CTS
CONNECTION TECHNOLOGY SYSTEMS

iCPE
Gateway Controller

Network Management User's Manual

Version 0.90

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 © 2016All 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.

Manual Version	**Firmware Version**	**Modification**	**Date**
0.90	1.00.00	First Release	20160119

Table of Content

1. OVERVIEW

This controller is a Z-Wave static controller.

This product can be included and operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers and/or other applications. All non-battery operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.

This device is a security enabled Z-Wave Plus product that is able to use encrypted Z-Wave Plus message to Enabled Z-Wave Plus devices.

Replication refers to the protocol replication between Controllers that is used to exchange protocol data between different Controllers of the same network.

The controller ignores any Basic Command class if receiving Basic Set from a sensor.

The controller supports Association Command Class. It has one association group, which is Lifeline group with grouping identifier equal to 1. Maximum number of devices that can be added to the group is 1. When the device is reset, this group returns Device Reset Locally notification.

The controller supports the listed browsers: IE, Firefox and Google Chrome.

1.1 Management Preparations

The gateway controller can be accessed through both Telnet connection and a web browser such as Internet Explorer, Google Chrome or Firefox, etc… Before you can access the gateway controller and configure it, you need to connect cables properly.

1.1.1 Connecting the gateway controller

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

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

Depending on the model that you purchased, 2 10/100/1000Base-T RJ-45 ports are located on the front panel of the Gateway controller. 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.

1.1.2 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.

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 Gateway controller via Telnet session. For first-time users, you must first assign a unique IP address to the Gateway Controller 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 Gateway Controller 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 Gateway Controller.

Step 2. Ask the DHCP server for IP address and run Telnet client and connect to the given IP address. 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 Gateway Controller via Telnet session again.

Limitation: Only one active Telnet session can access the Gateway Controller at a time.

2.2 Navigating CLI

After you successfully access to the Gateway Controller, 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 Gateway Controller. If you would like to configure advanced features of the Gateway Controller, 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 Gateway Controller.

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

***NOTE:** By default, the model name will be used for the prompt display. For convenience, the prompt display "ICPE" 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

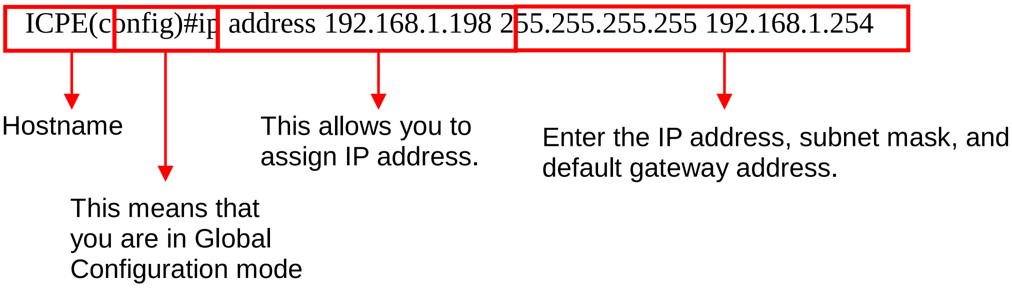
In CLI, there are several quick keys that you can use to perform several functions. The following table summarizes the most frequently used quick keys in CLI.

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 ?	Enter an unfinished command or keyword and press "?" key to complete the command and get command syntax help. Examples: ICPE#h? help Show available commands history Show history commands ICPE#he? <cr> ICPE#help
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 Gateway Controller, you need to enter the following command with the required parameter and IP, subnet mask and default gateway:

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



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

Hostname

This means that you are in Global Configuration mode

This allows you to assign IP address.

Enter the IP address, subnet mask, and default gateway address.

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

Symbols	Brief Description
>	Currently, the device is in User Mode.
#	Currently, the device is in Privileged Mode.
(config)#	Currently, the device is in Global Configuration Mode.
Syntax	**Brief Description**
[ ]	Brackets mean that this field is required information.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port-based | 802.1p | dscp | vid]	There are four options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.
[0-7] 802.1p_list [0-63] dscp_list	Specify one or more values or a range of values. For example: specifying one value ICPE(config)#qos 802.1p-map 1 0 ICPE(config)#qos dscp-map 10 3 For example: specifying three values (separated by commas) ICPE(config)#qos 802.1p-map 1,3 0 ICPE(config)#qos dscp-map 10,13,15 3 For example: specifying a range of values (separating by a hyphen) ICPE(config)#qos 802.1p-map 1-3 0 ICPE(config)#qos dscp-map 10-15 3

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 "ICPE>", 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 Gateway Controller, 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 Gateway Controller 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 gateway Controller feature. For a list of commands available in User Mode, enter the question mark (?) or "help" command after the system prompt displays "ICPE>".

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.
ping	Used to test the reachability of a host on an Internet Protocol (IP) network
logout	Logout from the Gateway Controller.
enable	Enter the Privileged mode.

2.4 Privileged Mode

The only place where you can enter the Privileged (Enable) Mode is in User Mode. When you successfully enter Enable mode, the prompt will be changed to ICPE# (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.
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 Gateway Controller.
ping	Used to test the reachability of a host on an Internet Protocol (IP) network
reload	Restart the Gateway Controller.
write	Save your configurations to Flash.
configure	Enter Global Configuration mode
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 Gateway Controller 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
ICPE# 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.
ICPE# 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		
ICPE# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
ICPE# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

2. **Restore the Gateway Controller back to default settings.**

Command / Example
ICPE# copy-cfg from default

NOTE: *There are two ways to set the Gateway Controller 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 Gateway Controller back to default settings but keep IP configurations.**

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

4. **Backup a configuration file to TFTP server.**

Command	**Parameter**	**Description**
ICPE# 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.
ICPE# 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		
ICPE# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz		
ICPE# 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**
ICPE# 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.
ICPE# 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		
ICPE# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin edgeswitch10 abcxyz		
ICPE# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin		

2.4.3 Reload Command

To restart the Gateway Controller, enter the reload command.

Command / Example
ICPE# 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 Gateway Controller.

Command / Example
ICPE# 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 “ICPE#” to “ICPE(config)#” once you successfully enter Global Configuration Mode.

Command / Example
ICPE# config ICPE(config)#
ICPE# configure ICPE(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 gateway Controller 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
exit	Exit the Configuration Mode.
help	Display a list of available commands in Configuration Mode.
history	Show commands that have been used.
ip	Set up the IP address and enable DHCP mode & IGMP snooping.
mac	Set up each port’s MAC learning function.
management	Set up the system service type.
mirror	Set up port mirror configuration
mqtt	Set up mqtt configuration.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Gateway Controller.
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.
usb	Enable or disable USB port functionality.
syslog	Enable or disable syslog server and assign server IP address.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.
zwave	Set up Z-Wave 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
ICPE(config)# interface 1 ICPE(config-if-1)#	Enter a single interface. Only interface 1 will apply to commands entered.
ICPE(config)# interface 1,2 ICPE(config-if-1,2)#	Enter three discontinuous interfaces, separating by a comma. Interface 1, 2 will apply to commands entered.

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

2.5.2 No Command

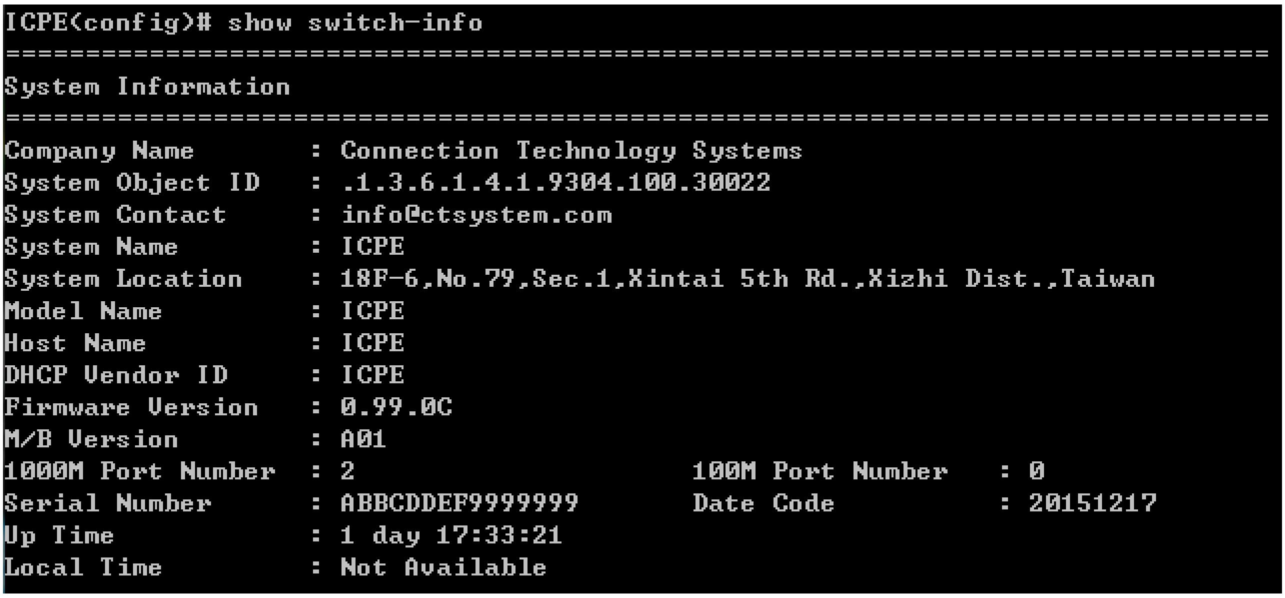
Most commands that you enter in Configuration mode can be negated using "no" command followed by the same or original command. The purpose of "no" command is to disable a function, remove a command, or set the setting back to the default value. In each sub-section below, the use of no command to fulfill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



```
ICPE(config)# show switch-info
===============================================================================
System Information
===============================================================================
Company Name        : Connection Technology Systems
System Object ID    : .1.3.6.1.4.1.9304.100.30022
System Contact      : info@ctsystem.com
System Name         : ICPE
System Location     : 18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan
Model Name          : ICPE
Host Name           : ICPE
DHCP Vendor ID      : ICPE
Firmware Version    : 0.99.0C
M/B Version         : A01
1000M Port Number   : 2                     100M Port Number    : 0
Serial Number       : ABBCDDEF9999999       Date Code           : 20151217
Up Time             : 1 day 17:33:21
Local Time          : Not Available
```

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

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

System Location: Display a brief location description for this Gateway Controller. 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 image 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

Serial Number: Display the serial number of this Gateway Controller.

Date Code: Displays the Gateway Controller Firmware date code.

Uptime: Display the time the device has been up.

Local Time: Display the time of the location where the Gateway Controller is.

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.

5. Show battery status

Refer to “show battery status” command.

2.5.4 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 Gateway Controller.

IP command	Parameter	Description
ICPE(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 Gateway Controller.
	[255.X.X.X]	Enter subnet mask of your IP address.
	[A.B.C.D]	Enter the default gateway address.
ICPE(config)# ip dhcp snooping		Enable DHCP Snooping function
ICPE(config)# ip dhcp snooping dhcp-server [port_list]	[port_list]	Specify DHCP server trust ports.
ICPE(config)# ip name-server server1 [A.B.C.D]	[A.B.C.D]	Specify IP Address for Domain Name System (DNS) Server 1
ICPE(config)# ip name-server server2 [A.B.C.D]	[A.B.C.D]	Specify IP Address for Domain Name System (DNS) Server 2
No command		
ICPE(config)# no ip address		Remove the Gateway Controller’s IP address.
ICPE(config)# ip name-server server1		Remove IP Address of Domain Name System (DNS) Server 1
ICPE(config)# ip name-server server2		Remove IP Address of Domain Name System (DNS) Server 2
Show command		
ICPE(config)# show ip address		Show the current IP configurations or verify the configured IP settings.
ICPE(config)# show ip name-server		Show the current configured DNS IP address
IP command example		
ICPE(config)# ip address 192.168.1.198 255.255.255.0 192.168.1.254		Set up the Gateway Controller’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 Gateway Controller to automatically get IP address from the DHCP server.

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

ICPE(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**
ICPE(config)# ip dhcp snooping		Enable DHCP snooping function.
ICPE(config)# ip dhcp snooping dhcp-server [port_list]	[port_list]	Specify DHCP server trust ports.
No command		
ICPE(config)# no ip dhcp snooping		Disable IGMP snooping function.
ICPE(config)# no ip dhcp snooping dhcp-server		Remove all the DHCP server trust ports
Show command		
ICPE(config)# show ip dhcp snooping		Show current DHCP snooping status including DHCP server trust ports.

4. Global IP address security configuration.

Command / Example	**Parameter**	**Description**
Switch(config)# ip source		Globally enable IP source security.
Switch(config)# ip source binding [1-12]	[1-12]	Specify IP address security binding number and enable it.
Switch(config)# ip source binding [1-12] ip-address [A.B.C.D]	[A.B.C.D]	Specify IP address
No command		
Switch(config)# no ip source		Globally disable IP source security.
Switch(config)# no ip source binding [1-12]		Disable IP address security binding.
Switch(config)# no ip source binding [1-12] ip-address [A.B.C.D]		Disable IP address security binding on the specified IP address.
Show command		
Switch(config)# show ip shource		Show current status of IP source.

2.5.5 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
ICPE(config)# mac address-table aging-time [7-600000]	[7-600000]	Enter aging time for MAC address table. Numbers available are from 7 to 600000.
No command		
ICPE(config)# no mac address-table aging-time		Set MAC address table aging time to the default value (300 seconds).
Show command		
ICPE(config)# show mac aging-time		Show current MAC address table aging time.
ICPE(config)# show mac address-table		Show MAC addresses learned by the Gateway Controller
ICPE(config)# show mac address-table interface [port_list]	[port_list]	Show MAC addresses learned by the selected ports.
ICPE(config)# show mac address-table top		Show MAC addresses learned from the first entry.
MAC command example		
ICPE(config)# mac address-table aging-time 600		Set MAC address table aging time to 600 seconds.

2.5.6 Management Command

Management command	Parameter	Description
ICPE(config)# management smart-home-server [domain_name]	[domain_name]	By default, DHCP server plays a role in gateway. You may assign other device a gateway by typing IP address or domain name.
ICPE(config)# management console timeout [0 | 5-300]	[0 | 5-300]	Under RS-232 interface commands, specify session aging time within the range: zero or 5-300 seconds. (“0” indicates never aging out)
ICPE(config)# management [ssh | telnet|web]	[ssh | telnet |web]	Select the system service type, SSH, telnet or web.
ICPE(config)# management telnet port [1-65535]	[1-65535]	Specify telnet port number.
No command		
ICPE(config)# no management [ssh | telnet | web]	[ssh | telnet | web]	Set system service type to Disabled.
ICPE(config)# no management telnet port		Disable telnet port number specified.
Show command		
ICPE(config)# show management		Show the current system service type.
Management command example		

ICPE(config)# management ssh	Enable SSH system service type.

2.5.7 Mirror Command

Mirror command	Parameter	Description
ICPE(config)# mirror mode [by-port]	[by-port]	Enable mirror mode by-port
ICPE(config)# mirror source [port_list]	[port_list]	Specify the source port(s) to be mirrored
ICPE(config)# mirror destination [port]	[port]	Specify the destination port for mirroring
No command		
ICPE(config)# no mirror mode		Disable mirror mode
Show command		
ICPE(config)# show mirror		Show port mirror information
Mirror command example		
ICPE(config)# mirror mode by-port ICPE(config)# mirror source 1 ICPE(config)# mirror destination 2		Enable mirror mode and set port 2 as mirror destination and port 1 as source port.

2.5.8 MQTT Command

Message Queue Telemetry Transport (MQTT) is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.

