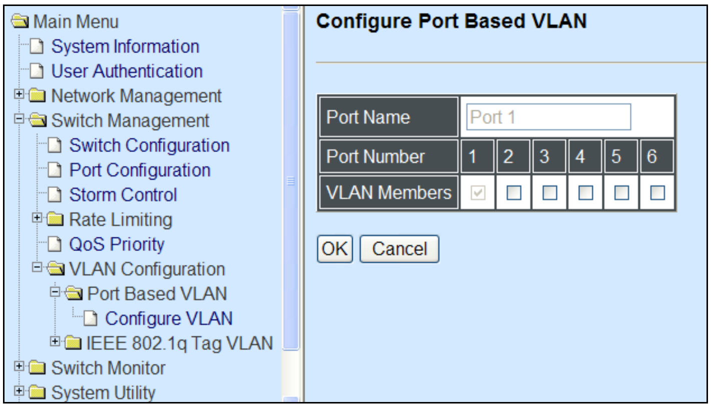


Configure Port Based VLAN

Port Name	1	2	3	4	5	6
Port 1	V	V	V	V	V	V
Port 2	V	V	V	V	V	V
Port 3	V	V	V	V	V	V
Port 4	V	V	V	V	V	V
Port 5	V	V	V	V	V	V
Port 6	V	V	V	V	V	V

Use **Edit** to view and edit the current VLAN setting, then the following screen page appears.

Click **Delete** to remove port-based VLAN setting.



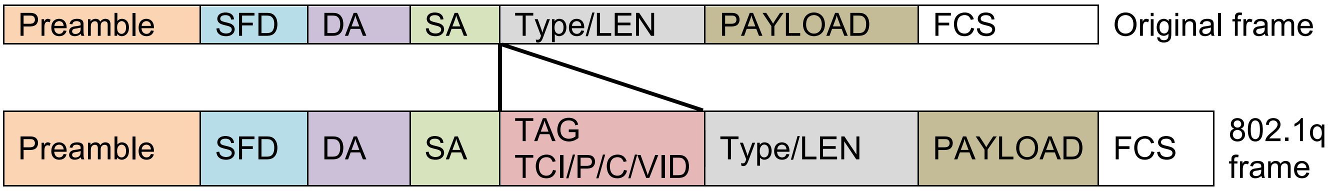
Configure Port Based VLAN

Port Name	Port 1					
Port Number	1	2	3	4	5	6
VLAN Members	☑	□	□	□	□	□

VLAN Members: Tick the checkbox(es) if you would like to allow the port(s) belong to the VLAN specified.

3.4.6.2 IEEE 802.1Q VLAN Concepts

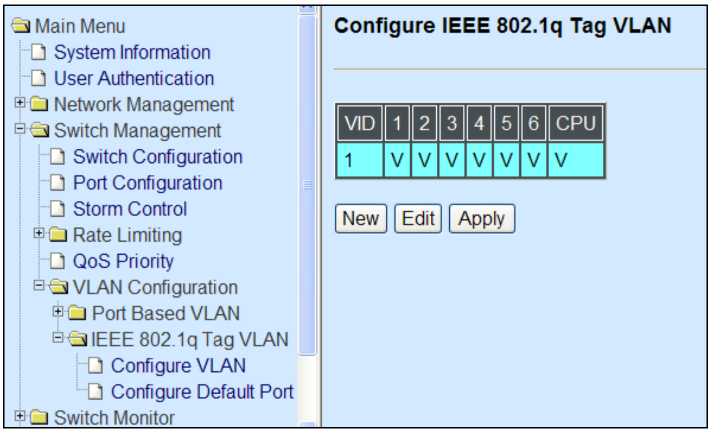
Introduction to 802.1Q frame format:



PRE	Preamble	62 bits	Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the destination
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes set to 8100 for 802.1p and Q tags	
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in Canonical format - Ethernet set to "0"
VID	VLAN Identifier	12 bits	Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length"
Payload	< or = 1500 bytes User data		
FCS	Frame Check Sequence	4 bytes	Cyclical Redundancy Check

2.4.6.3 IEEE 802.1q Tag VLAN

The following screen page appears when you choose **IEEE 802.1q Tag VLAN**.



Configure IEEE 802.1q Tag VLAN

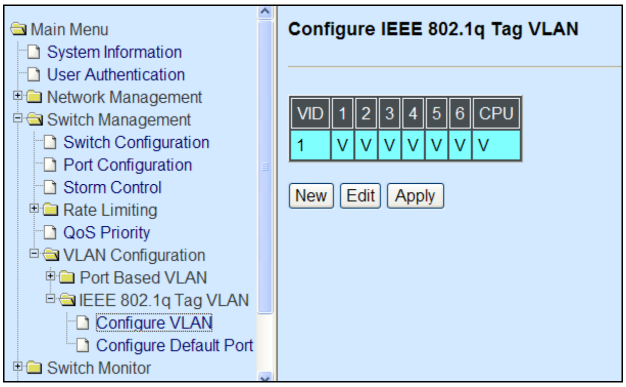
VID	1	2	3	4	5	6	CPU
1	V	V	V	V	V	V	V

1. **Configure VLAN:** To create, edit or delete 802.1Q Tag VLAN settings.

2. **Configure Default Port VLAN:** To set up 802.1q VLAN Tag mode, Port VLAN ID, Port Egress and Ingress Mode.

3.4.6.3.1 Configure VLAN

Click the option **Configure VLAN** from the **IEEE 802.1q Tag VLAN** menu and then the following screen page appears.



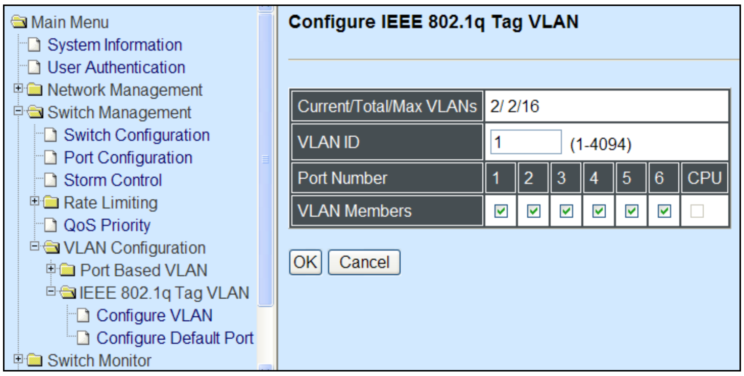
Configure IEEE 802.1q Tag VLAN

VID	1	2	3	4	5	6	CPU
1	V	V	V	V	V	V	V

Click **New** to add a new VLAN entity and then the following screen page appears.

Click **Edit** to view and edit current IEEE 802.1Q Tag VLAN setting.

Click **Delete** to remove a VLAN entity.



Configure IEEE 802.1q Tag VLAN

Current/Total/Max VLANs	2/ 2/16						
VLAN ID	1 (1-4094)						
Port Number	1	2	3	4	5	6	CPU
VLAN Members	☑	☑	☑	☑	☑	☑	□

Current/Total/Max VLANs: View-only field.

Current: This shows the current VLAN number.

Total: This shows the number of total registered VLANs.

Max VLANs: This shows the number of maximum number available for registration. The default maximum number is 16.

VLAN ID: Specify a VLAN ID between 1 and 4094.

CPU: By default, CPU belongs to Default VLAN. If you would like to move CPU from one VLAN to another, you can do so by following the steps below.

Example: Change CPU from Default VLAN ID 1 to VLAN ID 3

Step 1. Create a new VLAN 3.

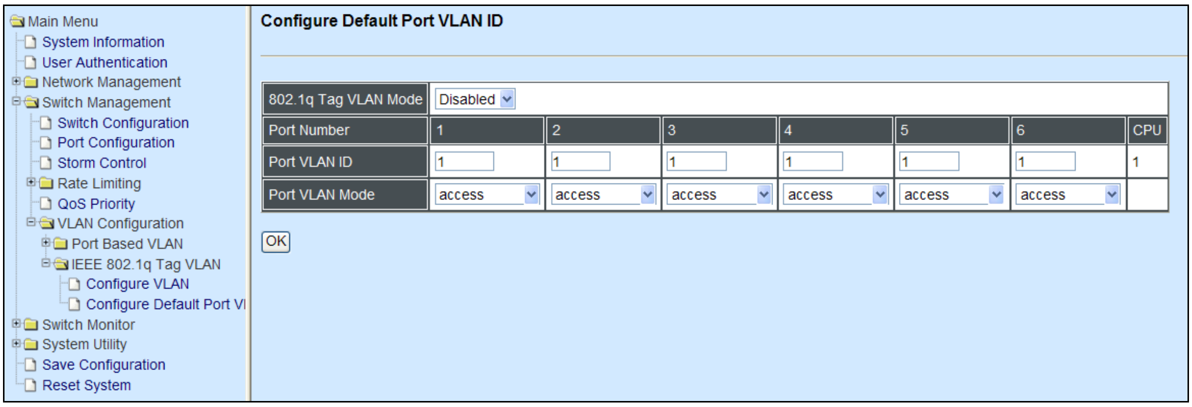
Step 2. Uncheck CPU membership in Default VLAN ID 1.

Step 3. Check CPU membership in VLAN ID 3.

VLAN Members: Tick the checkboxes to determine which ports belong to this VLAN.

3.4.6.3.2 Configure Default Port VLAN ID

The following screen page appears if you choose **IEEE 802.1q Tag VLAN** and then select **Configure Default Port VLAN ID**.



Configure Default Port VLAN ID

802.1q Tag VLAN Mode: Disabled

Port Number	1	2	3	4	5	6	CPU
Port VLAN ID	1	1	1	1	1	1	1
Port VLAN Mode	access	access	access	access	access	access	

802.1q Tag VLAN Mode:

Disabled: When "Disabled" is selected, all settings here will be ignored and the setting depends on Port-Based VLAN.

Enabled: Enable 802.1q tag VLAN settings. If a packet received on a port is untagged, the port VLAN ID will be added. If a packet received is tagged, it will follow the setting of existing VLAN table. If the packet matches entries in VLAN table, the packet will be forwarded based on the setting of VLAN table. If not, the packet will be dropped.

Isolation: When "Isolation" is selected, the device will be forced to follow the port-based VLAN rule shown below and the uplink port will be changed to "trunk" mode automatically. If you prefer the VLAN mode for uplink port other than trunk mode, you can do so by manually selecting its mode from the pull-down menu.

Port Name	1	2	3	4	5	6
Port 1	V					V
Port 2		V				V
Port 3			V			V
Port 4				V		V
Port 5					V	V
Port 6	V	V	V	V	V	V

Default Port VLAN ID: Specify the default port VLAN ID for each port.

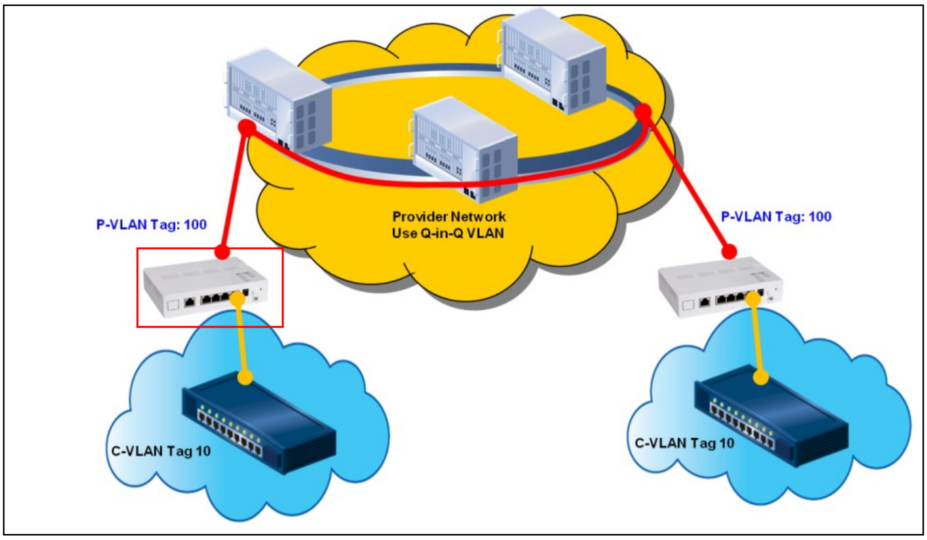
Port VLAN Member: To set up egress traffic as untagged or tagged.

