



HES-3106 SERIES

6 PORTS 10/100/1000BASE-T ETHERNET MANAGED SWITCH

**5 PORTS 10/100/1000BASE-T ETHERNET MANAGED SWITCH
WITH 1 PORT 1000BASE-X or 100/1000BASE-X UPLINK**

**5 PORTS 10/100/1000BASE-T ETHERNET MANAGED SWITCH
WITH 1 PORT 1000BASE-X or 100/1000BASE-X UPLINK AND
TV RF Module**

Network Management

User's Manual

Version 1.3

Trademarks

Contents are subject to revision without prior notice.
All other trademarks remain the properties of their owners.

Copyright Statement

This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from the owner.

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 not 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 an outlet on a circuit different from that to which 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 © 2012 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.

Revision History

| Version | Firmware | Date | Description |
|---------|----------|----------|---|
| 1.2 | 1.03.00 | 20150217 | Add Non-Blocking Switching Fabric Section 1.1 Add Section 2.3.1 PING Command |
| 1.3 | 1.04.00 | 20150805 | Add DHCP Option 60 (Section 2.5.17 & 3.4.6.2.3) Add Mirroring Configuration (Section 2.5.10 & 3.4.7) Revise photo (Section 1.1) |

Table of Content

| | |
|--|-----------|
| 1. INTRODUCTION | 7 |
| 1.1 Interfaces..... | 7 |
| 1.2 Management Preparations | 9 |
| 1.2.1 Connecting the Managed Switch | 9 |
| 1.2.2 Assigning IP Addresses | 9 |
| 1.3 LED Definitions..... | 10 |
| 1.4 Button Definitions | 10 |
| 2. Command Line Interface (CLI) | 11 |
| 2.1 Remote Console Management-Telnet | 11 |
| 2.2 Navigating CLI | 12 |
| 2.2.1 General Commands..... | 12 |
| 2.2.2 Quick Keys..... | 13 |
| 2.2.3 Command Format | 13 |
| 2.2.4 Login Username & Password | 15 |
| 2.3 User Mode..... | 15 |
| 2.3.1 PING Command | 15 |
| 2.4 Privileged Mode..... | 17 |
| 2.4.1 Copy-cfg Command..... | 17 |
| 2.4.2 Firmware Command | 18 |
| 2.4.3 Reload Command | 18 |
| 2.4.4 Write Command | 19 |
| 2.4.5 Configure Command..... | 19 |
| 2.5 Configuration Mode | 19 |
| 2.5.1 Entering Interface Numbers | 20 |
| 2.5.2 No Command..... | 20 |
| 2.5.3 Show Command | 20 |
| 2.5.4 Interface Command | 22 |
| 2.5.5 CATV Command | 24 |
| 2.5.6 IP Command | 24 |
| 2.5.7 Loop Detection Command | 28 |
| 2.5.8 MAC Command | 28 |
| 2.5.9 Management Command | 29 |

| | |
|--|-----------|
| 2.5.10 Mirror Command | 29 |
| 2.5.11 NTP Command | 29 |
| 2.5.12 QoS Command | 30 |
| 2.5.13 Security Command | 36 |
| 2.5.14 SNMP-Server Command | 37 |
| 2.5.15 Switch Command..... | 40 |
| 2.5.16 Switch-info Command..... | 40 |
| 2.5.17 User Command..... | 41 |
| 2.5.18 VLAN Command | 43 |
| 2.5.19 Show interface statistics Command | 46 |
| 2.5.20 Show sfp Command..... | 47 |
| 2.5.21 Show log Command..... | 47 |
| 2.5.22 Show default-config, running-config and start-up-config Command | 47 |
| 3. WEB MANAGEMENT | 48 |
| 3.1 System Information | 50 |
| 3.2 User Authentication | 51 |
| 3.3 Network Management | 53 |
| 3.3.1 Network Configuration | 54 |
| 3.3.2 System Service Configuration..... | 55 |
| 3.3.3 Time Server Configuration | 55 |
| 3.3.4 Device Community..... | 56 |
| 3.3.5 Trap Destination..... | 58 |
| 3.3.6 Trap Configuration | 58 |
| 3.4 Switch Management..... | 59 |
| 3.4.1 Switch Configuration | 60 |
| 3.4.2 Storm Control..... | 60 |
| 3.4.3 Port Configuration | 61 |
| 3.4.4 Rate Limit Configuration | 63 |
| 3.4.5 QoS Priority Configuration | 63 |
| 3.4.6 VLAN Configuration | 66 |
| 3.4.6.1 Port Based VLAN | 68 |
| 3.4.6.1.1 Configure VLAN..... | 69 |
| 3.4.6.2 IEEE 802.1q Tag VLAN..... | 71 |
| 3.4.6.2.1 Configure VLAN..... | 71 |

| | |
|---|-----------|
| 3.4.6.2.2 Configure Default Port VLAN ID | 72 |
| 3.4.6.2.3 DHCP-Option60-Based VLAN | 73 |
| 3.4.6.3 Q-in-Q VLAN Configuration | 75 |
| 3.4.7 Mirroring Configuration | 75 |
| 3.4.8 IGMP Snooping..... | 76 |
| 3.4.9 Loop Detection..... | 77 |
| 3.4.10 Filter Configuration..... | 78 |
| 3.5 Switch Monitor..... | 78 |
| 3.5.1 Switch Port State | 80 |
| 3.5.2 Port Counters Rates | 81 |
| 3.5.2.1 Port Traffic Statistics (Rates)..... | 81 |
| 3.5.2.2 Port Packet Error Statistics (Rates)..... | 82 |
| 3.5.2.3 Port Packet Analysis Statistics (Rates) | 83 |
| 3.5.3 Port Counters Events..... | 84 |
| 3.5.3.1 Port Traffic Statistics (Events) | 84 |
| 3.5.3.2 Port Packet Error Statistics (Events) | 85 |
| 3.5.3.3 Port Packet Analysis Statistics (Events)..... | 86 |
| 3.5.4 SFP Information | 87 |
| 3.5.4.1 SFP Port Info..... | 87 |
| 3.5.4.2 SFP Port State | 88 |
| 3.5.5 IGMP Snooping..... | 88 |
| 3.5.6 Loop Detection..... | 89 |
| 3.5.7 MAC Address Table | 89 |
| 3.6 System Utility..... | 90 |
| 3.6.1 Event Log..... | 91 |
| 3.6.2 Update | 91 |
| 3.6.3 Load Factory Settings | 92 |
| 3.6.4 Load Factory Settings Except Network Configuration..... | 93 |
| 3.7 Save Configuration | 93 |
| 3.8 Reset System | 94 |
| 3.9 Logout | 94 |
| APPENDIX A: DHCP Auto-Provisioning Setup | 95 |

1. INTRODUCTION

Thank you for using the 5 Ports 10/100/1000Base-T plus 1 Port 1000Base-X or 100/1000Base-X Uplink, or 6 Ports 10/100/1000Base-T Ethernet Managed Switch. The built-in management module allows users to configure this Switch and monitor the operation status locally or remotely through network.

The Managed Switch is fully compliant with IEEE 802.3, 802.3u, 802.3z and 802.3ab standards. By employing store and forward switching mechanism, the 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 Switch and monitor its real-time operational status via Command Line Interface (CLI). For detailed descriptions on how to use CLI, please refer to Section 2.

1.1 Interfaces

Depending on the main device and optional accessories that you purchased, the front panel and rear panel of your Switch may look differently from model to model. Figure 1 and 2 show the front and rear panel for 6-Port 10/100/1000Base-T Ethernet Managed Switch; whereas, Figure 3 and 4 show the front and rear panel for 5-Port 10/100/1000Base-T plus 1-Port 1000Base-X or 100/1000Base-X Uplink Ethernet Managed Switch with optional CATV RF module.

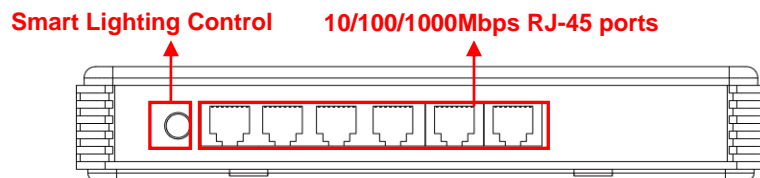


Figure 1. Front Panel for 6-Port 10/100/1000Base-T Managed Switch

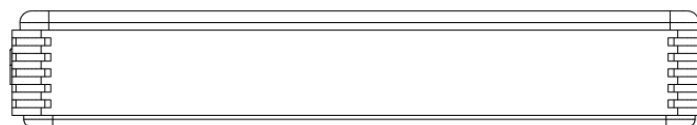


Figure 2. Rear Panel for 6-Port 10/100/1000Base-T Managed Switch

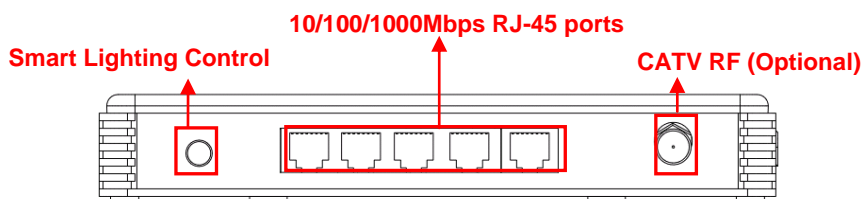


Figure 3. Front Panel for 5-Port 10/100/1000Base-T plus 1-Port 1000Base-X or 100/1000Base-X Uplink Ethernet Managed Switch with optional CATV RF Module

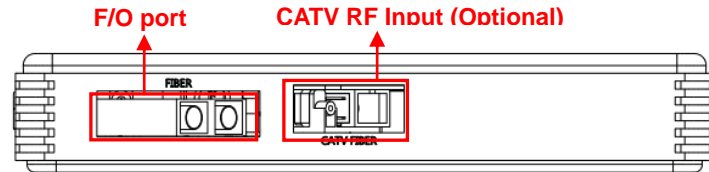


Figure 4. Rear Panel for 5-Port 10/100/1000Base-T plus 1-Port 1000Base-X or 100/1000Base-X Uplink Ethernet Managed Switch with optional CATV RF Module

All models have the same top, left and right panel as shown in Figure 5, 6 and 7.

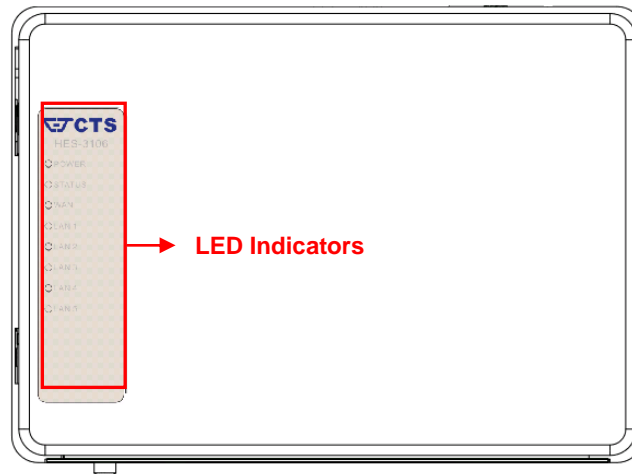


Figure 5 Top Panel with LEDs

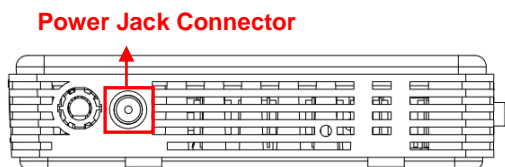


Figure 6. Left Panel

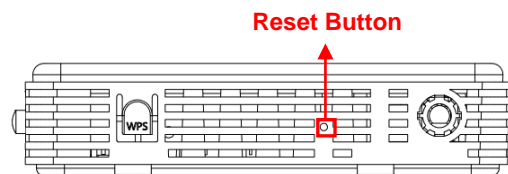


Figure 7. Right Panel

1.2 Management Preparations

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

1.2.1 Connecting the Managed Switch

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

1000Base-X Fiber Port or 100/1000 Base-X Fiber Port

The 1000Base-X fiber port is located at the rear panel of the Managed Switch. This port is primarily used for uplink connection and can operate at 1000M/Full or Half Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber cable to connect this port with the other Ethernet Fiber port.

Before connecting to other switches, workstations or media converters, make sure both sides of the fiber transfer are with the same media type, for example 1000Base-X Single-mode to 1000Base-X Single-mode, 1000Base-X Multimode to 1000Base-X Multimode. Check that the fiber-optic cable type matches the fiber transfer model. To connect to 1000Base-SX transfer, use the multimode fiber cable (one side must be male duplex SC connector type). To connect to 1000Base-LX transfer, use the single-mode fiber cable (one side must be male duplex LC connector type).

10/100/1000Base-T RJ-45 Ports

Depending on the model that you purchased, 5 or 6 10/100/1000Base-T RJ-45 ports are located on the front panel of the Managed Switch. These RJ-45 ports allow users to connect their traditional copper-based Ethernet devices to network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. the crossover or straight through CAT-5 cable may be used.

1.2.2 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) indicates network address identifying the network where 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 an address can be assigned to only one device on a network. 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 be connected.

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 a proper operation of a network with subnets defined.

1.3 LED Definitions

| LED | Definition | Color | Operation |
|---------|-----------------|-----------------|--|
| POWER | Power Status | Off | Device is powered off. |
| | | Green | Device is powered on. |
| STATUS | System Status | Orange | System is booting up. |
| | | Green | System is working normally. |
| | | Orange Blinking | When the system is set back to default factory setting, the Status LED indicator will blink in orange for 3 times. |
| | | | When the system is restarted, the Status LED indicator will blink in orange once. |
| WAN | WAN Port Status | OFF | Link is down. |
| | | Green | Link is up and works at 100Mbps. |
| | | Orange | Link is up and works at 1000Mbps. |
| | | Blinking | Link is transmitting or receiving data. |
| LAN 1~5 | LAN Port Status | Off | Link is down. |
| | | Green | Link is up and works at 10/100Mbps. |
| | | Orange | Link is up and works under 1000Mbps. |
| | | Blinking | Link is transmitting or receiving data. |

1.4 Button Definitions

| Button | Operation |
|-------------------------------|--|
| Smart Lighting Control Button | System Status LED and Port Link LEDs will be turned off by pressing the button. Only Power LED indicator stays on. |
| Reset Button | Insert a pin or paper clip to press the Reset button for 5 seconds to restart the device. |
| | Insert a pin or paper clip to press the Reset button for 10 seconds to reset the device to factory defaults. |

2. Command Line Interface (CLI)

This chapter guides you 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 Managed Switch via Telnet session. For first-time users, you must first assign a unique IP address to the Managed 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 device 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 Managed Switch through Telnet session:

- Step 1.** Use any one of the RJ-45 ports on the front panel as a temporary management console port to login to the Managed 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 4.** 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 5.** Once you enter CLI successfully, you can set up the Switch’s IP address, subnet mask and the default gateway using “IP” command in Global Configuration mode. The telnet session will be terminated immediately once the IP address of the Switch has been changed.
- Step 6.** Use new IP address to login to the Managed Switch via Telnet session again.

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

2.2 Navigating CLI

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

| Command Mode | Access Method | Prompt Displayed | Exit Method |
|--------------------|---|------------------|-----------------------|
| User Mode | Login username & password | Switch> | logout |
| Privileged Mode | From user mode, enter the <i>enable</i> command | Switch# | disable, exit, logout |
| Configuration Mode | From the enable mode, enter the <i>config</i> or <i>configure</i> 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 “host-name” 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 all modes, 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

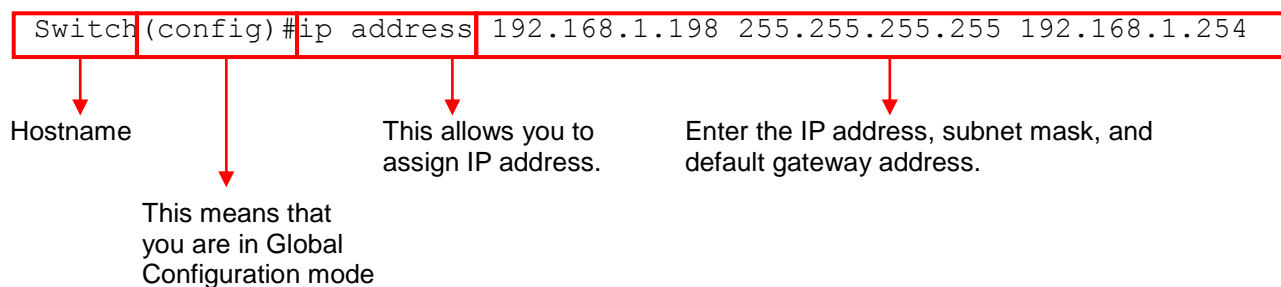
In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

| 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 ? | <p>Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.</p> <p>Examples:</p> <pre>Switch#h? help Show available commands history Show history commands</pre> <p>Switch#he? <cr></p> <p>Switch#help</p> |
| 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 Managed 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]



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. |
| [802.1p dscp vid] | 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 | <p>Specify one or more values or a range of values.</p> <p>For example: specifying one value</p> <pre>Switch(config)#qos 802.1p-map <u>1</u> 0 Switch(config)#qos dscp-map <u>10</u> 3</pre> <p>For example: specifying three values (separated by commas)</p> <pre>Switch(config)#qos 802.1p-map <u>1,3</u> 0 Switch(config)#qos dscp-map <u>10,13,15</u> 3</pre> <p>For example: specifying a range of values (separating by a hyphen)</p> <pre>Switch(config)#qos 802.1p-map <u>1-3</u> 0 Switch(config)#qos dscp-map <u>10-15</u> 3</pre> |

2.2.4 Login Username & Password

Default Login

After you enter Telnet session, a login prompt will appear to request a valid and authorized username and password combination. For first-time users, enter the default login username “**admin**” and “**press Enter key**” in password field (no password is required for default setting). When system prompt shows “Switch>”, it means that the user has successfully entered the User Mode.

For security reasons, it is strongly recommended that you add a new login username and password using User command in Configuration Mode. When you create your own login username and password, you can delete the default username (admin) to prevent unauthorized accesses.

Forgot Your Login Username & Password?

If you forgot your login username and password, you can use the “reset button” to set all configurations back to factory defaults. Once you have performed system reset to defaults, you can login with default username and password. Please note that if you use this method to gain access to the Managed Switch, all configurations saved in Flash will be lost. It is strongly recommended that a copy of configurations is backed up in your local hard-drive or file server from time to time so that previously-configured settings can be restored to the Managed Switch for use after you gain access again to the device.

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 Privileged 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 displays “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 Managed Switch. |
| ping | Test whether a specified network device or host is reachable or not. |
| enable | Enter the Privileged mode. |

2.3.1 PING Command

Ping is used to test the connectivity of end devices and also can be used to self test the network interface card. Enter the **ping** command in User mode. In this command, you can add an optional packet size value and an optional value for the number of times that packets are sent and received.

| Command | Parameter | Description |
|--|-----------|---|
| Switch> ping [A.B.C.D] [-s size (8-4000)bytes] [-t timeout (1-99)secs] | [A.B.C.D] | Enter the IP address that you would like to ping. |
| [-s size (8-4000)bytes] | | Enter the packet size that would be sent. The allowable packet size is from 8 to 4000 bytes. (optional) |
| [-t timeout (1-99) secs] | | Enter the timeout value when the specified IP address is not reachable. (optional) |
| Example | | |
| Switch> ping 8.8.8.8 | | |
| Switch> ping 8.8.8.8 -s 128 -t 10 | | |

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 FTP or 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 FTP or TFTP server. |
| help | Display a list of available commands in Enable Mode. |
| history | Show commands that have been used. |
| logout | Logout from the Managed Switch. |
| ping | Test whether a specified network device or host is reachable or not. |
| 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 FTP or TFTP server or restore the Managed Switch back to the defaults or to the defaults without changing IP configurations.

1. Restore a configuration file via FTP or TFTP server.

| Command | Parameter | Description |
|--|-------------|---|
| Switch# copy-cfg from ftp [A.B.C.D] [file_name] [user_name] [password] | [A.B.C.D] | Enter the IP address of your FTP server. |
| | [file_name] | Enter the configuration file name that you want to restore. |
| | [user_name] | Enter the username for FTP server login. |
| | [password] | Enter the password for FTP server login. |
| 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 ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz | | |
| Switch# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf | | |

2. Restore the Managed Switch back to default settings.

| Command / Example |
|-------------------------------|
| Switch# copy-cfg from default |

NOTE: There are two ways to set the Managed Switch back to the factory default settings. Users can use the “copy-cfg from default” command in CLI or simply press the “Reset Button” located on the front panel to restore the device back to the initial state.