MQTT command	Parameter	Description
ICPE(config)# mqtt [1-5]	[1-5]	Add a new MQTT ID
ICPE(config-mqtt-ID)# account enable		To activate the account
ICPE(config-mqtt-ID)# account name [user_name]	[user_name]	Specify the authorized user login name, up to 255 alphanumeric characters
ICPE(config-mqtt-ID)# account password [password]	[password]	Enter the desired user password, up to 255 alphanumeric characters.
ICPE(config-mqtt-ID)# active		Enable MQTT function for the MQTT ID
ICPE(config-mqtt-ID)# clean-session		The clean session flag indicates the broker, whether the client wants to establish a persistent session or not. A persistent session (CleanSession is false) means, that the broker will store all subscriptions for the client and also all missed messages, when subscribing with Quality of Service (QoS) 1 or 2. If clean

		session is set to true, the broker won’t store anything for the client and will also purge all information from a previous persistent session.
ICPE(config-mqtt-ID)# client-id [id]	[id]	The client identifier (short Client ID) is an identifier of each MQTT client connecting to a MQTT broker. Specify the client identifier name, up to 23 alphanumeric characters
ICPE(config-mqtt-ID)# domain-name [domain_name]	[domain_name]	Assign a domain name, IP address or website typically, to the broker. The broker is primarily responsible for receiving all messages, filtering them, decide who is interested in it and then sending the message to all subscribed clients.
ICPE(config-mqtt-ID)# keep-alive [0-65535]	[0-65535]	The keep alive is a time interval, the clients commits to by sending regular PING Request messages to the broker. The broker response with PING Response and this mechanism will allow both sides to determine if the other one is still alive and reachable. “0” refers to ”disable”. The default setting is 5.
ICPE(config-mqtt-ID)# port [0-65535]	[0-65535]	This refers to a list of Internet socket port numbers used by protocols of the transport layer of the Internet Protocol Suite for the establishment of host-to-host connectivity. The configurable range is 0 ~ 65535.
ICPE(config-mqtt-ID)# tls psk		Transport Layer Security pre-shared key ciphersuites (TLS-PSK) is a set of cryptographic protocols that provide secure communication based on pre-shared keys (PSKs). These pre-shared keys are symmetric keys shared in advance among the communicating parties.
ICPE(config-mqtt-ID)# tls psk-identity [identity]	[identity]	Specify a name to the Identity, up to 127 alphanumeric characters.
ICPE(config-mqtt-ID)# tls psk-key [identity]	[identity]	Enter the desired user password, up to 127 alphanumeric characters.
No Command		
ICPE(config)# no mqtt [1-5]		Remove MQTT ID
ICPE(config-mqtt-ID)# no account enable		Deactivate the account
ICPE(config-mqtt-ID)# no account name		Remove the authorized user login name
ICPE(config-mqtt-ID)# no account password		Remove the password
ICPE(config-mqtt-ID)# no active		Disable MQTT function for the MQTT ID
ICPE(config-mqtt-ID)# no clean-session		Disable clean session function
ICPE(config-mqtt-ID)# no client-id		Remove the client identifier

ICPE(config-mqtt-ID)# no domain-name	Remove a domain name
ICPE(config-mqtt-ID)# no keep-alive	Return to default value 5
ICPE(config-mqtt-ID)# no port	Return to default value 1883
ICPE(config-mqtt-ID)# no tls psk	Disable Transport Layer Security pre-shared key function
ICPE(config-mqtt-ID)# no tls psk-identity	Remove the Identity name
ICPE(config-mqtt-ID)# no tls psk-key	Remove the password
Show Command	
ICPE(config)# show mqtt [1-5]	Show the status of specified MQTT ID
ICPE(config-mqtt-ID)# show	Show the status of the MQTT ID

2.5.9 NTP Command

Set up required configurations for Network Time Protocol.

Command	Parameter	Description
ICPE(config)# ntp		Enable the Gateway Controller to synchronize the clock with a time server.
ICPE(config)# ntp daylight-saving [recurring | date]	[recurring | date]	Enable the day light savings.
ICPE(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Offset setting for daylight saving function of recurring mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat)** **Hh=0-23, mm=0-59, Days=1-365**
ICPE(config)# ntp offset [Days,hh:mm-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Offset setting for daylight saving function of date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat)** **Hh=0-23, mm=0-59, Days=1-365**
ICPE(config)# ntp server1 [A.B.C.D]	[A.B.C.D]	Specify the primary time server IP address.
ICPE(config)# ntp server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary time server IP address.
ICPE(config)# ntp syn-interval [1-8]	[1-8]	Specify the interval time to synchronize from NTP time server. The meanings of the value: **1:1hr, 2:2hrs 3:3hrs 4:4hrs** **5:6hrs 6:8hrs 7:12hrs 8:24hrs**
ICPE(config)# ntp time-zone [0-132]	[0-132]	Specify the time zone to that the Gateway Controller belongs. Use any key to view the

		complete code list of 132 time zones. For example, “ICPE(config)# ntp time-zone ?”
No command		
ICPE(config)# no ntp		Disable the Gateway Controller to synchronize the clock with a time server.
ICPE(config)# no ntp daylight-saving		Disable the daylight saving function.
ICPE(config)# no ntp offset		Set the offset value back to the default setting.
ICPE(config)# no ntp server1		Delete the primary time server IP address.
ICPE(config)# no ntp server2		Delete the secondary time server IP address.
ICPE(config)# no ntp syn-interval		Set the synchronization interval back to the default setting.
ICPE(config)# no ntp time-zone		Set the time-zone setting back to the default setting.
Show command		
ICPE(config)# show ntp		Show or verify current time server settings.
NTP command example		
ICPE(config)# ntp		Enable the Gateway Controller to synchronize the clock with a time server.
ICPE(config)# ntp server1 192.180.0.12		Set the primary time server IP address to 192.180.0.12.
ICPE(config)# ntp server2 192.180.0.13		Set the secondary time server IP address to 192.180.0.13.
ICPE(config)# ntp syn-interval 8		Set the synchronization interval to 24 hrs.
ICPE(config)# ntp time-zone 4		Set the time zone to GMT-8:00 Vancouver.

2.5.10 QoS Command

1. Specify the desired QoS mode.

QoS command	Parameter	Description
ICPE(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		
ICPE(config)# no qos		Disable QoS function.
Show command		
ICPE(config)# show qos		Show or verify QoS configurations.
QoS command example		
ICPE(config)# qos 802.1p		Enable QoS function and use 802.1p mode.
ICPE(config)# qos dscp		Enable QoS function and use DSCP mode.

2. Set up the DSCP and queue mapping.

DSCP-map command	Parameter	Description
ICPE(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		
ICPE(config)# no qos dscp-map [0-63] dscp_list		Set the queue of the specific DCSP value back to the default.
Show command		
ICPE(config)# show qos		Show or verify QoS configurations.
DSCP-map example		
ICPE(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
ICPE(config)# qos management-priority [0-7]	[0-7]	Specify management traffic default 802.1p priority bit.
No command		
ICPE(config)# no qos management-priority		Set management traffic priority back to the default.
Management-priority example		
ICPE(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
ICPE(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		
ICPE(config)# no qos queuing-mode		Set the queuing mode to Strict mode.
Show command		
ICPE(config)# show qos		Show or verify QoS configurations.
Queuing-mode example		
ICPE(config)# qos queuing-mode weight		Change the queuing mode from strict to Weight.

5. Set up queue weight.

Queuing-weighted command	Parameter	Description
ICPE(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		
ICPE(config)# no qos queuing-weight		Set the queuing weight back to the default.
Show command		
ICPE(config)# show qos		Show or verify QoS configurations.

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

5. Set up 802.1p and DSCP remarking

Remarking command	Parameter	Description
ICPE(config)# qos remarking [dscp | 802.1p]	[dscp | 802.1p]	Enable the specific remarking mode, DSCP or 802.1p Remarking.
ICPE(config)# qos remarking dscp [by-dscp]	[by-dscp]	Specify DSCP bit remarking mode.
ICPE(config)# qos remarking dscp-map [1-8]	[1-8]	Configure the DSCP and priority mapping ID.
ICPE(config)# qos remarking 802.1p-map [1-8]	[1-8]	Configure the 802.1p and priority mapping ID.
No command		
ICPE(config)# no qos remarking dscp		Undo specify DSCP bit remarking mode
ICPE(config)# no qos remarking dscp-map [1-8]	[1-8]	Undo specify DSCP and priority mapping ID
ICPE(config)# no qos remarking 802.1p		Disable 802.1p bit remarking
ICPE(config)# no qos remarking 802.1p-map [1-8]	[1-8]	Undo specify a 802.1p value
Show command		
ICPE(config)# show qos remarking		Show current DSCP, VID and 802.1p remarking configuration.
Remarking example		
ICPE(config)# qos remarking 802.1p		Enable 802.1p remarking.
ICPE(config)# no qos remarking dscp		Disable DSCP remarking.

6. Set up 802.1p priority mapping bit and queue mapping.

Mapping command	Parameter	Description
ICPE(config)# qos 802.1p-map [0-7] 802.1p_list [0-3]	[0-7] 802.1p_list	Specify 802.1p bit value.
	[0-3]	Specify queue value.
No command		
ICPE(config)# no qos 802.1p-map		Undo 802.1p mapping.

802.1p Remarking command		
ICPE(config)# qos remarking 802.1p-map [1-8]	[1-8]	Configure the mapping of 802.1p remarking mode. **[1-8]:** Select the mapping entry
ICPE(config-802.1p-map-ID)# active		Enable the mapping entry.
ICPE(config-802.1p-map-ID)# 802.1p [0-7]	[0-7]	Specify the 802.1p value to be remarked.
ICPE(config-802.1p-map-ID)# priority [0-7]	[0-7]	Specify the 802.1p remarking value.
ICPE(config-802.1p-map-ID)# exit		Exit the entry.
DSCP Remarking No command		
ICPE(config)# no qos remarking 802.1p-map [1-8]	[1-8]	Set the specific entry back to the default setting.
ICPE(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		
ICPE(config-dscp/802.1p-map-ID)# show		Display the mapping configuration of the specific entry.

7. Assign a tag priority to the specific queue.

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

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

QoS & Interface command	Parameter	Description
ICPE(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
ICPE(config-if-PORT-PORT)# qos default-class [0-3]	[0-3]	Specify the default class for the selected interfaces.
ICPE(config-if-PORT-PORT)# qos rate-limit ingress [32-1000000] kbps	[32-1000000] kbps	Specify the ingress rate between 32 and 1000000.
ICPE(config-if-PORT-PORT)# qos rate-limit egress [32-1000000] kbps	[32-1000000] kbps	Specify the egress rate between 32 and 1000000.
No command		
ICPE(config-if-PORT-PORT)# no qos default-class		Set QoS default class setting to the default.
ICPE(config-if-PORT-PORT)# no qos rate-limit ingress		Set QoS ingress rate limit setting to the default.
ICPE(config-if-PORT-PORT)# no qos rate-limit egress		Set QoS ingress rate limit setting to the default.
Show command		
ICPE(config)# show qos interface [port_list]	[port_list]	Show or verify the selected interfaces’ ingress and egress rate configurations.
ICPE(config)# show qos interface		Show or verify each interface’s ingress and

	egress rate configurations.
ICPE(config)# show qos	Show or verify QoS configurations.
QoS & Interface example	
ICPE(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
ICPE(config-if-1-3)# qos rate-limit ingress 1550	Configure the selected interfaces’ ingress rate-limit to 1550.
ICPE(config-if-1-3)# qos rate-limit egress 3 1550	Set the selected interfaces’ queue 3 to egress rate 1550.

2.5.11 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 Gateway Controller allows users to set a threshold rate for broadcast traffic on a per Gateway Controller basis so as to protect network from broadcast storms. Any broadcast packet exceeding the specified value will then be dropped.

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

2.5.12 SNMP-Server Command

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

Snmp-server command	Parameter	Description
ICPE(config)# snmp-server community [community]	[community]	Specify a SNMP community name up to 20 alphanumeric characters.
ICPE(config-community-NAME)# active		Enable this SNMP community account.
ICPE(config-community-NAME)# description [Description]	[Description]	Enter the description up to 35 alphanumerical characters for this SNMP community.
ICPE(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. By default, when you create a community, the access privilege for this account is set to “read only”.

		Admin: Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
No command		
ICPE(config)# no snmp-server community [community]	[community]	Delete the specified community.
ICPE(config-community-NAME)# no active		Disable this SNMP community account.
ICPE(config-community-NAME)# no description		Remove the entered SNMP community descriptions.
ICPE(config-community-NAME)# no level		Remove the configured level. This will set this community's level to read only.
Show command		
ICPE(config)# show snmp-server community [community]	[community]	Show the specified SNMP server account's settings.
ICPE(config)# show snmp-server community		Show SNMP community account's information in Global Configuration Mode.
ICPE(config-community-NAME)# show		View or verify the configured SNMP community account's information.
Exit command		
ICPE(config-community-NAME)# exit		Return to Global Configuration Mode.
Snmp-server example		
ICPE(config)# snmp-server community mycomm		Create a new community "mycomm" and edit the details of this community account.
ICPE(config-community-mycomm)# active		Activate the SNMP community "mycomm".
ICPE(config-community-mycomm)# description rddeptcomm		Add a description for "mycomm" community.
ICPE(config-community-mycomm)# level admin		Set "mycomm" community level to admin.

2. Set up a SNMP trap destination.

Trap-dest command	Parameter	Description
ICPE(config)# snmp-server trap-destination [1-3]	[1-3]	Create a trap destination account.
ICPE(config-trap-ACCOUNT)# active		Enable this SNMP trap destination account.
ICPE(config-trap-ACCOUNT)# community [community]	[community]	Enter the community name of network management system.

ICPE(config-trap-ACCOUNT)# destination [A.B.C.D]	[A.B.C.D]	Enter the SNMP server IP address.
No command		
ICPE(config)# no snmp-server trap-destination [1-3]	[1-3]	Delete the specified trap destination account.
ICPE(config-trap-ACCOUNT)# no active		Disable this SNMP trap destination account.
ICPE(config-trap-ACCOUNT)# no community		Delete the configured community name.
ICPE(config-trap-ACCOUNT)# no description		Delete the configured trap destination description.
Show command		
ICPE(config)# show snmp-server trap-destination [1-3]	[1-3]	Show the specified trap destination information.
ICPE(config)# show snmp-server trap-destination		Show SNMP trap destination information in Global Configuration mode.
ICPE(config-trap-ACCOUNT)# show		View this trap destination account's information.
Exit command		
ICPE(config- trap-ACCOUNT)# exit		Return to Global Configuration Mode.
Trap-destination example		
ICPE(config)# snmp-server trap-destination 1		Create a trap destination account.
ICPE(config-trap-1)# active		Activate the trap destination account.
ICPE(config-trap-1)# community mycomm		Refer this trap destination account to the community "mycomm".
ICPE(config-trap-1)# description redepttrapdest		Add a description for this trap destination account.
ICPE(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
ICPE(config)# snmp-server trap-type [all |auth-fail | cold-start | port-link | power-down | warm-start]	[all |auth-fail | cold-start | battery-mode | port-link | power-down | warm-start]	Specify the trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, the device cold /warm starts, port link is up or down, power is down. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **cold-start:** A trap will be sent when the device boots up. **battery-mode:** Enable the SNMP trap. **port-link:** A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the device's power is down. **warm-start:** A trap will be sent when the device restarts.
No command		
ICPE(config)# no snmp-server trap-type auth-fail		Authentication failure trap will not be sent.
Show command		
ICPE(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
ICPE(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

2.5.13 Switch Command

Switch command	Description
ICPE(config)# switch statistics polling	Enable the Gateway Controller to refresh counter information and current state in a fixed interval.
No command	
ICPE(config)# no switch statistics polling	Disable the Gateway Controller to refresh counter information and current state in a fixed interval.

2.5.14 Switch-info Command

Set up the Gateway Controller's basic information including company name, hostname, system name, etc..

Switch-info Command	Parameter	Description
ICPE(config)# switch-info company-name [company_name]	[company_name]	Enter a company name for this Gateway Controller, up to 55 alphanumeric characters.
ICPE(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.
ICPE(config)# switch-info system-contact [system_contact]	[system_contact]	Enter contact information up to 55 alphanumeric characters for this Gateway Controller.
ICPE(config)# switch-info system-location [system_location]	[system_location]	Enter a brief description of the Gateway Controller location up to 55 alphanumeric characters. Like the name, the location is for reference only, for example, "13th Floor".
ICPE(config)# switch-info system-name [system_name]	[system_name]	Enter a unique name up to 55 alphanumeric characters for this Gateway Controller. Use a descriptive name to identify the Gateway Controller in relation to your network, for example, "Backbone 1". This name is mainly used for reference only.

ICPE(config)# switch-info host-name [host_name]	[host_name]	Enter a new hostname up to 15 alphanumeric characters for this Gateway Controller. By default, the hostname prompt shows the model name of this Gateway Controller. 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		
ICPE(config)# no switch-info company-name		Delete the entered company name information.
ICPE(config)# no switch-info dhcp-vendor-id		Delete the entered DHCP vendor ID information.
ICPE(config)# no switch-info system-contact		Delete the entered system contact information.
ICPE(config)# no switch-info system-location		Delete the entered system location information.
ICPE(config)# no switch-info system-name		Delete the entered system name information.
ICPE(config)# no switch-info host-name		Set the hostname to the factory default.
Show command		
ICPE(config)# show switch-info		Show Gateway Controller information including company name, system contact, system location, system name, model name, firmware version and fiber type.
Switch-info example		
ICPE(config)# switch-info company-name telecomxyz		Set the company name to "telecomxyz".
ICPE(config)# switch-info system-contact info@company.com		Set the system contact field to "info@compnay.com".
ICPE(config)# switch-info system-location 13thfloor		Set the system location field to "13thfloor".
ICPE(config)# switch-info system-name backbone1		Set the system name field to "backbone1".