Mode	Port Behavior	
Access	Receive untagged packets only. Drop tagged packets.	
	Send untagged packets only.	
Trunk	Receive tagged packets only. Drop untagged packets.	
	Send tagged packets only.	
Trunk Native	Receive both untagged and tagged packets.	Untagged packets: PVID is added
		Tagged packets: Stay intact
	When sending packets, PVID and VID will be compared. If PVID and VID are the same, PVID will be removed. If PVID and VID are different, the packets with the original tag will be sent.	
Dot1q Tunnel	Receive both untagged and tagged packets and force to add PVID to both untagged and tagged packets.	
	Remove the outer tag when sending packets.	

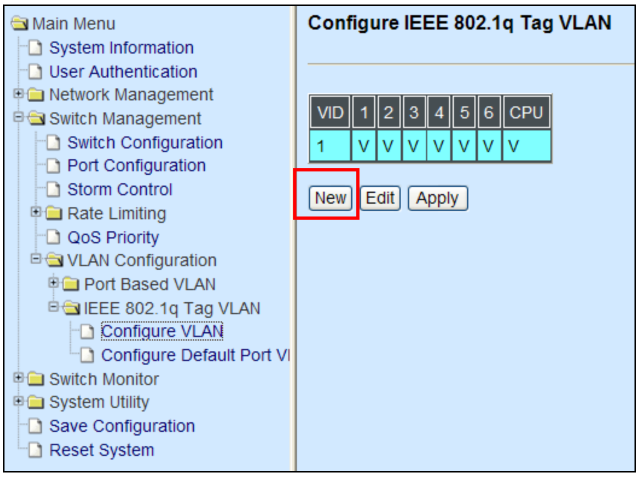
3.4.6.3.3 Configure Q in Q VLAN

This section provides an example on how to configure Q-in-Q using 802.1q function. Follow the steps described below or use them as reference to set up configurations that are suitable for your networking environment.

Scenario:



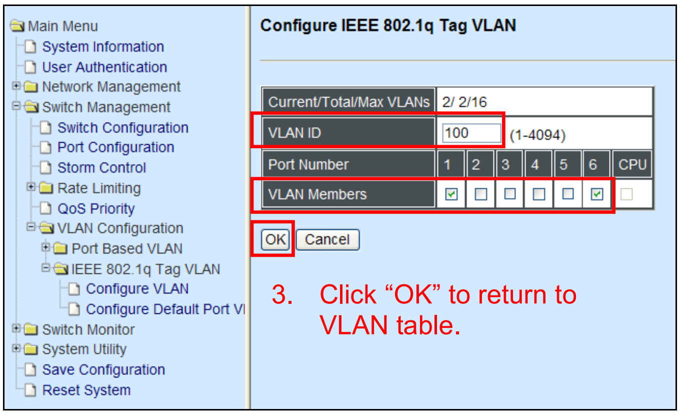
Step 1. Create a VID 100 and select Port 1 & Port 6 as member ports



Configure IEEE 802.1q Tag VLAN

VID	1	2	3	4	5	6	CPU
1	V	V	V	V	V	V	V

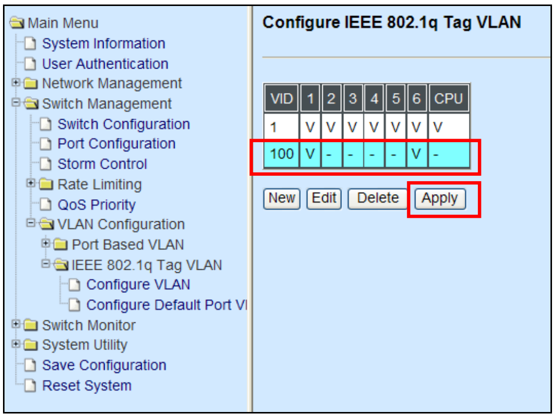
Click "New" to create a new VID



Configure IEEE 802.1q Tag VLAN

Current/Total/Max VLANs	2/ 2/16						
VLAN ID	100	(1-4094)					
Port Number	1	2	3	4	5	6	CPU
VLAN Members	☑	□	□	□	□	☑	□

1. Key in (VLAN ID) 100
2. Select members (Port 1 & Port 6) in this VLAN ID.
3. Click "OK" to return to VLAN table.

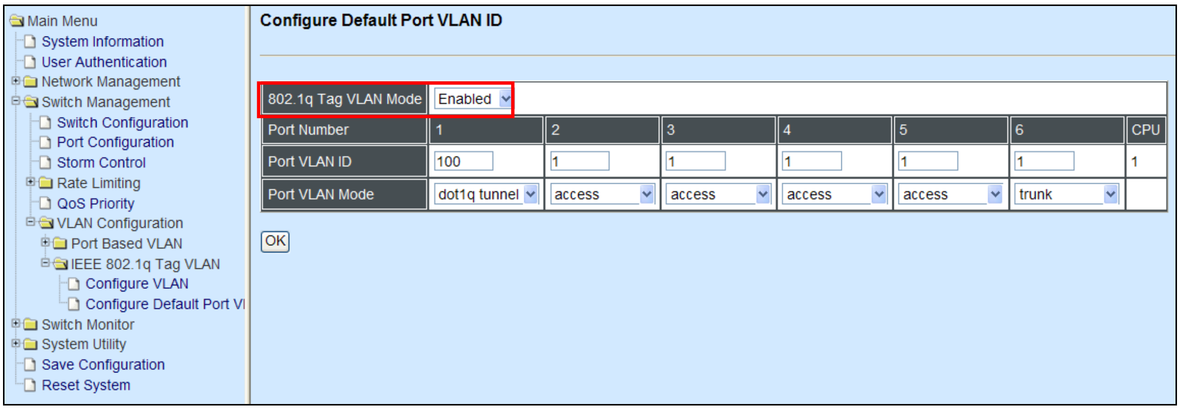


Configure IEEE 802.1q Tag VLAN

VID	1	2	3	4	5	6	CPU
1	V	V	V	V	V	V	V
100	V	-	-	-	-	V	-

1. Check whether VID 100 has been created in VLAN table or not.
2. Click "Apply" to make current settings effective.

Step 2. Enable 802.1q VLAN Mode

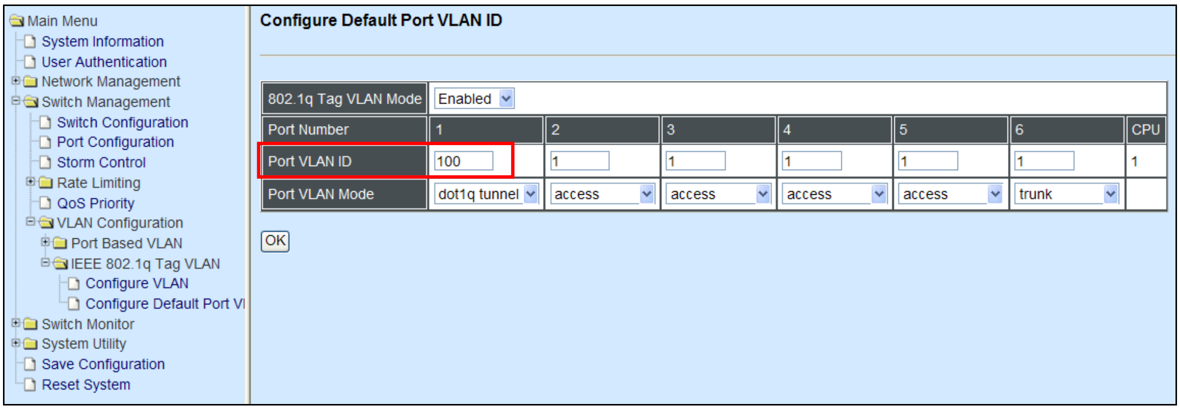


Configure Default Port VLAN ID

802.1q Tag VLAN Mode	Enabled						
Port Number	1	2	3	4	5	6	CPU
Port VLAN ID	100	1	1	1	1	1	1
Port VLAN Mode	dot1q tunnel	access	access	access	access	trunk	

Select “Enabled” from the pull-down menu.

Step 3. Change Port 1’s Port VLAN ID to 100

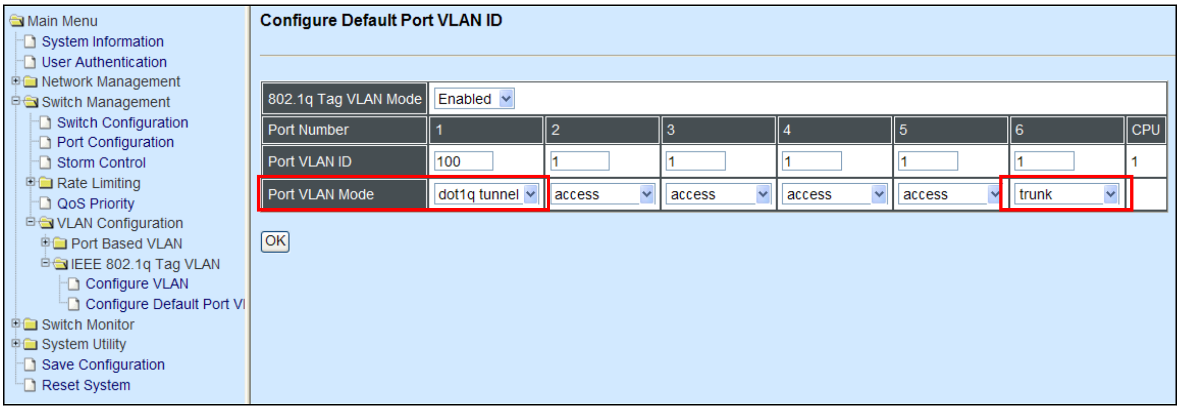


Configure Default Port VLAN ID

802.1q Tag VLAN Mode	Enabled						
Port Number	1	2	3	4	5	6	CPU
Port VLAN ID	100	1	1	1	1	1	1
Port VLAN Mode	dot1q tunnel	access	access	access	access	trunk	

Change Port 1’s Port VLAN ID to 100.

Step 4. Assign Port VLAN Mode to Port 1 & Port 6



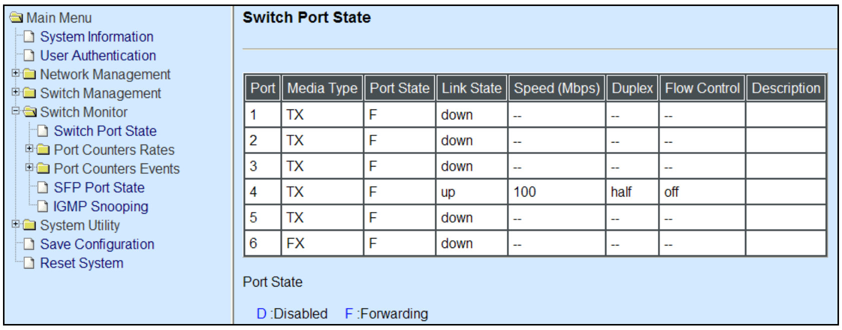
Configure Default Port VLAN ID

802.1q Tag VLAN Mode	Enabled						
Port Number	1	2	3	4	5	6	CPU
Port VLAN ID	100	1	1	1	1	1	1
Port VLAN Mode	dot1q tunnel	access	access	access	access	trunk	

Set Port 1’s mode to “dot1q tunnel” and Port 2’s mode to “trunk”.

3.5 Switch Monitor

Switch Monitor allows users to monitor the real-time operation status of the Smart Switch. Users may monitor the port link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Switch Monitor** from the **Main Menu** and then the following screen page appears.