3. Restore the Managed 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 ftp [A.B.C.D] [file_name] [user_name] [password] | [A.B.C.D] | Enter the IP address of your FTP server. |
| | [file_name] | Enter the configuration file name that you want to backup. |
| | [user_name] | Enter the username for FTP server login. |
| | [password] | Enter the password for FTP server login. |
| 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 ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz | | |
| Switch# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf | | |

2.4.2 Firmware Command

To upgrade Firmware via FTP or TFTP server.

| Command | Parameter | Description |
|---|-------------|--|
| Switch# firmware upgrade ftp [A.B.C.D] [file_name] [user_name] [password] | [A.B.C.D] | Enter the IP address of your FTP server. |
| | [file_name] | Enter the firmware file name that you want to upgrade. |
| | [user_name] | Enter the username for FTP server login. |
| | [password] | Enter the password for FTP server login. |
| 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 ftp 192.168.1.198 HS_0600_file.bin edgeswitch10 abcxyz | | |
| Switch# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin | | |

2.4.3 Reload Command

To restart the Managed 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 Managed Switch.

| Command / Example |
|-------------------|
| Switch# write |

2.4.5 Configure Command

You can enter Global Configuration Mode only from Privileged Mode. You can type in “configure” or “config” 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 command entered will be applied 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 |
|-----------------------|--|
| catv | Enable or disable CATV RF module |
| 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. |
| loop-detection | Enable or disable Loop Detection function |
| mac | Set up each port’s MAC learning function. |
| management | Set up the system service type. |
| mirror | Set up port mirroring configuration |
| ntp | Set up required configurations for Network Time Protocol. |
| qos | Set up the priority of packets within the Managed Switch. |
| security | Set up storm control settings. |
| snmp-server | Create a new SNMP community and trap destination and specify the trap types. |
| switch | Enable or disable SFP and counter polling function. |
| switch-info | Specify company name, host name, system location, 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 | Set up the selected interfaces’ advanced features. |
| 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 is only applied to interfaces specified. For example, you can set up each interface's VLAN assignment, speed, or duplex mode. 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-1)# | Enter a single interface. Only interface 1 will apply to commands entered. |
| Switch(config)# interface 1,3,5 Switch(config-if-1,3,5)# | 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-1-3)# | 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-1,3-5)# | Enter a single interface number together with a range of interface numbers. Use both commas and hyphens 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 “Loop Detection”, “QoS”, “VLAN” and “Security” commands. For detailed usages, please refer to Loop Detection, QoS, VLAN and Security sections below.

2.5.2 No Command

Most commands that you enter in Configuration mode can be negated using “no” command followed by the same or 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

The command “show” 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 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, and then the following similar screen page will appear.

```
=====
System Information
=====
Company Name       : Connection Technology Systems
System Object ID   : .1.3.6.1.4.1.9304.100.3006
System Contact     : info@cts-system.com
System Name        : Managed 6 Ports 1000M Switch
System Location    : 18F-6, No. 79, Sec. 1, Xintai 5th Rd., Xizhi Dist., Taiwan
Model Name         : HES-3106
Host Name          : HES-3106
DHCP Vendor ID     : HES-3106
Firmware Version   : 0.99.01           M/B Version       : A01
1000M Port Number  : 6               100M Port Number  : 0
Fiber 1 Type       : SFP 1000Mbps 550M
Fiber 1 Vendor     : CTS INC.
Fiber 1 PM         : SFP-31FC
Serial Number      : PM3106RF00000000    Date Code         : 20120515
Up Time            : 0 day 00:24:36
Local Time         : Not Available
CATU RF TU State   : Off               CATU RF TU Output : On
=====
```

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

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

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

DHCP Vendor ID: Display the product’s DHCP Vendor ID.

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

M/B Version: Display the main board version.

1000M Port Number: The number of ports transmitting at the speed of 1000Mbps

100M Port Number: The number of ports transmitting at the speed of 100Mbps

Fiber 1 Type: Display the information about the slide-in or fixed fiber type.

Fiber 1 Vendor: Display the vendor of the slide-in or fixed fiber.

Fiber 1 PN: Displays the PN of the slide-in or fixed fiber.

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

Date Code: Displays the Managed Switch Firmware date code.

Uptime: Display the time the device has been up.

Local Time: Display the time of the location where the switch is.

CATV RF TV State: View-only field that shows whether RF TV is ready or not.

CATV RF TV Output: Turn on or off the RF TV Output.

2. Display or verify currently-configured settings

Refer to “interface command”, “ip command”, “mac command”, “qos command”, “security command”, “snmp-server command”, “user command”, and “vlan command” sections.

3. Display interface information or statistics

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

4. Show default, running and startup configurations

Refer to “show default-config command”, “show running-config command” and “show start-up-config 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 separated by commas or a range of port numbers. For example: 1,3 or 2-4 |
| Switch(config-if-PORT-PORT)# auto-negotiation | | Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored. |
| Switch(config-if-PORT-PORT)# duplex full | | Set the selected interfaces' to full duplex mode. |
| Switch(config-if-PORT-PORT)# flowcontrol | | Enable the selected interfaces' flow control function. |

| | | |
|---|------------------|---|
| Switch(config-if-PORTR-PORT)# speed [1000 100 10] | [1000 100 10] | Set up the selected interfaces' speed. Speed configuration only works when "no auto-negotiation" command is issued. |
| Switch(config-if-PORTR-PORT)# description [description] | [description] | Specify a descriptive name for the selected interfaces. |
| Switch(config-if-PORTR-PORT)# shutdown | | Administratively disable the selected ports' status. |
| Switch(config-if-PORTR-PORT)# vlan option60 | | Enable the ports to receive Option60 packet. |
| No command | | |
| Switch(config-if-PORTR-PORT)# no auto-negotiation | | Set auto-negotiation setting to the default setting. |
| Switch(config-if-PORTR-PORT)# no duplex | | Set the selected ports' duplex mode to the default setting. |
| Switch(config-if-PORTR-PORT)# no speed | | Set the selected ports' speed to the default setting. |
| Switch(config-if-PORTR-PORT)# no flowcontrol | | Set the selected ports' flow control function to the default setting. |
| Switch(config-if-PORTR-PORT)# no description | | Remove the entered description name for the selected ports. |
| Switch(config-if-PORTR-PORT)# no shutdown | | Administratively enable the selected ports' status. |
| Switch(config-if-PORTR-PORT)# no vlan option60 | | Disable the ports to receive Option60 packet. |
| 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. |
| Switch(config)# show interface status [port_list] | [port_list] | Show the selected ports' 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-1-3)# auto-negotiation | | Set the selected interfaces' to auto-negotiation. |
| Switch(config-if-1-3)# duplex full | | Set the selected interfaces' to full duplex mode. |
| Switch(config-if-1-3)# speed 100 | | Set the selected ports' speed to 100Mbps. |
| Switch(config-if-1-3)# shutdown | | Administratively disable the selected ports' status. |

2.5.5 CATV Command

Enable or disable CATV RF module.

| CATV command | Description |
|----------------------------------|-------------------------------------|
| Switch(config)# catv | Enable CATV RF module. |
| No command | |
| Switch(config)# no catv | Disable CATV RF module. |
| Show command | |
| Switch(config)# show switch-info | Show current CATV RF module status. |

2.5.6 IP Command

Configure IP address and related settings such as DHCP snooping and IGMP snooping.

1. Set up or remove the IP address of the Managed 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 the Managed Switch. |
| | [255.X.X.X] | Enter subnet mask of your IP address. |
| | [A.B.C.D] | Enter the default gateway address. |
| Switch(config)# ip dhcp snooping | | Enable DHCP Snooping function |
| Switch(config)# ip dhcp snooping dhcp-server [port_list] | [port_list] | Specify DHCP server trust ports. |
| No command | | |
| Switch(config)# no ip address | | Remove the 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 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 Managed 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 DHCP snooping globally.

| Command / Example | Parameter | Description |
|--|-------------|--|
| Switch(config)# ip dhcp snooping | | Enable DHCP snooping function. |
| Switch(config)# ip dhcp snooping dhcp-server [port_list] | [port_list] | Specify DHCP server trust ports. |
| No command | | |
| Switch(config)# no ip dhcp snooping | | Disable IGMP snooping function. |
| Switch(config)# no ip dhcp snooping dhcp-server | | Remove all the DHCP server trust ports |
| Show command | | |
| Switch(config)# show ip dhcp snooping | | Show current DHCP snooping status including DHCP server trust ports. |

4. 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 | Parameter | Description |
|--|-------------------|--|
| Switch(config)# ip igmp snooping | | Enable IGMP snooping function. |
| Switch(config)# ip igmp snooping aging-time | [1-3000] /10 sec. | Specify the IGMP querier aging time. If the switch does not receive join packets from the end device within the specified time, the entry associated with this end device will be removed from the IGMP table. |
| No command | | |
| Switch(config)# no ip igmp snooping | | Disable IGMP snooping function. |
| Switch(config)# no ip igmp snooping aging time | | Remove IGMP querier aging time setting. |
| 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 Switch is able to read multicast group IP and the corresponding MAC address from IGMP packets that enter the device. |

5. Enable or disable IGMP snooping immediate-leave function.

This works only when IGMP Snooping is enabled. When Immediate Leave is enabled, the 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. |

6. Enable or disable IP source binding function.

| IP command | Parameter | Description |
|-----------------------------------|-----------|--|
| Switch(config)# ip source binding | [1-12] | Enter the desired IP source binding index 1-12 |

| | | |
|---|-----------|--|
| [1-12] ip-address [A.B.C.D] | [A.B.C.D] | Enter the desired IP address for source binding |
| Switch(config)# ip source binding [1-12] | [1-12] | Enable specific IP source binding index 1-12 |
| Switch(config)#ip source | | Globally enable IP source binding function |
| No command | | |
| Switch(config)# no ip source binding [1-12] ip-address | | Remove the IP address of specific index |
| Switch(config)# no ip source binding [1-12] | | Disable IP source binding function of specific index |
| Switch(config)# no ip source | | Globally disable IP source binding function |
| Show command | | |
| Switch(config)# show ip source | | Show the current IP source binding configurations |
| IP command example | | |
| Switch(config)# ip source binding 1 ip-address 192.168.0.210 | | Set up IP for source binding in index 1 |
| Switch(config)# ip source binding 1 | | Enable IP source binding index 1 |
| Switch(config)# ip source | | Globally enable IP source binding function |

2.5.7 Loop Detection Command

Loop Detection allows users to configure the Managed Switch to lock a port when it detects packets which are sent out on that port loop back to the switch. When loops occur, it will cause broadcast storm and affect the performance of layer two Access switch. To avoid this, Loop Detection can be enabled on LAN ports of the Managed Switch. When it detects the loop, it will lock the port which receives the loop packet immediately and send out SNMP trap to inform the network administrator.

| Loop Detection command | Parameter | Description |
|--|-----------|---|
| Switch(config)# loop-detection | | Globally enable Loop Detection function. By default, this function is disabled. |
| No command | | |
| Switch(config)# no loop-detection | | Globally disable Loop Detection function. |
| Show command | | |
| Switch(config)# show loop-detection | | Show current Loop Detection configuration information. |
| Switch(config)# show loop-detection status | | Show information concerning locked ports and locked cause. |

Note: Please note that Loop Detection function is only available on LAN 1~5 port.

2.5.8 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 the specified aging time.

| MAC Command | Parameter | Description |
|--|-------------|---|
| Switch(config)# mac address-table aging-time [1-800] | [7-600000] | Enter aging time for MAC address table. Numbers available are from 7 to 600000. |
| 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. |
| Switch(config)# show mac address-table | | Show MAC addresses learned by the Managed Switch |
| Switch(config)# show mac address-table interface [port_list] | [port_list] | Show MAC addresses learned by the selected ports. |
| Switch(config)# show mac address-table top | | Show MAC addresses learned from the first entry. |
| MAC command example | | |
| Switch(config)# mac address-table aging-time 600 | | Set MAC address table aging time to 600 seconds. |

2.5.9 Management Command

| Management command | Parameter | Description |
|--|----------------|--|
| Switch(config)# management [ssh telnet] | [ssh telnet] | Select the system service type, SSH or telnet. |
| No command | | |
| Switch(config)# no management [ssh telnet] | [ssh telnet] | Set system service type to Disabled. |
| Show command | | |
| Switch(config)# show management | | Show the current system service type. |
| Management command example | | |
| Switch(config)# management ssh | | Enable SSH system service type. |

2.5.10 Mirror Command

Set up port mirroring function.

| Mirror Command | Parameter | Description |
|--|-----------|---|
| Switch(config)# mirror destination [port_list] | [1-6] | Specify the destination port to which the mirrored traffic will be forwarded. |
| Switch(config)# mirror mode [by-port] | [by-port] | Enable port mirroring function. |
| Switch(config)# mirror source [port_list] | [1-6] | Specify the port to be mirrored. |
| No command | | |
| Switch(config)# no mirror destination | | Set the destination port to port 1. |
| Switch(config)# no mirror mode | | Disable port mirroring function. |
| Switch(config)# no mirror source | | Disable source port. |
| Show command | | |
| Switch(config)# show mirror | | Show current port mirroring destination port and source port settings |
| Mirror command example | | |
| Switch(config)# mirror destination 5 | | Enable port mirroring function and select port 5 as the destination port. |

2.5.11 NTP Command

Set up required configurations for Network Time Protocol.

| Command | Parameter | Description |
|--|-----------|--|
| Switch(config)# ntp | | Enable the Managed Switch to synchronize the clock with a time server. |
| Switch(config)# ntp server1 [A.B.C.D] | [A.B.C.D] | Specify the primary time server IP address. |
| Switch(config)# ntp server2 [A.B.C.D] | [A.B.C.D] | Specify the secondary time server IP address. |
| Switch(config)# ntp syn-interval [1-99999] | [1-99999] | Specify the interval time to synchronize from NTP time server. The allowable |

| | | |
|--|---------|--|
| | | value is between 1 and 99999 minutes. |
| Switch(config)# ntp time-zone [0-132] | [0-132] | Specify the time zone to that the Managed Switch belongs. Use any key to view the complete code list of 132 time zones. For example, "Switch(config)# ntp time-zone ?" |
| No command | | |
| Switch(config)# no ntp | | Disable the Managed Switch to synchronize the clock with a time server. |
| Switch(config)# no ntp server1 | | Delete the primary time server IP address. |
| Switch(config)# no ntp server2 | | Delete the secondary time server IP address. |
| Switch(config)# no ntp syn-interval | | Set the synchronization interval back to the default setting. |
| Switch(config)# no ntp time-zone | | Set the time-zone setting back to the default setting. |
| Show command | | |
| Switch(config)# show ntp | | Show or verify current time server settings. |
| NTP command example | | |
| Switch(config)# ntp | | Enable the Managed Switch to synchronize the clock with a time server. |
| Switch(config)# ntp server1 192.180.0.12 | | Set the primary time server IP address to 192.180.0.12. |
| Switch(config)# ntp server2 192.180.0.13 | | Set the secondary time server IP address to 192.180.0.13. |
| Switch(config)# ntp syn-interval 6000 | | Set the synchronization interval to 6000 minutes. |
| Switch(config)# ntp time-zone 4 | | Set the time zone to GMT-8:00 Vancouver. |

2.5.12 QoS Command

1. Specify the desired QoS mode.

| QoS command | Parameter | Description |
|-------------------------------------|-----------------|---|
| Switch(config)# qos [802.1p dscp] | [802.1p dscp] | Specify one QoS mode. 802.1p: Use "qos 802.1p_map" command to assign priority bits to a queue. dscp: Use "qos dscp-map [0-63] dscp_list [0-3]" to assign several DSCP values to a priority value. |
| No command | | |
| Switch(config)# no qos | | Disable QoS function. |
| Show command | | |
| 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. |

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 you want to map to a priority queue. |
| | [0-3] | Specify a queue to which the specified DSCP value is assigned. |
| No command | | |
| Switch(config)# no qos dscp-map [0-63] dscp_list | | Set the queue of the specific DCSP value back to the default. |
| Show command | | |
| Switch(config)# show qos | | Show or verify QoS configurations. |
| DSCP-map example | | |
| Switch(config)# qos dscp-map 50 3 | | Mapping DSCP value 50 to priority queue 3. |

3. Set up management traffic priority and port user priority.

| Management-priority command | Parameter | Description |
|---|-----------|---|
| Switch(config)# qos management-priority [0-7] | [0-7] | Specify management traffic default 802.1p priority bit. |
| No command | | |
| Switch(config)# no qos management-priority | | Set management traffic priority back to the default. |
| Management-priority example | | |
| Switch(config)# qos management-priority 4 | | Set management traffic priority to 4. |

NOTE: To check the setting of management traffic priority, please refer to 2.5.17 VLAN Command.

4. Set up QoS queuing mode.

| Queuing-mode command | Parameter | Description |
|---|-----------|---|
| Switch(config)# qos queuing-mode [weight] | [weight] | By default, “strict” queuing mode is used. If you want to use “weight” queuing mode, you need to disable “strict” queuing mode. Strict mode: Traffic assigned to queue 3 will be transmitted first, and the traffic assigned to queue 2 will not be transmitted until queue 3’s traffic is all transmitted, and so forth. Weight mode: All queues have fair opportunity of dispatching. Each queue has the specific amount of bandwidth according to its assigned weight. |
| 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. |

5. Set up queue weight.

| Queuing-weighted command | Parameter | Description |
|--|---------------------|--|
| Switch(config)# qos queuing-weight [1:2:4:8] | [_:_:_] (1-32) | By default, queuing weight is “1:2:4:8”. Specify the value from 1 to 32. |
| No command | | |
| Switch(config)# no qos queuing-weight | | Set the queuing weight back to the default. |
| Show command | | |
| Switch(config)# show qos | | Show or verify QoS configurations. |

| Queuing-weighted example | |
|--|--|
| Switch(config)# qos queuing-weighted 1:7:14:21 | Specify the queue weight as 1:7:14:21. |

5. Set up 802.1p, VID and DSCP remarking

| Remarking command | Parameter | Description |
|--|-----------------------|---|
| Switch(config)# qos remarking [dscp vid 802.1p] | [dscp vid 802.1p] | Enable the specific remarking mode, DSCP, VID, or 802.1p Remarking. |
| No command | | |
| Switch(config)# no qos remarking [dscp vid 802.1p] | | Disable DSCP, VID or 802.1p remarking. |
| Show command | | |
| Switch(config)# show qos remarking | | Show current DSCP, VID and 802.1p remarking configuration. |
| Remarking example | | |
| Switch(config)# qos remarking 802.1p | | Enable 802.1p remarking. |
| Switch(config)# no qos remarking dscp | | Disable DSCP remarking. |

6. Set up DSCP, VID and 802.1p priority mapping

| DSCP Remarking command | Parameter | Description |
|--|-----------------------------|---|
| Switch(config)# qos remarking dscp-map [1-8] | [1-8] | Configure the mapping of DSCP remarking mode. [1-8]: Select the mapping entry |
| Switch(config-dscp-map-ID)# active | | Enable the mapping entry. |
| Switch(config-dscp-map-ID)# dscp [0-63] | [0-63] | Specify the DSCP value to be remarked. |
| Switch(config-dscp-map-ID)# priority [0-63] | [0-63] | Specify the DSCP remarking value. |
| Switch(config-dscp-map-ID)# exit | | Exit the entry. |
| No command | | |
| Switch(config)# no qos remarking dscp-map [1-8] | [1-8] | Set the specific entry back to the default setting. |
| Switch(config-dscp-map-ID)# no [active dscp priority] | [active dscp priority] | Disable the mapping entry, or set DSCP value or DSCP remarking value back to the default setting. |
| VID Remarking command | | |
| Switch(config)# qos remarking vid-map [1-8] | [1-8] | Configure the mapping of VID remarking mode. [1-8]: Select the mapping entry |
| Switch(config-vid-map-ID)# active | | Enable the mapping entry. |

| | | |
|---|--------------------------------------|---|
| Switch(config-vid-map-ID)# vlan-id [1-4094] | [1-4094] | Specify the VLAN ID to be remarked. |
| Switch(config-vid-map-ID)# priority [0-63] | [0-7] | Specify the 802.1p remarking value. |
| Switch(config-vid-map-ID)# exit | | Exit the entry. |
| No command | | |
| Switch(config)# no qos remarking vid-map [1-8] | [1-8] | Set the specific entry back to the default setting. |
| Switch(config-vid-map-ID)# no [active vlan-id priority] | [active vlan-id priority] | Disable the mapping entry, or set VLAN ID or 802.1p remarking value back to the default setting. |
| 802.1p Remarking command | | |
| Switch(config)# qos remarking 802.1p-map [1-8] | [1-8] | Configure the mapping of 802.1p remarking mode. [1-8]: Select the mapping entry |
| Switch(config-802.1p-map-ID)# active | | Enable the mapping entry. |
| Switch(config-802.1p-map-ID)# 802.1p [0-7] | [0-7] | Specify the 802.1p value to be remarked. |
| Switch(config-802.1p-map-ID)# priority [0-7] | [0-7] | Specify the 802.1p remarking value. |
| Switch(config-802.1p-map-ID)# exit | | Exit the entry. |
| DSCP Remarking No command | | |
| Switch(config)# no qos remarking 802.1p-map [1-8] | [1-8] | Set the specific entry back to the default setting. |
| Switch(config-802.1p-map-ID)# no [active 802.1p priority] | [active 802.1p priority] | Disable the mapping entry, or set 802.1p value or 802.1p remarking value back to the default setting. |
| Show command | | |
| Switch(config-dscp/vid/802.1p-map-ID)# show | | Display the mapping configuration of the specific entry. |
| Priority mapping example (VID for example) | | |
| Switch(config)# qos remarking vid-map 1 | | Configure vid-map entry 1. |
| Switch(config-vid-map-1)# active | | Enable vid-map entry 1. |
| Switch(config-vid-map-1)# vlan-id 100 | | Assign VID 100 to vid-map entry 1. |
| Switch(config-vid-map-1)# priority 2 | | Set 802.1p remarking value as 2. |
| Switch(config-vid-map-1)# exit | | Exit vid-map entry 1. |