2.5.15 Syslog Command

Syslog command	Parameter	Description
ICPE(config)# syslog		Enable syslog server
ICPE(config)# syslog server1/server2/server3 [A.B.C.D]	[A.B.C.D]	Configure syslog server1/server2/server3
No command		
ICPE(config)# no syslog		Disable syslog server
Show command		
ICPE(config)#show syslog		Show syslog status
Syslog example		

ICPE(config)# syslog ICPE(config)# syslog server1 192.168.0.222	Enable syslog and assign server1 IP address 192.168.0.222

2.5.16 USB Command

USB command	Parameter	Description
ICPE(config)# usb [usb_list]	[usb_list]	Enable specified usb ports
No Command		
ICPE(config)# no usb [usb_list]		Disable specified usb ports.
Show Command		
ICPE(config)# show usb		Display USB status

2.5.17 User Command

1. Create a new login account.

User command	Parameter	Description
ICPE(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.
ICPE(config-user-USERNAME)# active		Activate this user account.
ICPE(config-user-USERNAME)# description [description]	[description]	Enter the brief description for this user account.
ICPE(config-user-USERNAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify user account level. By default, when you create a community, the access privilege for this account is set to "read only". **Admin:** Full access right, including maintaining user account, system information, loading factory settings, etc.. **rw:** Read & Write access privilege. Partial access right, unable to modify system information, user account, load factory settings and upgrade firmware. **Ro:** Read Only access privilege.
ICPE(config-user-USERNAME)# password [password]	[password]	Enter the password for this user account up to 20 alphanumeric characters.
No command		
ICPE(config)# no user name [user_name]	[user_name]	Delete the specified user account.

ICPE(config-user-USERNAME)# no description		Remove the configured description.
ICPE(config-user-USERNAME)# no level		Remove the configured level value. The account level will return to the default setting.
ICPE(config-user-USERNAME)# no password		Remove the configured password value.
Show command		
ICPE(config)# show user name [user_name]	[user_name]	Show the specified account's information.
ICPE(config)# show user name		List all user accounts.
ICPE(config-user-USERNAME)# show		Show or verify the newly-created user account's information.
User command example		
ICPE(config)# user name miseric		Create a new login account "miseric".
ICPE(config-user-USERNAME)# description misengineer		Add a description to this new account "miseric".
ICPE(config-user-USERNAME)# level rw		Set this new account's access privilege to "read & write".
ICPE(config-user-USERNAME)# password mis2256i		Set up a password for this new account "miseric"

2. Configure RADIUS server settings.

User command	Parameter	Description
ICPE(config)# user radius		Enable RADIUS authentication.
ICPE(config)# user radius radius-port [1025-65535]	[1025-65535]	Specify RADIUS server port number.
ICPE(config)# user radius retry-time [0-2]	[0-2]	Specify the retry value. This is the number of times that the Gateway Controller will try to reconnect if the RADIUS server is not reachable.
ICPE(config)# user radius secret [secret]	[secret]	Specify a secret up to 31 alphanumeric characters for RADIUS server. This secret key is used to validate communications between RADIUS servers.
ICPE(config)# user radius server1 [A.B.C.D]	[A.B.C.D]	Specify the primary RADIUS server IP address.
ICPE(config)# user radius server2 [A.B.C.D]	[A.B.C.D]	Specify the secondary RADIUS server IP address.
No command		
ICPE(config)# no user radius		Disable RADIUS authentication.
ICPE(config)# no user radius radius-port		Set the radius port setting back to the factory default.
ICPE(config)# no user radius retry-time		Set the retry time setting back to the factory default.
ICPE(config)# no user radius secret		Remove the configured secret value.
ICPE(config)# no user radius server1		Delete the specified IP address.

ICPE(config)# no user radius server2	Delete the specified IP address.
Show command	
ICPE(config)#show user radius	Show current RADIUS settings.
User command example	
ICPE(config)# user radius	Enable RADIUS authentication.
ICPE(config)# user radius radius-port 1812	Set RADIUS server port number to 1812.
ICPE(config)# user radius retry-time 2	Set the retry value to 2. The Gateway Controller will try to reconnect twice if the RADIUS server is not reachable.
ICPE(config)# user radius secret abcxyzabc	Set up a secret for validating communications between RADIUS clients.
ICPE(config)# user radius server1 192.180.3.1	Set the primary RADIUS server address to 192.180.3.1.
ICPE(config)# user radius server2 192.180.3.2	Set the secondary RADIUS server address to 192.180.3.2.

2.5.18 VLAN Command

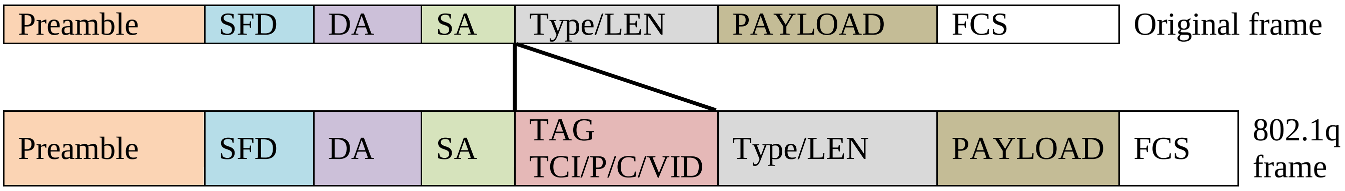
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast 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.

802.1Q VLAN Concept

Port-Based VLAN is simple to implement and use, but it cannot be deployed cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution to this problem. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help network administrators break large switched networks into smaller segments so that broadcast and multicast traffic will not occupy too much available bandwidth as well as provide a higher level security between segments of internal networks.

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

Important VLAN Concepts for 802.1Q VLAN Configuration:

There are two key concepts to understand.

- **Access-VLAN** specifies the VLAN ID to the switch port that will assign the VLAN ID to **untagged** traffic from that port. A port can only be assigned to one Access-VLAN at a time. When the port is configured as **Access Mode**, the port is called an **Access Port**, the link to/from this port is called an **Access Link**. The VLAN ID assigned is called **PVID**.

- **Trunk-VLAN** specifies the set of VLAN IDs that a given port is allowed to receive and send **tagged** packets. A port can be assigned to multiple Trunk-VLANs at a time. When the port is configured as **Trunk Mode**, the port is called a **Trunk Port**, the link to/from this port is called a **Trunk Link**. The VLAN ID assigned is called **VID**.

A port can be configured as below 802.1q VLAN modes :

- **Access Mode :**

  Access Links (the link to/from access ports) are the most common type of links on any VLAN switch. All **network hosts (such as PCs)** connect to the switch's Access Links in order to gain access to the local network. We configure only one **Access-VLAN** per port, that is, the VLAN ID the **network hosts** will be allowed to access.

  It is important to note at this point that any **network host** connected to an Access Port is totally unaware of the VLAN assigned to the port. The **network host** simply assumes it is part of a single broadcast domain, just as it happens with any normal switch. During data transfers, any VLAN information or data from other VLANs is removed so the recipient has no information about them.

- **Trunk Mode :**
  Trunk Links (the link to/from trunk ports) is configured to carry packets for multiple VLANs. These types of ports are usually found in connections between switches. These links require the ability to carry packets from multiple VLANs because VLANs span over multiple switches.

- **Trunk Native Mode :**
  A Trunk-native port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN. This Access-VLAN is referred to as the native VLAN ID for a Trunk-native Port. The native VLAN ID is the VLAN ID that carries untagged traffic on trunk-native ports.

Example : PortX configuration

Configuration	Result

Trunk-VLAN = 10, 11, 12
Access-VLAN = 20
Mode = Access
	PortX is an **Access Port**
	PortX's **VID** is ignored
	PortX's **PVID** is 20
	PortX sends **Untagged** packets (PortX takes away VLAN tag if the PVID is 20)
	PortX receives **Untagged** packets only

Trunk-VLAN = 10,11,12
Access-VLAN = 20
Mode = Trunk
	PortX is a **Trunk Port**
	PortX's **VID** is 10,11 and 12
	PortX's **PVID** is ignored
	PortX sends and receives **Tagged** packets VID 10,11 and 12

Trunk-VLAN = 10,11,12
Access-VLAN = 20
Mode = Trunk-native
	PortX is a **Trunk-native Port**
	PortX's **VID** is 10,11 and 12
	PortX's **PVID** is 20
	PortX sends and receives **Tagged** packets VID 10,11 and 12
	PortX receives **Untagged** packets and add PVID 20

1. **Use "Interface" command to configure a group of ports' 802.1q VLAN settings.**

VLAN & Interface command	Parameter	Description
ICPE(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,2
ICPE(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify the selected ports' Access-VLAN ID (PVID).
ICPE(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Specify the selected ports' Trunk-VLAN ID (VID).
ICPE(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
ICPE(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Set the selected ports to trunk mode (tagged).

ICPE(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Set the selected ports to trunk-native mode. (Tagged and untagged) **Note : When you assign a default Access-VLAN to the trunk-native port, all untagged traffic travels on the default Access-VLAN for the trunk-native port, and all untagged traffic is assumed to belong to this Access-VLAN.**
ICPE(config-if-PORT-PORT)# vlan port-based [name]	[name]	Set the selected ports to a specified port-based VLAN. **Note :** **Need to create a port-based VLAN group under VLAN global configuration mode before joining it.**
No command		
ICPE(config-if-PORT-PORT)# no vlan dot1q-vlan access-vlan		Set the selected ports' PVID to the default setting.
ICPE(config-if-PORT-PORT)# no vlan dot1q-vlan mode		Remove VLAN dot1q mode.
ICPE(config-if-PORT-PORT)# no vlan dot1q-vlan mode trunk native		Disable native VLAN for untagged traffic.
ICPE(config-if-PORT-PORT)# no vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Remove the selected ports' from the specified trunk VLAN.
ICPE(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Delete the selected ports from the specified port-based VLAN.
VLAN & interface command example		
ICPE(config)# interface 1-2		Enter port 1 to port 2's interface mode.
ICPE(config-if-1-2)# vlan dot1q-vlan access-vlan 10		Set port 1 to port 3's Access-VLAN ID (PVID) to 10.
ICPE(config-if-1-2)# vlan dot1q-vlan mode access		Set the selected ports to access mode (untagged).
ICPE(config-if-1-2)# vlan dot1q-vlan mode trunk native		Enable native VLAN for untagged traffic.
ICPE(config-if-1-2)# vlan port-based mktpbvlan		Set the selected ports to the specified port-based VLAN "mktpbvlan".

2. Modify a 802.1q VLAN and a management VLAN rule or create a port-based VLAN group.

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

VLAN dot1q command	Parameter	Description

<table>
<tr><td>ICPE(config)# vlan dot1q-vlan</td><td></td><td>Globally enable 802.1q VLAN.</td></tr>
<tr><td>ICPE(config)# vlan dot1q-vlan [1-4094]</td><td>[1-4094]</td><td>Enter a VID number to create a 802.1q VLAN.

<b>Note :</b>
<b>802.1q VLAN ID need to be created under interface global command. In here you can only modify it instead of creating a new VLAN ID.</b></td></tr>
<tr><td>ICPE(config)# vlan dot1q-vlan isolation</td><td></td><td>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).

In other words, the device will be forced to follow the rule shown below.

<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></td></tr>
<tr><td>ICPE(config-vlan-ID)# name [vlan_name]</td><td>[vlan_name]</td><td>Specify a descriptive name for this VLAN ID, max 15 characters.</td></tr>
<tr><td>ICPE(config)# vlan isolation up-link-port [port_list]</td><td>[port_list]</td><td>To assign uplink ports which will form a port-based VLAN group with all other downlink ports seperatedly so to isolated downlink ports from each other except from uplink ports.</td></tr>
<tr><td rowspan="3">ICPE(config)# vlan management-vlan [1-4094] management-port [port_list] mode [access | trunk | trunk-native]</td><td>[1-4094]</td><td>Enter the management VLAN ID.</td></tr>
<tr><td>[port_list]</td><td>Specify the management port number.</td></tr>
<tr><td>[access | trunk | trunk-native]</td><td>Specify whether the management port is in trunk or access mode.

<b>“trunk” mode:</b> Set the selected ports to tagged.

<b>“access” mode:</b> Set the selected ports to untagged.

<b>“trunk-native” mode:</b> Set all untagged traffic travels on the default Access-VLAN for the trunk-native</td></tr>
</table>

		port, and all untagged traffic is assumed to belong to this Access-VLAN.
ICPE(config)# vlan port-based		Enable port-based VLAN.
ICPE(config)# vlan port-based [name]	[name]	Specify a name for this port-based VLAN.
ICPE(config)# vlan port-based [name] include-cpu		Include CPU into this Port-Based VLAN.
No command		
ICPE(config)# no vlan dot1q-vlan		Disable 802.1q VLAN
ICPE(config)# no vlan dot1q-vlan isolation		Disable 802.1q VLAN isolation
ICPE(config-vlan-ID)# no name		Remove the descriptive name for the specified VLAN ID.
ICPE(config)# no vlan isolation up-link-port [port_list]		Undo uplink ports.
ICPE(config)# no vlan port-based		Disable port-based VLAN.
ICPE(config)# no vlan port-based [name]	[name]	Delete the specified port-based VLAN.
ICPE(config)# no vlan port-based [name] include-cpu		Exclude CPU from this Port-Based VLAN
Show command		
ICPE(config)# show vlan dot1q-vlan tag-vlan		Show IEEE 802.1q tag VLAN table
ICPE(config)# show vlan dot1q-vlan trunk-vlan		Show configure trunk VLAN table
ICPE(config-vlan-ID)# show		Show the membership status of this VLAN ID
ICPE(config)# show vlan interface		Show all ports' VLAN assignment and VLAN mode.
ICPE(config)# show vlan interface [port_list]	[port_list]	Show the selected ports' VLAN assignment and VLAN mode.
ICPE(config)# show vlan isolation		Show VLAN isolation information.
ICPE(config)# show vlan port-based		Show port-based VLAN table.
Exit command		
ICPE(config-vlan-ID)# exit		Return to Global configuration mode.
Port-based VLAN example		
ICPE(config)# vlan port-based MKT_Office		Create a port-based VLAN "MKT_Office".
ICPE(config)# vlan management-vlan 1 management-port 1-2 mode access		Set VLAN 1 to management VLAN (untagged) and port 1~2 to management ports.

2.5.19 Z-Wave Command

Z-Wave is a wireless communications specification designed to allow devices in the home (lighting, access controls, entertainment systems and household appliances, for example) to communicate with one another for the purposes of home automation. The section shows the configuration and displays the status.

1. **Restore a Z-Wave configuration file via FTP or TFTP server.**

Command	Parameter	Description
ICPE# z-wave 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.
ICPE# 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.

2. **Restore the Z-Wave of Gateway Controller back to default settings.**

Command / Example
ICPE# z-wave copy-cfg from default

3. **Backup a configuration file to TFTP server.**

Command	Parameter	Description
ICPE# z-wave copy-cfg to ftp [A.B.C.D] [file_name] [running | startup] [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.
	[running | startup]	**running:** Back up the data you're processing **start-up:** Back up the data same as last saved data.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
ICPE# z-wave copy-cfg to tftp [A.B.C.D] [file_name] [running | startup]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the configuration file name that you want to backup.
	[running | startup]	**running:** Back up the data you're processing **start-up:** Back up the data same as last saved data.

4. **Set up a Z-Wave configuration and view status.**

Command	Parameter	Description
ICPE# z-wave mode exclude [0-99999999]	[0-99999999]	Under Exnclude mode, the Gateway Controller is allowed to disconnect a sensor. At the moment, data transmission doesn't work. Set the time interval in

		second after which you want to switch back to Normal mode. The range is between 0 ~ 99999999. The default setting is 0.
ICPE# z-wave mode include [0-99999999]	[0-99999999]	Under Include mode, the Gateway Controller is allowed to join a sensor. At the moment, data transmission doesn't work. Set the time interval in second after which you want to switch back to Normal mode. The range is between 0 ~ 99999999. The default setting is 0.
ICPE# z-wave mode normal		Under Normal mode, the Gateway Controller is in operation and allowed to data transmission.
ICPE# z-wave node [2-232] [0xWX] [0xWXYZWXYZ]	[2-232] [0xWX] [0xWXYZWXYZ]	**[2-232]:** The identification number that a sensor is assigned. The maximum number of nodes is 231 nodes connected with the Gateway Controller. **[0xWX]:** The Command Class field defines a group of commands representing a given functionality. **[0xWXYZWXYZ]:** This is to make inquiry or settings with a sensor. Specify a string of certain value for the sensor.
ICPE# z-wave node send [2-232] [0xWX] [0xHHHHHH…]	[2-232] [0xWX] [0xHHHHHH…]	**[2-232]:** The identification number that a sensor is assigned. The maximum number of nodes is 231 nodes connected with the Gateway Controller. **[0xWX]:** The Command Class field defines a group of commands representing a given functionality. **[0xHHHHHH…]:** This is to make inquiry or settings with a sensor. Specify a string of certain value for the sensor.
ICPE# z-wave save		In order to save configuration setting permanently, users need to save configuration first before resetting the Gateway Controller.
Show Command		
ICPE# show zwave event		Show Z-Wave Event log that keeps a record of Z-Wave information.
ICPE# show zwave mode		Show the current status of zwave mode
ICPE# show zwave node		Show the current status of valid zwave node

2.5.20 Interface Command

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

1. **Entering interface numbers.**

Command	Parameter	Description
ICPE(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

Note : You need to enter interface numbers first before issuing below 2-15 commands.

2. **Enable port auto-negotiation.**

Command	Parameter	Description
ICPE(config-if-PORT-PORT)# auto-negotiation		Set the selected interfaces' to auto-negotiation. When auto-negotiation is enabled, speed configuration will be ignored.
No command		
ICPE(config-if-PORT-PORT)# no auto-negotiation		Set auto-negotiation setting to the default setting.