Switch Port State

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	F	down	--	--	--	
2	TX	F	down	--	--	--	
3	TX	F	down	--	--	--	
4	TX	F	up	100	half	off	
5	TX	F	down	--	--	--	
6	FX	F	down	--	--	--	

Port State

D :Disabled F :Forwarding

1. **Switch Port State:** View the current port media type, port state, etc.

2. **Port Counters Rates:** This folder includes port traffic statistics (rates), port packet error statistics (rates), and port packet analysis statistics (rates).

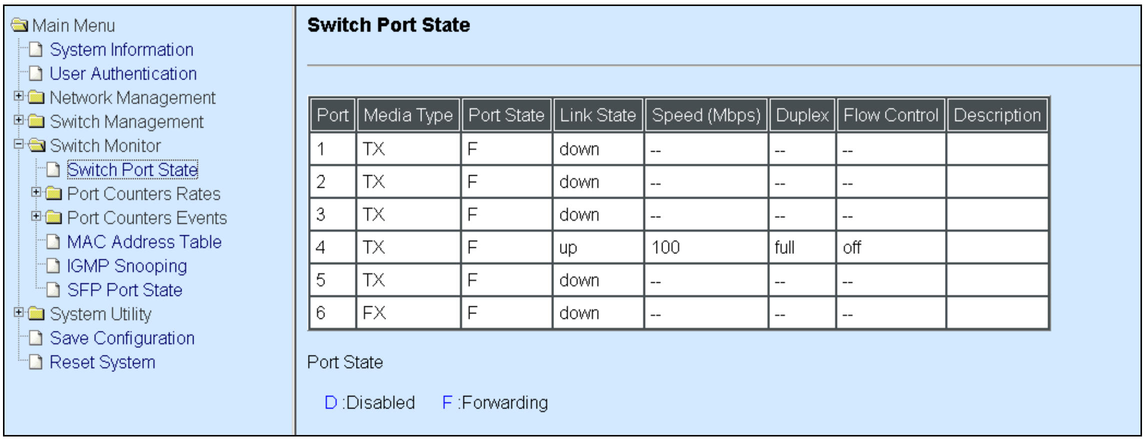
3. **Port Counters Events** This folder includes port traffic statistics (events), port packet error statistics (events), and port packet analysis statistics (events).

4. **SFP Port State:** View the current port's SFP information, e.g. temperature, voltage, TX Bias, TX power, etc.

5. **IGMP Snooping:** View a list of IGMP queries' information in VLAN(s) such as VLAN ID, Querier and reports.

3.5.1 Switch Port State

The following screen page appears if you choose **Switch Monitor** menu and then select **Switch Port State**.



Switch Port State

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	F	down	--	--	--	
2	TX	F	down	--	--	--	
3	TX	F	down	--	--	--	
4	TX	F	up	100	full	off	
5	TX	F	down	--	--	--	
6	FX	F	down	--	--	--	

Port State

D :Disabled F :Forwarding

Port Number: The number of the port.

Media Type: The media type of the port, either Copper (TX) or Fiber (FX).

Port Sate: This shows each port's state which can be **D** (Disabled) or **F** (Forwarding).

> **Disabled:** A port in this state can not receive and forward packets.
>
> **Forwarding:** Packets can be forwarded.

Link State: The current link status of the port, either up or down.

Speed (Mbps): The current operation speed of each port.

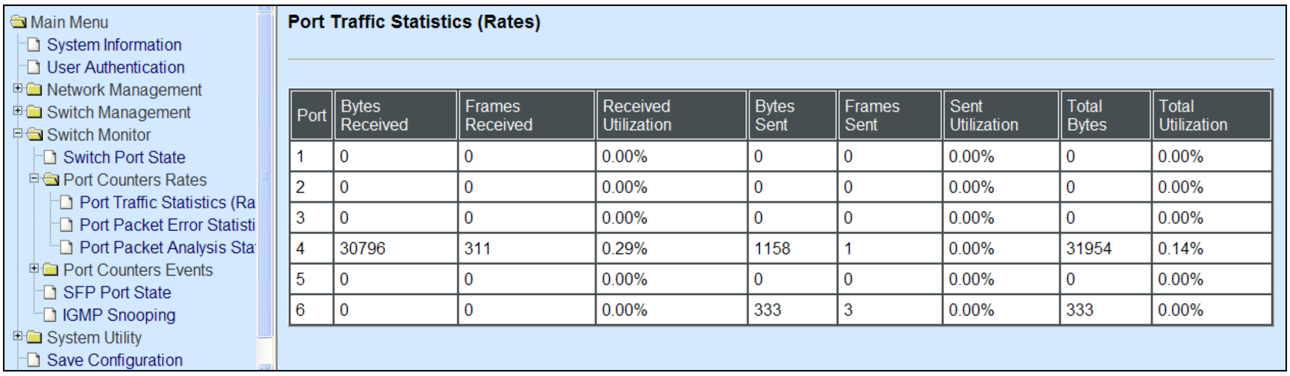
Duplex: The current operation Duplex mode of each port, either Full or Half.

Flow Control: The current state of Flow Control, either on or off.

Description: This shows the description of this port described in "Port Configuration".

3.5.2 Port Counters Rates

Click the **Port Counters Rates** from the **Switch Monitor** menu and then the following screen page appears.



Port Traffic Statistics (Rates)

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	30796	311	0.29%	1158	1	0.00%	31954	0.14%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	333	3	0.00%	333	0.00%

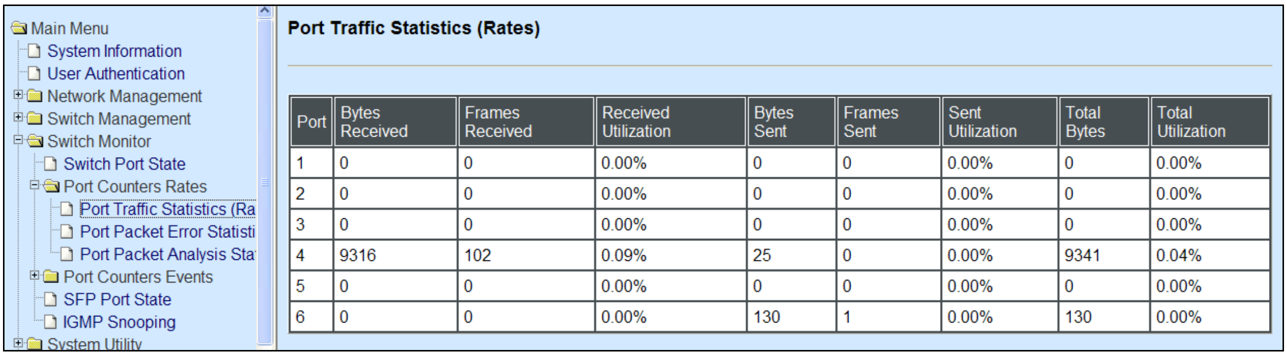
1. **Port Traffic Statistics (Rates):** View each port's frames and bytes received or sent, utilization, etc.

2. **Port Packet Error Statistics (Rates):** View each port's traffic condition of error packets, e.g. CRC, fragment, Jabber, etc.

3. **Port Packet Analysis Statistics (Rates):** View each port's analysis history.

3.5.2.1 Port Traffic Statistics (Rates)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Traffic Statistics (Rates)**.



Port Traffic Statistics (Rates)

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	0	0	0.00%	0	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%
3	0	0	0.00%	0	0	0.00%	0	0.00%
4	9316	102	0.09%	25	0	0.00%	9341	0.04%
5	0	0	0.00%	0	0	0.00%	0	0.00%
6	0	0	0.00%	130	1	0.00%	130	0.00%

Bytes Received: The total bytes received from each port.

Frames Received: The total frames received from each port.

Received Utilization: The ratio of each port receiving traffic and current port's total bandwidth.

Bytes Sent: The total bytes sent from current port.

Frames Sent: The total frames sent from current port.

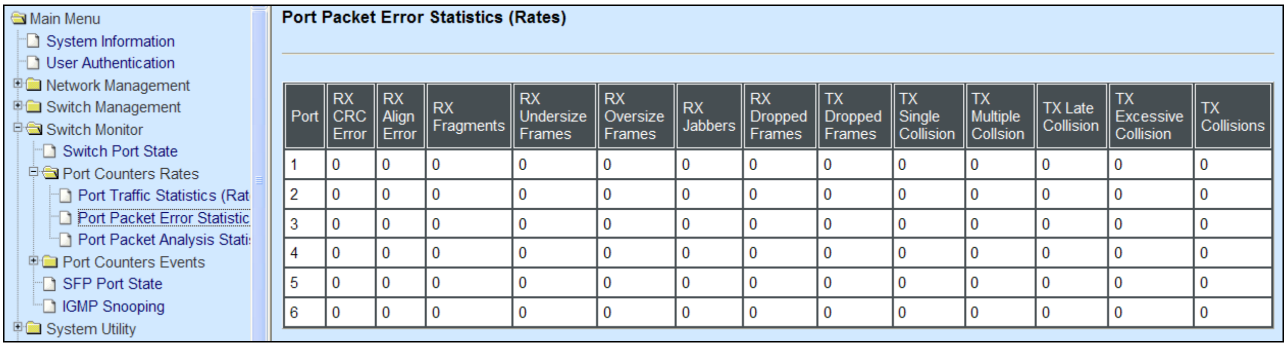
Sent Utilization: The ratio of real port sending traffic ratio to current port of total bandwidth.

Total Bytes: The total bytes of receiving and send from current port.

Total Utilization: Real traffic of received and sent to current port of total bandwidth.

3.5.2.2 Port Packet Error Statistics (Rates)

Port Packet Error Statistics mode counters allow users to view the port error of the Smart Switch. The event mode counter is calculated since the last time that counter was reset or cleared. Select **Port Packet Error Statistics** from the **Switch Monitor** menu and then the following screen page appears.



Port Packet Error Statistics (Rates)

Port	RX CRC Error	RX Align Error	RX Fragments	RX Undersize Frames	RX Oversize Frames	RX Jabbers	RX Dropped Frames	TX Dropped Frames	TX Single Collision	TX Multiple Collsion	TX Late Collision	TX Excessive Collision	TX Collisions
1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0

RX CRC Errors: The number of packets received by a port that are between 64 and 1522 bytes long in length (excluding framing bits but including FCS) and have a bad FCS with an integral number of bytes.

RX Alignment Errors: The number of packets received by a port that have are between 64 and 1522 bytes in length (excluding framing bits but including FCS) and have a bad FCS with a non-integral number of bytes.

RX Fragments: Total frames received which are less than 64 bytes or frames without SFD and are less than 64 bytes in length.

RX Filtered Error: The number of packets that are filtered or dropped due to security reasons or lack of destination.

RX Undersized Frames: Total frames received shorter than 64 bytes.

RX Oversized Frames: Total frames received longer than maximum frame size.

RX Jabbers: Total frames received that have both Oversize and CRC error.

RX Dropped frames: Total received frames dropped due to resources shortage.

TX Dropped frames: The total frames that are not transmitted due to resources shortage.

TX Single Collisions: The total single collision detected.

TX Multiple Collisions: The total multiple collision detected.

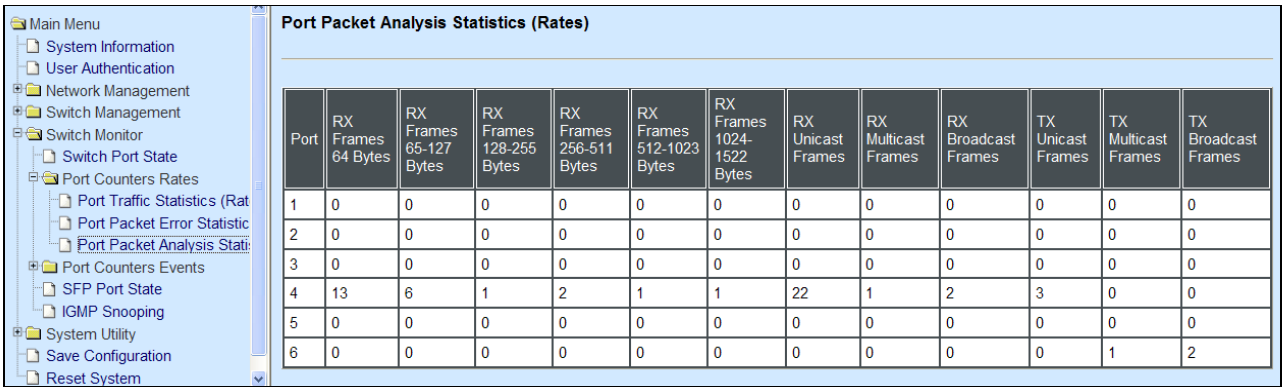
TX Late Collisions: The total late collision detected.