7. Assign a tag priority to the specific queue.

| 802.1p-map command | Parameter | Description | | | | | | | | | | | | | | | | | | |
|--|----------------------|--|--|----------------|--------|--------|------|--------|--------|--------|------|------|--------------|---|---|---|---|---|---|---|
| Switch(config)# qos 802.1p-map [0-7] 802.1p_list [0-3] | [0-7] 802.1p_list | Assign one 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> | Priority Level | Low | Low | Low | Normal | Medium | Medium | High | High | 802.1p Value | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| Priority Level | Low | Low | Low | Normal | Medium | Medium | High | High | | | | | | | | | | | | |
| 802.1p Value | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | | | | | | | | | | | | |
| | [0-3] | Assign a queue value for mapping. | | | | | | | | | | | | | | | | | | |
| No command | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# no qos 802.1p-map [0-7] 802.1p_list | [0-7] 802.1p_list | Assign an 802.1p priority bit or several 802.1p priority bits that you want to delete or remove. | | | | | | | | | | | | | | | | | | |
| Show command | | | | | | | | | | | | | | | | | | | | |
| 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. | | | | | | | | | | | | | | | | | | |

8. Use interface command to set up default class and ingress and egress rate limit.

| QoS & Interface command | Parameter | Description |
|---|-------------------|--|
| Switch(config)# interface [port_list] | [port_list] | Enter several port numbers separated by commas or a range of port numbers. For example: 1,3 or 2-4 |
| Switch(config-if-PORT-PORT)# qos default-class [0-3] | [0-3] | Specify the default class for the selected interfaces. |
| Switch(config-if-PORT-PORT)# qos rate-limit ingress [32-1000000] kbps | [32-1000000] kbps | Specify the ingress rate between 32 and 1000000. |
| Switch(config-if-PORT-PORT)# qos rate-limit egress [32-1000000] kbps | [32-1000000] kbps | Specify the egress rate between 32 and 1000000. |
| No command | | |
| Switch(config-if-PORT-PORT)# no qos default-class | | Set QoS default class setting to the default. |
| Switch(config-if-PORT-PORT)# no qos rate-limit ingress | | Set QoS ingress rate limit setting to the default. |
| Switch(config-if-PORT-PORT)# no qos rate-limit egress | | Set QoS ingress rate limit setting to the default. |
| Show command | | |
| Switch(config)# show qos interface [port_list] | [port_list] | Show or verify the selected interfaces' ingress and egress rate configurations. |

| | |
|---|--|
| Switch(config)# show qos interface | Show or verify each interface's ingress and egress rate configurations. |
| Switch(config)# show qos | Show or verify QoS configurations. |
| QoS & Interface example | |
| Switch(config)# interface 1-3 | Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4 |
| Switch(config-if-1-3)# qos rate-limit ingress 1550 | Configure the selected interfaces' ingress rate-limit to 1550. |
| Switch(config-if-1-3)# qos rate-limit egress 3 1550 | Set the selected interfaces' queue 3 to egress rate 1550. |

2.5.13 Security Command

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

| Security command | Parameter | Description |
|---|-------------------|--|
| Switch(config)# security storm-protection | | Enable storm protection function. |
| Switch(config)# security storm-protection rates [32-1000000] kbps | [32-1000000] kbps | Specify the maximum broadcast packet rate. |
| No command | | |
| Switch(config)# no security storm-protection | | Disable storm protection globally. |
| Switch(config)# no security storm-protection rates | | Set broadcast packet rate back to the default. |
| Show command | | |
| Switch(config)# show security storm-protection | | Show storm control settings. |

2.5.14 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 up to 20 alphanumeric characters. |
| Switch(config-community-NAME)# active | | Enable this SNMP community account. |
| Switch(config-community-NAME)# description [Description] | [Description] | Enter the description up to 35 alphanumeric characters for this SNMP community. |
| Switch(config-community-NAME)# level [admin rw ro] | [admin rw ro] | <p>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”.</p> <p>Admin: Full access right, including maintaining user account, system information, loading factory settings, etc..</p> <p>rw: Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware.</p> <p>Ro: Read Only access privilege.</p> |
| No command | | |
| Switch(config)# no snmp-server community [community] | [community] | Delete the specified community. |
| Switch(config-community-NAME)# no active | | Disable this SNMP community account. |
| Switch(config-community-NAME)# no description | | Remove the entered SNMP community descriptions. |
| Switch(config-community-NAME)# no level | | Remove the configured level. This will set this community’s level to read only. |
| Show command | | |
| Switch(config)# show snmp-server community [community] | [community] | Show the specified SNMP server account’s settings. |
| Switch(config)# show snmp-server community | | Show SNMP community account’s information in Global Configuration Mode. |
| Switch(config-community-NAME)# show | | View or verify the configured SNMP community account’s information. |
| Exit command | | |
| Switch(config-community-NAME)# 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-community-mycomm)# active | Activate the SNMP community “mycomm”. |
| Switch(config-community-mycomm)# description rddeptcomm | Add a description for “mycomm” community. |
| Switch(config-community-mycomm)# 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 [1-3] | [1-3] | Create a trap destination account. |
| Switch(config-trap-ACCOUNT)# active | | Enable this SNMP trap destination account. |
| Switch(config-trap-ACCOUNT)# community [community] | [community] | Enter the community name of network management system. |
| Switch(config-trap-ACCOUNT)# destination [A.B.C.D] | [A.B.C.D] | Enter the SNMP server IP address. |
| No command | | |
| Switch(config)# no snmp-server trap-destination [1-3] | [1-3] | Delete the specified trap destination account. |
| Switch(config-trap-ACCOUNT)# no active | | Disable this SNMP trap destination account. |
| Switch(config-trap-ACCOUNT)# no community | | Delete the configured community name. |
| Switch(config-trap-ACCOUNT)# no description | | Delete the configured trap destination description. |
| Show command | | |
| Switch(config)# show snmp-server trap-destination [1-3] | [1-3] | Show the specified trap destination information. |
| Switch(config)# show snmp-server trap-destination | | Show SNMP trap destination information in Global Configuration mode. |
| Switch(config-trap-ACCOUNT)# show | | View this trap destination account’s information. |
| Exit command | | |
| Switch(config- trap-ACCOUNT)# exit | | Return to Global Configuration Mode. |
| Trap-destination example | | |
| Switch(config)# snmp-server trap-destination 1 | | Create a trap destination account. |
| Switch(config-trap-1)# active | | Activate the trap destination account. |
| Switch(config-trap-1)# community mycomm | | Refer this trap destination account to the community “mycomm”. |
| Switch(config-trap-1)# description redepttrapdest | | Add a description for this trap destination account. |
| Switch(config-trap-1)# destination 172.168.1.254 | | 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 catv port-link power-down warm-start] | <p>Specify the trap type that will be sent when a certain situation occurs.</p> <p>all: A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down, power is down, or the CATV optical-fiber source is less than -9 dBm.</p> <p>auth-fail: A trap will be sent when any unauthorized user attempts to login.</p> <p>cold-start: A trap will be sent when the device boots up.</p> <p>catv: A trap will be sent when the optical-fiber source is less than -9 dBm.</p> <p>port-link: A trap will be sent when the link is up or down.</p> <p>power-down: A trap will be sent when the device's power is down.</p> <p>warm-start: A trap will be sent when the device restarts.</p> |
| 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. |

2.5.15 Switch Command

| Switch command | Description |
|--|--|
| Switch(config)# switch sfp polling | Enable the Switch to refresh SFP DMI information and current state in a fixed interval. |
| Switch(config)# switch statistics polling | Enable the Switch to refresh counter information and current state in a fixed interval. |
| No command | |
| Switch(config)# no switch sfp polling | Disable the Switch to refresh SFP DMI information and current state in a fixed interval. |
| Switch(config)# no switch statistics polling | Disable the Switch to refresh counter information and current state in a fixed interval. |

2.5.16 Switch-info Command

Set up the Managed 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 Switch, up to 55 alphanumeric characters. |
| Switch(config)# switch-info dhcp-vendor-id [dhcp_vendor_id] | [dhcp_vendor_id] | Enter the user-defined DHCP vendor ID up to 55 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcp.conf file. For detailed information, see Appendix A . |
| Switch(config)# switch-info system-contact [system_contact] | [system_contact] | Enter contact information up to 55 alphanumeric characters for this Managed switch. |
| 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, "13 th Floor". |
| Switch(config)# switch-info system-name [system_name] | [system_name] | Enter a unique name up to 55 alphanumeric characters for this Managed Switch. 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. |

| | | |
|---|-------------|---|
| Switch(config)# switch-info host-name [host_name] | [host_name] | Enter a new hostname up to 15 alphanumeric characters for this Managed Switch. By default, the hostname prompt shows the model name of this Managed Switch. You can change the factory-assigned hostname prompt to the one that is easy for you to identify during network configuration and maintenance. |
| No command | | |
| Switch(config)# no switch-info company-name | | Delete the entered company name information. |
| Switch(config)# no switch-info dhcp-vendor-id | | Delete the entered DHCP vendor ID 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. |
| Switch(config)# no switch-info host-name | | Set the hostname to the factory default. |
| 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". |

2.5.17 User Command

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-USERNAME)# active | | Activate this user account. |

| | | |
|--|-------------------|--|
| Switch(config-user-USERNAME)# description [description] | [description] | Enter the brief description for this user account. |
| Switch(config-user-USERNAME)# level [admin rw ro] | [admin rw ro] | <p>Specify user account level. By default, when you create a community, the access privilege for this account is set to “read only”.</p> <p>Admin: Full access right, including maintaining user account, system information, loading factory settings, etc..</p> <p>rw: Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware.</p> <p>Ro: Read Only access privilege.</p> |
| Switch(config-user-USERNAME)# password [password] | [password] | Enter the password for this user account up to 20 alphanumeric characters. |
| No command | | |
| Switch(config)# no user name [user_name] | [user_name] | Delete the specified user account. |
| Switch(config-user-USERNAME)# no description | | Remove the configured description. |
| Switch(config-user-USERNAME)# no level | | Remove the configured level value. The account level will return to the default setting. |
| Switch(config-user-USERNAME)# no password | | Remove the configured password value. |
| Show command | | |
| Switch(config)# show user name [user_name] | [user_name] | Show the specified account’s information. |
| Switch(config)# show user name | | List all user accounts. |
| Switch(config-user-USERNAME)# 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-USERNAME)# description misengineer | | Add a description to this new account “miseric”. |
| Switch(config-user-USERNAME)# level rw | | Set this new account’s access privilege to “read & write”. |
| Switch(config-user-USERNAME)# password mis2256i | | Set up a password for this new account “miseric” |

2.5.18 VLAN Command

Create a 802.1q VLAN and management VLAN rule.

| VLAN dot1q command | Parameter | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------------|--|------|---|---|---|---|---|---|---|---|--|--|--|--|---|---|--|---|--|--|--|---|---|--|--|---|--|--|---|---|--|--|--|---|--|---|---|--|--|--|--|---|---|---|---|---|---|---|---|---|
| Switch(config)# vlan dot1q-vlan | | Enable 802.1q VLAN mode. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan dot1q-vlan [1-4094] | [1-4094] | Enter a VID number to create a 802.1q VLAN. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan dot1q-vlan isolation | | <p>Enable VLAN isolation mode. When enabled, each LAN port is separated and can not communicate with each other except for forwarding packets to port 6 (WAN port).</p> <p>In other words, the device will be forced to follow the rule shown below.</p> <table><tr><td>Port</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td></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> | Port | 1 | 2 | 3 | 4 | 5 | 6 | 1 | V | | | | | V | 2 | | V | | | | V | 3 | | | V | | | V | 4 | | | | V | | V | 5 | | | | | V | V | 6 | V | V | V | V | V | V |
| Port | 1 | 2 | 3 | 4 | 5 | 6 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | V | | | | | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | | V | | | | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | V | | | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | V | | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | | | | | V | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | V | V | V | V | V | V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config-vlan-VID)# name | [vlan_name] | Specify a descriptive name up to 15 characters for this VLAN. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan management-vlan [1-4094] | [1-4094] | Enter the management VLAN ID. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| management-port [port_list] | [port_list] | Specify the management port number. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan port-based | | Enable port based VLAN mode | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan port-based [name] include-cpu | [name] | Specify the port based VLAN name and add CPU in this VLAN group. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan | | Enable Q-in-Q (double tag) VLAN. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan bypass-ctag | | Ignore the C-tag checking. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan pass-through-mode | | Enable VLAN pass-through mode. This enables the device to be managed remotely via the specified VLAN. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan pass-through-vlan [1-4094] | [1-4094] | Specify pass-through VLAN ID. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan isp-port [port_list] | [port_list] | Specify ISP ports. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan management-stag [1-4094] | [1-4094] | Specify the service tag VID of management traffic. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan qinq-vlan stag-ethertype [0xWXYZ] | [0xWXYZ] | Specify the ether type for the service tag. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Switch(config)# vlan option60 vlan-map [1-6] vlan-id [1-4094] | [1-6] | Specify the ports able to verify Vendor-ID and send the corresponding VID value. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vendor-id [vendor-id] | [1-4094] | VID: The value this option is set to gives the DHCP server a hint about any required extra | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | | |
|-------------------------------|-------------|---|
| | | information that this client needs in a DHCP response. |
| | [vendor-id] | Vendor-ID: The information is a variable-length string of characters which has a meaning specified by the vendor of the DHCP client. |
| Switch(config)# vlan option60 | | <p>An option exists to identify the vendor and functionality of a DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is to set a value in its DHCP requests called the Vendor Class Identifier (VCI) (Option 60).</p> <p>This method allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately.</p> <p>This command enables DHCP option60. To do so, finish settings of vlan-map, vlan-id and vendor-id above and DHCP Option60 of a port in VLAN & Interface command below first.</p> |

| VLAN & Interface command | | |
|---|-------------|--|
| Switch(config)# interface [port_list] | [port_list] | Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4 |
| Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094] | [1-4094] | Set up the selected ports' PVID. |
| Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094] | [1-4094] | Assign the selected ports to a specified VLAN. |
| Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access | | Set the selected ports to access mode (untagged). |
| Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk | | Set the selected ports to trunk mode (tagged). |
| Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native | | Enable native VLAN for untagged traffic. |
| Switch(config-if-PORT-PORT)# vlan port-based [name] | [name] | Add the selected port(s) to the specified port base VLAN. |
| Switch(config-if-PORT-PORT)# vlan qinq-vlan stag-vid [1-4094] | [1-4094] | Specify the service tag VID for the selected port(s) |
| Switch(config-if-PORT-PORT)# vlan option60 | | Enable the ports to receive Option60 packet. |
| No command | | |
| Switch(config)# no vlan dot1q- | [1-4094] | Delete the specified VID. |

| | | |
|---|----------|---|
| vlan [1-4094] | | |
| Switch(config)# no vlan dot1q-vlan isolation | | Disable VLAN Isolation mode. |
| Switch(config)# no vlan qinq-vlan | | Disable Q-in-Q VLAN. |
| Switch(config)# no vlan qinq-vlan bypass-ctag | | Activate C-tag checking. |
| Switch(config)# no vlan qinq-vlan pass-through-mode | | Disable pass-through mode. |
| Switch(config)# no vlan qinq-vlan pass-through-vlan | | Set the pass-through VLAN ID to the default setting. |
| Switch(config)# no vlan qinq-vlan isp-port | | Remove ISP port settings. |
| Switch(config)# no vlan qinq-vlan management-stag | | Remove the service tag VID of the management traffic. |
| Switch(config)# no vlan qinq-vlan stag-ethertype | | Remove the ether type for the service tag settings. |
| Switch(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan | | Set the selected ports' PVID to the default setting. |
| Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode | | Remove port mode. |
| Switch(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk native | | Disable native VLAN for untagged traffic. |
| Switch(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094] | [1-4094] | Remove the selected ports' VLAN membership. The selected ports are no longer member ports in the specified VLAN. |
| Switch(config)# no vlan option60 | | Disable DHCP Option60 of a switch. |
| Switch(config)# no vlan option60 vlan-map [1-6] | | Disable the ports able to verify Vendor-ID and send the corresponding VID value. |
| Switch(config)# no vlan option60 vlan-map [1-6] vlan-id | | Remove information and VID of a port. Note: Disable DHCP Option60 of the switch first if there is one set of vendor ID mapping left only. |
| Switch(config-if-PORT-PORT)# no vlan option60 | | Disable the ports receiving Option60 packet. Note: Disable DHCP Option60 of the switch first if there is one enabled port left only. |
| Switch(config-if-PORT-PORT)# no vlan port-based [name] | [name] | Remove the selected port(s) from the specified port based VLAN. |
| Switch(config-if-PORT-PORT)# no vlan qinq-vlan stag-vid | | Remove the service tag VID of selected port(s) |

Show command

| | | |
|---|-------------|---|
| Switch(config)# show vlan dot1q-vlan | | Show 802.1q VLAN configuration. |
| Switch(config)# show vlan interface | | Show each interface's VLAN ID, user priority and VLAN mode information. |
| Switch(config)# show vlan interface [port_list] | [port_list] | Show the selected ports' VLAN ID user priority and VLAN mode information. |

| | | |
|---|--|---|
| Switch(config)#show vlan port-based | | Show port based VLAN configuration. |
| Switch(config)# show vlan qinq-vlan | | Show Q-in-Q VLAN configuration. |
| Switch(config)# show vlan option60 | | Show the current status of DHCP Option60 |
| VLAN dot1q & interface example | | |
| 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 port 3's interface mode. |
| Switch(config-if-1-3)# vlan dot1q-vlan trunk-vlan 100 | | Assign the selected ports to VLAN 100. |
| Switch(config-if-1-3)# vlan dot1q-vlan mode access | | Set the selected ports to access mode (untagged). |
| Switch(config-if-1-3)# vlan dot1q-vlan access-vlan 100 | | Set the selected ports' PVID to 100. |
| Switch(config)# vlan option60 vlan-map 1 vlan-id 20 vendor-id 123 | | Set up DHCP Option60 configuration |

2.5.19 Show interface statistics Command

The 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 | Parameter | Description |
|--|-------------|---|
| Switch(config)# show interface statistics analysis | | Display packets analysis (events) for each port. |
| Switch(config)# show interface statistics analysis [port_list] | [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 error | | Display error packets statistics (events) for each port. |
| Switch(config)# show interface statistics error [port_list] | [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 traffic | | Display traffic statistics (events) for each port. |
| Switch(config)# show interface statistics traffic [port_list] | [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 clear | | Clear all statistics. |

2.5.20 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, and RX power. |

2.5.21 Show log Command

| Command | Description |
|--------------------------|--|
| Switch(config)# show log | Show event logs currently stored in the Managed Switch. The total number of event logs that can be displayed is 500. |

2.5.22 Show default-config, running-config and start-up-config Command

| Command | Description |
|--------------------------------------|---|
| Switch(config)# show default-config | Show the original configurations assigned to the Managed Switch by the factory. |
| Switch(config)# show running-config | Show configurations currently used in the Managed Switch. Please note that you must save running configurations into your switch flash before rebooting or restarting the device. |
| Switch(config)# show start-up-config | Display system configurations that are stored in flash. |

3. WEB MANAGEMENT

The Managed Switch can be managed via a Web browser. The default IP of the Managed Switch can be reached at “**http://192.168.0.1**”. You can change the Switch’s IP address to the intended one later in its **Network Management** menu.