3. Set up port description.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# description [description]	[description]	Type in the description for the port(s), max 35 characters.
No command		
Switch(config-if-PORT-PORT)# no description		Remove the entered description name for the selected ports.

4. Set up duplex mode

Command	Parameter	Description
Switch(config-if-PORT-PORT)# duplex [full]	[full]	Configure port duplex to **full.**
No command		
Switch(config-if-PORT-PORT)# no duplex		Set the selected ports' duplex mode to the default setting. **Note1 : Auto-negotiation needs to be disabled before configuring duplex mode.**

5. Enable flow control operation

Command	Parameter	Description
Switch(config-if-PORT-PORT)# flowcontrol		Enable the selected interfaces' flow control function.
No command		
Switch(config-if-PORT-PORT)# no flowcontrol		Set the selected ports' flow control function to the default setting.

6. QoS configuration.

Command	Parameter	Description
Switch(config-if-PORT-PORT)# qos rate-limit ingress [0|32-1000000]	[0|32-1000000]	Configure **ingress** rate limit, set zero or from 32Kbps to 1000Mbps.

Switch(config-if-PORT-PORT)# qos rate-limit egress [0|32-1000000]	[0|32-1000000]	Configure **egress** rate limit, set zero or from 32Kbps to 1000Mbps.
Switch(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Port default 802.1p bit. Specify desired port default 802.1p bit between 0 and 7.
No command		
Switch(config-if-PORT-PORT)# no qos rate-limit ingress		Undo **ingress** rate limit.
Switch(config-if-PORT-PORT)# no qos rate-limit egress		Undo **egress** rate limit.
Switch(config-if-PORT-PORT)# no user-priority		Undo User-priority.

7. Shutdown interface.

Command	**Parameter**	**Description**
Switch(config-if-PORT-PORT)# shutdown		Administratively disable the selected ports' status.
No command		
Switch(config-if-PORT-PORT)# no shutdown		Administratively enable the selected ports' status.

8. Speed configuration.

Command	**Parameter**	**Description**
Switch(config-if-PORT-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.
No command		
Switch(config-if-PORT-PORT)# no speed		Set the selected ports' speed to the default setting.

9. VLAN configuration.

Command	**Parameter**	**Description**
Switch(config-if-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Configure port PVID.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode access		Configure port as dot-1q access port.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk		Configure port as dot-1q trunk port.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan mode trunk native		Configure port as dot-1q trunk native port.
Switch(config-if-PORT-PORT)# vlan dot1q-vlan trunk-vlan [1-4094]	[1-4094]	Configure port VID.
Switch(config-if-PORT-PORT)#	[name]	Join port to specific port-based VLAN group.

vlan port-based [name]		**Note : Need to create a port-based VLAN group first at Switch Management-->VLAN Configuration-->Port Based VLAN-->Configure VLAN.**
No command		
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 VLAN dot1q 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' from the specified trunk VLAN.
Switch(config-if-PORT-PORT)# no vlan port-based [name]	[name]	Delete the selected ports from the specified port-based VLAN.

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.

2.5.21 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.

2.5.22 Show log Command

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

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

Command	Description
Switch(config)# show default-config	Show the original configurations assigned to the Gateway Controller by the factory.
Switch(config)# show running-config	Show configurations currently used in the Gateway Controller. 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.

2.5.24 Show battery status Command

Command	Description
Switch(config)# show battery-state	This is to show the information regarding the battery connected, including Vendor Name, Serial Number, Date Code, Battery Status.

3. WEB MANAGEMENT

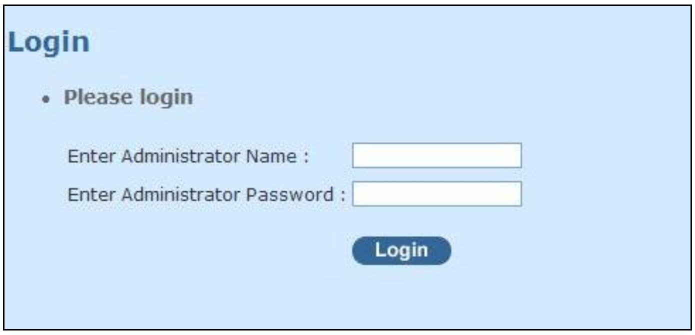
The Gateway Controller can be managed via a Web browser. The default IP of the Gateway Controller is set under DHCP mode. You can change the Switch’s IP address to the intended one later in its **Network Management** menu.

Follow these steps to manage the Gateway Controller through a Web browser:

1. Ask DHCP server to acquire IP address. Run a Web browser and specify the Gateway Controller address to reach it.

2. Login to the Gateway Controller.

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



Login

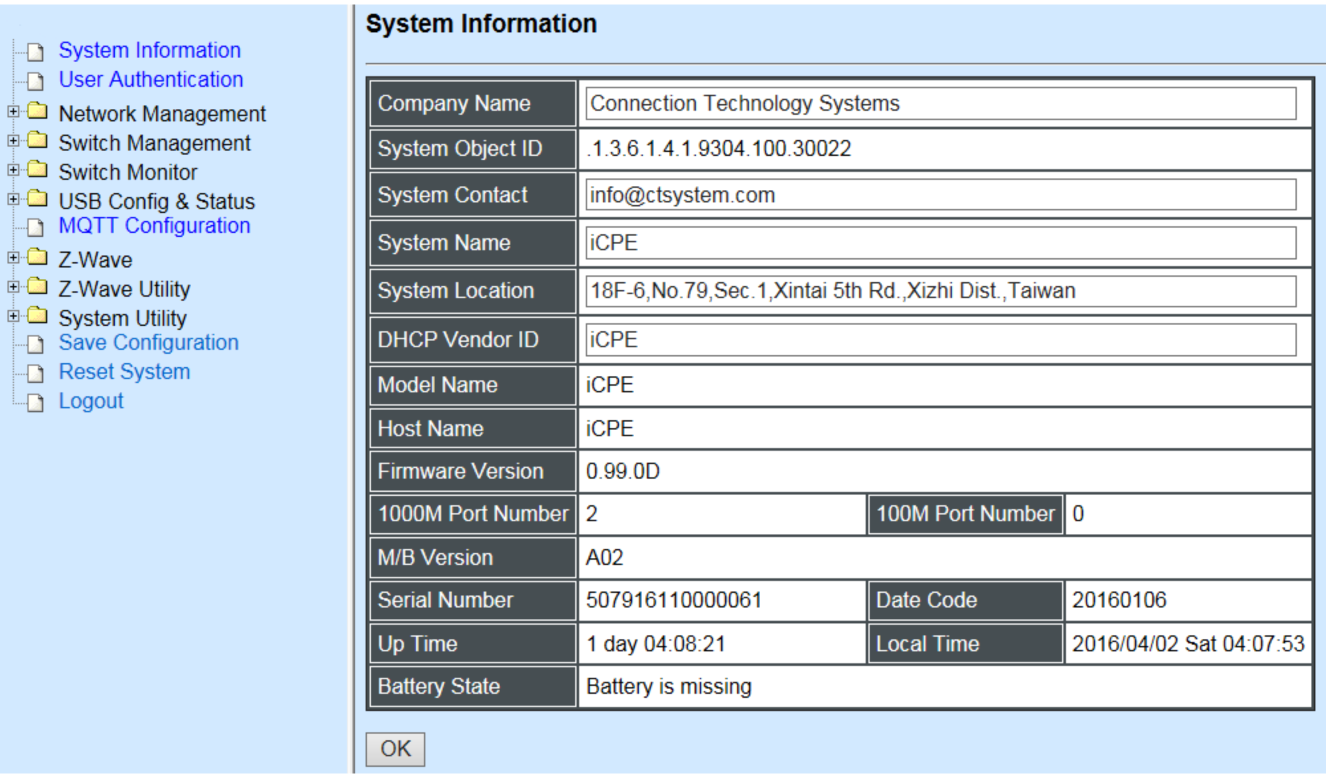
- Please login

Enter Administrator Name :

Enter Administrator Password :

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	.1.3.6.1.4.1.9304.100.30022		
System Contact	info@ctsystem.com		
System Name	iCPE		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCP Vendor ID	iCPE		
Model Name	iCPE		
Host Name	iCPE		
Firmware Version	0.99.0D		
1000M Port Number	2	100M Port Number	0
M/B Version	A02		
Serial Number	507916110000061	Date Code	20160106
Up Time	1 day 04:08:21	Local Time	2016/04/02 Sat 04:07:53
Battery State	Battery is missing		

1. **System Information:** Name the Gateway Controller, 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 Gateway Controller 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. **USB Config & Status:** Set up USB power configuration and show the status of it.

7. **MQTT Configuration:** Set up MQTT Configuration and view MQTT status.

8. **Z-Wave Congig & Status:** Set up Z-Wave Configuration and view MQTT status.

9. **System Utility:** Upgrade firmware and load factory settings.

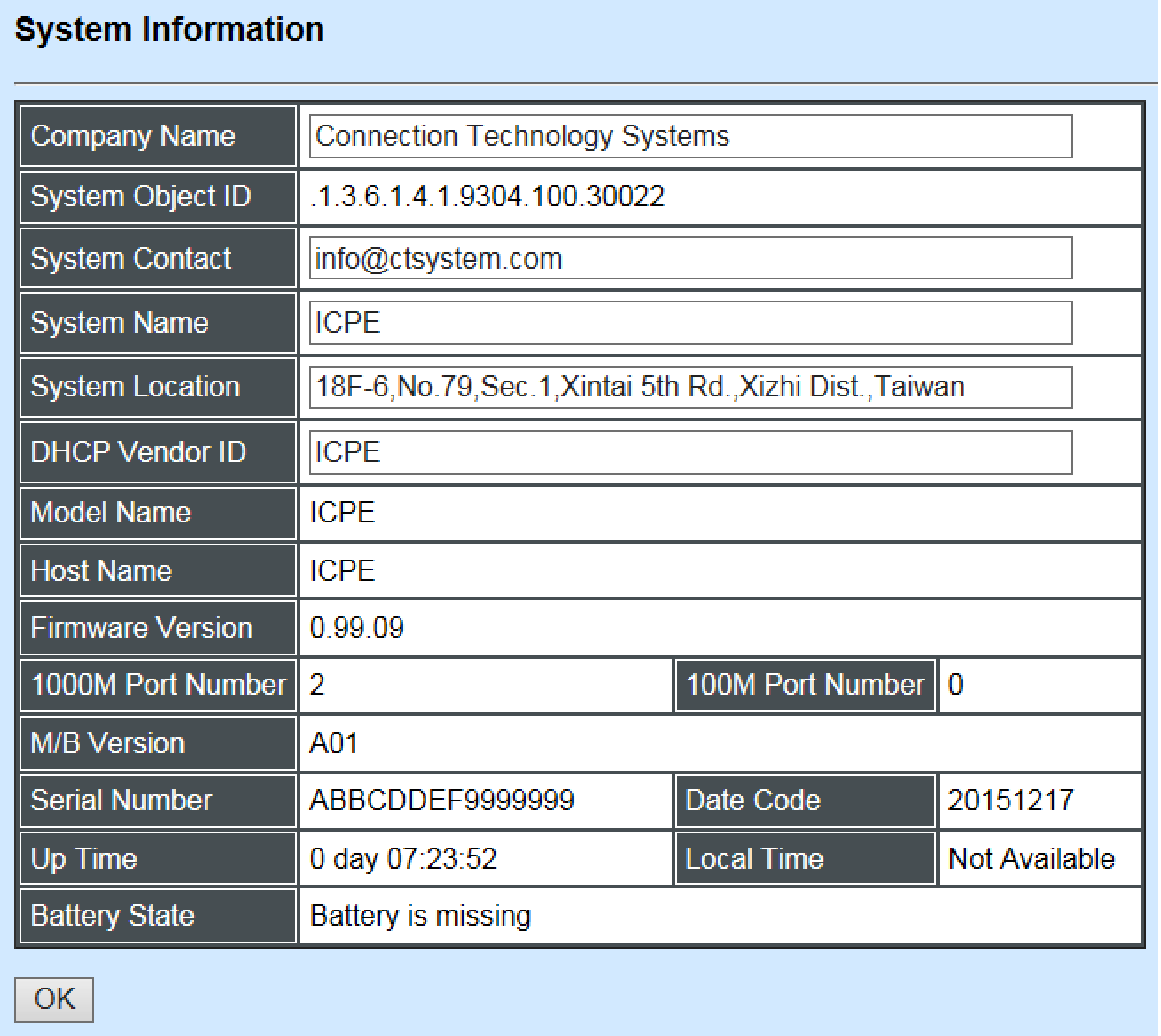
10. **Save Configuration:** Save all changes to the system.

11. **Reset System:** Reset the Gateway Controller.

12. **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	.1.3.6.1.4.1.9304.100.30022		
System Contact	info@ctsystem.com		
System Name	ICPE		
System Location	18F-6,No.79,Sec.1,Xintai 5th Rd.,Xizhi Dist.,Taiwan		
DHCP Vendor ID	ICPE		
Model Name	ICPE		
Host Name	ICPE		
Firmware Version	0.99.09		
1000M Port Number	2	100M Port Number	0
M/B Version	A01		
Serial Number	ABBCDDEF9999999	Date Code	20151217
Up Time	0 day 07:23:52	Local Time	Not Available
Battery State	Battery is missing		

Company Name: Enter a company name up to 55 alphanumeric characters for this Gateway Controller.

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

System Contact: Enter contact information up to 55 alphanumeric characters for this Gateway Controller.

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

System Location: Enter a brief description of the Gateway Controller 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: The firmware version of the first image.

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.

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

Date Code: View-only field that shows the Gateway Controller 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 Gateway Controller is.

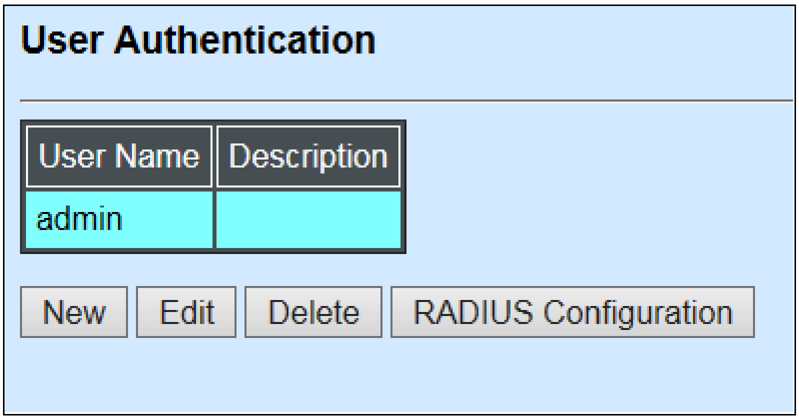
Battery State: Shows the status of battery.

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

3.2 User Authentication

To prevent any un-authorized operation, only registered users are allowed to operate the Gateway Controller. Users who want to operate the Gateway Controller 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.



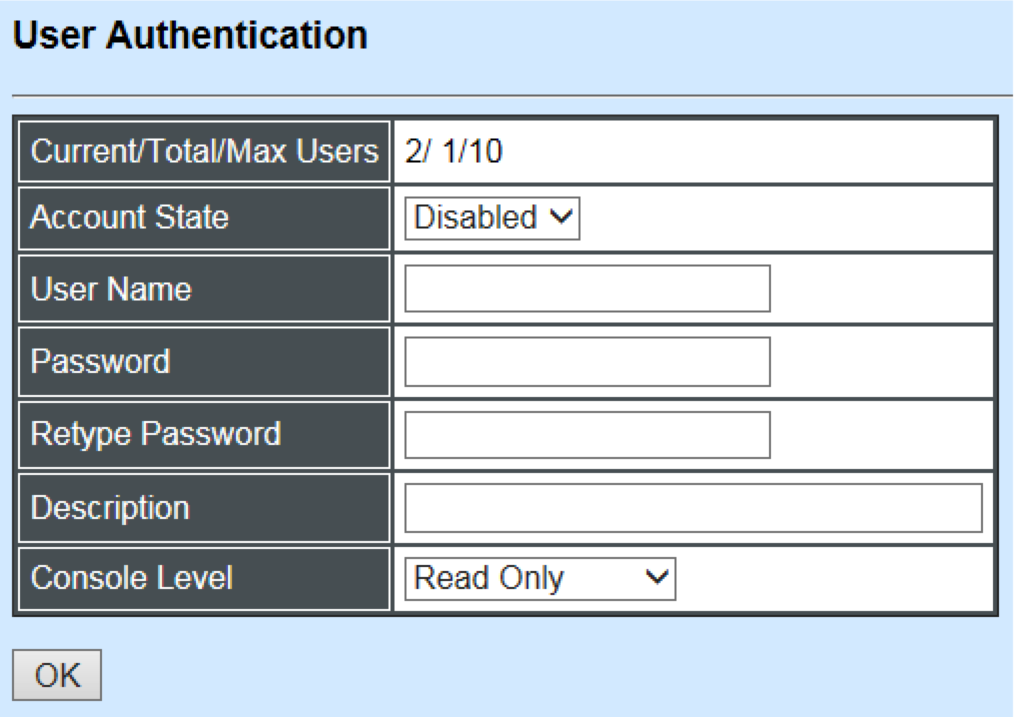
User Authentication

User Name	Description
admin	

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.