TX Excessive Collisions: The total excessive collision detected.

TX Total Collisions: The total frames collision detected.

3.5.2.3 Port Packet Analysis Statistics (Rates)

Port Packet Analysis Statistics Mode Counters allow users to view the port analysis history of the Smart Switch. Event mode counters are calculated since the last time that counter was reset or cleared. Select **Port Packet Analysis Statistics** from the **Switch Monitor** menu and then the following screen page appears.



Port Packet Analysis Statistics (Rates)

Port	RX Frames 64 Bytes	RX Frames 65-127 Bytes	RX Frames 128-255 Bytes	RX Frames 256-511 Bytes	RX Frames 512-1023 Bytes	RX Frames 1024-1522 Bytes	RX Unicast Frames	RX Multicast Frames	RX Broadcast Frames	TX Unicast Frames	TX Multicast Frames	TX Broadcast Frames
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0
4	13	6	1	2	1	1	22	1	2	3	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	1	2

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-127 Bytes: 65-127 bytes frames received.

RX Frames 128-255 Bytes: 128-255 bytes frames received.

RX Frames 256-511 Bytes: 256-511 bytes frames received.

RX Frames 512-1023 Bytes: 512-1023 bytes frames received.

RX Frames 1024-1522 Bytes: 1024-1522 bytes frames received.

RX Unicast Frames: Good unicast frames received.

RX Multicast Frames: Good multicast frames received.

RX Broadcast Frames: Good broadcast frames received.

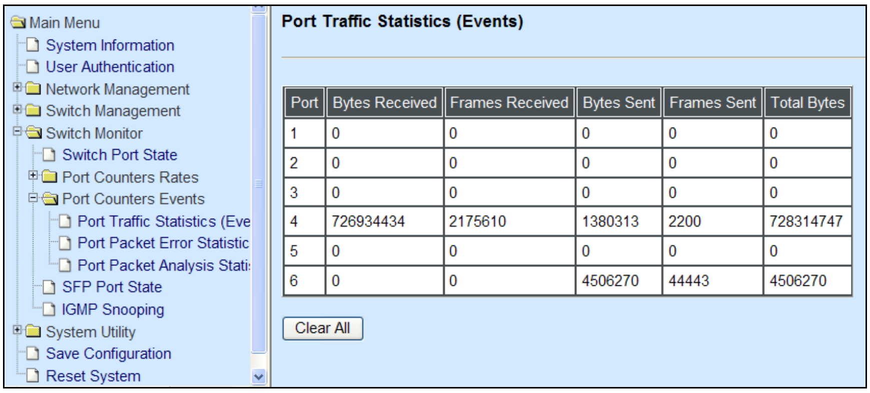
TX Unicast Frames: Good unicast packets sent.

TX Multicast Frames: Good multicast packets sent.

TX Broadcast Frames: Good broadcast packets sent.

3.5.3 Port Counters Events

The event mode of port counters will be re-calculated when that counter is reset or cleared. Click **Port counters Events** folder and then three options appear.



Port Traffic Statistics (Events)

Port	Bytes Received	Frames Received	Bytes Sent	Frames Sent	Total Bytes
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	726934434	2175610	1380313	2200	728314747
5	0	0	0	0	0
6	0	0	4506270	44443	4506270

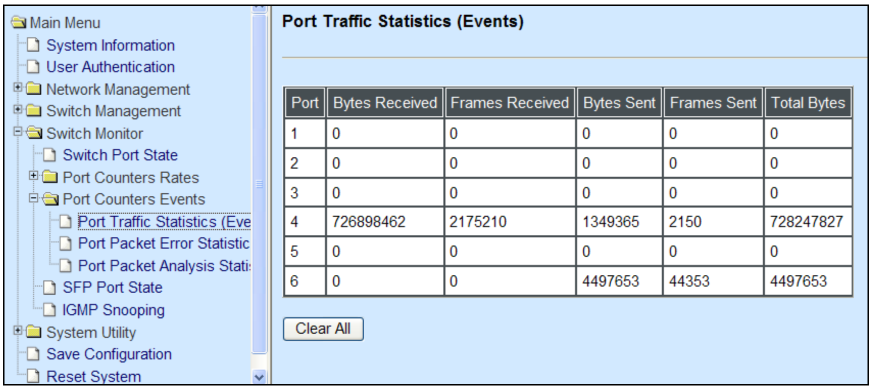
1. **Port Traffic Statistics (Events):** View the number of bytes received, frames received, bytes sent, frames sent, and total bytes and clear each row's statistics.

2. **Port Packet Error Statistics (Events):** View the number of CRC errors, undersize frames, oversize frames, etc and clear each row's statistics.

3. **Port Packet analysis Statistics (Events):** View each port's analysis history and clear each row's statistics.

3.5.3.1 Port Traffic Statistics (Events)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Traffic Statistics (Events)**.



Port Traffic Statistics (Events)

Port	Bytes Received	Frames Received	Bytes Sent	Frames Sent	Total Bytes
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	726898462	2175210	1349365	2150	728247827
5	0	0	0	0	0
6	0	0	4497653	44353	4497653

Bytes Received: Total bytes received from each port.

Frames Received: Total frames received from each port.

Bytes Sent: The total bytes sent from current port.

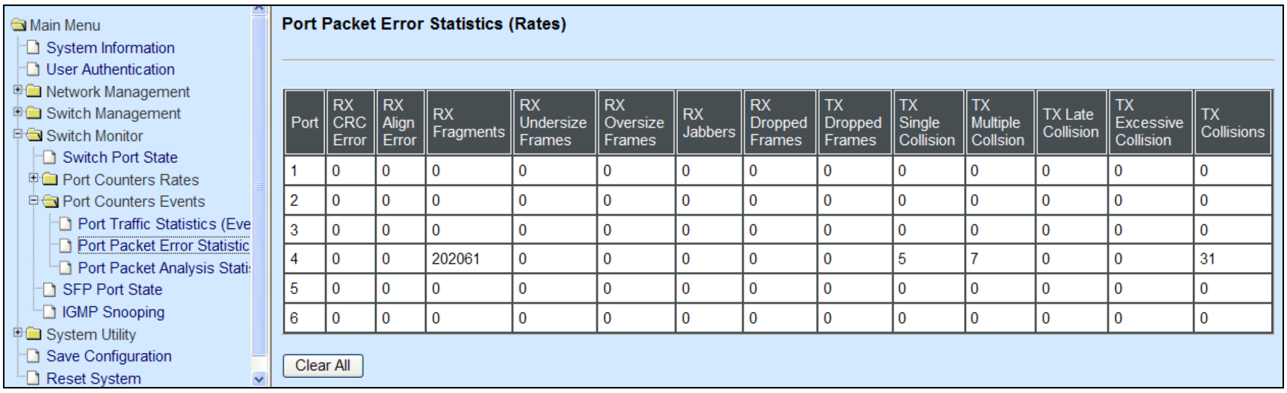
Frames Sent: The total frames sent from current port.

Total Bytes: Total bytes of receiving and send from current port.

Clear All: Click “Click All” button to clear all ports’ statistics.

3.5.3.2 Port Packet Error Statistics (Events)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Error Statistics (Events)**.



Port Packet Error Statistics (Rates)

Port	RX CRC Error	RX Align Error	RX Fragments	RX Undersize Frames	RX Oversize Frames	RX Jabbers	RX Dropped Frames	TX Dropped Frames	TX Single Collision	TX Multiple Collsion	TX Late Collision	TX Excessive Collision	TX Collisions
1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	202061	0	0	0	0	0	5	7	0	0	31
5	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0

RX CRC Error: CRC error frames received.

RX Alignment Error: The number of packets received that have a bad FCS with an integral number of bytes.

RX Fragments: Fragment frames received.

RX Undersize Frames: Undersize frames received.

RX Oversize Frames: Oversize frames received.

RX Jabbers: Jabber frames received.

RX Dropped Frames: The number of packets received that are dropped.

TX Dropped Frames: The number of packets transmitted that are dropped.

TX Single Collision: Total single collision detected.

TX Multiple Collision: Total multiple collision detected.

TX Late Collision: Total late collision detected.

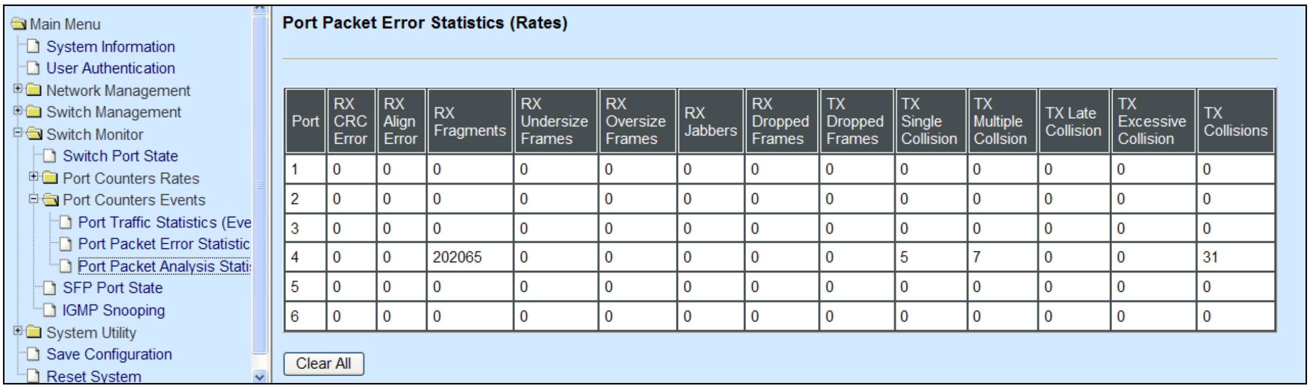
TX Excessive Collision: Total excessive collision detected.

TX Collision: Total frames collision detected.

Clear All: Click **"Click All"** button to clear all ports' statistics.

3.5.3.3 Port Packet Analysis Statistics (Events)

The following screen page appears if you choose **Port Counters Rates** and then select **Port Packet Analysis Statistics (Events)**.



Port Packet Error Statistics (Rates)

Port	RX CRC Error	RX Align Error	RX Fragments	RX Undersize Frames	RX Oversize Frames	RX Jabbers	RX Dropped Frames	TX Dropped Frames	TX Single Collision	TX Multiple Collsion	TX Late Collision	TX Excessive Collision	TX Collisions
1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	202065	0	0	0	0	0	5	7	0	0	31
5	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-127 Bytes: 65-127 bytes frames received.

RX Frames 128-255 Bytes: 128-255 bytes frames received.

RX Frames 256-511 Bytes: 256-511 bytes frames received.

RX Frames 512-1023 Bytes: 512-1023 bytes frames received.

RX Frames 1024-MAX Bytes: Over 1024 bytes frames received.

RX Unicast Frames: Good unicast frames received.

RX Multicast Frames: Good multicast frames received.

RX Broadcast Frames: Good broadcast frames received.

TX Unicast Frames: Good unicast packets sent.