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

1. Use one of the 10/100/1000Base-TX RJ-45 ports (as the temporary RJ-45 Management console port) to set up the assigned IP parameters of the Managed Switch including the following:
 - IP address
 - Subnet Mask
 - Default Switch IP address, if required
2. Run a Web browser and specify the Managed Switch’s IP address to reach it. (The default IP address for the Managed Switch can be reached at “**http://192.168.0.1**” before any change.)
3. Login to the Managed Switch.

Once you gain the access, you are requested to login.

The image shows a web browser window with a light blue background. At the top left, the word "Login" is written in a bold, dark blue font. Below it, there is a bullet point followed by the text "Please login". Further down, there are two text input fields. The first field is preceded by the label "Enter Administrator Name :" and the second by "Enter Administrator Password :". Both labels are in a small, dark grey font. Below the password field, there is a dark blue button with the word "Login" in white text.

Enter the administrator name and password for the initial login and then click “Login”. The default administrator name is **admin** and without password (leave the password field blank).

After a successful login, the screen appears as below.

| System Information | | | |
|--------------------|---|------------------|---------------|
| Company Name | Connection Technology Systems | | |
| System Object ID | .1.3.6.1.4.1.9304.100.3006 | | |
| System Contact | info@ctsystem.com | | |
| System Name | Managed 6 Ports 1000M Switch | | |
| System Location | 18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan | | |
| DHCP Vendor ID | HES-3106 | | |
| Model Name | HES-3106 | | |
| Host Name | HES-3106 | | |
| Firmware Version | 0.99.01 | | |
| 1000M Port Number | 6 | 100M Port Number | 0 |
| M/B Version | A01 | | |
| Fiber 1 Type | SFP -- -- | | |
| Fiber 1 Vendor | | Fiber 1 PN | |
| Serial Number | PM3106RF0000000 | Date Code | 20120515 |
| Up Time | 0 day 00:13:54 | Local Time | Not Available |
| CATV Module | RF TV State | Off | |
| | RF TV Output | On | |

OK

1. **System Information:** Name the Managed 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 Managed 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 Managed Switch.
9. **Logout:** Exit the management interface.

3.1 System Information

Select **System Information** from the left column and then the following screen shows up.

| System Information | | | |
|-----------------------------------|--|------------------|---------------|
| Company Name | Connection Technology Systems | | |
| System Object ID | .1.3.6.1.4.1.9304.100.3006 | | |
| System Contact | info@ctsystem.com | | |
| System Name | Managed 6 Ports 1000M Switch | | |
| System Location | 18F-6, No. 79, Sec. 1, Xintai 5th Rd., Xizhi Dist., Taiwan | | |
| DHCP Vendor ID | HES-3106 | | |
| Model Name | HES-3106 | | |
| Host Name | HES-3106 | | |
| Firmware Version | 0.99.01 | | |
| 1000M Port Number | 6 | 100M Port Number | 0 |
| M/B Version | A01 | | |
| Fiber 1 Type | SFP -- -- | | |
| Fiber 1 Vendor | | Fiber 1 PN | |
| Serial Number | PM3106RF0000000 | Date Code | 20120515 |
| Up Time | 0 day 00:13:54 | Local Time | Not Available |
| CATV Module | RF TV State | Off | |
| | RF TV Output | On | |
| <input type="button" value="OK"/> | | | |

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

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

System Contact: Enter contact information up to 55 alphanumeric characters for this Managed Switch.

System Name: Enter a unique name up to 55 alphanumeric characters for this Managed Switch. 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.

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

DHCP Vendor ID: Enter the user-defined vendor ID up to 55 alphanumeric characters. Please make sure you have an exact DHCP Vendor ID with the value specified in "vendor-classes" in your dhcp.conf file. For detailed information, see [Appendix A](#).

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

Host Name: View-only field that shows the product's host name.

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

1000M Port Number: The number of ports transmitting at the speed of 1000Mbps

100M Port Number: The number of ports transmitting at the speed of 100Mbps

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

Fiber 1 Type: View-only field that shows information about the slide-in or fixed fiber type.

Fiber 1 Vendor: View-only field that shows the vendor of the slide-in or fixed fiber.

Fiber 1 PN: View-only field that shows the PN of the slide-in or fixed fiber.

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

Date Code: View-only field that shows the Managed Switch firmware date code.

Up time: View-only field that shows how long the device has been powered on.

Local Time: View-only field that shows the time of the location where the switch is.

***CATV Module- RF TV State:** View-only field that shows whether RF TV is ready or not.

***CATV Module- RF TV Output:** Turn on or off the RF TV Output.

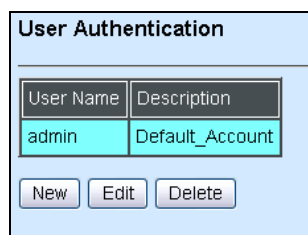
Click the “**OK**” button to apply the modifications.

**For models with CATV RF module only.*

3.2 User Authentication

To prevent any un-authorized operation, only registered users are allowed to operate the Managed Switch. Users who want to operate the Managed Switch need to register into the user’s list first.

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



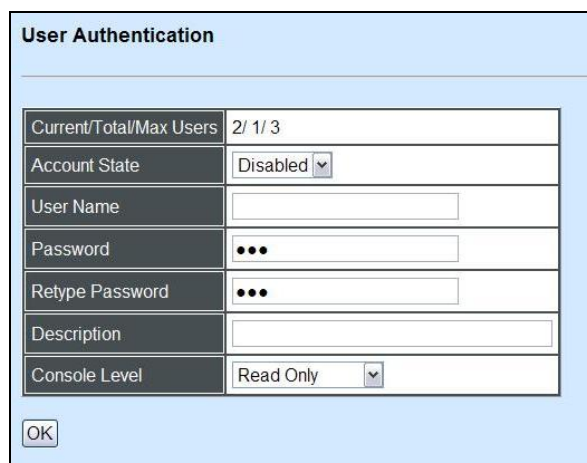
| User Name | Description |
|-----------|-----------------|
| admin | Default_Account |

New Edit Delete

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.



The image shows a 'User Authentication' dialog box with a light blue header and a white body. It contains a table with the following fields:

| | |
|-------------------------|--------------------------|
| Current/Total/Max Users | 2/ 1/ 3 |
| Account State | Disabled ▼ |
| User Name | <input type="text"/> |
| Password | <input type="password"/> |
| Retype Password | <input type="password"/> |
| Description | <input type="text"/> |
| Console Level | Read Only ▼ |

At the bottom left of the dialog box is an 'OK' button.

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

Current: This shows the number of current registered user.

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

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

Account State: Enable or disable the selected account.

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 up to 35 alphanumeric characters for this user. This is mainly for reference only.

Console Level: Select the preferred access level for this newly created account.

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

Read & Write: Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware.

Read Only: Read only access right.

NOTE: If you forget the login password, the only way to gain access to the Web Management is to set the Managed Switch back to the factory default setting by pressing the Reset button for 10 seconds (The Reset button is located on the Right Panel of the Managed Switch.). When the Managed Switch returns back to the default setting, you can login with the default login username and password (By default, no password is required. Leave the field empty and then press Login.)

Click the “**OK**” button to apply the settings.

3.3 Network Management

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

HES-3106

- System Information
- User Authentication
- Network Management**
 - Network Configuration
 - System Service Configuration
 - Time Server Configuration
 - Device Community
 - Trap Destination
 - Trap Configuration
- Switch Management
- Switch Monitor
- System Utility
 - Save Configuration
 - Reset System
 - Logout

Network Configuration

| | | |
|--------------------|-------------------|---------------|
| MAC Address | 00-06-19-67-01-62 | |
| Configuration Type | Manual ▼ | Current State |
| IP Address | 192.168.0.1 | 192.168.0.1 |
| Subnet Mask | 255.255.255.0 | 255.255.255.0 |
| Gateway | 0.0.0.0 | 0.0.0.0 |

IP Source Binding:

| Source Binding | Enabled ▼ | |
|----------------|------------|---------------|
| Index | State | IP Address |
| 1 | Enabled ▼ | 192.168.0.210 |
| 2 | Disabled ▼ | 0.0.0.0 |
| 3 | Disabled ▼ | 0.0.0.0 |
| 4 | Disabled ▼ | 0.0.0.0 |
| 5 | Disabled ▼ | 0.0.0.0 |
| 6 | Disabled ▼ | 0.0.0.0 |
| 7 | Disabled ▼ | 0.0.0.0 |
| 8 | Disabled ▼ | 0.0.0.0 |
| 9 | Disabled ▼ | 0.0.0.0 |
| 10 | Disabled ▼ | 0.0.0.0 |
| 11 | Disabled ▼ | 0.0.0.0 |
| 12 | Disabled ▼ | 0.0.0.0 |

OK

1. **Network Configuration:** Set up the required IP configuration of the Managed Switch.
2. **System Service Configuration:** Set up the system service type.
3. **Time Server Configuration:** Set up the time server's configuration.
4. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.
5. **Trap Destination:** View the registered SNMP trap destination list.
6. **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.

HES-3106

- System Information
- User Authentication
- Network Management
 - Network Configuration**
 - System Service Configuration
 - Time Server Configuration
 - Device Community
 - Trap Destination
 - Trap Configuration
- Switch Management
- Switch Monitor
- System Utility
 - Save Configuration
 - Reset System
 - Logout

Network Configuration

| | | |
|--------------------|-------------------|---------------|
| MAC Address | 00-06-19-67-01-62 | |
| Configuration Type | Manual ▼ | Current State |
| IP Address | 192.168.0.1 | 192.168.0.1 |
| Subnet Mask | 255.255.255.0 | 255.255.255.0 |
| Gateway | 0.0.0.0 | 0.0.0.0 |

IP Source Binding:

| Index | State | IP Address |
|-------|------------|---------------|
| 1 | Enabled ▼ | 192.168.0.210 |
| 2 | Disabled ▼ | 0.0.0.0 |
| 3 | Disabled ▼ | 0.0.0.0 |
| 4 | Disabled ▼ | 0.0.0.0 |
| 5 | Disabled ▼ | 0.0.0.0 |
| 6 | Disabled ▼ | 0.0.0.0 |
| 7 | Disabled ▼ | 0.0.0.0 |
| 8 | Disabled ▼ | 0.0.0.0 |
| 9 | Disabled ▼ | 0.0.0.0 |
| 10 | Disabled ▼ | 0.0.0.0 |
| 11 | Disabled ▼ | 0.0.0.0 |
| 12 | Disabled ▼ | 0.0.0.0 |

OK

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

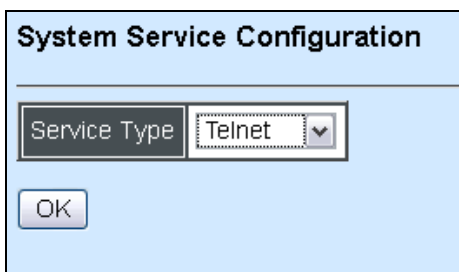
Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Managed Switch. This address is required when the Managed Switch and the network management station are on different networks or subnets. The default value of this parameter is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

IP source binding: For security reason, this function can be enabled for only specific IP address allowed to access the WEB and telnet of the Managed Switch. Overall 12 IP addresses could be set in this function. For example, If IP address 192.168.0.210 is enabled in IP source binding, only the client from this IP address could access the WEB and telnet of the Managed Switch.

Click the “**OK**” button to apply the settings.

3.3.2 System Service Configuration

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

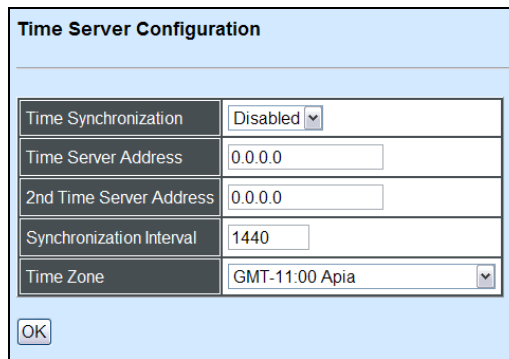


Service Type: Select **disabled**, **Telnet** or **SSH** for the system service type.

Click the “**OK**” button to apply the settings.

3.3.3 Time Server Configuration

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



Time Server Configuration

| | |
|--------------------------|------------------|
| Time Synchronization | Disabled ▼ |
| Time Server Address | 0.0.0.0 |
| 2nd Time Server Address | 0.0.0.0 |
| Synchronization Interval | 1440 |
| Time Zone | GMT-11:00 Apia ▼ |

OK

Time Synchronization: Enable or disable time synchronization.

Time Server Address: Specify the primary NTP time server address.

2nd Time Server Address: When the default time server is down, the Managed Switch will automatically connect to the 2nd time server.

Synchronization Interval: The time interval to synchronize from NTP time server. The allowable value is from 1 to 99999 minutes.

Time Zone: Select the appropriate time zone from the pull-down menu.

Click the “**OK**” button to apply the settings.

3.3.4 Device Community

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



Device Community

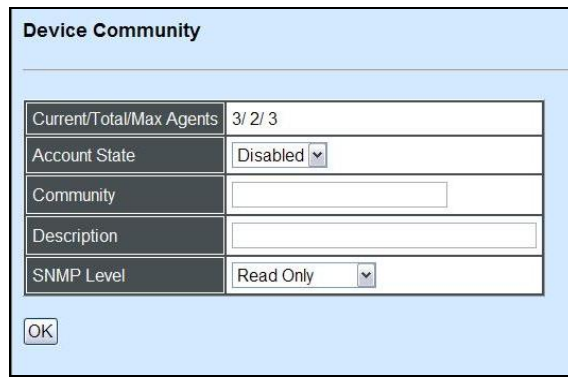
| Community | Description |
|-----------|-----------------|
| public | Default_Account |
| admin | Default_Account |

New Edit Delete

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.



The image shows a 'Device Community' configuration window. It contains a table with the following fields:

| | |
|--------------------------|----------------------|
| Current/Total/Max Agents | 3/ 2/ 3 |
| Account State | Disabled ▼ |
| Community | <input type="text"/> |
| Description | <input type="text"/> |
| SNMP Level | Read Only ▼ |

At the bottom left of the window is an 'OK' button.

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

Current: This shows the number of currently registered communities.

Total: This shows the number of total registered communities.

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 up to 35 alphanumeric characters for this community name. This is mainly for reference only.

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

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

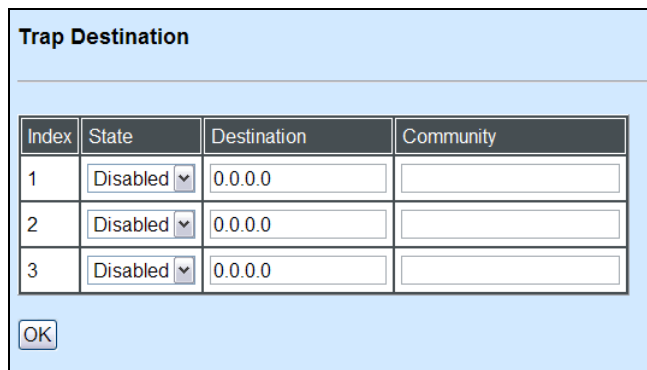
Read & Write: Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware.

Read Only: Read only access right.

Click the “**OK**” button to apply the settings.

3.3.5 Trap Destination

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



The 'Trap Destination' window contains a table with four columns: Index, State, Destination, and Community. There are three rows, each with a 'Disabled' dropdown in the State column, '0.0.0.0' in the Destination column, and an empty field in the Community column. An 'OK' button is at the bottom left.

| Index | State | Destination | Community |
|-------|----------|-------------|-----------|
| 1 | Disabled | 0.0.0.0 | |
| 2 | Disabled | 0.0.0.0 | |
| 3 | Disabled | 0.0.0.0 | |

State: Enable or disable the function of sending traps to the specified destination.

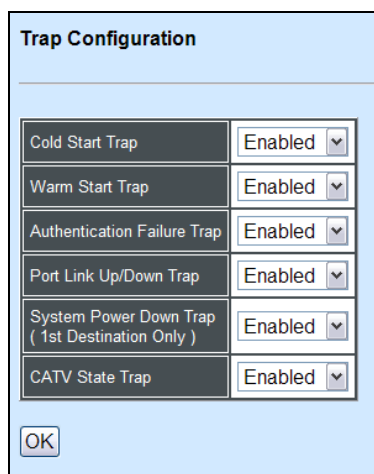
Destination: Enter the specific IP address of the network management system that will receive traps.

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

Click the “**OK**” button to apply the settings.

3.3.6 Trap Configuration

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



The 'Trap Configuration' window lists six trap types, each with an 'Enabled' dropdown: Cold Start Trap, Warm Start Trap, Authentication Failure Trap, Port Link Up/Down Trap, System Power Down Trap (1st Destination Only), and CATV State Trap. An 'OK' button is at the bottom left.

| | |
|--|---------|
| 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 |
| CATV State Trap | Enabled |

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: Enable or disable the Managed Switch to send a trap while the Managed Switch is power down.

***CATV State Trap:** Enable or disable the Managed Switch to send a trap when the optical-fiber source is less than -9 dBm.

Click the “**OK**” button to apply the settings.

**For models with CATV RF module only.*

3.4 Switch Management

To manage the Managed Switch and set up required switching functions, click the folder **Switch Management** from the left column and then several options and folders will be displayed for your selection.

| Switch Configuration | |
|------------------------|--------------------|
| MAC Address Aging Time | 300 (7-600000)Secs |
| SFP Polling | Enabled ▼ |
| Statistics Polling | Enabled ▼ |

OK

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

2. **Storm Control:** Prevent the Managed Switch from unicast, broadcast, and multicast storms.
3. **Port Configuration:** Enable or disable port speed, flow control, etc..
4. **Rate Limit Configuration:** Enable or disable Port Priority and set up Port Rate Limit, etc..
5. **QoS Priority Configuration:** Set up QoS Priority based on IEEE 802.1p, ToS/DSCP and VID Qos mode.
6. **VLAN Configuration:** Set up IEEE 802.1q Tag VLAN and Q in Q VLAN configuration.
7. **Mirroring Configuration:** Set up port mirroring configuration.
8. **IGMP Snooping:** Set up IGMP Snooping function.
9. **Loop Detection:** Enable or disable Loop Detection function.
10. **Filter Configuration:** Set up DHCP snooping and DHCP server trust ports.

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 (7-600000)Secs |
| SFP Polling | Enabled <input type="button" value="v"/> |
| Statistics Polling | Enabled <input type="button" value="v"/> |

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

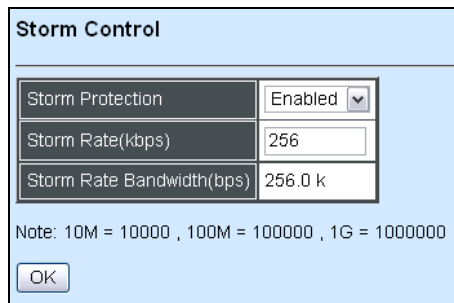
SFP Polling: Enable or disable SFP Polling.

Statistics Polling: Enable or disable Statistics Polling.

Click the “**OK**” button to apply the settings.

3.4.2 Storm Control

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



Storm Control

| | |
|---------------------------|-----------|
| Storm Protection | Enabled ▾ |
| Storm Rate(kbps) | 256 |
| Storm Rate Bandwidth(bps) | 256.0 k |

Note: 10M = 10000 , 100M = 100000 , 1G = 1000000

OK

Storm Protection: Enable or disable Storm Protection function.

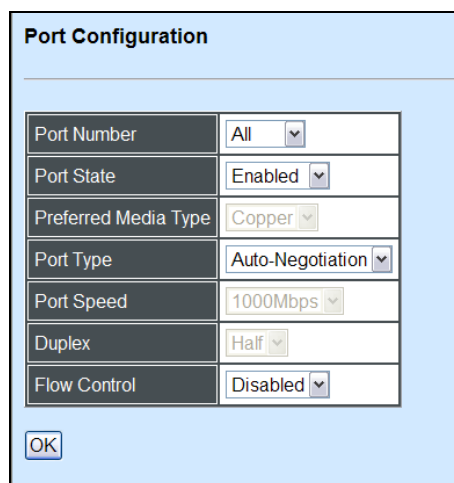
Storm Rate: Set up storm rate value. Packets exceeding the value will be dropped.

Storm Rate Bandwidth: Display the current configured storm rate bandwidth.