User Authentication

Current/Total/Max Users	2/ 1/10
Account State	Disabled
User Name	
Password	
Retype Password	
Description	
Console Level	Read Only

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 10.

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.

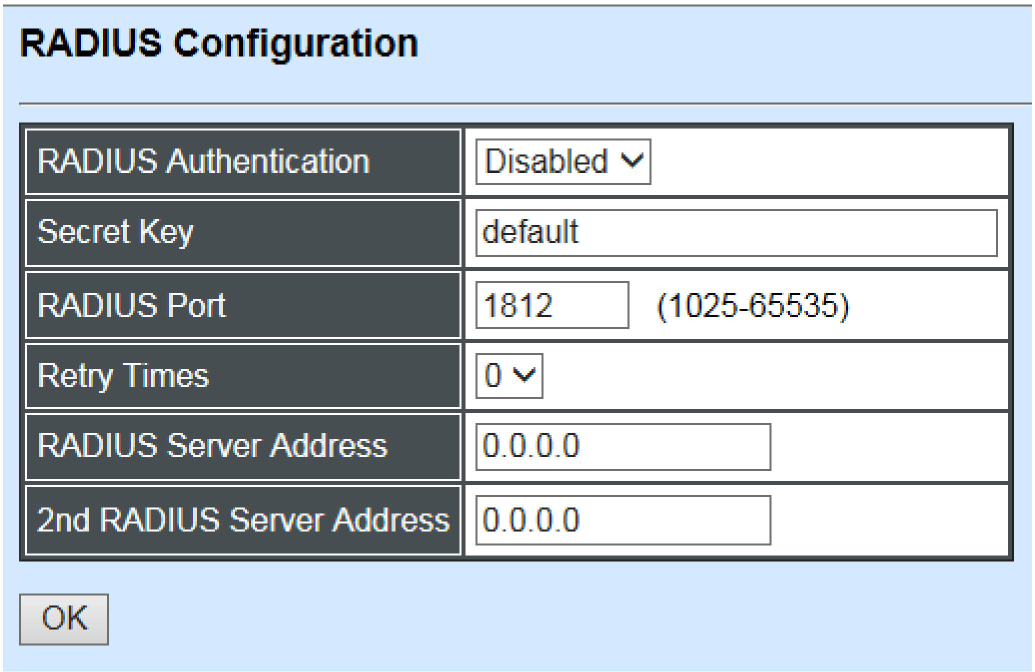
Read Only: Read only access right.

***NOTE:** If you forget the login password, the only way to gain access to the Web Management is to set the Gateway Controller back to the factory default setting by pressing the Reset button for more than10 seconds (The Reset button is located on the Upper Panel of the Gateway Controller.). When the Gateway Controller 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.

RADIUS Configuration

Click **RADIUS Configuration** in **User Authentication** and then the following screen page appears.



RADIUS Configuration

RADIUS Authentication	Disabled
Secret Key	default
RADIUS Port	1812 (1025-65535)
Retry Times	0
RADIUS Server Address	0.0.0.0
2nd RADIUS Server Address	0.0.0.0

When **RADIUS Authentication** is enabled, User login will be according to those settings on the RADIUS server(s).

***NOTE:** For advanced RADIUS Server setup, please refer to APPENDIX B or the "free RADIUS readme.txt" file on the disc provided with this product.*

Secret Key: The word to encrypt data of being sent to RADIUS server.

RADIUS Port: The RADIUS service port on RADIUS server.

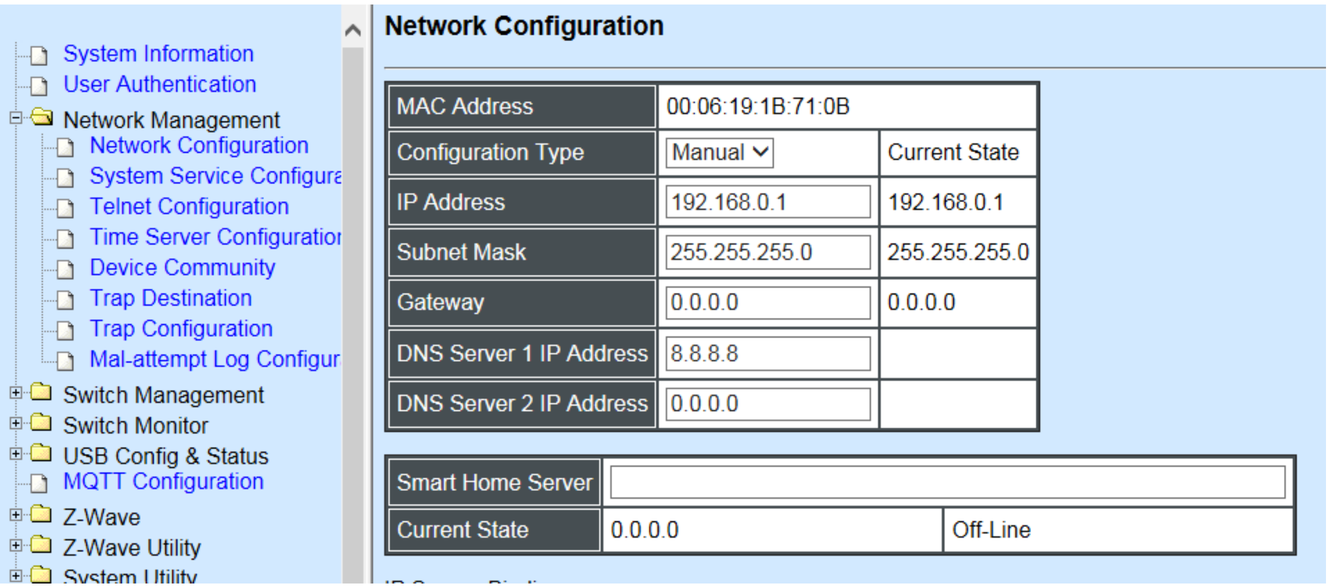
Retry Time: Times of trying to reconnect if the RADISU server is not reachable.

RADIUS Server Address: IP address of the first RADIUS server.

2nd RADIUS Server Address: IP address of the second RADIUS server.

3.3 Network Management

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



Network Configuration

MAC Address	00:06:19:1B:71:0B	
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
DNS Server 1 IP Address	8.8.8.8	
DNS Server 2 IP Address	0.0.0.0	

Smart Home Server		
Current State	0.0.0.0	Off-Line

1. **Network Configuration:** Set up the required IP configuration of the Gateway Controller.

2. **System Service Configuration:** Set up the system service type.

3. **Telnet Configuration:** Set up Telnet configuration.

4. **Time Server Configuration:** Set up the time server’s configuration.

5. **Device Community:** Set up the device’s community for SNMP.

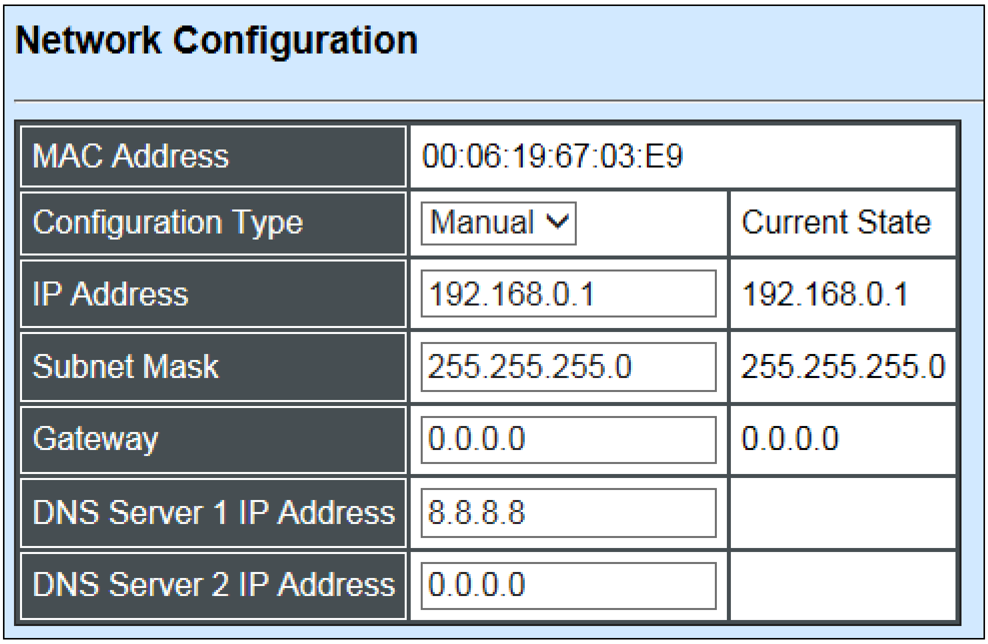
6. **Trap Destination:** Set up the trap destination’s IP address for specific community.

7. **Trap Configuration:** Enable or disable specific trap types.

8. **Mal-attempt Log Configuration:** Enable or disable Log server and its configuration.

3.3.1 Network Configuration

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



Network Configuration

MAC Address	00:06:19:67:03:E9	
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
DNS Server 1 IP Address	8.8.8.8	
DNS Server 2 IP Address	0.0.0.0	

MAC Address: This view-only field shows the unique and permanent MAC address pre-assigned to the Gateway Controller. You cannot change the Gateway Controller'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 Gateway Controller 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 Gateway Controller 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 Gateway Controller. 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.)

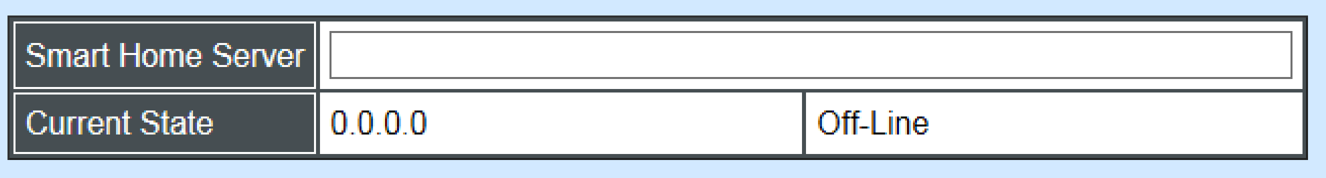
Subnet Mask: Specify the subnet mask. The default subnet mask values for the three Internet address classes are as follows:

- 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 Gateway Controller. This address is required when the Gateway Controller 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 Gateway Controller are on the same network.

DNS Server 1 IP Address: Specify IP Address for Domain Name System (DNS) Server 1.

DNS Server 2 IP Address: Specify IP Address for Domain Name System (DNS) Server 2.

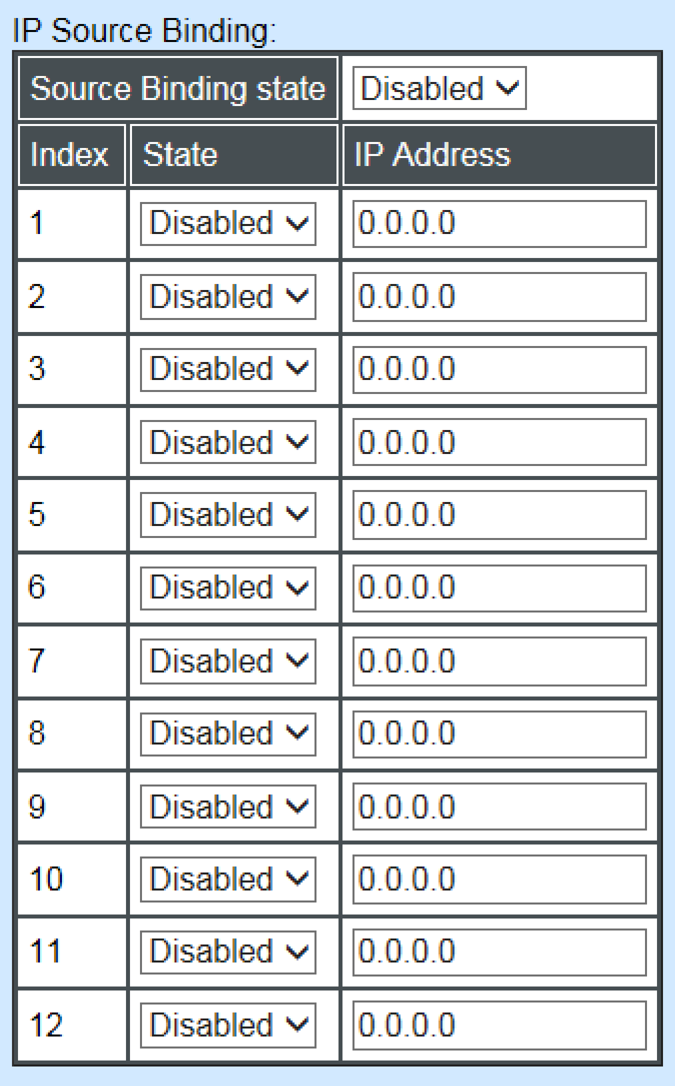


Smart Home Server		
Current State	0.0.0.0	Off-Line

Smart Home Server: By default, DHCP server plays a role in gateway. You may assign other device a gateway by typing IP address or domain name.

Current State: It shows the current IP address of gateway connected and the status of connection.

IP Source Binding:



IP Source Binding:

Source Binding state: Disabled

Index	State	IP Address
1	Disabled	0.0.0.0
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

Source Binding state: Enable or disable IP source binding.

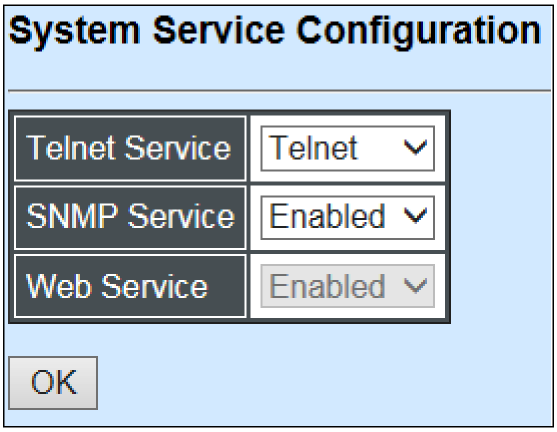
State: Disable or enable

IP/IPv6 Address: Specify the IP address for source binding.

NOTE: *This Gateway Controller also 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 B.*

3.3.2 System Service Configuration

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



System Service Configuration

Telnet Service	Telnet
SNMP Service	Enabled
Web Service	Enabled

Telnet Service: Select **Disabled** or **Telnet** or **SSH** for the system service type.

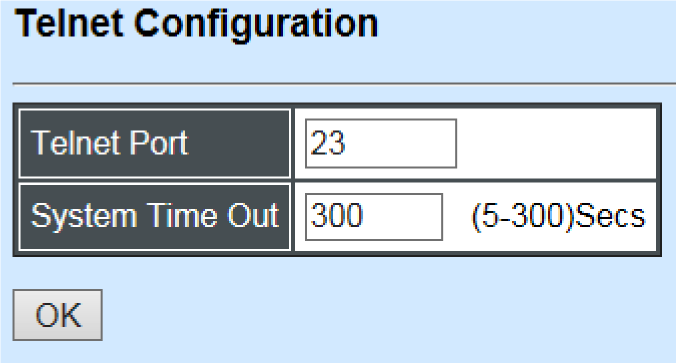
SNMP Service: Select **Disabled** or **Enabled** for the SNMP service.

Web Service: It’s view-only field. Web service cannot be disabled.

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

3.3.3 Telnet Configuration

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



Telnet Configuration

Telnet Port	23
System Time Out	300 (5-300)Secs

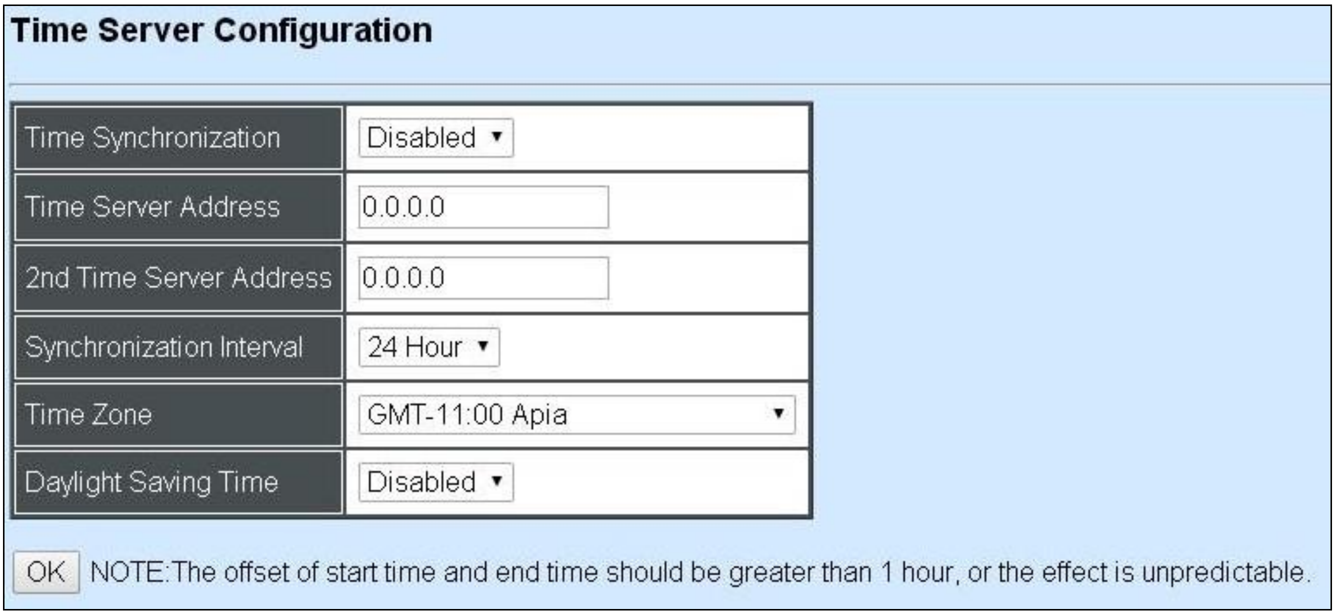
Telnet Port: Specify the desired TCP port number for the Telnet console. The default TCP port number of the Telnet is 23.