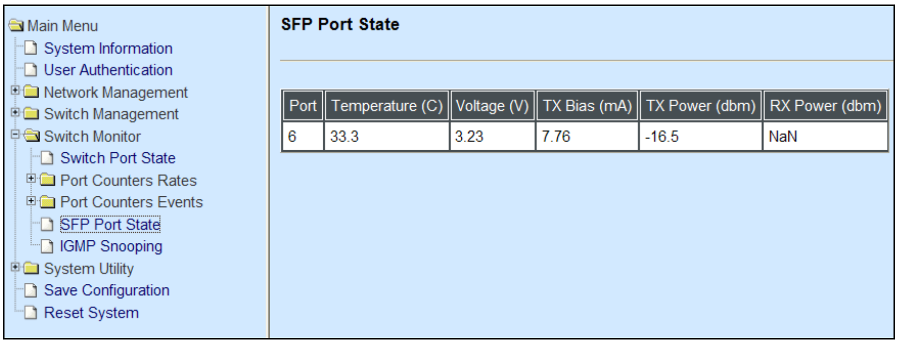
TX Multicast Frames: Good multicast packets sent.

TX Broadcast Frames: Good broadcast packets sent.

Clear All & Clear: Click "Click All" to clear all ports' statistics or click "Clear" in each row to clear the corresponding port's statistics.

3.5.4 SFP Port State

SFP Port State displays the information about slide-in SFP transceiver e.g. Temperature, Voltage, TX Bias, etc. Select **SFP Port State** and then the following screen page appears.



SFP Port State

Port	Temperature (C)	Voltage (V)	TX Bias (mA)	TX Power (dbm)	RX Power (dbm)
6	33.3	3.23	7.76	-16.5	NaN

Port Number: The port number of the slide-in SFP module.

Temperature (C): The Slide-in SFP module operation temperature.

Voltage (V): The Slide-in SFP module operation voltage.

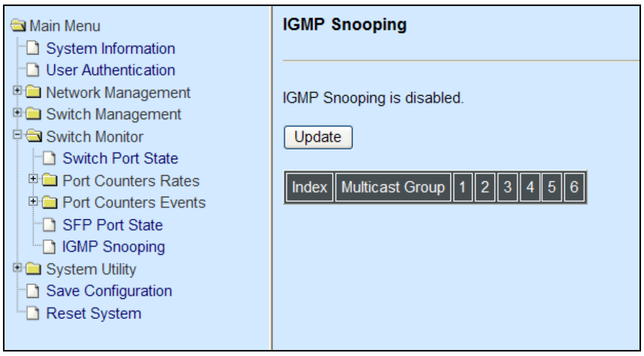
TX Bias (mA): The Slide-in SFP module operation current.

TX Power (dbm): The Slide-in SFP module optical Transmission power.

RX Power (dbm): The Slide-in SFP module optical Receiver power.

3.5.5 IGMP Snooping

Click the option **IGMP Snooping** from the **Switch Monitor** menu and then the following screen page appears.



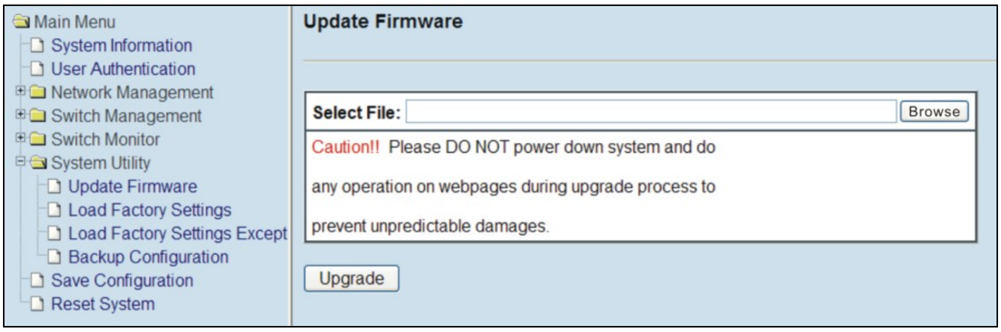
IGMP Snooping

IGMP Snooping is disabled.

Index	Multicast Group	1	2	3	4	5	6

3.6 System Utility

Select the folder **System Utility** from the main menu and then the following screen page appears.



Update Firmware

Select File:

Caution!! Please DO NOT power down system and do

any operation on webpages during upgrade process to

prevent unpredictable damages.

1. **Update Firmware:** This allows users to update the latest firmware.

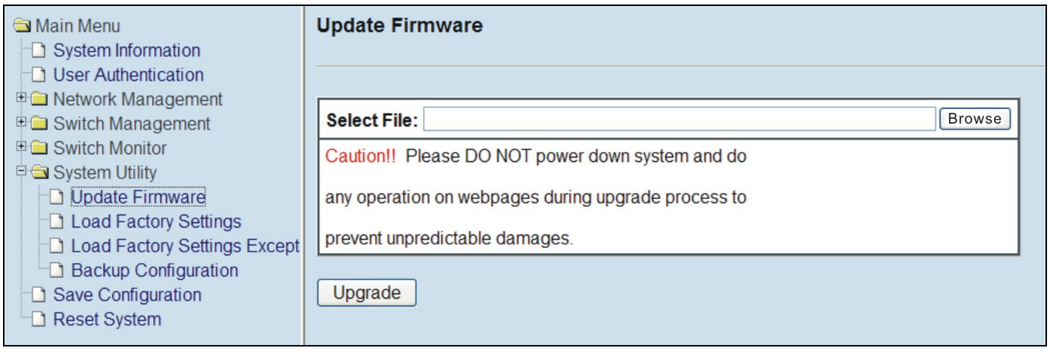
2. **Load Factory Setting:** Load Factory Setting will set the configuration of the Smart Switch back to the factory default settings. The IP and Gateway addresses will be set to the factory default as well.

3. **Load Factory Setting Except Network Configuration:** Selecting this function will also restore the configuration of the Smart Switch to its original factory default settings. However, this will not reset the IP and Gateway addresses to the factory default.

4. **Backup Configuration:** To backup a configuration file and restore the previously-saved configuration via TFTP server.

3.6.1 Update Firmware

Click the option **Update Firmware** from the **System Utility** menu and then the following screen page appears.



Update Firmware

Select File:

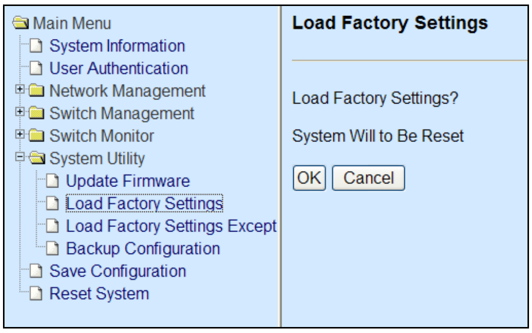
Caution!! Please DO NOT power down system and do any operation on webpages during upgrade process to prevent unpredictable damages.

Click the **"Browse"** button to select the Firmware that you would like to update.

3.6.2 Load Factory Settings

Load Factory Settings will set all configurations of the Smart Switch back to the factory default settings, including the IP and Gateway address. This function is useful when network administrators would like to re-configure the system. A system reset is required to make all changes effective after Load Factory Setting.

Select **Load Factory Setting** from the **System Utility** menu and then the following screen page appears.



Load Factory Settings

Load Factory Settings?

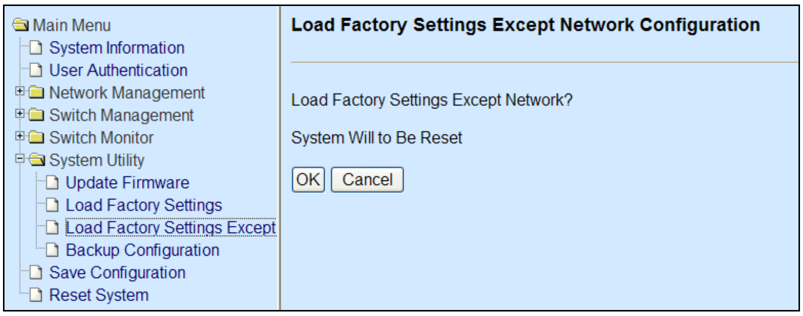
System Will to Be Reset

Click the **"OK"** button to restore the Smart Switch back to the defaults.

3.6.3 Load Factory Settings Except Network Configuration

Load Factory Settings Except Network Configuration will set all configurations of the Smart Switch back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. **Load Factory Settings Except Network Configuration** is very useful when network administrators need to re-configure the system "REMOTELY" because conventional Factory Reset will bring network settings back to default and lose all remote network connections.

Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, then the following screen page shows up.



Load Factory Settings Except Network Configuration

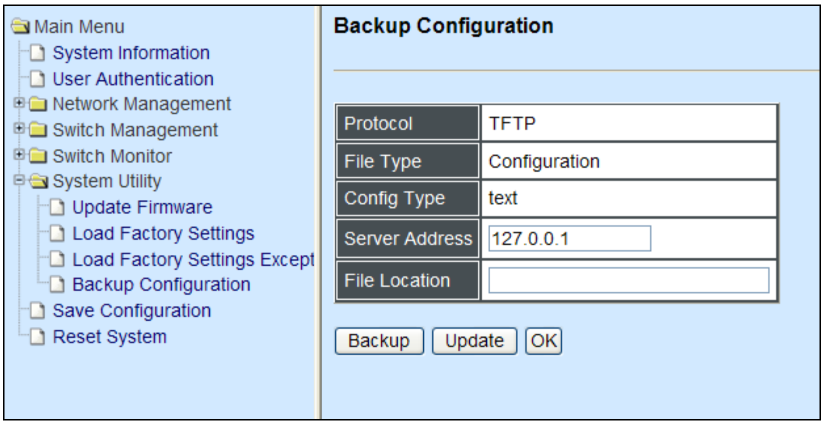
Load Factory Settings Except Network?

System Will to Be Reset

Click the **"OK"** button to restore the Smart Switch back to the defaults excluding network configurations.

3.6.4 Backup Configuration

Select **Backup Configuration** from the **System Utility** menu and then the following screen page appears.



Backup Configuration

Protocol	TFTP
File Type	Configuration
Config Type	text
Server Address	127.0.0.1
File Location	

Protocol: Backup or restore process can only be made via TFTP.

File Type: Backup or restore a configuration file.

Config Type: Currently, the configuration file backed up will be stored in text file format.

Server Address: Specify the TFTP server IP address.

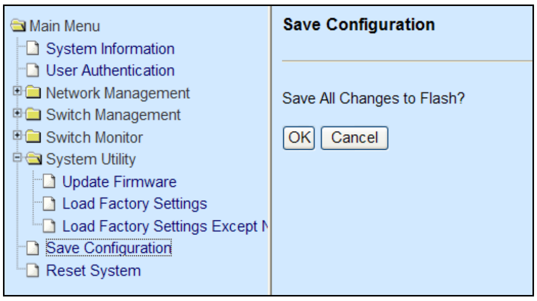
File Location: Specify a file name for the configuration that you would like to backup or a file name that you would like to restore to the Smart Switch.

Click the **"Backup"** button to save a copy of configuration file via TFTP.

Click the **"Update"** button to restore a previously-saved configuration file via TFTP.

3.7 Save Configuration

In order to save configuration settings permanently, users need to save configuration first before resetting the Smart Switch. Select **Save Configuration** from the **Main Menu** and then the following screen page appears.



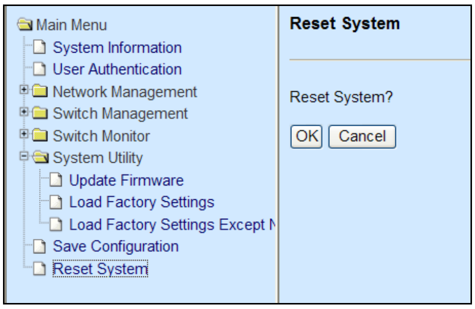
Save Configuration

Save All Changes to Flash?

Click the **"OK"** button to save changes or running configurations to Flash.

3.8 Reset System

After any configuration changes, **Reset System** can make changes effective. Select **Reset System** from the **Main menu** and then the following screen page appears.



Reset System

Reset System?

Click the **"OK"** button to restart the Smart Switch.