Click the “**OK**” button to apply the settings.

3.4.3 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 ▾ |
| Preferred Media Type | Copper ▾ |
| Port Type | Auto-Negotiation ▾ |
| Port Speed | 1000Mbps ▾ |
| Duplex | Half ▾ |
| Flow Control | Disabled ▾ |

OK

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

Port State: Enable or disable the current port state.

Preferred Media Type: This shows the media type (either Fiber or Copper) of the selected port. This field is open to select only when ports of the device have two media type.

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/1000Mbps) 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 Flow Control function.

Click the “**OK**” button to apply the settings.

3.4.4 Rate Limit Configuration

Click the folder **Rate Limit Configuration** from the left column and then the following screen page appears.

| Rate Limit Configuration | | | | | | |
|--------------------------|--------|--------|--------|--------|--------|--------|
| Port Number | 1 | 2 | 3 | 4 | 5 | 6 |
| Ingress Rate | Off ▼ | Off ▼ | Off ▼ | Off ▼ | Off ▼ | Off ▼ |
| Ingress Limiter(kbps) | 32 | 32 | 32 | 32 | 32 | 32 |
| Ingress Bandwidth(bps) | 32.0 k | 32.0 k | 32.0 k | 32.0 k | 32.0 k | 32.0 k |
| Egress Rate | Off ▼ | Off ▼ | Off ▼ | Off ▼ | Off ▼ | Off ▼ |
| Egress Limiter(kbps) | 32 | 32 | 32 | 32 | 32 | 32 |
| Egress Bandwidth(bps) | 32.0 k | 32.0 k | 32.0 k | 32.0 k | 32.0 k | 32.0 k |

Note: 10M = 10000 , 100M = 100000 , 1G = 1000000

OK

Ingress Rate: Click the pull-down menu to set up Port Ingress Rate, on or off.

Ingress Limiter: Enter ingress bandwidth for each port (the allowable bandwidth is between 32 and 1000000).

Ingress Bandwidth (Kbps): Display current configured ingress bandwidth.

Egress Rate: Click the pull-down menu to set up Port Egress Rate, on or off.

Egress Limiter (Kbps): Enter egress bandwidth for each port (the allowable bandwidth is between 32 and 1000000).

Egress Bandwidth (Kbps): Display current configured egress bandwidth.

Click the “**OK**” button to apply the settings.

3.4.5 QoS Priority Configuration

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

QoS Priority Configuration

QoS Priority:

Priority Mode

Disabled

Queue Mode

Strict

Queue Weight(Q0:Q1:Q2:Q3)

1 : 2 : 4 : 8

802.1p Priority Map

0

Q0

DSCP Priority Map

DSCP(0)

Q0

Note: Uses 802.1p priority mode must open 802.1Q vlan mode.

Remarking:

Remarking Mode

Disabled

DSCP Remarking

Disabled

Note: The VID remarking has high priority.(VID remarking > 802.1p remarking > DSCP remarking)

Note: Remarking rule won't affect priority map rule.

OK

QoS Priority

Priority Mode: Three options are available, Disabled, IEEE 802.1p, and DSCP.

Queue Mode: Click the pull-down menu to select the Queue Mode, Strict or Weight.

Strict mode: This indicates that egress traffic is prioritized based on a queue value assigned to each port. When congestion happens, traffic assigned to queue 3 will be transmitted first. The traffic assigned to queue 2 will not be transmitted until queue 3's traffic is done transmitting, and so forth.

Weight mode: This mode enables users to assign different weights to 4 queues, which have fair opportunity of dispatching. Each queue has the specific amount of bandwidth according to its assigned weight.

Queue Weight (Q0:Q1:Q2:Q3): Specify the weight of four queues.

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 |

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.

Note: 802.1p priority mode can only be applied under 802.1q VLAN mode.

Remarking

Remarking Mode: Four options are available, Disabled, VID Remarking, 802.1p Remarking, and VID + 802.1p Remarking.

➤ VID Remarking

| Remarking Mode | VID Remarking ▼ | | | | | | | |
|-------------------|-----------------|------------|-----|----------|-------|------------|-----|----------|
| VID Remarking Map | Index | State | VID | Priority | Index | State | VID | Priority |
| | 1 | Disabled ▼ | 1 | 0 ▼ | 2 | Disabled ▼ | 1 | 0 ▼ |
| | 3 | Disabled ▼ | 1 | 0 ▼ | 4 | Disabled ▼ | 1 | 0 ▼ |
| | 5 | Disabled ▼ | 1 | 0 ▼ | 6 | Disabled ▼ | 1 | 0 ▼ |
| | 7 | Disabled ▼ | 1 | 0 ▼ | 8 | Disabled ▼ | 1 | 0 ▼ |

State: Disable or enable the mapping entry.

VID: Specify the VLAN ID to be remarked.

Priority: Specify the remarking 802.1p value.

➤ 802.1p Remarking

| Remarking Mode | 802.1p Remarking ▼ | | | | | | | |
|----------------------|--------------------|------------|--------|----------|-------|------------|--------|----------|
| 802.1p Remarking Map | Index | State | 802.1p | Priority | Index | State | 802.1p | Priority |
| | 1 | Disabled ▼ | 0 | 0 ▼ | 2 | Disabled ▼ | 0 | 0 ▼ |
| | 3 | Disabled ▼ | 0 | 0 ▼ | 4 | Disabled ▼ | 0 | 0 ▼ |
| | 5 | Disabled ▼ | 0 | 0 ▼ | 6 | Disabled ▼ | 0 | 0 ▼ |
| | 7 | Disabled ▼ | 0 | 0 ▼ | 8 | Disabled ▼ | 0 | 0 ▼ |

State: Disable or enable the mapping entry.

802.1p: Specify the 802.1p value to be remarked.

Priority: Specify the remarking 802.1p value.

➤ VID + 802.1p Remarking

| | | | | | | | | |
|----------------------|--------------------------|------------|--------|----------|-------|------------|--------|----------|
| Remarking Mode | VID + 802.1p Remarking ▼ | | | | | | | |
| VID Remarking Map | Index | State | VID | Priority | Index | State | VID | Priority |
| | 1 | Disabled ▼ | 1 | 0 ▼ | 2 | Disabled ▼ | 1 | 0 ▼ |
| | 3 | Disabled ▼ | 1 | 0 ▼ | 4 | Disabled ▼ | 1 | 0 ▼ |
| | 5 | Disabled ▼ | 1 | 0 ▼ | 6 | Disabled ▼ | 1 | 0 ▼ |
| | 7 | Disabled ▼ | 1 | 0 ▼ | 8 | Disabled ▼ | 1 | 0 ▼ |
| 802.1p Remarking Map | Index | State | 802.1p | Priority | Index | State | 802.1p | Priority |
| | 1 | Disabled ▼ | 0 | 0 ▼ | 2 | Disabled ▼ | 0 | 0 ▼ |
| | 3 | Disabled ▼ | 0 | 0 ▼ | 4 | Disabled ▼ | 0 | 0 ▼ |
| | 5 | Disabled ▼ | 0 | 0 ▼ | 6 | Disabled ▼ | 0 | 0 ▼ |
| | 7 | Disabled ▼ | 0 | 0 ▼ | 8 | Disabled ▼ | 0 | 0 ▼ |

DSCP Remarking: Enable or disable 802.1p Remarking.

| | | | | | | | | |
|--------------------|-----------|------------|------|-----------|-------|------------|------|-----------|
| DSCP Remarking | Enabled ▼ | | | | | | | |
| DSCP Remarking Map | Index | State | DSCP | Priority | Index | State | DSCP | Priority |
| | 1 | Disabled ▼ | 0 | DSCP(0) ▼ | 2 | Disabled ▼ | 0 | DSCP(0) ▼ |
| | 3 | Disabled ▼ | 0 | DSCP(0) ▼ | 4 | Disabled ▼ | 0 | DSCP(0) ▼ |
| | 5 | Disabled ▼ | 0 | DSCP(0) ▼ | 6 | Disabled ▼ | 0 | DSCP(0) ▼ |
| | 7 | Disabled ▼ | 0 | DSCP(0) ▼ | 8 | Disabled ▼ | 0 | DSCP(0) ▼ |

State: Disable or enable the mapping entry.

DSCP: Specify the DSCP value to be remarked.

Priority: Specify the remarking DSCP value.

Click the “OK” button to apply the settings.

Note: The VID remarking has higher priority than the other remarking modes. (VID remarking > 802.1p remarking > DSCP remarking)

3.4.6 VLAN Configuration

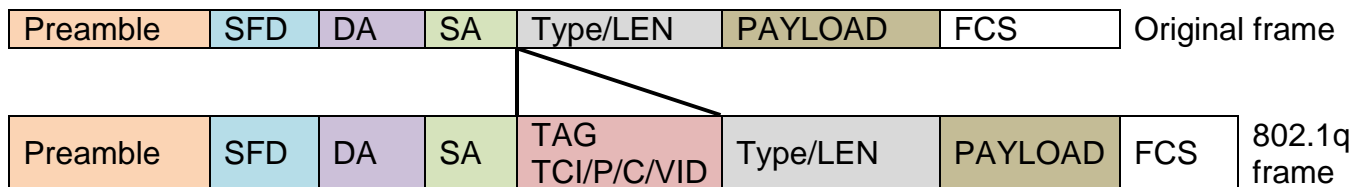
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast 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 Managed Switch supports two types of VLAN, these are: **IEEE 802.1q Tag VLAN** and **Q in Q VLAN**.

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 |

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

- System Information
- User Authentication
- Network Management
- Switch Management
 - Switch Configuration
 - Storm Control
 - Port Configuration
 - Rate Limit Configuration
 - QoS Priority Configuration
 - VLAN Configuration
 - Port Based VLAN
 - IEEE 802.1q Tag VLAN
 - QinQ VLAN Configuration
 - Mirroring Configuration
 - IGMP Snooping
 - Loop Detection
 - Filter Configuration
- Switch Monitor
- System Utility
- Save Configuration
- Reset System
- Logout

Configure Port Based VLAN

| Port Name | 1 | 2 | 3 | 4 | 5 | 6 | CPU |
|-----------|---|---|---|---|---|---|-----|
| port1vlan | - | V | V | V | V | V | V |
| port2vlan | V | - | V | V | V | V | V |
| port3vlan | V | V | - | V | V | V | V |
| port4vlan | V | V | V | - | V | V | V |
| port5vlan | V | V | V | V | - | V | V |
| port6vlan | V | V | V | V | V | - | V |

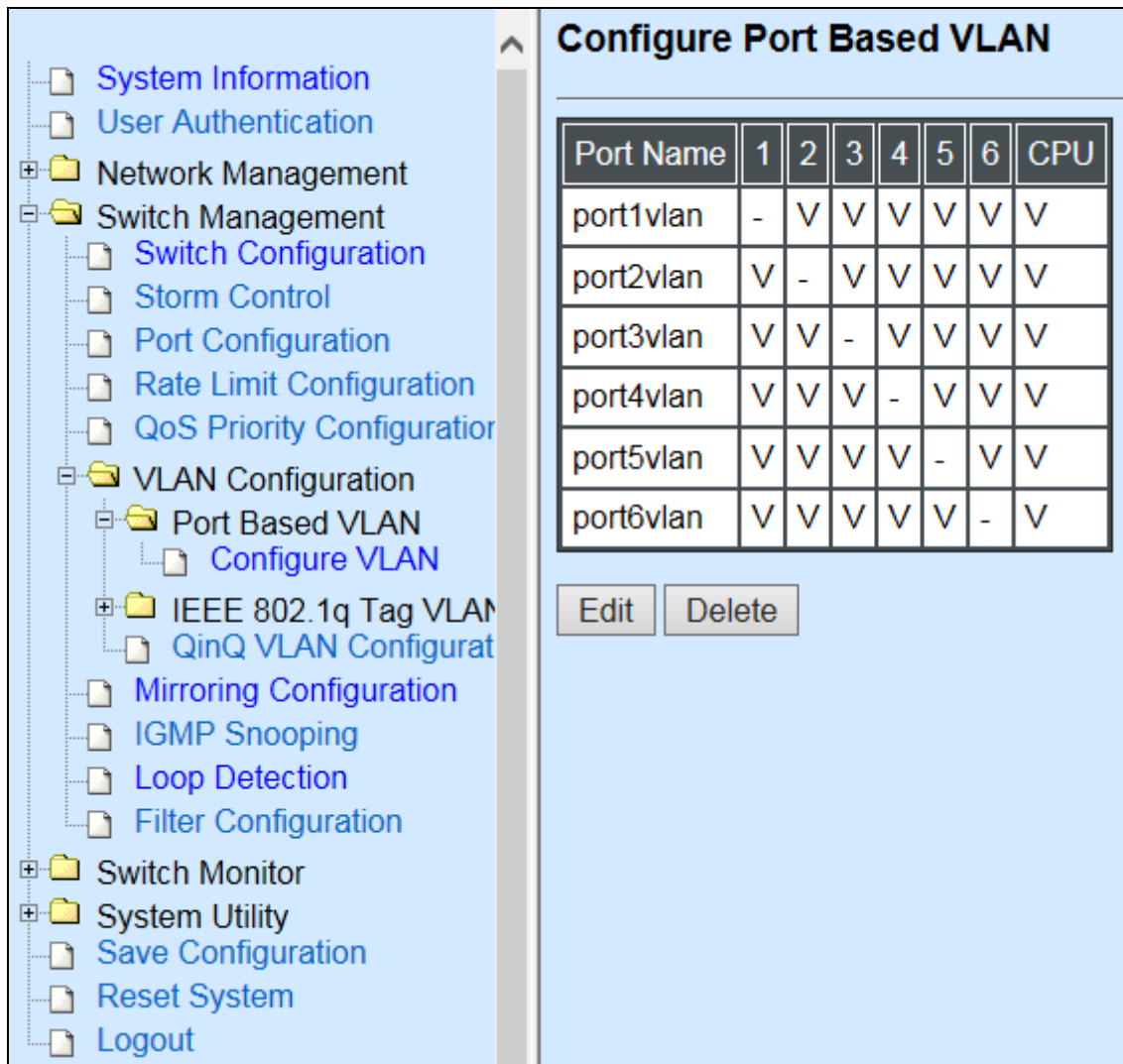
1. Port Based VLAN: Configure Port-Based VLAN settings.

2. IEEE 802.1Q Tag VLAN: Configure IEEE 802.1Q Tag VLAN settings.

3. QinQ VLAN Configuration: Configure Q-in-Q VLAN settings.

3.4.6.1 Port Based VLAN

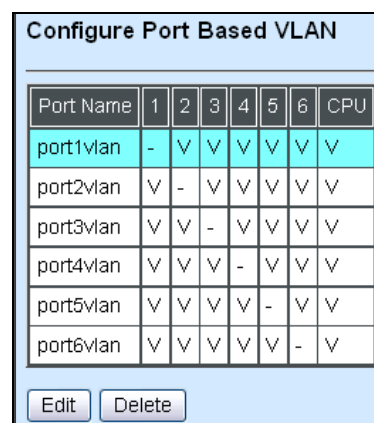
Click the folder **Port Based VLAN** from the **VLAN Configuration** menu and then the following screen page appears.



1. **Configure VLAN:** To edit, delete, or apply Port Based VLAN settings.

3.4.6.1.1 Configure VLAN

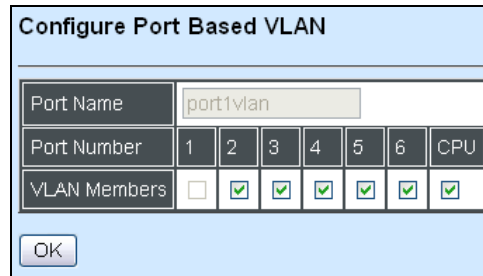
Click the option **Configure VLAN** from the **Port Based VLAN** folder and then the following screen page appears.



Click **Edit** to view and edit current Port Based VLAN setting, and then the following screen

page appears.

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



The dialog box titled "Configure Port Based VLAN" contains a form with three rows and seven columns. The first row is for the "Port Name", with a text input field containing "port1vlan". The second row is for "Port Number", with buttons for "1", "2", "3", "4", "5", "6", and "CPU". The third row is for "VLAN Members", with checkboxes for each port number; the checkboxes for "2" through "6" and "CPU" are checked, while the checkbox for "1" is unchecked. An "OK" button is located at the bottom left of the dialog box.

| Port Name | 1 | 2 | 3 | 4 | 5 | 6 | CPU |
|--------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| port1vlan | | | | | | | |
| VLAN Members | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

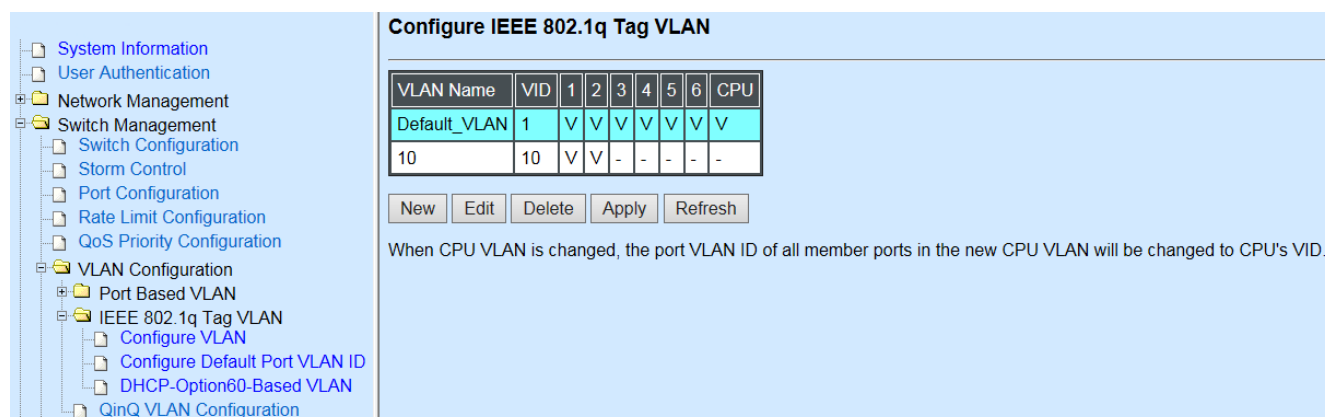
OK

Port Name: View-only field that shows the name of the port based VLAN

VLAN Members: Select the member ports of the port based VLAN

3.4.6.2 IEEE 802.1q Tag VLAN

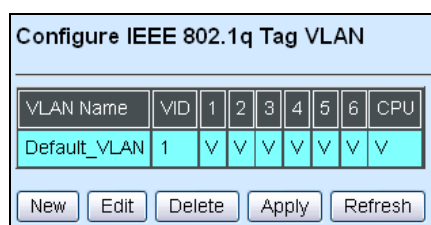
Click the folder **IEEE 802.1Q Tag VLAN** from the **VLAN Configuration** menu and then the following screen page appears.



1. **Configure VLAN:** To create, edit, delete, or apply 802.1Q Tag VLAN settings.
2. **Configure Default Port VLAN ID:** To set up 802.1q Port VLAN ID.
3. **DHCP-Option60-Based VLAN:** To set up Vendor ID and VID...etc. for Vendor Class Identifier

3.4.6.2.1 Configure VLAN

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



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.

Click **Apply** to make the current VLAN settings effective.

Click **Refresh** to get the latest status of VLAN membership table.

| Configure VLAN | | | | | | | |
|-------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Current/Total/Max VLANs | 2/ 1/128 | | | | | | |
| VLAN ID | 0 (1-4094) | | | | | | |
| VLAN Name | | | | | | | |
| Port Number | 1 | 2 | 3 | 4 | 5 | 6 | CPU |
| VLAN Members | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| OK | | | | | | | |

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

Current: This shows the number of currently registered VLAN.

Total: This shows the number of total registered VLANs.

Max: This shows the maximum number of available VLANs to be registered.

VLAN ID: Specify the ID for the currently registered VLAN.

VLAN Name: Specify the name for the currently registered VLAN.

VLAN Member: Assign ports to be the members of the currently registered VLAN.

3.4.6.2.2 Configure Default Port VLAN ID

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

| Configure Default Port VLAN ID | | | | | | | |
|---|--------------------------------|----------|----------|----------|----------|----------|-----|
| 802.1q Tag VLAN Mode | Port Based VLAN(Bypass ctag) ▼ | | | | | | |
| Port Number | 1 | 2 | 3 | 4 | 5 | 6 | CPU |
| Port VLAN ID | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Port User Priority | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ | 0 ▼ |
| Port VLAN Mode | access ▼ | access ▼ | access ▼ | access ▼ | access ▼ | access ▼ | |
| Note: The Port Based VLAN mode is enabled, QinQ mode will setting to disabled | | | | | | | |
| OK | | | | | | | |

802.1q Tag VLAN Mode: Select Port Based VLAN, IEEE802.1q VLAN, Bypass C-tag or Port Isolation mode.