System Time Out: Specify the desired time that the Managed Switch will wait before disconnecting an inactive console/telnet. Specifying “0” means an inactive connection will never be disconnected.

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

3.3.4 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	24 Hour
Time Zone	GMT-11:00 Apia
Daylight Saving Time	Disabled

NOTE:The offset of start time and end time should be greater than 1 hour, or the effect is unpredictable.

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 Gateway Controller 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 hours to 24 hours.

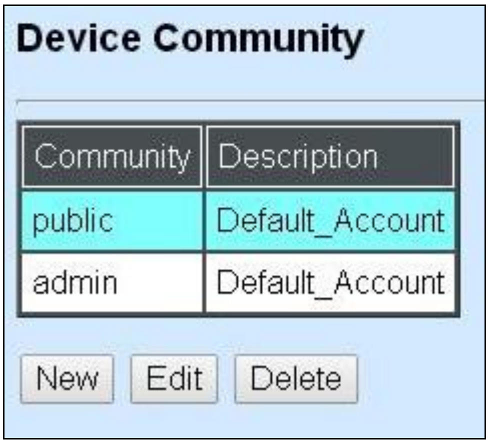
Time Zone: Select the appropriate time zone from the pull-down menu.

Daylight Saving Time: Disabled, recurring, date

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

3.3.5 Device Community

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



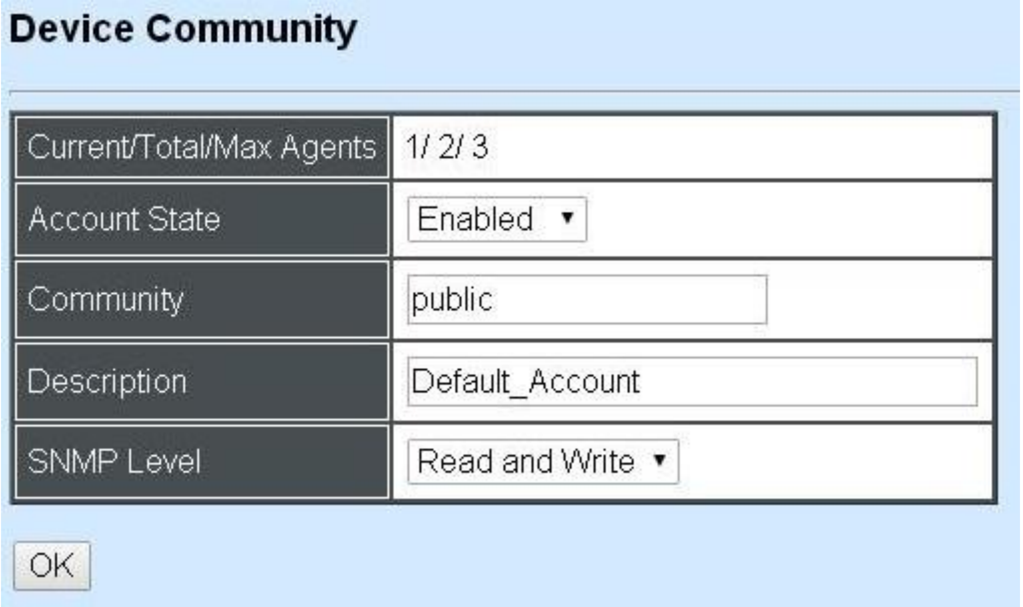
Device Community

Community	Description
public	Default_Account
admin	Default_Account

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

Click **Edit** to view and edit a community setting.

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



Device Community

Current/Total/Max Agents	1/ 2/ 3
Account State	Enabled
Community	public
Description	Default_Account
SNMP Level	Read and Write

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

Current: This shows the number of current community agents.

Total: This shows the total number of the community agents.

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

Account State: Enable or disable the selected account.

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

Description: Enter the description of the community, up to 20 alphanumeric characters.

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

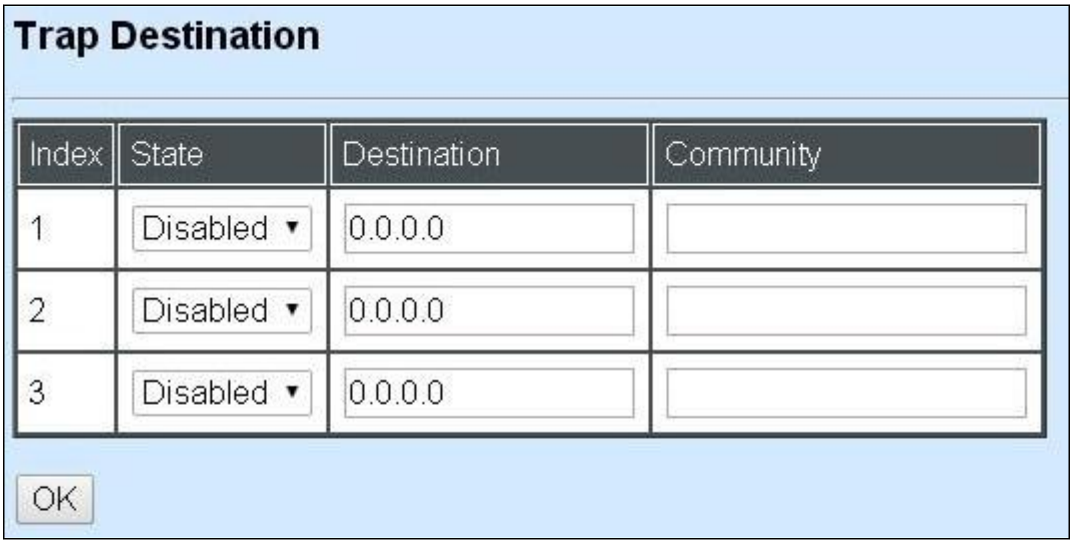
Administrator: Full access right.

Read & Write: Partial access right.

Read Only: Read only access right.

3.3.6 Trap Destination

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



Trap Destination

Index	State	Destination	Community
1	Disabled ▾	0.0.0.0	
2	Disabled ▾	0.0.0.0	
3	Disabled ▾	0.0.0.0	

Index: The index of the SNMP trap destination.

State: Select **Disabled** or **Enabled** for the trap destination.

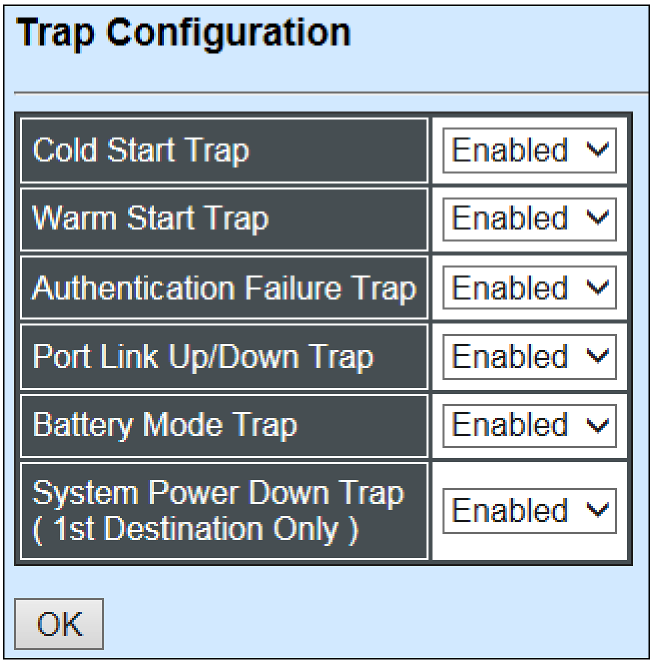
Destination: Set up IP address for the trap destination.

Community: Set up community for the specific trap destination.

Click the **"OK"** button to apply the settings.

3.3.7 Trap Configuration

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



Trap Configuration

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

Cold Start Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Warm Start Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Authentication Failure Trap: Select **Disabled** or **Enabled** for the SNMP trap.

Port Link Up/Down Trap: Select **Disabled** or **Enabled** for the SNMP trap.

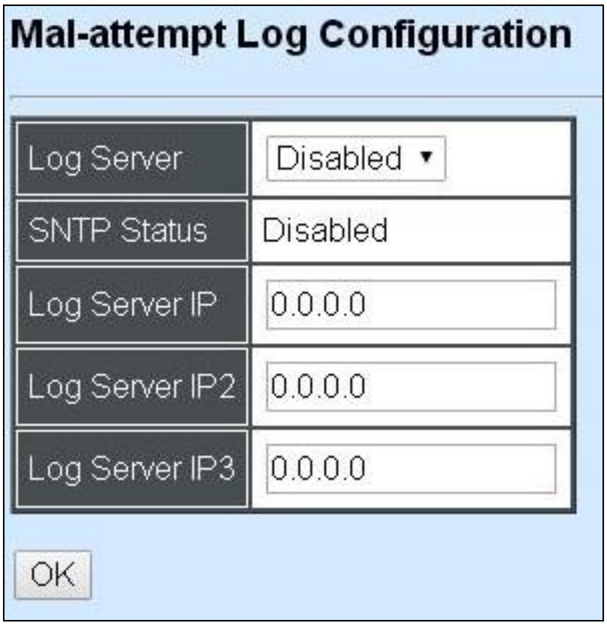
Battery Mode Trap: Select **Disabled** or **Enabled** for the SNMP trap.

System Power Down Trap: Select **Disabled** or **Enabled** for the SNMP trap. This trap will only be sent to 1st trap destination.

Click the **"OK"** button to apply the settings.

3.3.8 Mal-attempt Log Configuration

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



Mal-attempt Log Configuration

Log Server	Disabled ▾
SNTP Status	Disabled
Log Server IP	0.0.0.0
Log Server IP2	0.0.0.0
Log Server IP3	0.0.0.0

Log server: Select **Disabled** or **Enabled** for the Log server.

SNTP Status: View-only filed for the SNTP status.

Log server IP: Set up the first Log server's IP address.

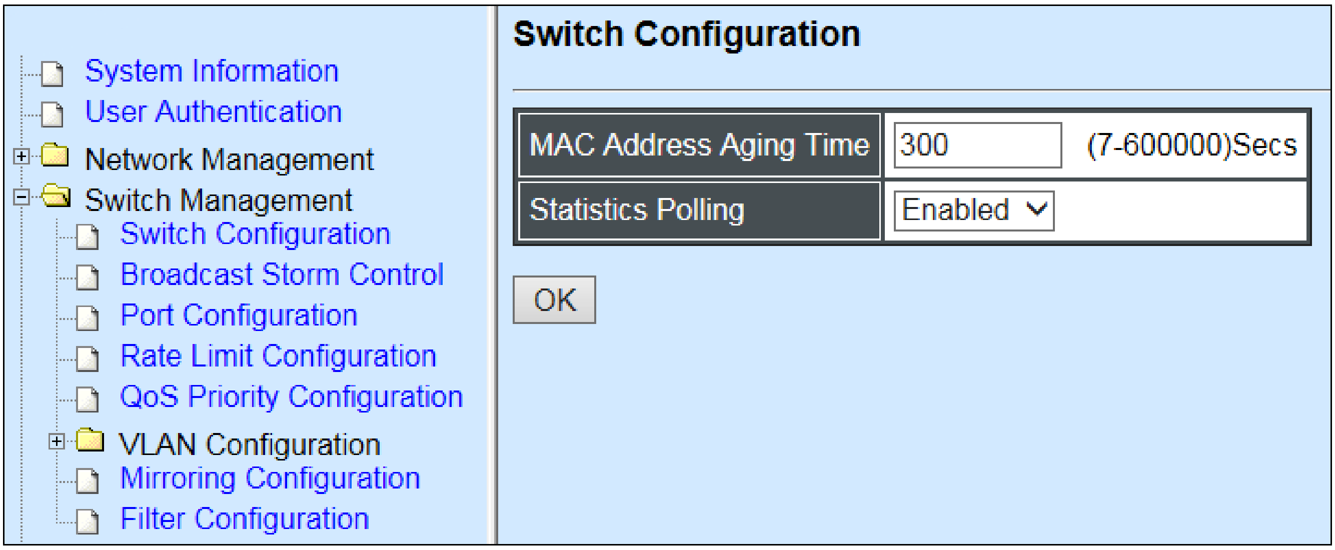
Log server IP2: Set up the second Log server's IP address if needed

Log server IP3: Set up the third Log server's IP address if needed.

Click the **"OK"** button to apply the settings.

3.4 Switch Management

To manage the Gateway Controller 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
Statistics Polling	Enabled

1. **Switch Configuration:** Set up address learning aging time and enable or disable Statistics Polling.

2. **Broadcast Storm Control:** Prevent the Gateway Controller from broadcast storms.

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

4. **Rate Limit Configuration:** Set up Port Rate Limit.

5. **QoS Priority Configuration:** Set up QoS Priority based on Port-based, IEEE 802.1p and DSCP…etc.

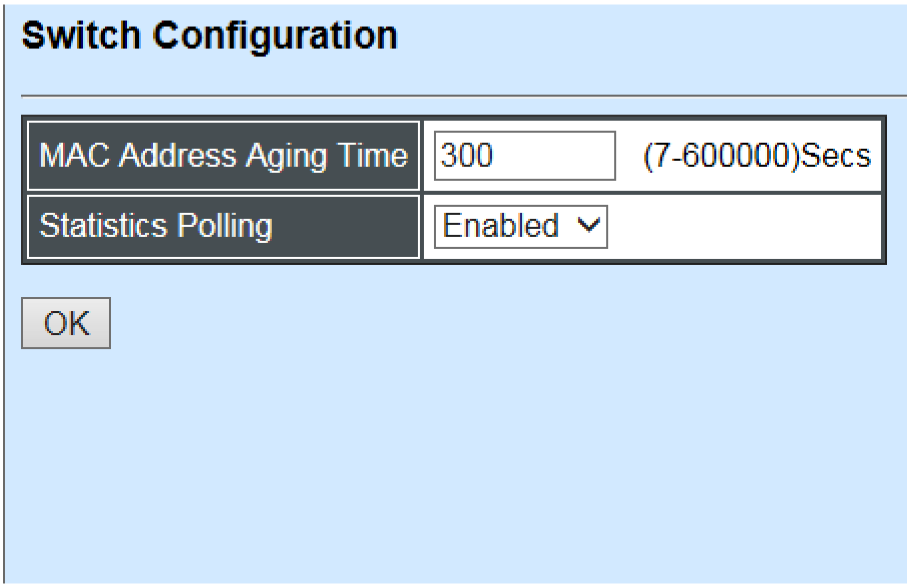
6. **VLAN Configuration:** Set up Port-Based VLAN and IEEE 802.1q Tag VLAN.

7. **Mirroring Configuration:** Set up Target Port to mirror Source Port and enable traffic monitoring

8. **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
Statistics Polling	Enabled

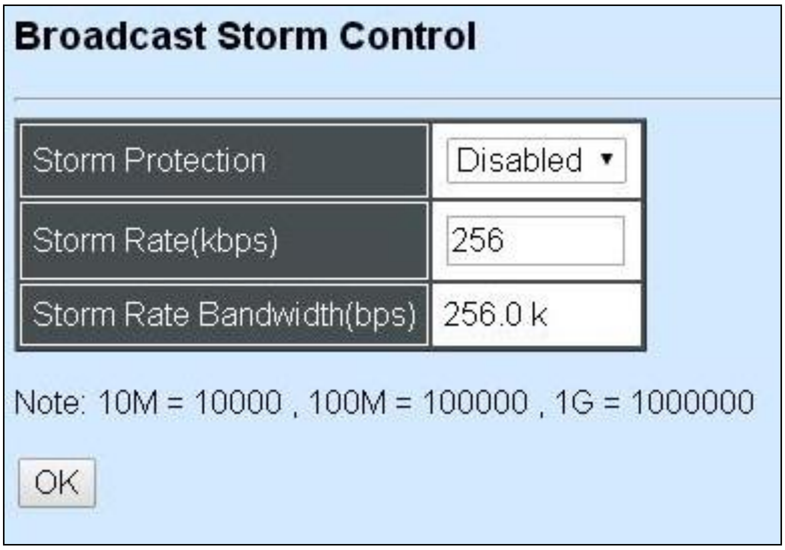
MAC Address Aging Time: Set up MAC Address aging time manually. Entries in the MAC address table containing source MAC addresses and their associated ports will be deleted if they are not accessed within the aging time.