APPENDIX A: Set Up DHCP Auto-Provisioning

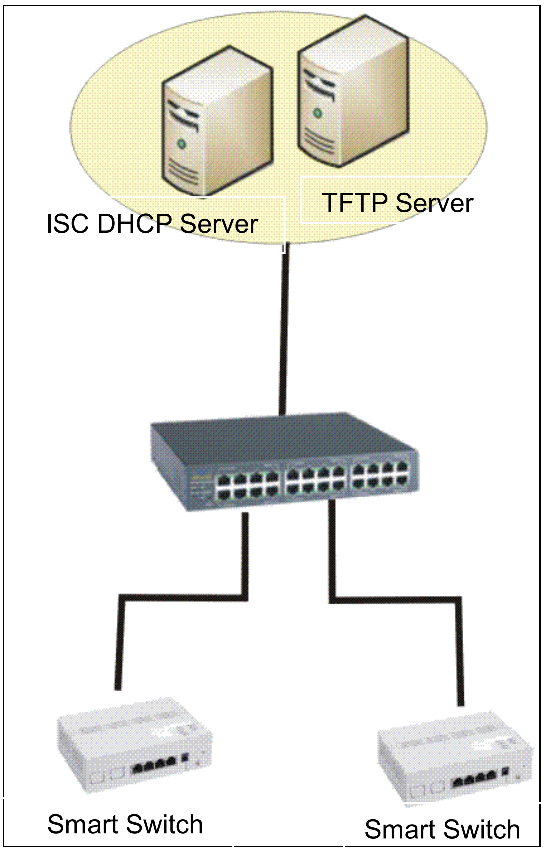
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased can support DHCP Auto-provisioning. Setup procedures and auto-provisioning process are described below for your reference.

A. Setup Procedures

Follow the steps below to set up Auto Provisioning server, modify dhcpd.conf file and generate a copy of configuration file.

Step 1. Setup Environment

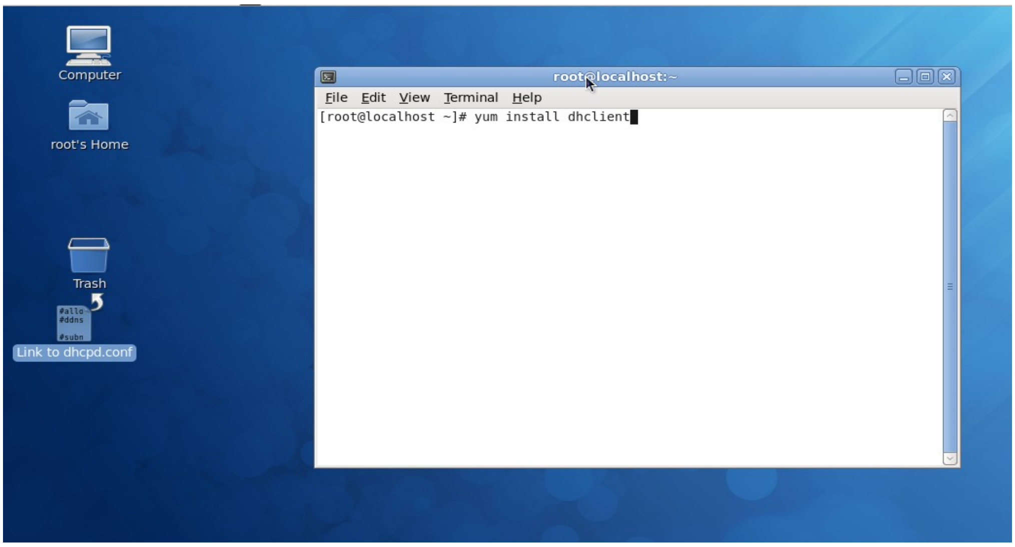
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Typology Example

Step 2. Set up Auto Provision Server

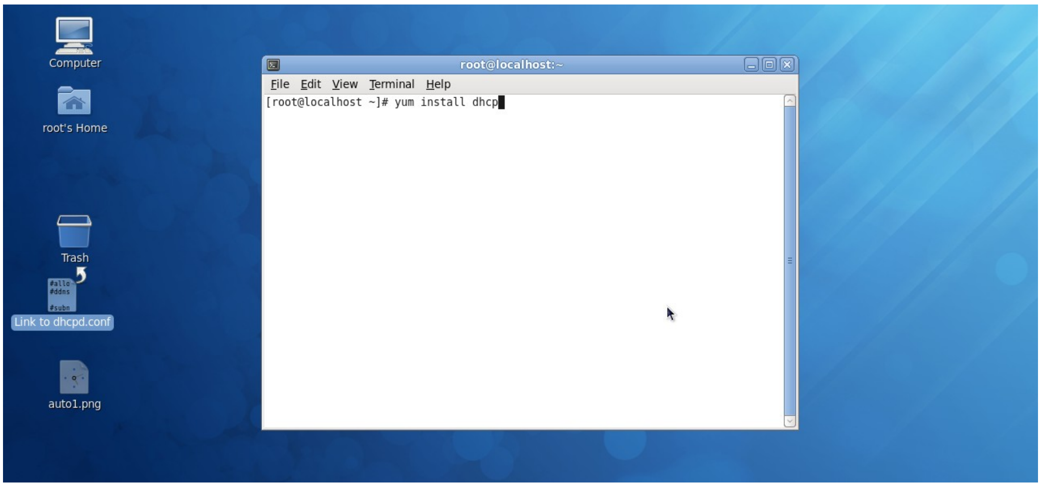
- **Update DHCP Client**



```
[root@localhost ~]# yum install dhclient
```

Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

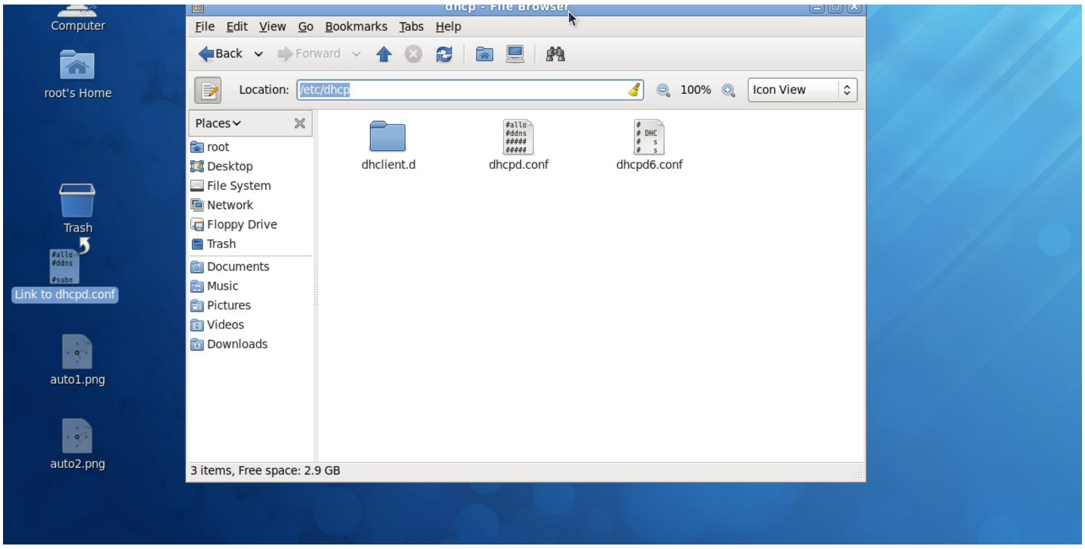
- **Install DHCP Server**



```
[root@localhost ~]# yum install dhcp
```

Issue “yum install dhcp” command to install DHCP server.

- **Copy dhcpd.conf to /etc/dhcp/ directory**

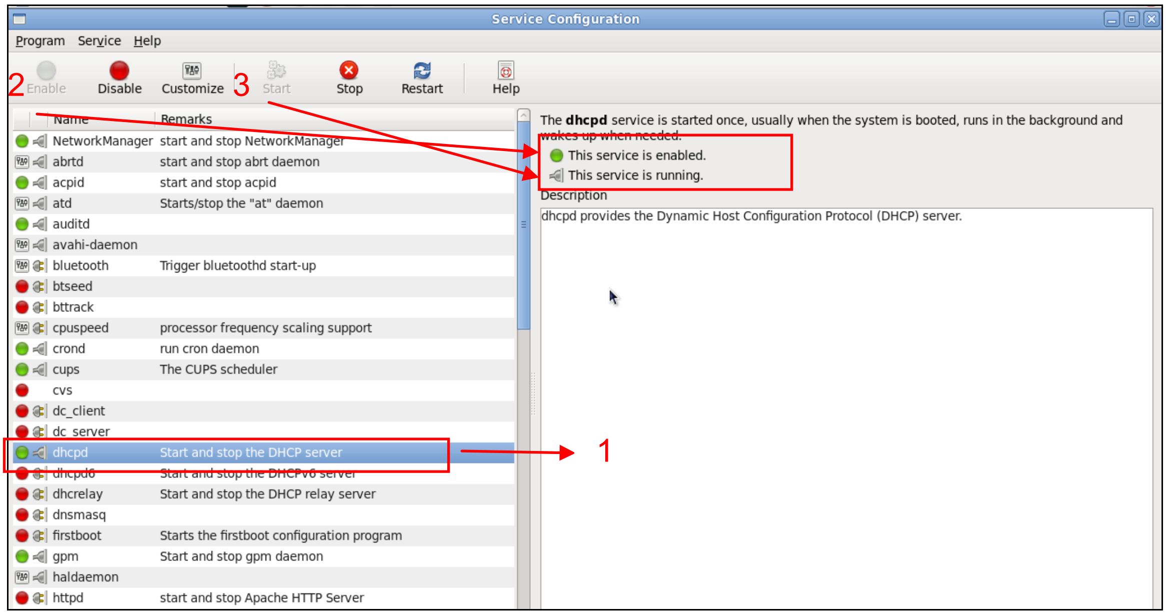


3 items, Free space: 2.9 GB

Copy dhcpd.conf file provided by the vendor to /etc/dhcp/ directory.

Please note that each vendor has their own way to define auto provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



Name	Remarks
NetworkManager	start and stop NetworkManager
abrtd	start and stop abrt daemon
acpid	start and stop acpid
atd	Starts/stop the "at" daemon
auditd	
avahi-daemon	
bluetooth	Trigger bluetoothd start-up
btseed	
bttrack	
cpuspeed	processor frequency scaling support
crond	run cron daemon
cups	The CUPS scheduler
cvs	
dc_client	
dc_server	
dhcpd	Start and stop the DHCP server
dhcpd6	Start and stop the DHCPv6 server
dhcrelay	Start and stop the DHCP relay server
dnsmasq	
firstboot	Starts the firstboot configuration program
gpm	Start and stop gpm daemon
haldaemon	
httpd	start and stop Apache HTTP Server

The **dhcpd** service is started once, usually when the system is booted, runs in the background and wakes up when needed.

● This service is enabled.

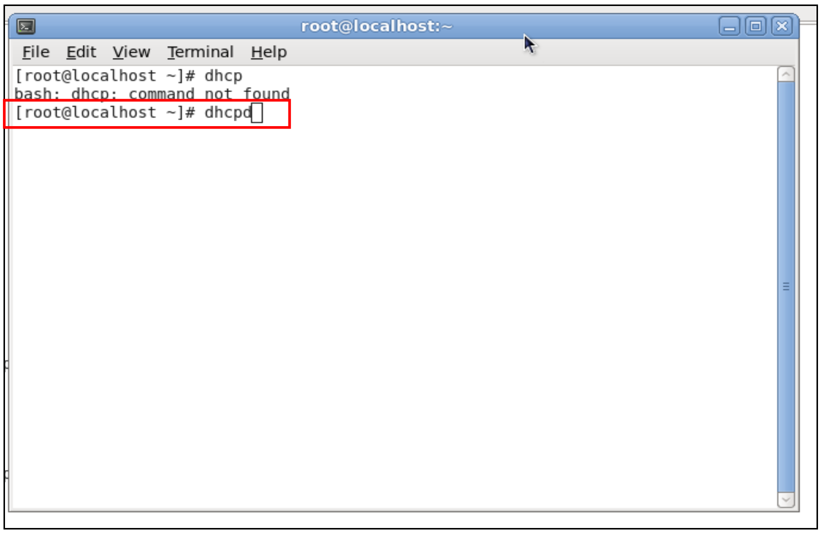
This service is running.