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

Port User Priority: Specify the user priority for each port.

Port VLAN Mode: 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 (VID) will be sent. | |

Click the “**OK**” button to apply the settings.

Note: Q-in-Q mode will be disabled when Port Based VLAN mode is enabled

3.4.6.2.3 DHCP-Option60-Based VLAN

This is an option existing to identify the vendor and functionality of a DHCP client. One method that a DHCP client can utilize to communicate to the server that it is using a certain type of hardware or firmware is to set a value in its DHCP requests called the Vendor Class Identifier (VCI) (Option 60).

This method allows a DHCP server to differentiate between the two kinds of client machines and process the requests from the two types of modems appropriately.

To enable DHCP option60, following steps are required:

1. Create a new VLAN entity. (Refer to section 3.4.6.1.1)
2. Set the ports sending tagged packets as trunk mode. (Refer to section 3.4.6.1.2)

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

DHCP-Option60-Based VLAN

Note: The run-time access VLAN of an VLAN-access port is determined by the lastest received DHCP-option60 vendoe ID on the port.

System-wide Configuration

| | |
|----------|------------|
| Option60 | Disabled ▼ |
|----------|------------|

Port Configuration

| | | | | | | |
|----------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Port-ID | 1 | 2 | 3 | 4 | 5 | 6 |
| Option60 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

DHCP-Option60 Vendor ID mapping

| Index | Enable | Vendor-ID | VID | Clean |
|-------|--------------------------|-----------|-----|-------|
| 1 | <input type="checkbox"/> | | 1 | Clean |
| 2 | <input type="checkbox"/> | | 1 | Clean |
| 3 | <input type="checkbox"/> | | 1 | Clean |
| 4 | <input type="checkbox"/> | | 1 | Clean |
| 5 | <input type="checkbox"/> | | 1 | Clean |
| 6 | <input type="checkbox"/> | | 1 | Clean |

OK

System-wide Configuration: Enable or disable Option60 of the switch.

Port Configuration: The ports receiving Option60 packet. Check the box to enable Option60 of the port and vice versa.

DHCP-Option60 Vendor ID mapping

Index: The ports able to verify Vendor-ID and send the corresponding VID value.

Enable: Check enable box to activate mapping function.

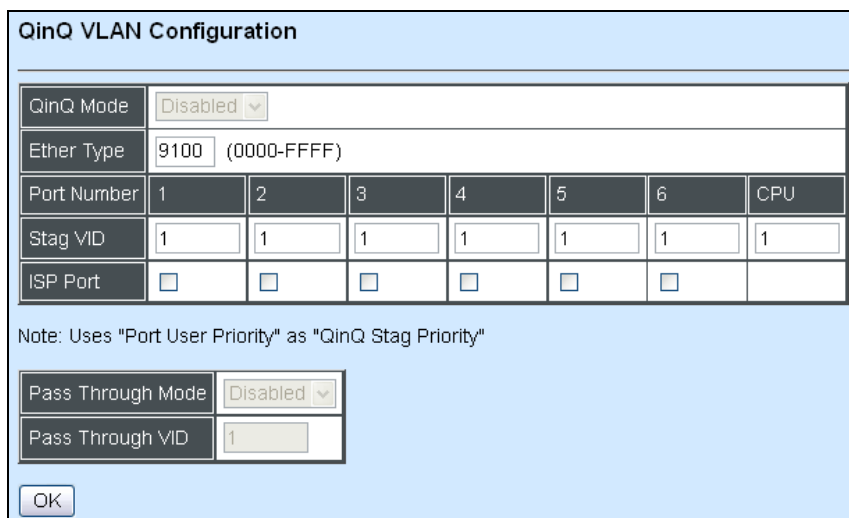
Vendor-ID: The information is a variable-length string of characters which has a meaning specified by the vendor of the DHCP client.

VID: The value this option is set to gives the DHCP server a hint about any required extra information that this client needs in a DHCP response.

Click "**Clean**" to delete information of a port.

3.4.6.3 Q-in-Q VLAN Configuration

Click the **Option Q-in-Q VLAN Configuration** from the **VLAN Configuration** folder and then the following screen page appears.



The dialog box is titled "QinQ VLAN Configuration". It contains the following fields and controls:

- QinQ Mode:** A dropdown menu set to "Disabled".
- Ether Type:** A text field containing "9100" with a range "(0000-FFFF)" in parentheses.
- Port Number:** A row of seven buttons labeled 1, 2, 3, 4, 5, 6, and CPU.
- Stag VID:** A row of seven text fields, each containing the value "1".
- ISP Port:** A row of seven checkboxes, all of which are unchecked.
- Note:** "Uses 'Port User Priority' as 'QinQ Stag Priority'".
- Pass Through Mode:** A dropdown menu set to "Disabled".
- Pass Through VID:** A text field containing the value "1".
- OK:** A button at the bottom left.

QinQ Mode: Enable or disable Q-in-Q VLAN.

Ether Type: Specify the ether type for the service tag.

Priority: Specify a priority bit for the service tag.

VID: Specify a VID for the service tag.

ISP Port: Select ISP ports.

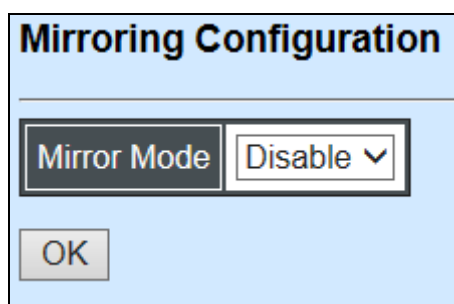
Pass Through Mode: Enable or disable Pass Through mode. This enables the device to be managed remotely via the specified VLAN.

Pass Through VID: Specify the Pass Through VLAN ID.

Click the **“OK”** button to apply the settings.

3.4.7 Mirroring Configuration

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



The dialog box is titled "Mirroring Configuration". It contains the following fields and controls:

- Mirror Mode:** A dropdown menu set to "Disable".
- OK:** A button at the bottom left.

Mirror Mode: Click drop-down box and select “By Port” to access configuration as below.

| Mirroring Configuration | | | | | | |
|-------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Mirror Mode | By Port ▼ | | | | | |
| Destination Port | Port 1 ▼ | | | | | |
| Port Number | 1 | 2 | 3 | 4 | 5 | 6 |
| Source Port | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| OK | | | | | | |

Destination Port: Enable or disable port mirroring function, and select the destination port to which the mirrored traffic will be forwarded.

Source Port: Select the port corresponding to Port Number to be mirrored.

3.4.8 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.

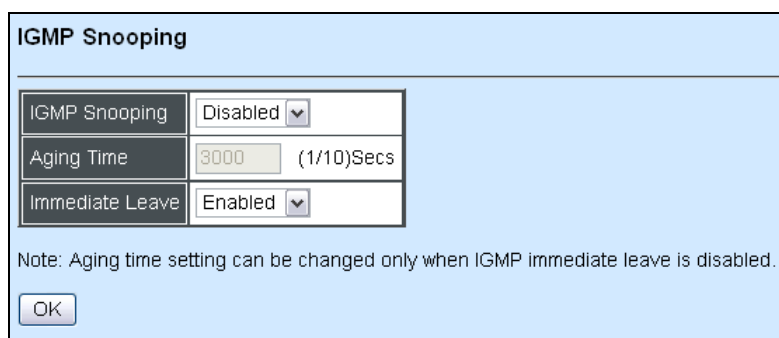
IGMP Snooping is the process of listening to IGMP traffic. IGMP snooping, as implied by the name, is a feature that allows the switch to “listen in” on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

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.

Click the option **IGMP Snooping** from the **Management** menu and then the following screen

page appears.



The image shows a configuration window titled "IGMP Snooping". It contains three settings: "IGMP Snooping" set to "Disabled", "Aging Time" set to "3000" with "(1/10)Secs" next to it, and "Immediate Leave" set to "Enabled". Below these settings is a note: "Note: Aging time setting can be changed only when IGMP immediate leave is disabled." At the bottom left is an "OK" button.

IGMP Snooping: Enable or disable IGMP Snooping.

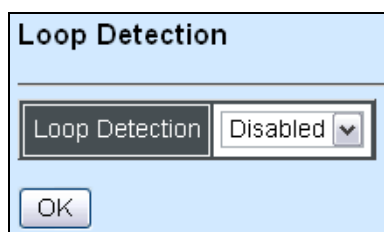
Aging Time: Specify the IGMP querier aging time. If the switch does not receive join packets from the end device within the specified time, the entry associated with this end device will be removed from the IGMP table.

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

Click the “**OK**” button to apply the settings.

3.4.9 Loop Detection

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



The image shows a configuration window titled "Loop Detection". It contains one setting: "Loop Detection" set to "Disabled". At the bottom left is an "OK" button.

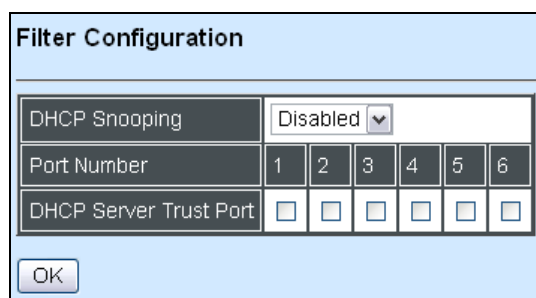
Loop Detection: Enable or disable Loop Detection Function.

Loop Detection allows users to configure the Managed Switch to lock a port when it detects packets which are sent out on that port loop back to the switch. When loops occur, it will cause broadcast storm and affect the performance of layer two Access switch. To avoid this, Loop Detection can be enabled on LAN ports of the Managed Switch. When it detects the loop, it will lock the port which receives the loop packet immediately and send out SNMP trap to inform the network administrator.

Click the “**OK**” button to apply the settings.

3.4.10 Filter Configuration

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



The Filter Configuration dialog box has a title bar 'Filter Configuration'. It contains three rows of settings. The first row is 'DHCP Snooping' with a dropdown menu set to 'Disabled'. The second row is 'Port Number' with six buttons labeled 1 through 6. The third row is 'DHCP Server Trust Port' with six checkboxes, all of which are currently unchecked. An 'OK' button is located at the bottom left of the dialog.

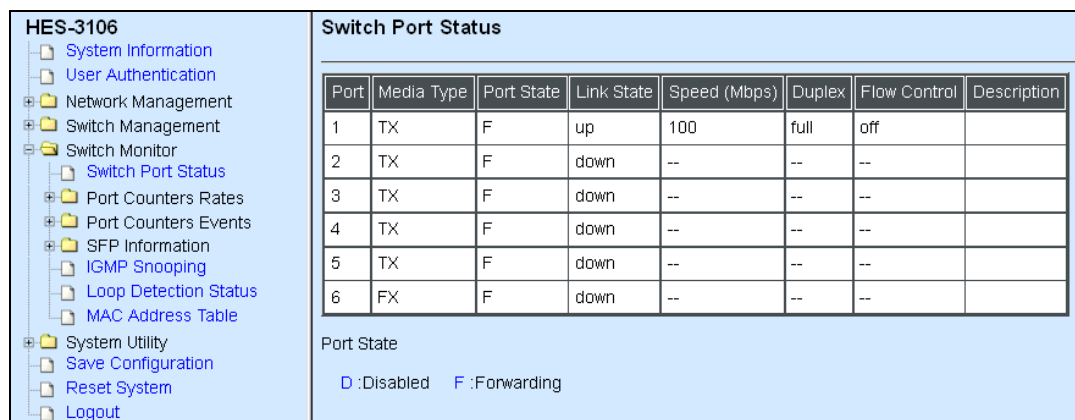
DHCP Snooping: Enable or disable DHCP Snooping function.

DHCP Server Trust Port: Assign the specific port(s) to be the DHCP Server Trust Port(s).

Click the “OK” button to apply the settings.

3.5 Switch Monitor

Switch Monitor allows users to monitor the real-time operation status of the Managed 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.



The Switch Monitor interface is divided into two main sections. On the left is a tree view titled 'HES-3106' containing various system folders like 'System Information', 'User Authentication', 'Network Management', 'Switch Management', 'Switch Monitor', 'Port Counters Rates', 'Port Counters Events', 'SFP Information', 'IGMP Snooping', 'Loop Detection Status', 'MAC Address Table', 'System Utility', 'Save Configuration', 'Reset System', and 'Logout'. The 'Switch Monitor' folder is selected. On the right is a table titled 'Switch Port Status' with columns: Port, Media Type, Port State, Link State, Speed (Mbps), Duplex, Flow Control, and Description. Below the table is a legend for 'Port State' showing 'D : Disabled' and 'F : Forwarding'.

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

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 Information:** View the current port's SFP information, e.g. speed, distance, vendor name, vendor PN, Vendor SN, 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.
6. **Loop Detection Status:** View the current Loop Detection status of each port.
7. **MAC Address Table:** List current MAC addresses learned by the Managed Switch.

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

Port State
D :Disabled F :Forwarding

Port: The number of the port.

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

Port State: 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: This shows the status of Flow Control function, either on or off.

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

3.5.2 Port Counters Rates

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

| | | | | | | | | | |
|--|--|----------------|-----------------|----------------------|------------|-------------|------------------|-------------|-------------------|
| HES-3106 <ul style="list-style-type: none">System InformationUser AuthenticationNetwork Management<ul style="list-style-type: none">Switch ManagementSwitch Monitor<ul style="list-style-type: none">Switch Port StatusPort Counters Rates<ul style="list-style-type: none">Port Traffic Statistics (Rates)Port Packet Error Statistics (Rates)Port Packet Analysis Statistics (Rates)Port Counters EventsSFP Information<ul style="list-style-type: none">IGMP SnoopingLoop Detection StatusMAC Address TableSystem Utility<ul style="list-style-type: none">Save ConfigurationReset SystemLogout | 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 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |
| | 5 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |
| | 6 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |

1. **Port Traffic Statistics (Rates):** 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 (Rates):** View the number of CRC errors, undersize frames, oversize frames, etc and clear each row's statistics.
3. **Port Packet analysis Statistics (Rates):** View each port's analysis history and clear each row's statistics.

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 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |
| 5 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |
| 6 | 0 | 0 | 0.00% | 0 | 0 | 0.00% | 0 | 0.00% |

Bytes Received: Total bytes received from each port.

Frames Received: Total frames received from each port.

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

Total Bytes: Total bytes received and sent from current port.

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

3.5.2.2 Port Packet Error Statistics (Rates)

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

| Port Packet Error Statistics (Rates) | | | | | | | |
|--------------------------------------|--------------|----------------|--------------|--------------|------------|---------------|--------------|
| Port | Rx CRC Error | Rx Align Error | Rx Undersize | Rx Fragments | Rx Jabbers | Tx Collisions | Total Errors |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

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

RX Align Error: The number of packets received without a valid integral number of bytes and an invalid FCS.

RX Undersize: Undersize frames received.

RX Fragments: Fragment frames received.

RX Jabbers: Jabber frames received.

TX Collisions: Total frames collision detected.

Total Errors: The number of total errors occurred.

3.5.2.3 Port Packet Analysis Statistics (Rates)

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

| Port Packet Analysis Statistics (Rates) | | | | | | | | | | |
|---|-----------------------|------------------------------|-------------------------------|-------------------------------|--------------------------------|---------------------------------|---------------------------|---------------------------|---------------------------|---------------------------|
| Port | Rx Frames 64 Bytes | Rx Frames 65-128 Bytes | Rx Frames 129-256 Bytes | Rx Frames 257-512 Bytes | Rx Frames 513-1024 Bytes | Rx Frames 1025-1518 Bytes | Rx Multicast Frames | Tx Multicast Frames | Rx Broadcast Frames | Tx Broadcast Frames |
| 1 | 44 | 9 | 0 | 21 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-128 Bytes: 65-128 bytes frames received.

RX Frames 129-256 Bytes: 129-256 bytes frames received.

RX Frames 257-512 Bytes: 257-512 bytes frames received.

RX Frames 513-1024 Bytes: 513-1024 bytes frames received.

RX Frames 1025-1518 Bytes: 1025-1518 bytes frames received.

RX Multicast Frames: Good multicast frames received.

TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

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 | Bytes Received | Frames Received | Bytes Sent | Frames Sent | Total Bytes |
|------|----------------|-----------------|------------|-------------|-------------|
| 1 | 624446 | 4528 | 3671442 | 4444 | 4295888 |
| 2 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 41325 | 318 | 41325 |

Clear All

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 Events** and then select **Port Traffic Statistics (Events)**.

| Port Traffic Statistics (Events) | | | | | |
|----------------------------------|----------------|-----------------|------------|-------------|-------------|
| Port | Bytes Received | Frames Received | Bytes Sent | Frames Sent | Total Bytes |
| 1 | 624446 | 4528 | 3671442 | 4444 | 4295888 |
| 2 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 41325 | 318 | 41325 |

Clear All

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 received and sent from current port.

Clear All: Click “**Clear 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 Events** and then select **Port Packet Error Statistics (Events)**.

| Port Packet Error Statistics (Events) | | | | | | | |
|---------------------------------------|--------------|----------------|--------------|--------------|------------|---------------|--------------|
| Port | Rx CRC Error | Rx Align Error | Rx Undersize | Rx Fragments | Rx Jabbers | Tx Collisions | Total Errors |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Clear All

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

RX Align Error: The number of packets received without a valid integral number of bytes and an invalid FCS.

RX Undersize: Undersize frames received.

RX Fragments: Fragment frames received.

RX Jabbers: Jabber frames received.

RX Collisions: Total frames collision detected.

Total Errors: The number of total errors occurred.

Clear All: Click “**Clear 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 Events** and then select **Port Packet Analysis Statistics (Events)**.

| Port Packet Analysis Statistics (Events) | | | | | | | | | | |
|--|-----------------------|------------------------------|-------------------------------|-------------------------------|--------------------------------|---------------------------------|------------------------|------------------------|------------------------|------------------------|
| Port | Rx Frames 64 Bytes | Rx Frames 65-128 Bytes | Rx Frames 129-256 Bytes | Rx Frames 257-512 Bytes | Rx Frames 513-1024 Bytes | Rx Frames 1025-1518 Bytes | Rx Multicast Frames | Tx Multicast Frames | Rx Broadcast Frames | Tx Broadcast Frames |
| 1 | 3370 | 759 | 45 | 1145 | 11 | 0 | 5 | 0 | 321 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 5 | 0 | 321 |
| <input type="button" value="Clear All"/> | | | | | | | | | | |

RX Frames 64 Bytes: 64 bytes frames received.

RX Frames 65-128 Bytes: 65-128 bytes frames received.

RX Frames 129-256 Bytes: 129-256 bytes frames received.

RX Frames 257-512 Bytes: 257-512 bytes frames received.

RX Frames 513-1024 Bytes: 513-1024 bytes frames received.

RX Frames 1025-1518 Bytes: 1025-1518 bytes frames received.

RX Multicast Frames: Good multicast frames received.

TX Multicast Frames: Good multicast packets sent.

RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

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

3.5.4 SFP Information

Click **SFP Information** folder from the left column and then two options appear.

| | | | | | | |
|--|----------------------|----------|----------|-------------|-----------|-----------------|
| HES-3106 <ul style="list-style-type: none">System InformationUser AuthenticationNetwork ManagementSwitch Management<ul style="list-style-type: none">Switch Monitor<ul style="list-style-type: none">Switch Port StatusPort Counters RatesPort Counters EventsSFP Information<ul style="list-style-type: none">SFP Port InfoSFP Port StateIGMP SnoopingLoop Detection StatusMAC Address TableSystem Utility<ul style="list-style-type: none">Save ConfigurationReset SystemLogout | SFP Port Info | | | | | |
| | Port | Speed | Distance | Vendor Name | Vendor PN | Vendor SN |
| | 6 | 1000Mbps | 550M | CTS INC. | SFP-31FC | 400910150000098 |

SFP Port Info: This shows the information of Speed, Distance, Vendor Name, Vendor PN, and Vendor SN of the SFP Port.

SFP Port State: This shows the state of Temperature, Voltage, TX Bias, TX Power, and RX Power of the SFP Port.

3.5.4.1 SFP Port Info

The following screen page appears if you choose **SFP Information** and then select **SFP Port Info**.

| SFP Port Info | | | | | |
|---------------|----------|----------|-------------|-----------|-----------------|
| Port | Speed | Distance | Vendor Name | Vendor PN | Vendor SN |
| 6 | 1000Mbps | 550M | CTS INC. | SFP-31FC | 400910150000098 |

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

Speed: The transmitting speed of the slide-in SFP module.