Statistics Polling: Enable or disable Statistics Polling.

Click the **"OK"** button to apply the settings.

3.4.2 Broadcast Storm Control

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



Broadcast Storm Control

Storm Protection	Disabled
Storm Rate(kbps)	256
Storm Rate Bandwidth(bps)	256.0 k

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

Storm Protection: Enable or disable Storm Protection function.

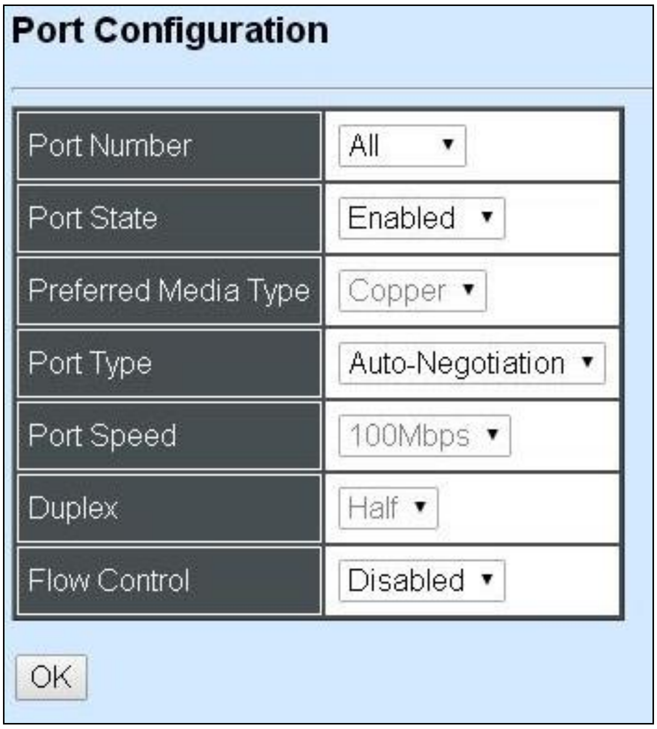
Storm Rate(kbps): Set up storm rate value. Packets exceeding the value will be dropped. (The Storm Rate range can be configured within 32~1000000kbps)

Storm Rate Bandwidth(bps): 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	100Mbps ▾
Duplex	Half ▾
Flow Control	Disabled ▾

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

Port State: Enable or disable the current port state.

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).

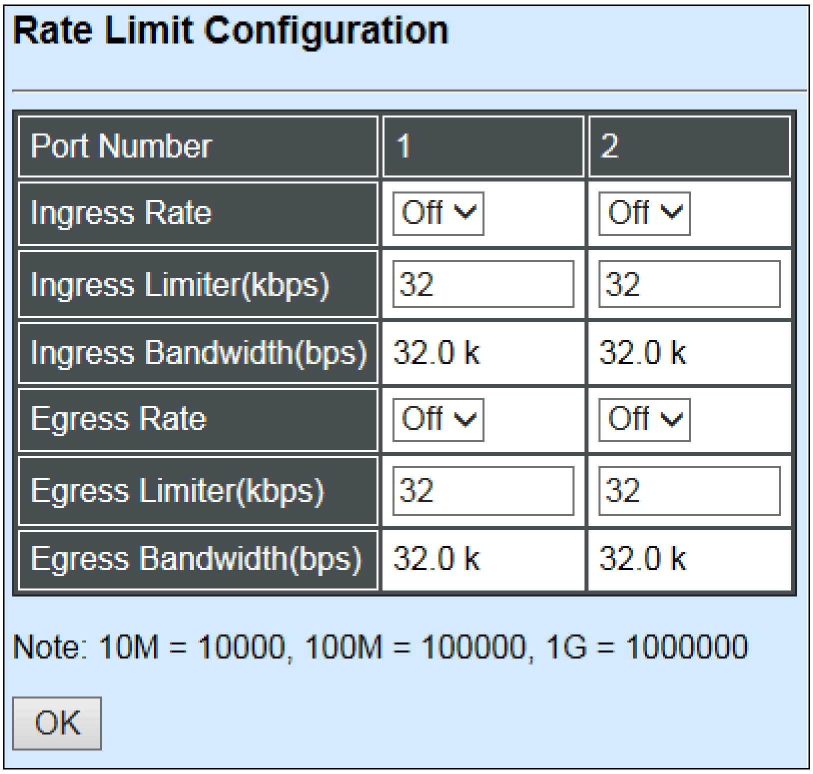
Duplex: When you select Manual port type, you can further specify the current operation Duplex mode (full or half duplex) of the port(s).

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
Ingress Rate	Off	Off
Ingress Limiter(kbps)	32	32
Ingress Bandwidth(bps)	32.0 k	32.0 k
Egress Rate	Off	Off
Egress Limiter(kbps)	32	32
Egress Bandwidth(bps)	32.0 k	32.0 k

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

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).

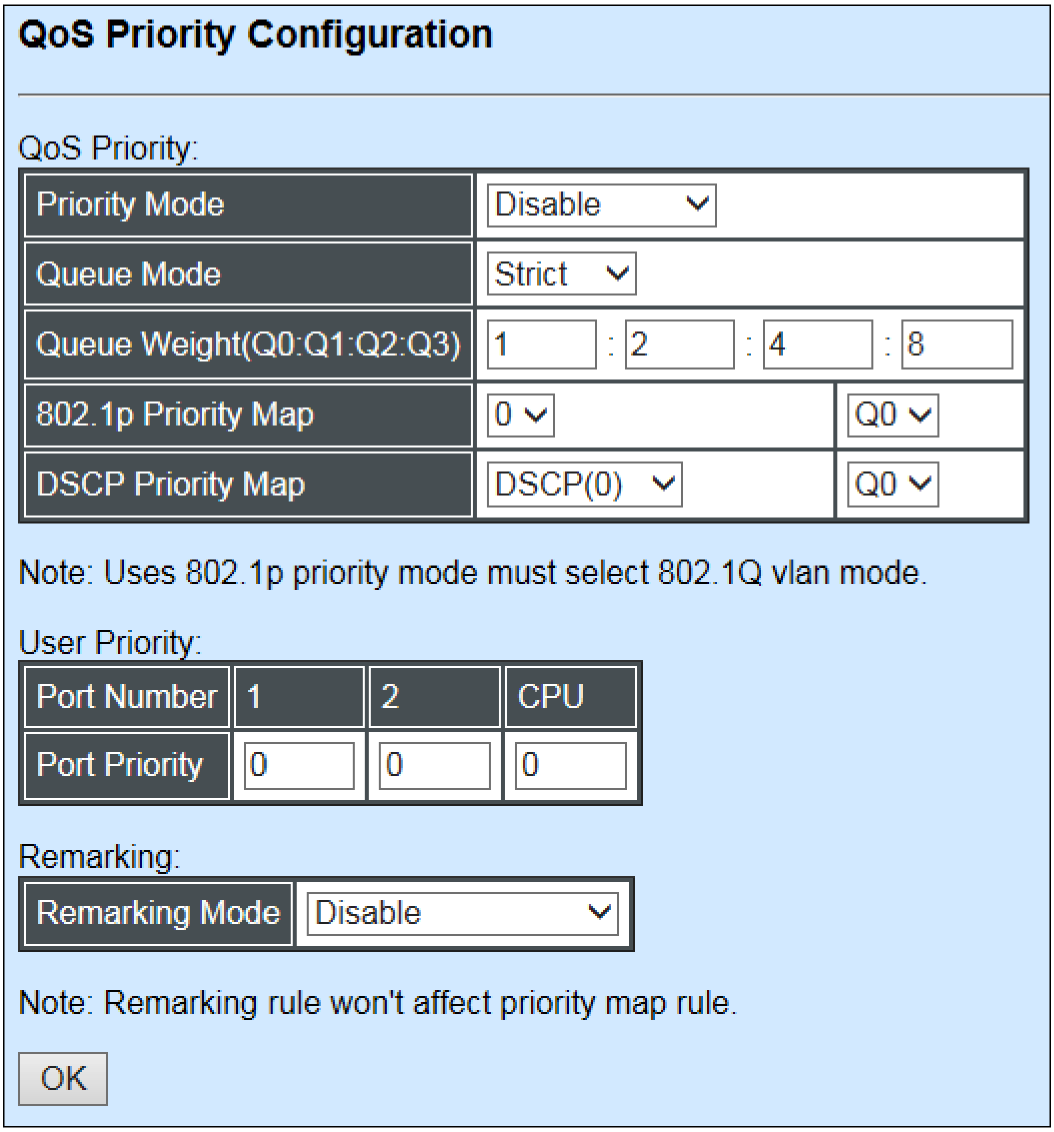
Egress Bandwidth (Kbps): Display current configured egress bandwidth.

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	Disable	
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 select 802.1Q vlan mode.

User Priority:

Port Number	1	2	CPU
Port Priority	0	0	0

Remarking:

Remarking Mode	Disable

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

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.

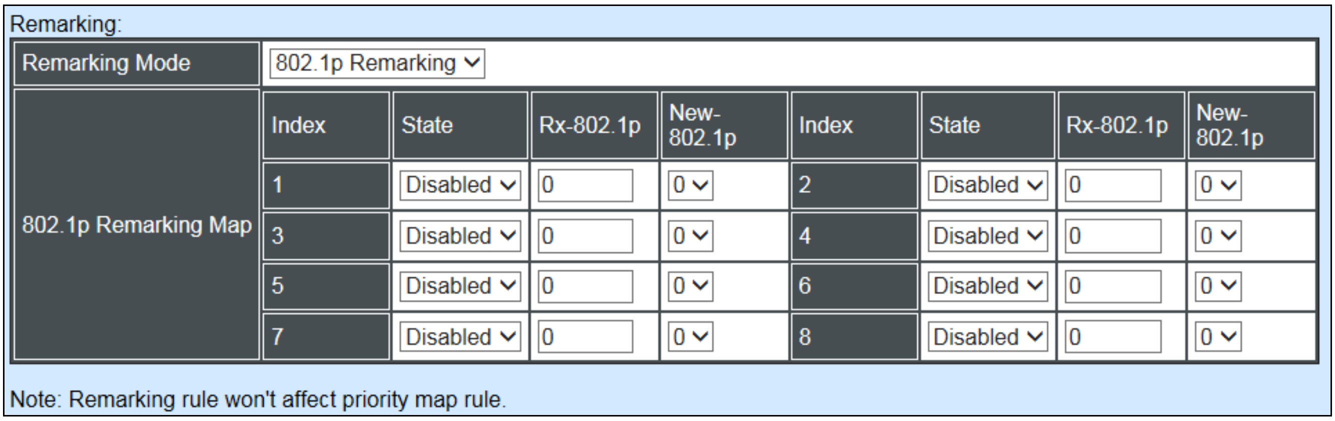
Note: *802.1p priority mode can only be applied under 802.1q VLAN mode.*

User Priority: Select priority queue for ingress traffic per-port.

Remarking

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

➢ 802.1p Remarking



Remarking:

Remarking Mode	802.1p Remarking ⌄							
802.1p Remarking Map	Index	State	Rx-802.1p	New-802.1p	Index	State	Rx-802.1p	New-802.1p
	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 ⌄

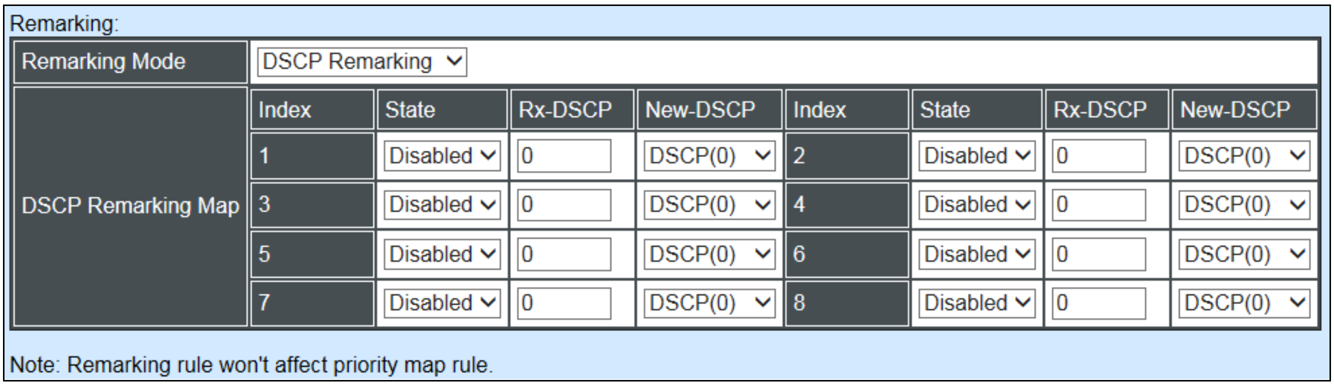
Note: Remarking rule won't affect priority map rule.

State: Disable or enable the mapping entry.

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

New-802.1p: Specify the remarking 802.1p value.

- **DSCP Remarking:** Enable or disable DSCP Remarking.



Remarking:

Remarking Mode	DSCP Remarking							
DSCP Remarking Map	Index	State	Rx-DSCP	New-DSCP	Index	State	Rx-DSCP	New-DSCP
	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)

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

State: Disable or enable the mapping entry.

Rx-DSCP: Specify the DSCP value to be remarked.

New-DSCP: 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

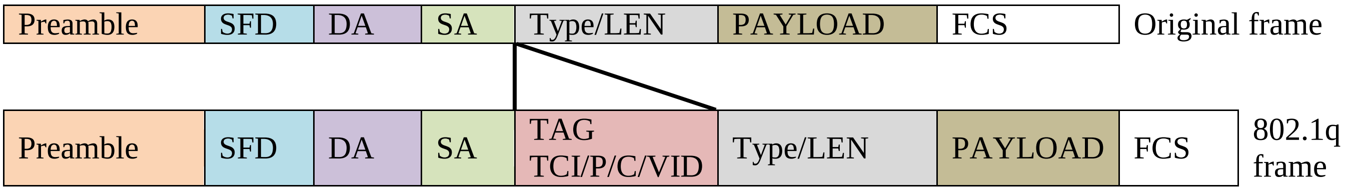
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collections of LAN segments into a group that appears as a single LAN. VLAN also logically segments the network into different broadcast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

IEEE 802.1Q VLAN Concepts

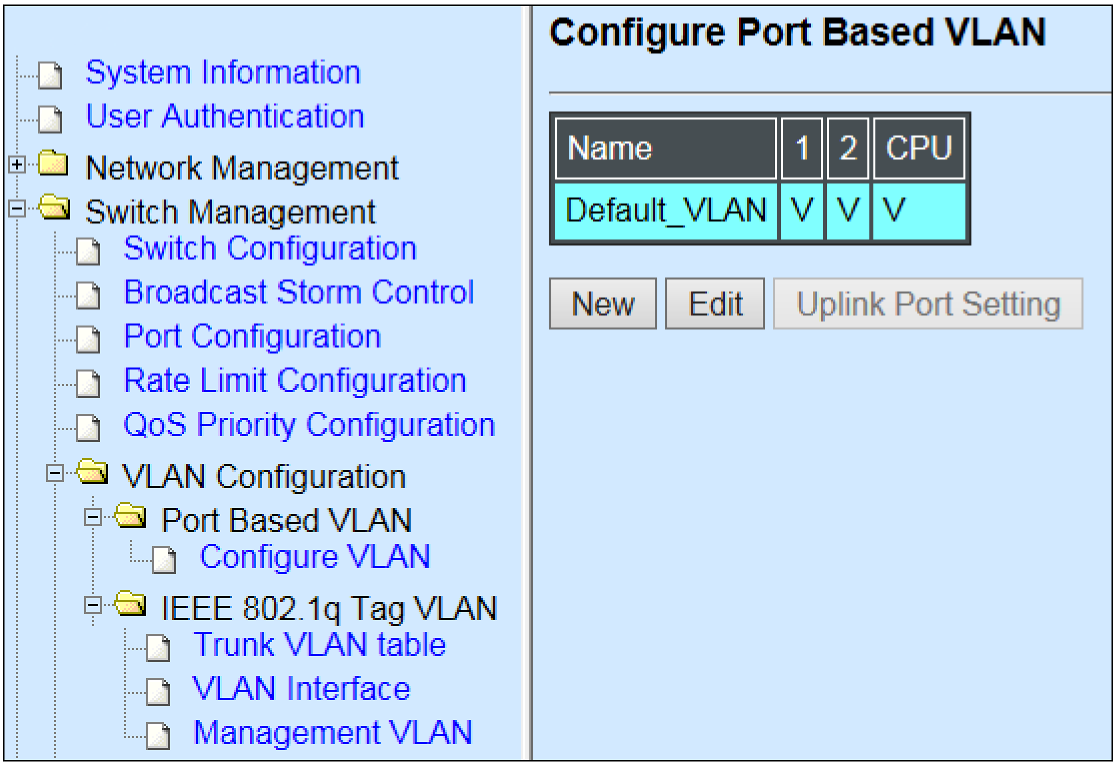
Introduction to 802.1Q frame format:



Preamble	SFD	DA	SA	Type/LEN	PAYLOAD	FCS		Original frame
Preamble	SFD	DA	SA	TAG TCI/P/C/VID	Type/LEN	PAYLOAD	FCS	802.1q frame

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.