Description

dhcpd provides the Dynamic Host Configuration Protocol (DHCP) server.

1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

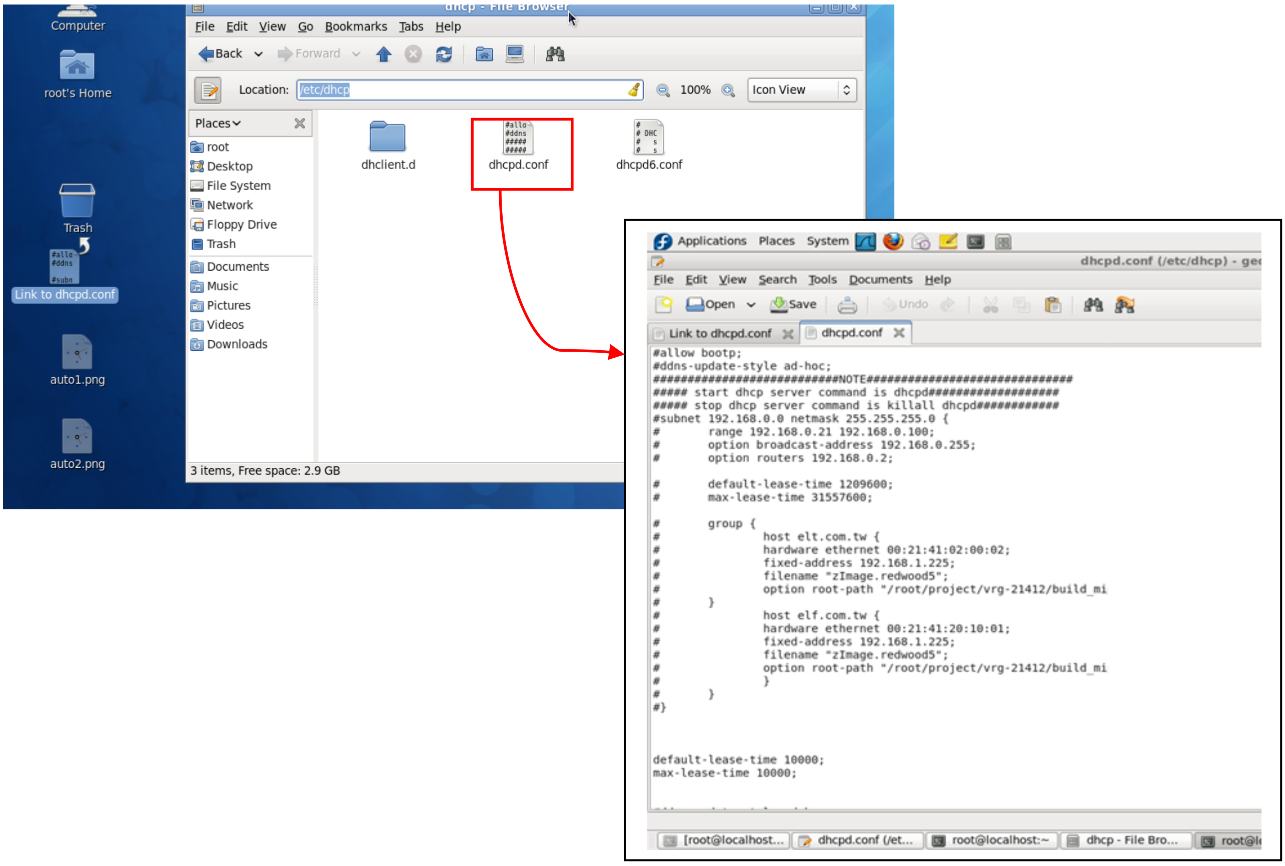
NOTE: *DHCP service can also be enabled using CLI. Issue "dhcpd" command to enable DHCP service.*



```
[root@localhost ~]# dhcp
bash: dhcp: command not found
[root@localhost ~]# dhcpd
```

Step 3. Modify dhcpd.conf file

- **Open dhcpd.conf file in /etc/dhcp/ directory**

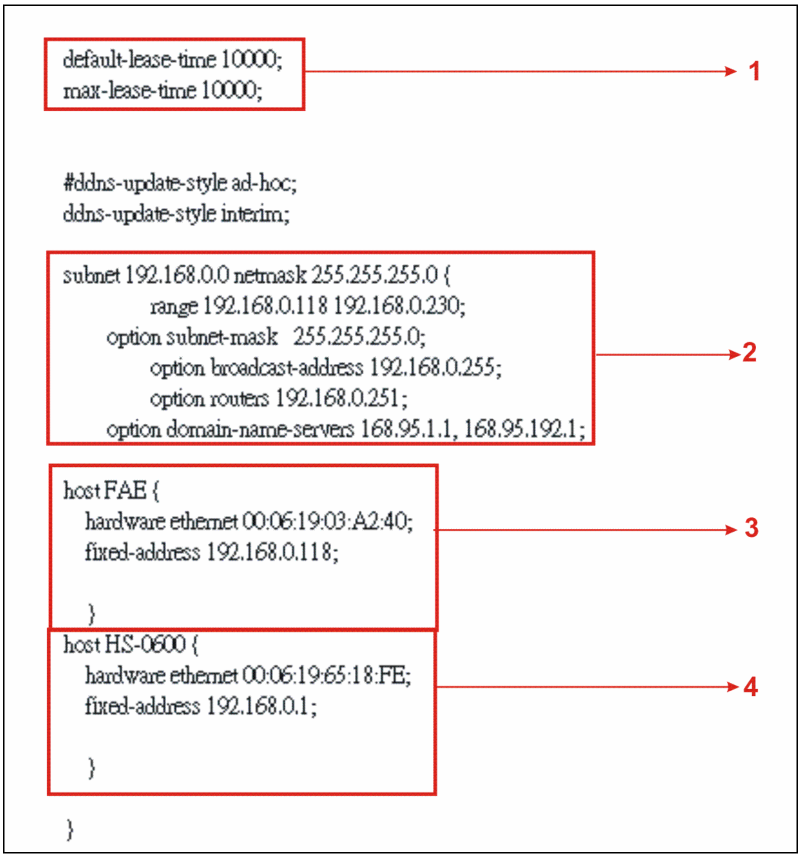


```
#allow bootp;
#ddns-update-style ad-hoc;
############################NOTE################################
##### start dhcp server command is dhcpd###################
##### stop dhcp server command is killall dhcpd############
#subnet 192.168.0.0 netmask 255.255.255.0 {
#       range 192.168.0.21 192.168.0.100;
#       option broadcast-address 192.168.0.255;
#       option routers 192.168.0.2;

#       default-lease-time 1209600;
#       max-lease-time 31557600;

#       group {
#               host elt.com.tw {
#               hardware ethernet 00:21:41:02:00:02;
#               fixed-address 192.168.1.225;
#               filename "zImage.redwood5";
#               option root-path "/root/project/vrg-21412/build_mi
#       }
#               host elf.com.tw {
#               hardware ethernet 00:21:41:20:10:01;
#               fixed-address 192.168.1.225;
#               filename "zImage.redwood5";
#               option root-path "/root/project/vrg-21412/build_mi
#               }
#       }
#}


default-lease-time 10000;
max-lease-time 10000;
```

Double-click dhcpd.conf placed in /etc/dhcp/ directory to open it.

● Modify dhcpd.conf file

The following marked areas in dhcpd.conf file can be modified with values that work with your networking environment.



```
default-lease-time 10000;
max-lease-time 10000;


#ddns-update-style ad-hoc;
ddns-update-style interim;

subnet 192.168.0.0 netmask 255.255.255.0 {
            range 192.168.0.118 192.168.0.230;
      option subnet-mask   255.255.255.0;
            option broadcast-address 192.168.0.255;
            option routers 192.168.0.251;
      option domain-name-servers 168.95.1.1, 168.95.192.1;
host FAE {
   hardware ethernet 00:06:19:03:A2:40;
   fixed-address 192.168.0.118;

   }
host HS-0600 {
   hardware ethernet 00:06:19:65:18:FE;
   fixed-address 192.168.0.1;

   }

}
```

1. Define DHCP default and maximum lease time in seconds.

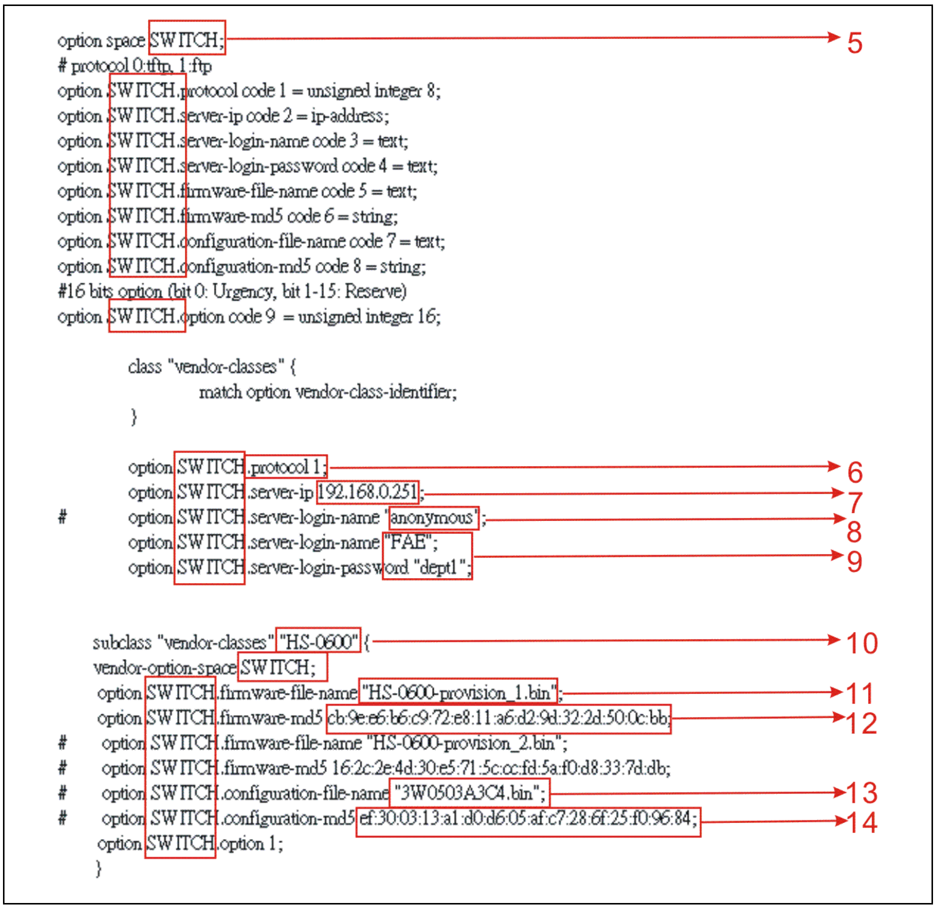
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

   Maximum lease time: This is the maximum length of time that the server will lease for.

2. Define subnet, subnet mask, IP range, broadcast address, router address and DNS server address.

3. Map a host's MAC address to a fixed IP address.

4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.