Distance: The transmitting distance of the slide-in SFP module.

Vendor Name: The vendor name of the slide-in SFP module.

Vendor PN: The vendor part number of the slide-in SFP module.

Vendor SN: The vendor serial number of the slide-in SFP module.

3.5.4.2 SFP Port State

The following screen page appears if you choose **SFP Information** and then select **SFP Port State**.

| SFP Port State | | | | | |
|----------------|----------------|------------|-------------|---------------|---------------|
| Port | Temperature(C) | Voltage(V) | TX Bias(mA) | TX Power(dbm) | RX Power(dbm) |
| 6 | 40.0 | 3.27 | 4.50 | -5.2 | -28.0 |

Port: 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

The following screen page appears if you choose **Switch Monitor** and then select **IGMP Snooping**.

IGMP Snooping

IGMP Snooping is disabled.

| | | | | | | | | |
|-------|-----------------|-----|---|---|---|---|---|---|
| Index | Multicast Group | VID | 1 | 2 | 3 | 4 | 5 | 6 |
|-------|-----------------|-----|---|---|---|---|---|---|

Multicast Group: This shows the multicast IP address of IGMP querier.

Port: The port(s) grouped in the specific multicast group.

Click **Update** to update the IGMP Table.

3.5.6 Loop Detection

The following screen page appears if you choose **Switch Monitor** and then select **Loop Detection Status**.

| Loop Detection Status | | |
|-----------------------|--------|------------|
| Port | Status | Lock Cause |
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

Status: This shows the status of the port, Lock or Un-lock.

Lock Cause: This shows the factor that causes the port to be locked.

3.5.7 MAC Address Table

MAC Address Table displays MAC addresses learned after the system reset.

| MAC Address Table | | | |
|-------------------------|---------|-------------------|------|
| Page 1 ▾ All ▾ Top Next | | | |
| Total | 8 | | |
| Index | Type | MAC Address | Port |
| 1 | dynamic | 00:16:E6:50:89:5C | 1 |
| 2 | static | 00:06:19:05:D6:F5 | CPU |
| 3 | dynamic | 00:06:19:25:E6:C8 | 2 |
| 4 | dynamic | 00:7P:3F:89:41:E3 | 2 |
| 5 | dynamic | 00:7P:3F:P5:DC:FP | 3 |
| 6 | dynamic | 00:7P:3F:95:D2:AU | 4 |
| 7 | dynamic | 00:06:19:0A:0E:P2 | 5 |
| 8 | dynamic | 00:06:19:41:A9:U0 | 6 |

The table above shows the MAC addresses learned from each port of the Managed Switch.

Click **Update** to update the MAC Address Table.

3.6 System Utility

Select the folder **System Utility** from the left column and then the following screen page appears.

HES-3106

- System Information
- User Authentication
- Network Management
- Switch Management
- Switch Monitor
- System Utility
 - Event Log
 - Upgrade
 - Load Factory Settings
 - Load Factory Settings Except Network Configuration
 - Save Configuration
 - Reset System
 - Logout

Event Log

| Index | Type | Time | Up Time | Description | Source | Event | Name/Community | Address |
|-------|------|------|----------------|-----------------------------------|--------|------------|----------------|---------------|
| 1 | I | | 0 day 00:00:55 | User from web login succeeded. | web | login | admin | 192.168.0.155 |
| 2 | I | | 0 day 00:00:58 | System warm start. | local | warm start | | |
| 3 | I | | 0 day 00:01:01 | Local port 1 copper link up. | local | link up | | |
| 4 | I | | 0 day 00:01:01 | Local port 2 copper link down. | local | link down | | |
| 5 | I | | 0 day 00:01:01 | Local port 3 copper link down. | local | link down | | |
| 6 | I | | 0 day 00:01:01 | Local port 4 copper link down. | local | link down | | |
| 7 | I | | 0 day 00:01:01 | Local port 5 copper link down. | local | link down | | |
| 8 | I | | 0 day 00:01:01 | Local port 6 fiber link down. | local | link down | | |
| 9 | I | | 0 day 00:01:21 | User from telnet login succeeded. | telnet | login | admin | 192.168.0.155 |
| 10 | I | | 0 day 00:02:28 | Local port 1 copper link down. | local | link down | | |
| 11 | I | | 0 day 00:02:32 | Local port 2 copper link up. | local | link up | | |
| 12 | I | | 0 day 00:03:12 | Local port 2 copper link down. | local | link down | | |
| 13 | I | | 0 day 00:03:12 | Local port 5 copper link up. | local | link up | | |
| 14 | I | | 0 day 00:03:28 | Local port 3 copper link up. | local | link up | | |
| 15 | I | | 0 day 00:03:28 | Local port 5 copper link down. | local | link down | | |
| 16 | I | | 0 day 00:06:00 | Local port 3 copper link down. | local | link down | | |
| 17 | I | | 0 day 00:06:03 | Local port 4 copper link up. | local | link up | | |

Clear All

- Event Log:** Event log can keep a record of system's log events such as system warm start, cold start, link up/down, user login/logout, etc. They will be kept only when your CPU version is A06 with Boot ROM version A08 or later version. If your CPU or Boot ROM version is older than the one mentioned above, all events will lose when the system is shut down or rebooted.
- Update:** This allows users to update the latest firmware.
- Load Factory Settings:** Load Factory Setting will set the configuration of the Managed Switch back to the factory default settings. The IP and Gateway addresses will be set to the factory default as well.
- Load Factory Settings Except Network Configuration:** Selecting this function will also restore the configuration of the Managed Switch to its original factory default settings. However, this will not reset the IP and Gateway addresses to the factory default.

3.6.1 Event Log

Event log keeps a record of user login and logout timestamp information. Select **Event Log** from the **System Utility** menu and then the following screen page appears.

| Event Log | | | | | | | | |
|-----------|------|------|----------------|-----------------------------------|--------|------------|----------------|---------------|
| Index | Type | Time | Up Time | Description | Source | Event | Name/Community | Address |
| 1 | I | | 0 day 00:00:55 | User from web login succeeded. | web | login | admin | 192.168.0.155 |
| 2 | I | | 0 day 00:00:58 | System warm start. | local | warm start | | |
| 3 | I | | 0 day 00:01:01 | Local port 1 copper link up. | local | link up | | |
| 4 | I | | 0 day 00:01:01 | Local port 2 copper link down. | local | link down | | |
| 5 | I | | 0 day 00:01:01 | Local port 3 copper link down. | local | link down | | |
| 6 | I | | 0 day 00:01:01 | Local port 4 copper link down. | local | link down | | |
| 7 | I | | 0 day 00:01:01 | Local port 5 copper link down. | local | link down | | |
| 8 | I | | 0 day 00:01:01 | Local port 6 fiber link down. | local | link down | | |
| 9 | I | | 0 day 00:01:21 | User from telnet login succeeded. | telnet | login | admin | 192.168.0.155 |
| 10 | I | | 0 day 00:02:28 | Local port 1 copper link down. | local | link down | | |
| 11 | I | | 0 day 00:02:32 | Local port 2 copper link up. | local | link up | | |
| 12 | I | | 0 day 00:03:12 | Local port 2 copper link down. | local | link down | | |
| 13 | I | | 0 day 00:03:12 | Local port 5 copper link up. | local | link up | | |
| 14 | I | | 0 day 00:03:28 | Local port 3 copper link up. | local | link up | | |
| 15 | I | | 0 day 00:03:28 | Local port 5 copper link down. | local | link down | | |
| 16 | I | | 0 day 00:06:00 | Local port 3 copper link down. | local | link down | | |
| 17 | I | | 0 day 00:06:03 | Local port 4 copper link up. | local | link up | | |

Clear All

The Event Log table stores the latest 500 logs in the Managed Switch. Click **Clear All** to clear all Event Log records.

3.6.2 Update

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

| Update Firmware | |
|--------------------|---------------|
| Protocol | FTP |
| File Type | Configuration |
| Server Address | 127.0.0.1 |
| User Name | anonymous |
| Password | ... |
| File Location | config.rom |
| Put | Update |
| Transmitting State | |
| OK | |

Protocol: Select the preferred protocol, either FTP or TFTP.

File Type: Select the file type to process, either Configuration or Firmware.

Server Address: Enter the specific IP address of the File Server.

User Name: Enter the specific username to access the File Server.

Password: Enter the specific password to access the File Server.

File Location: Enter the specific path and filename within the File Server.

Put: Click **Put** to start the upload process and transmit files to the server.

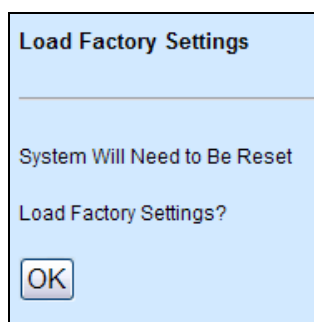
Update: Click **Update** to instruct the Managed Switch to update existing firmware or configuration to the latest one received. After a successful update, a message will pop up. The Managed Switch will need a reset to make changes effective.

Transmitting State: This field displays the uploading or updating progress.

3.6.3 Load Factory Settings

Load Factory Settings will set all configurations of the Managed 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 Settings** from the **System Utility** menu and then the following screen page appears.

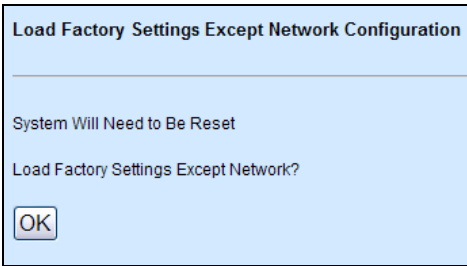


Click the **“OK”** button to restore the Managed Switch back to the defaults.

3.6.4 Load Factory Settings Except Network Configuration

Load Factory Settings Except Network Configuration will set all configurations of the Managed 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.

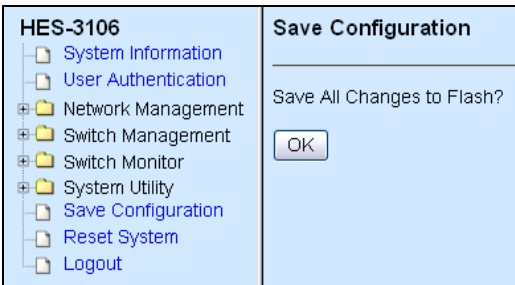
Select **Load Factory Setting Except Network Configuration** from the **System Utility** menu, then the following screen page shows up.



Click the “**OK**” button to restore the Managed Switch back to the defaults excluding network configurations.

3.7 Save Configuration

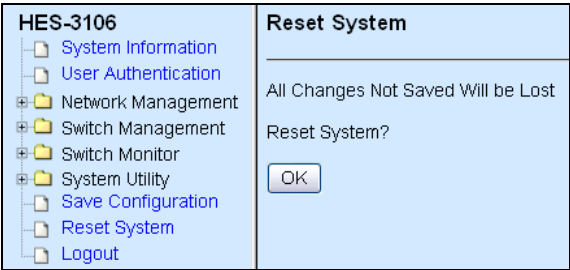
In order to save configuration settings permanently, users need to save configuration first before resetting the Managed Switch. Select **Save Configuration** from the **Main Menu** and then the following screen page appears.



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

3.8 Reset System

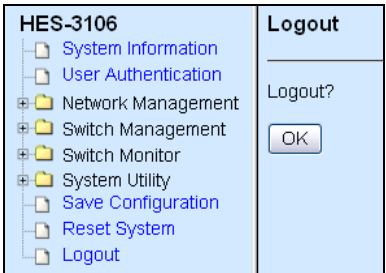
After any configuration changes, **Reset System** can make changes effective. Select **Reset System** from the **Main menu** and then the following screen page appears.



Click the “**OK**” button to restart the Managed Switch.

3.9 Logout

Select **Logout** from the **Main menu** and then the following screen page appears.



Click the “**OK**” button to logout the Managed Switch.

APPENDIX A: DHCP Auto-Provisioning Setup

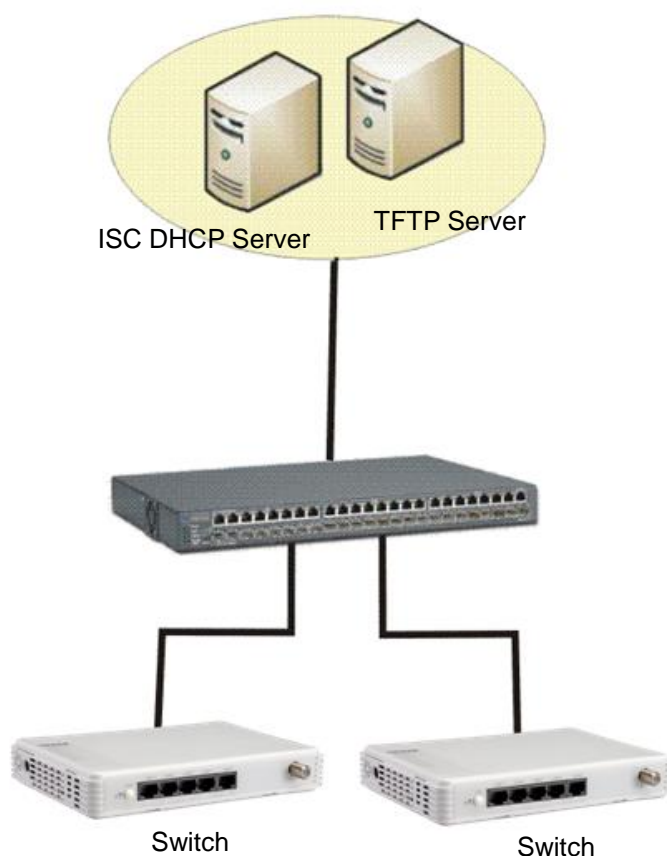
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the Managed Switch that you purchased supports 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. Set Up Environment

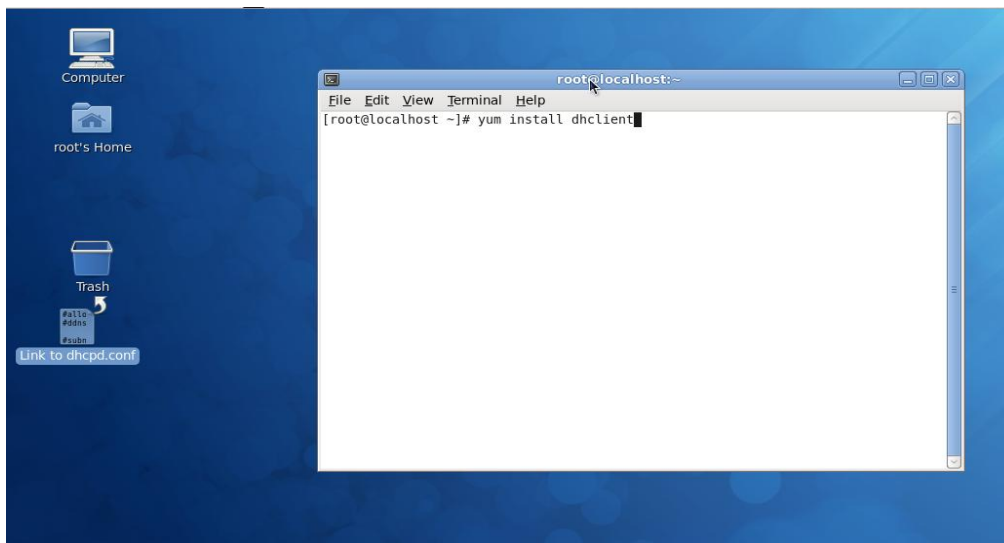
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

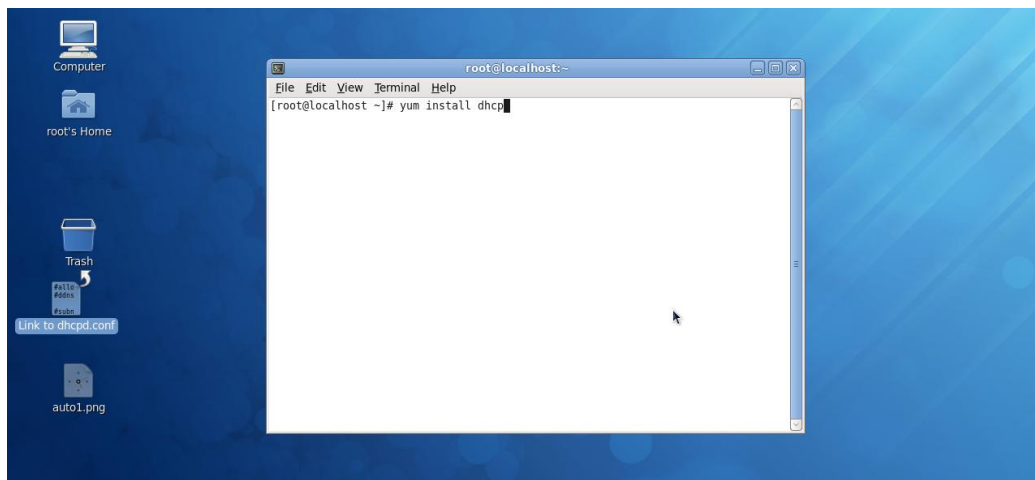
Step 2. Set Up Auto Provision Server

- **Update DHCP client**



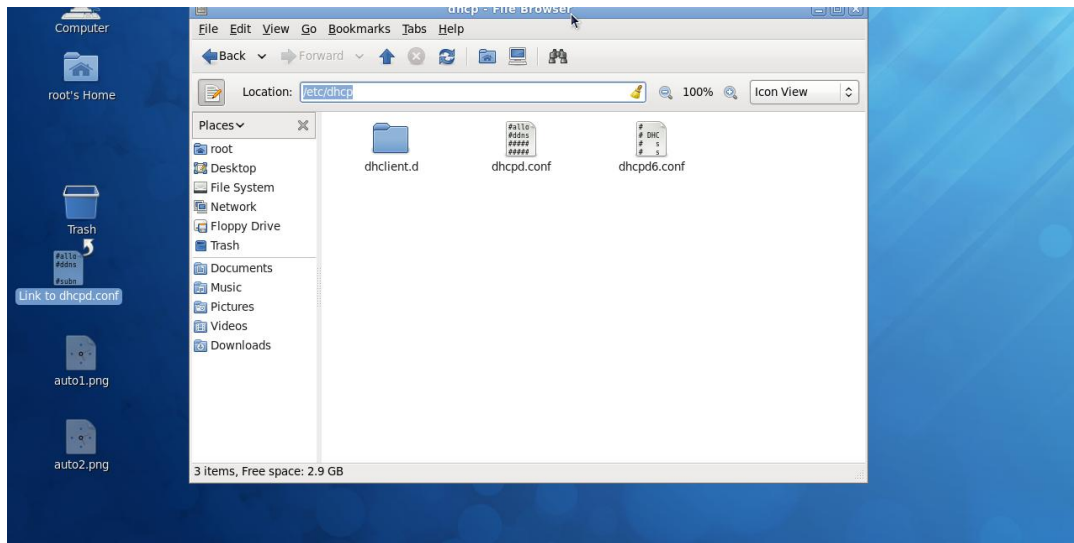
Linux Fedora 12 supports “yum” function by default. First of all, update DHCP client function by issuing “yum install dhclient” command.