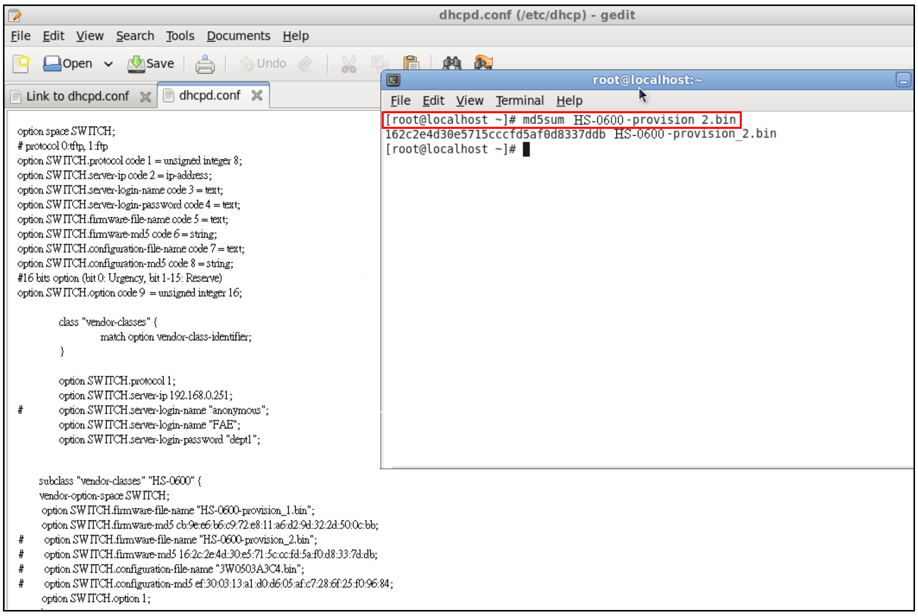


```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name 'anonymous';
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
     }
```

5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify the product model name.
11. Specify the firmware filename.
12. Specify the MD5 for firmware image.
13. Specify the configuration filename.
14. Specify the MD5 for configuration file.

NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs in the initial of each line.*

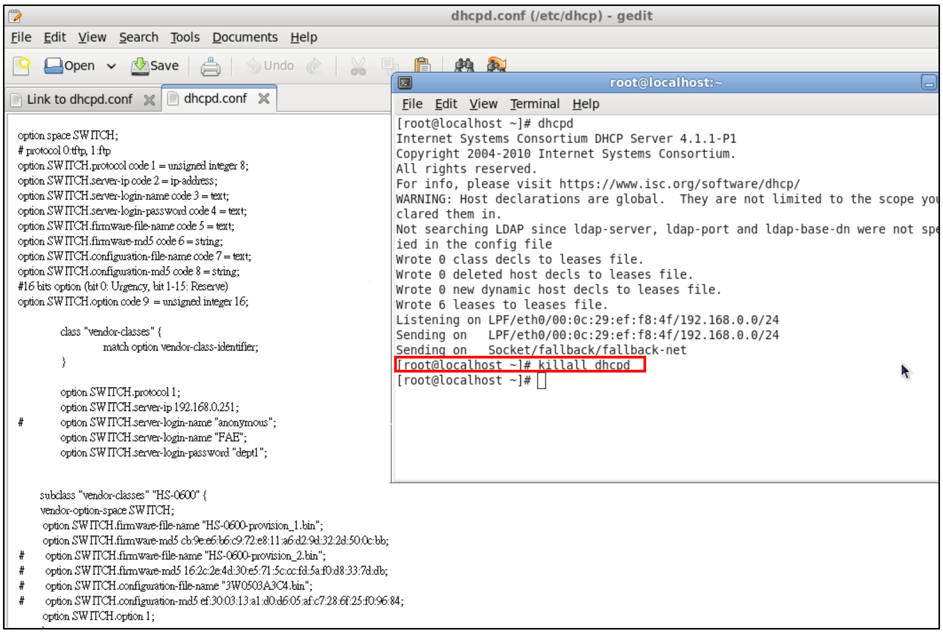
NOTE 2: *You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

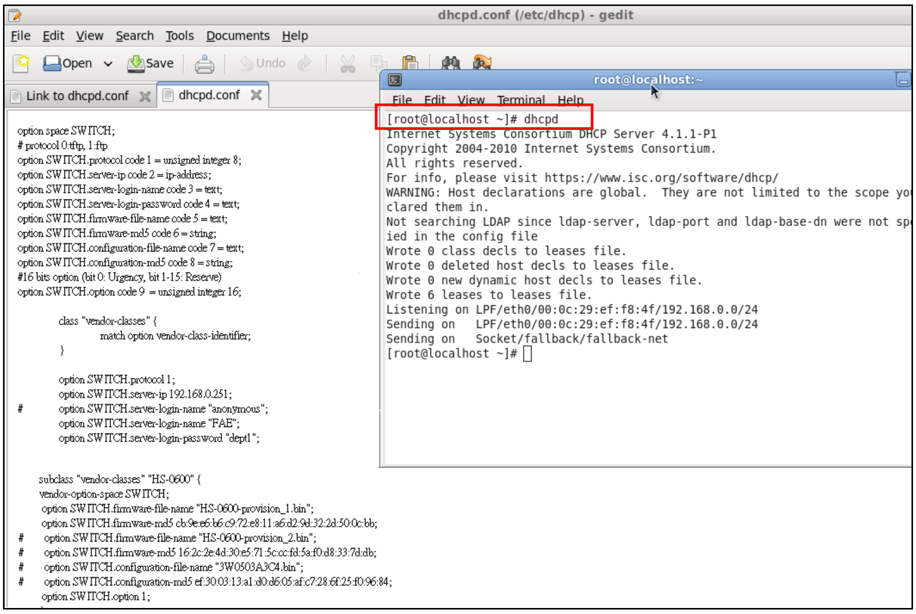
```
[root@localhost ~]# md5sum  HS-0600-provision_2.bin
162c2e4d30e5715cccfd5af0d8337ddb  HS-0600-provision_2.bin
[root@localhost ~]# 
```

- **Restart DHCP service**


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

```
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global.  They are not limited to the scope you
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not spe
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   Socket/fallback/fallback-net
[root@localhost ~]# killall dhcpd
[root@localhost ~]# 
```


dhcpd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Link to dhcpd.conf
dhcpd.conf
root@localhost:~
File Edit View Terminal Help

```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5 code 6 = string;
option SWITCH.configuration-file-name code 7 = text;
option SWITCH.configuration-md5 code 8 = string;
#16 bits option (bit 0: Urgency, bit 1-15: Reserve)
option SWITCH.option code 9  = unsigned integer 16;

        class "vendor-classes" {
                match option vendor-class-identifier;
        }

        option SWITCH.protocol 1;
        option SWITCH.server-ip 192.168.0.251;
#       option SWITCH.server-login-name "anonymous";
        option SWITCH.server-login-name "FAE";
        option SWITCH.server-login-password "dept1";


    subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
     option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
     option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
#     option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
#     option SWITCH.firmware-md5 16:2c:2e:4d:30:e5:71:5c:cc:fd:5a:f0:d8:33:7d:db;
#     option SWITCH.configuration-file-name "3W0503A3C4.bin";
#     option SWITCH.configuration-md5 ef:30:03:13:a1:d0:d6:05:af:c7:28:6f:25:f0:96:84;
     option SWITCH.option 1;
```

```
[root@localhost ~]# dhcpd
Internet Systems Consortium DHCP Server 4.1.1-P1
Copyright 2004-2010 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
WARNING: Host declarations are global.  They are not limited to the scope yo
clared them in.
Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not sp
ied in the config file
Wrote 0 class decls to leases file.
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 6 leases to leases file.
Listening on LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   LPF/eth0/00:0c:29:ef:f8:4f/192.168.0.0/24
Sending on   Socket/fallback/fallback-net
[root@localhost ~]# 
```

Every time when you modify dhcpd.conf file, DHCP service must be restarted. Issue “killall dhcpd” command to disable DHCP service and then issue “dhcpd” command to enable DHCP service.

Step 4. Backup a Configuration File

Before preparing a configuration file in TFTP/FTP Server, make sure the device generating the configuration file is set to **“Get IP address from DHCP”** assignment. This is because that DHCP Auto-provisioning is running under DHCP mode, so if the configuration file is uploaded by the network type other than DHCP mode, the downloaded configuration file has no chance to be equal to DHCP when provisioning, and it results in MD5 never match and causes the device to reboot endless.

In order for your Managed Switch to retrieve the correct configuration image in TFTP/FTP Server, please make sure the filename of your configuration file is defined exactly the same as the one specified in in **dhcpd.conf**. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile”, the configuration image filename should be named to “metafile” as well.

Step 5. Place a copy of Firmware and Configuration File in TFTP/FTP

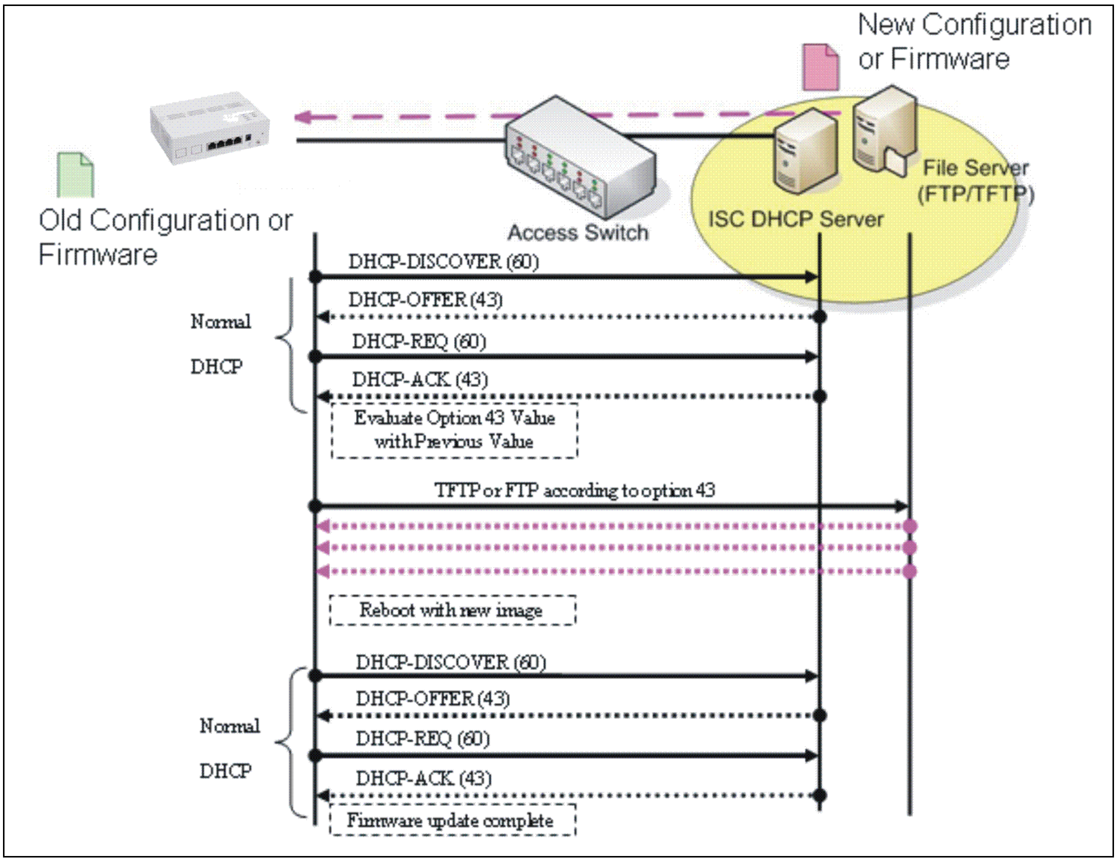
The TFTP/FTP File server should include the following items:

1. Firmware image (This file is provided by the vendor.)
2. Configuration file (This file is generally created by users.)
3. User account for your device (For FTP server only.)

B. Auto-Provisioning Process

This switching device is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

1. The ISC DHCP server will recognize the device whenever it sends an IP address request to it. And ISC DHCP server will tell the device how to get a new firmware or configuration.
2. The device will compare the firmware and configuration MD5 code form of DHCP option every time when it communicates with DHCP server.
3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated right after.
4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.
5. The device will retry for 3 times if the file is incorrect, then it gives up until getting another DHCP ACK packet again.



This page is intentionally left blank.