- **Install DHCP server**



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

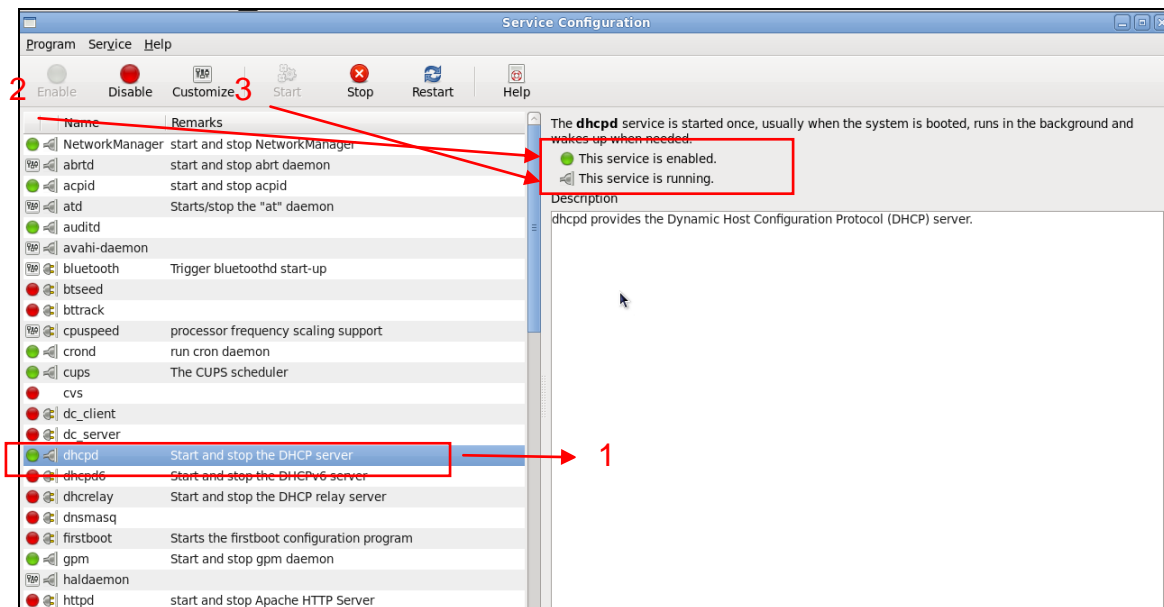
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

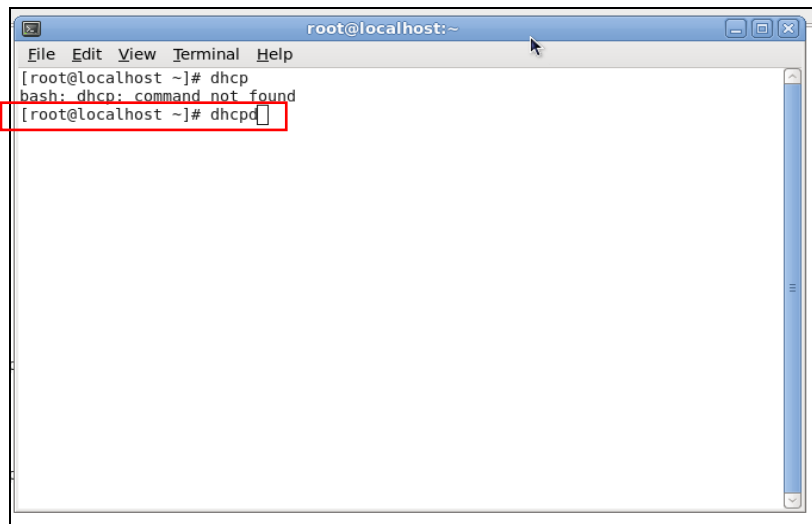
Please note that each vendor has its own way to define auto-provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



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

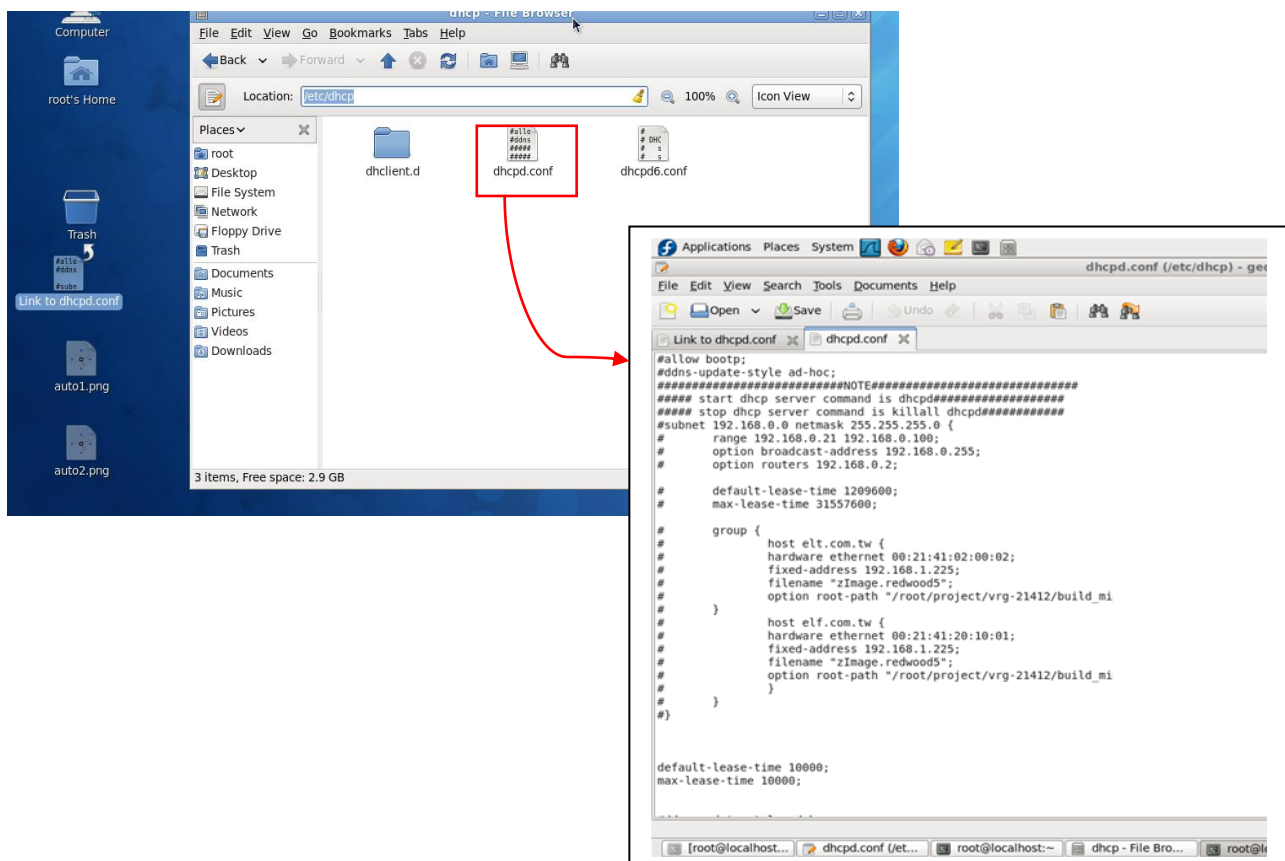
NOTE: DHCP service can also be enabled using CLI. Issue “dhcpd” command to enable DHCP service.



```
root@localhost:~  
File Edit View Terminal Help  
[root@localhost ~]# dhcp  
bash: dhcp: command not found  
[root@localhost ~]# dhcpd
```

Step 3. Modify dhcpd.conf File

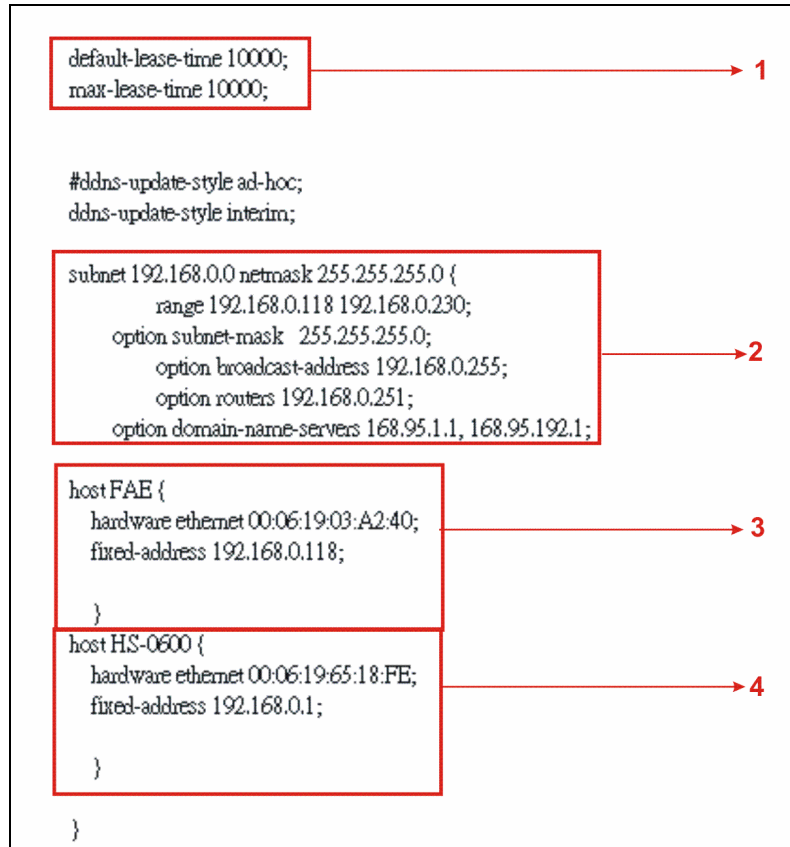
- Open dhcpd.conf file in /etc/dhcp/ directory



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.



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 "depl";

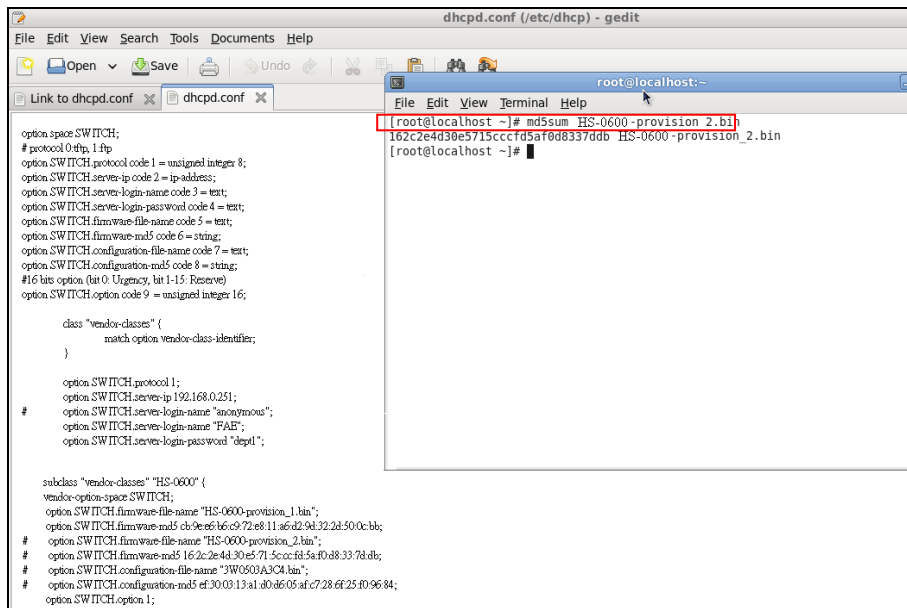
subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
    option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
    option SWITCH.firmware-md5 cb:9e:e6:b6:c9:72:e8:11:a6:d2:9d:32:2d:50:0c:bb;
# option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
# option SWITCH.firmware-md5 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:afc7:28:6f: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.



```
dhcpcd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Link to dhcpd.conf x dhcpd.conf x
option space SWITCH;
# protocol 0 fhp, 1 fhp
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;

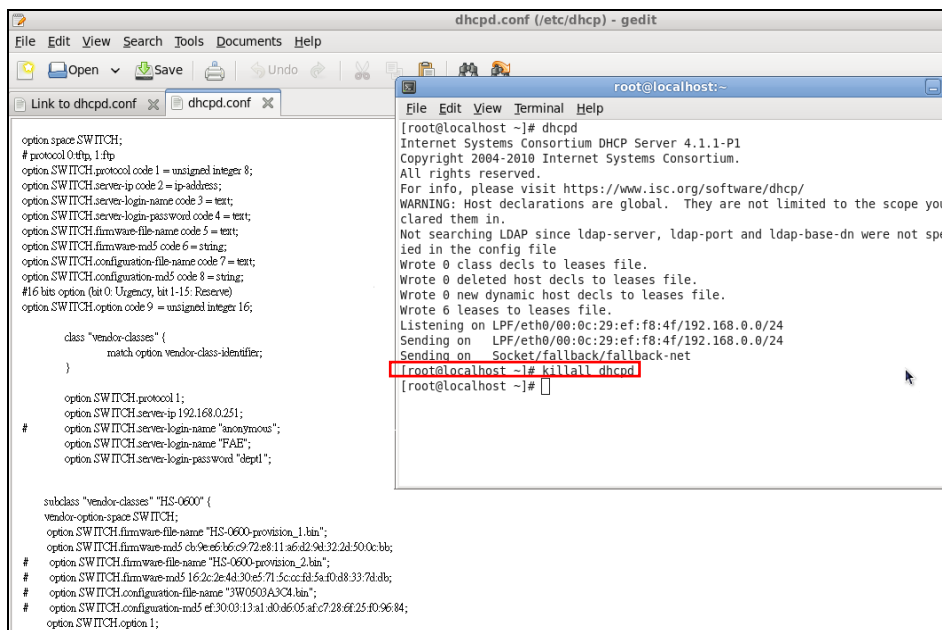
class "vendor-classes" {
    match option vendor-class-identifier;
}

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 "depl";

subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
    option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
    option SWITCH.firmware-md5 cb9e6b6c972e811a6d29d322d500cbb;
    option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    option SWITCH.firmware-md5 162c2e4d30e5715cccfd5af0d8337dab;
    option SWITCH.configuration-file-name "3W0503A3C4.bin";
    option SWITCH.configuration-md5 ef300313a1a0d605afc7286f25f09684;
    option SWITCH.option 1;
}

[root@localhost ~]# md5sum HS-0600-provision_2.bin
162c2e4d30e5715cccfd5af0d8337dab HS-0600-provision_2.bin
[root@localhost ~]#
```

● Restart DHCP service



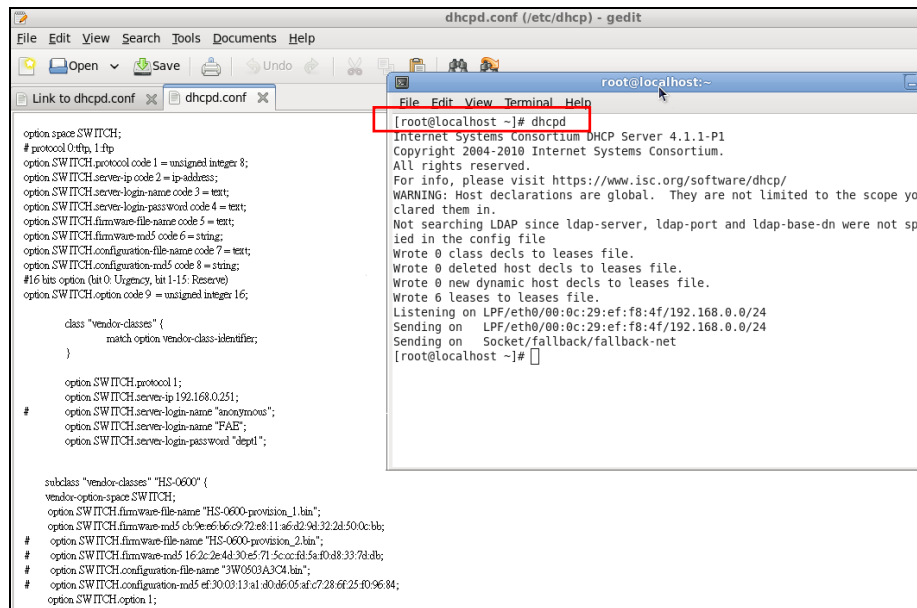
```
dhcpcd.conf (/etc/dhcp) - gedit
File Edit View Search Tools Documents Help
Link to dhcpd.conf x dhcpd.conf x
option space SWITCH;
# protocol 0 fhp, 1 fhp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
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 "depl";

subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
    option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
    option SWITCH.firmware-md5 cb9e6b6c972e811a6d29d322d500cbb;
    option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    option SWITCH.firmware-md5 162c2e4d30e5715cccfd5af0d8337dab;
    option SWITCH.configuration-file-name "3W0503A3C4.bin";
    option SWITCH.configuration-md5 ef300313a1a0d605afc7286f25f09684;
    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/eth0/08:0c:29:ef:f8:4f/192.168.0.0/24
Sending on LPF/eth0/08:0c: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
Link to dhcpd.conf x dhcpd.conf x
option space SWITCH;
# protocol 0 ftp, 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-md5 code 5 = string;
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 "depl1";

subclass "vendor-classes" "HS-0600" {
    vendor-option-space SWITCH;
    option SWITCH.firmware-file-name "HS-0600-provision_1.bin";
    option SWITCH.firmware-md5 cb9e6b6c972e811a6d29d322d450cbb;
    option SWITCH.firmware-file-name "HS-0600-provision_2.bin";
    option SWITCH.firmware-md5 162c2e4d30e5715c0cf85af0d8337dab;
    option SWITCH.configuration-file-name "SW0600ADCM.bin";
    option SWITCH.configuration-md5 ef300313a1a0d605afc7286f25f09684;
    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 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 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. 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 matching and causes the device to reboot endlessly.

In order to have your Managed Switch 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 **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

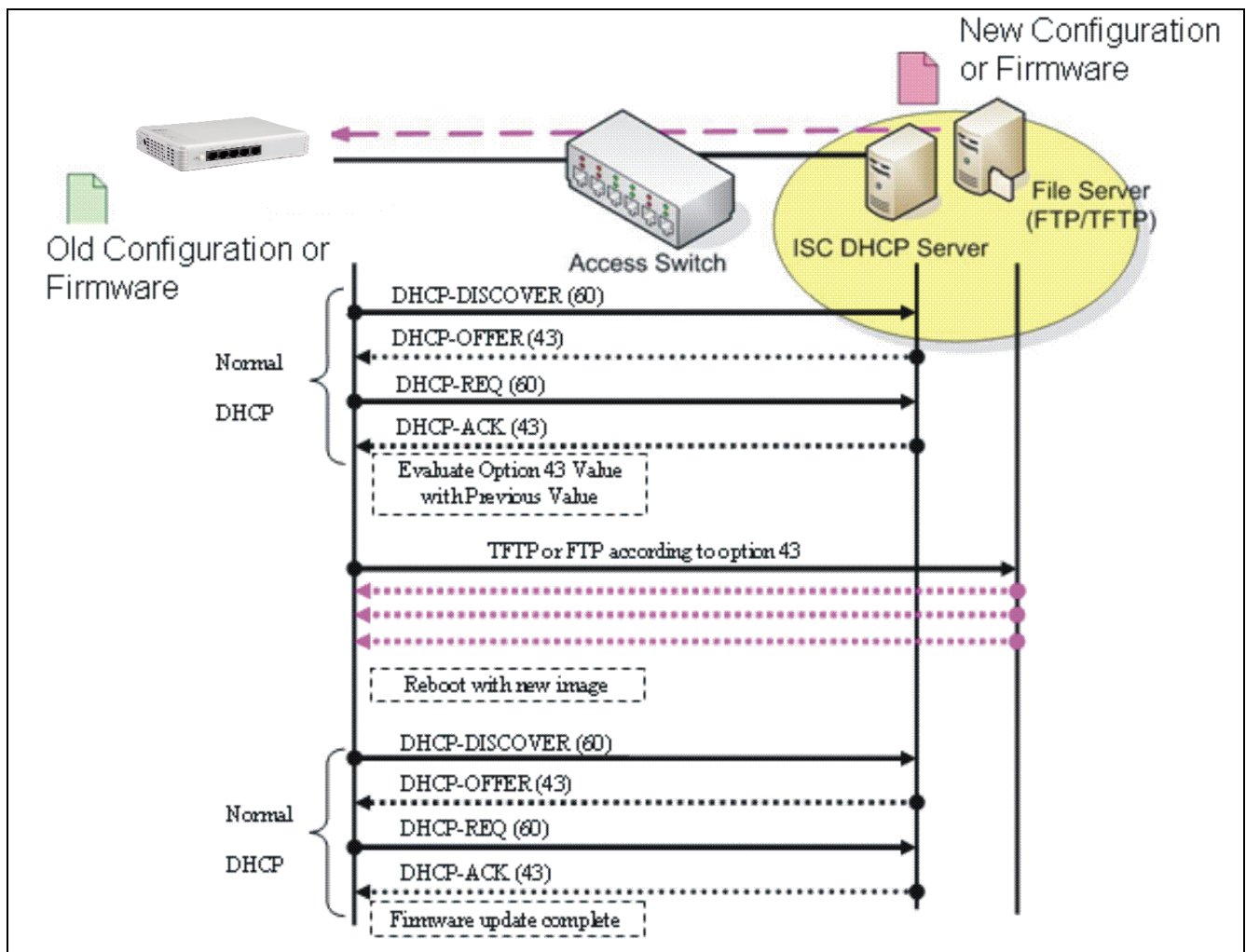
The TFTP/FTP File server should include the following items:

- 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. ISC DHCP server will recognize the device when it receives an IP address request sent by the device, and it 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 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 immediately.
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, and then it gives up until getting another DHCP ACK packet again.



This page is intentionally left blank.