Configure Port Based VLAN

Name	1	2	CPU
Default_VLAN	V	V	V

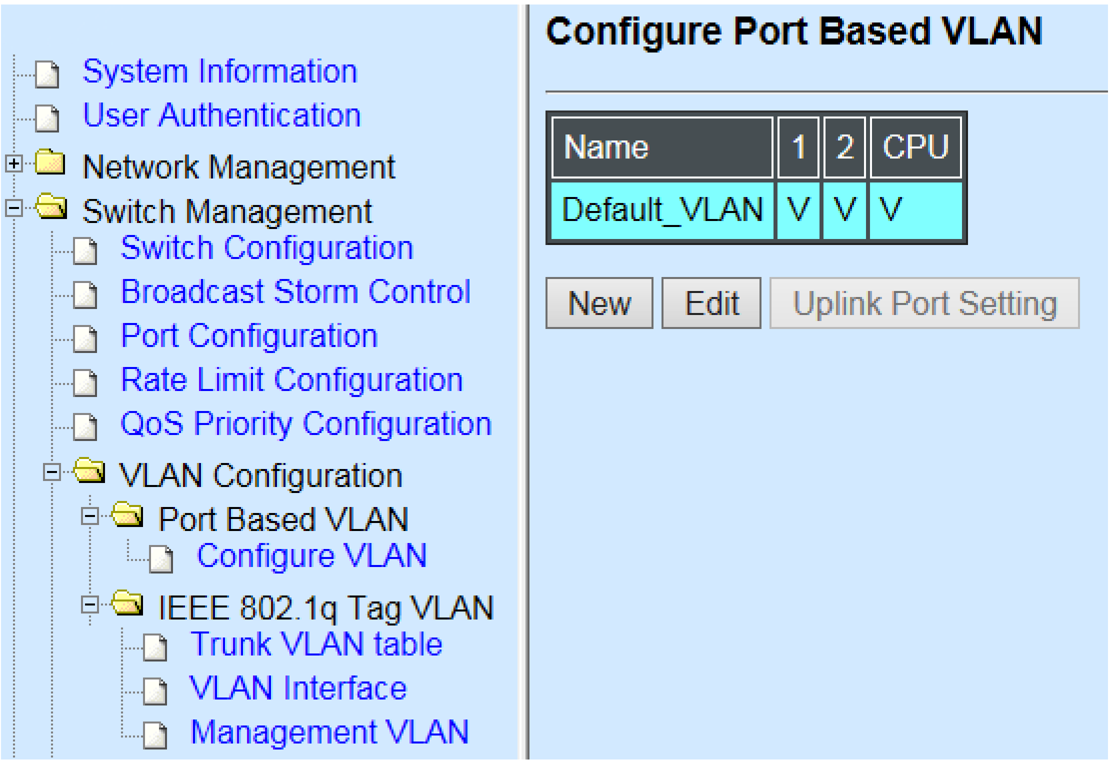
1. Port Based VLAN: Configure Port-Based VLAN settings.

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

3.4.6.1 Port Based VLAN

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

The following screen page appears when you choose **Port-Based VLAN** mode and then select **Configure VLAN**.



Configure Port Based VLAN

Name	1	2	CPU
Default_VLAN	V	V	V

Since source addresses of the packets are listed in MAC address table of specific VLAN (except broadcast/multicast packets), in every VLAN the traffic between two ports will be two-way without restrictions.

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

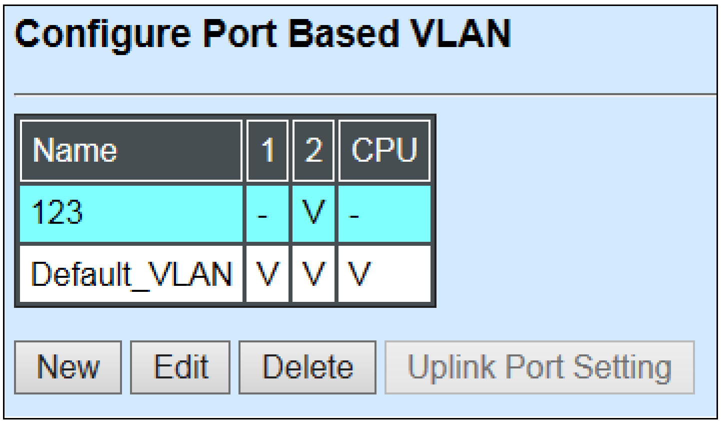
Use **Edit** to view and edit the current VLAN setting.

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

Click **Uplink Port Setting** to configure uplink port members.

3.4.6.1.1 Configure Port Based VLAN

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

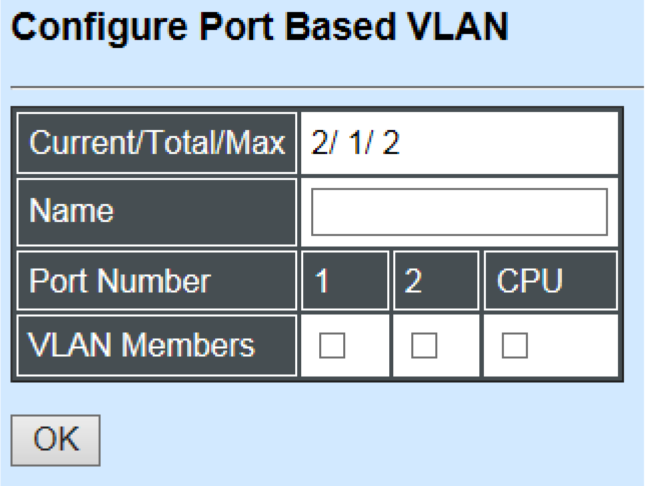


Configure Port Based VLAN

Name	1	2	CPU
123	-	V	-
Default_VLAN	V	V	V

Click **New** or **Edit** to add, view and edit current Port Based VLAN setting, and then the following screen page appears.

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



Configure Port Based VLAN

Current/Total/Max	2/ 1/ 2		
Name			
Port Number	1	2	CPU
VLAN Members	□	□	□

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

Current/Total/Max: View-only field that shows the name of the port based VLAN.

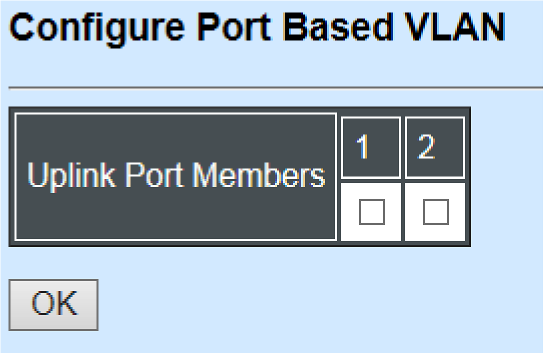
Current: This shows the number of current VLAN.

Total: This shows the total number of the VLANs.

Max: This shows the maximum number available for configuration. The maximum number is 2.

Port Number & VLAN Members: Assign the port to VLAN member.

Uplink Port Setting: Click **Uplink Port Setting** to configure uplink port members.



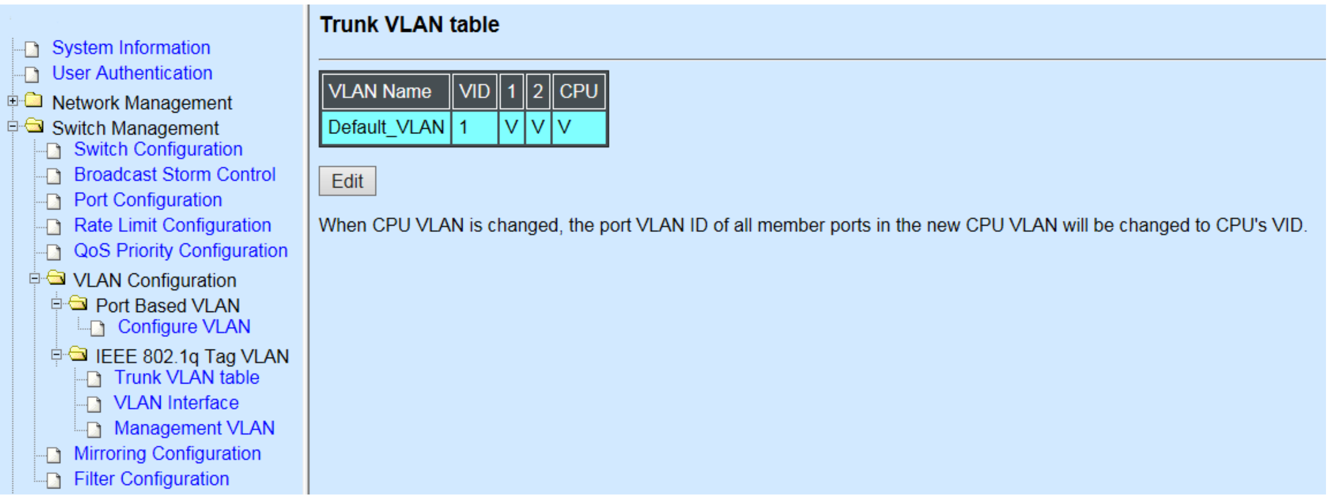
Configure Port Based VLAN

Uplink Port Members	1	2
	□	□

Check the box you want and click **"OK"**

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.



Trunk VLAN table

VLAN Name	VID	1	2	CPU
Default_VLAN	1	V	V	V

When CPU VLAN is changed, the port VLAN ID of all member ports in the new CPU VLAN will be changed to CPU's VID.

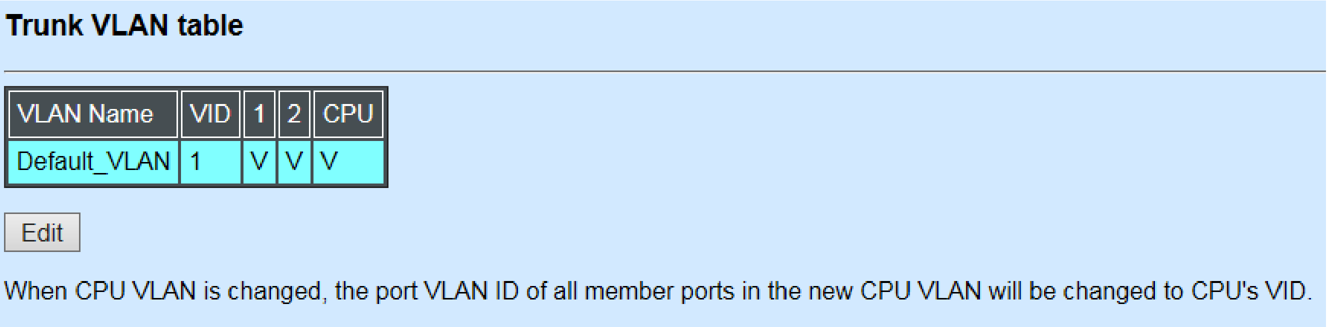
Trunk VLAN table: To edit or apply 802.1Q Tag VLAN settings.

VLAN Interface: To globally set up switch VLAN mode and per port VLAN mode.

Management VLAN: To set up management VLAN and management port(s).

3.4.6.2.1 Trunk VLAN Table

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



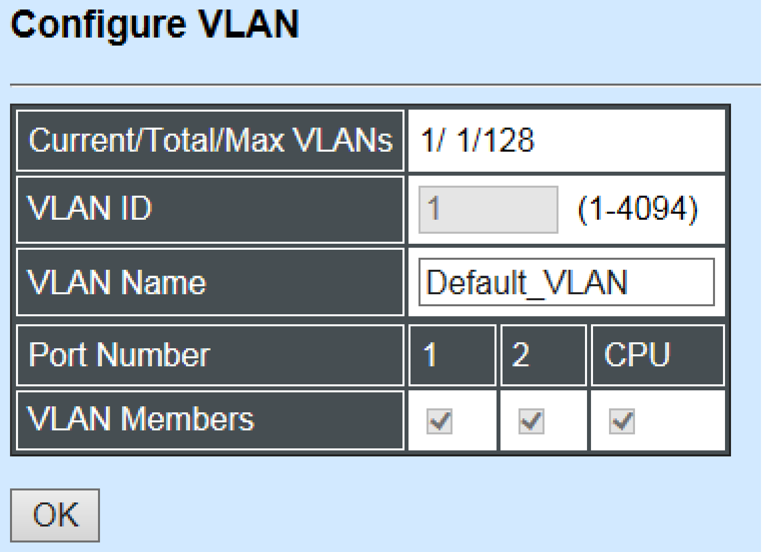
Trunk VLAN table

VLAN Name	VID	1	2	CPU
Default_VLAN	1	V	V	V

When CPU VLAN is changed, the port VLAN ID of all member ports in the new CPU VLAN will be changed to CPU's VID.

Click **Edit** to view and edit current IEEE 802.1Q Tag VLAN setting and then the following screen page appears.

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



Configure VLAN

Current/Total/Max VLANs	1/ 1/128		
VLAN ID	1 (1-4094)		
VLAN Name	Default_VLAN		
Port Number	1	2	CPU
VLAN Members	☑	☑	☑

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 concurrent VLANs to be registered.

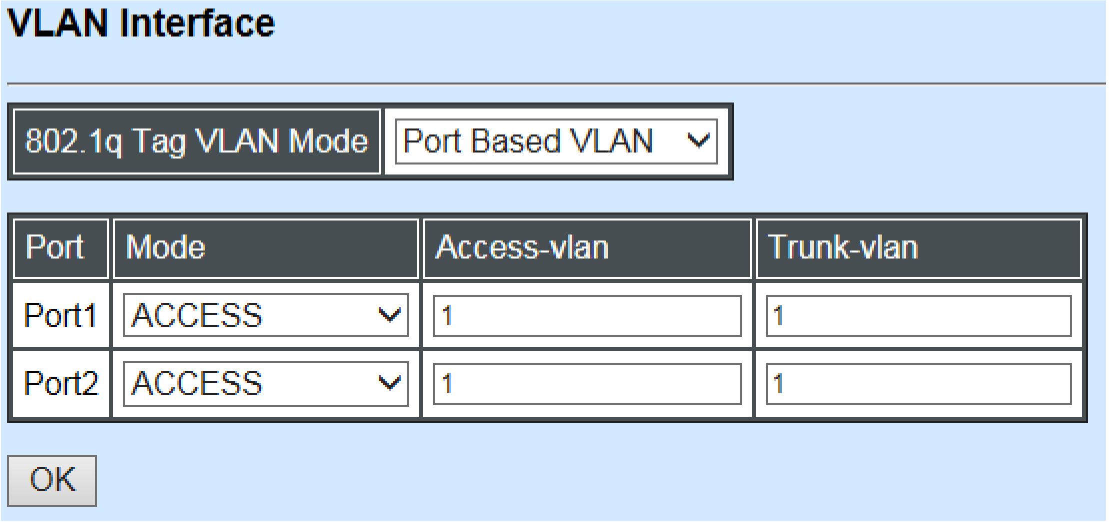
VLAN ID: the ID for the currently registered VLAN.

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

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

3.4.6.2.2 VLAN Interface

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



VLAN Interface

802.1q Tag VLAN Mode: Port Based VLAN

Port	Mode	Access-vlan	Trunk-vlan
Port1	ACCESS	1	1
Port2	ACCESS	1	1

802.1q Tag VLAN Mode: Four options are available, Port Based VLAN, IEEE 802.1q VLAN and Port isolation.

Mode: To specify VLAN mode for each port. Three options are available, ACCESS, TRUNK, TRUNK NATIVE.

Access-VLAN: To specify Access-VLAN ID(PVID) for each port.

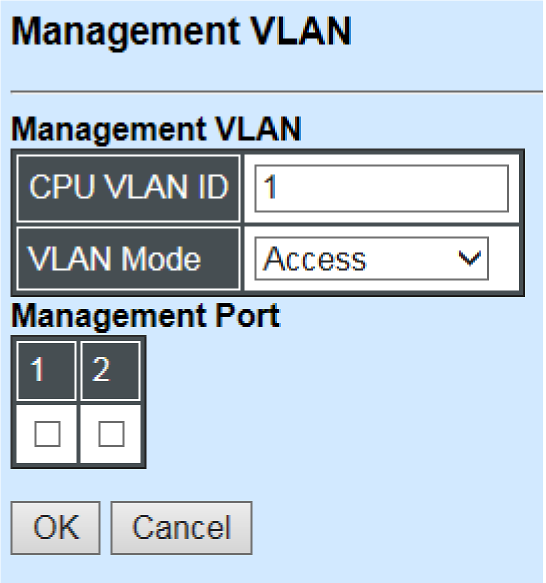
Trunk-VLAN: To specify Trunk-VLAN ID(802.1q tag) for each port. Use "-" or "," to assign multiple VIDs. EX: 1-4 or 1,2,3,4.

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 Management VLAN

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



Management VLAN

Management VLAN

CPU VLAN ID	1
VLAN Mode	Access

Management Port

1	2
□	□

CPU VLAN ID: To assign current VID for CPU (management)

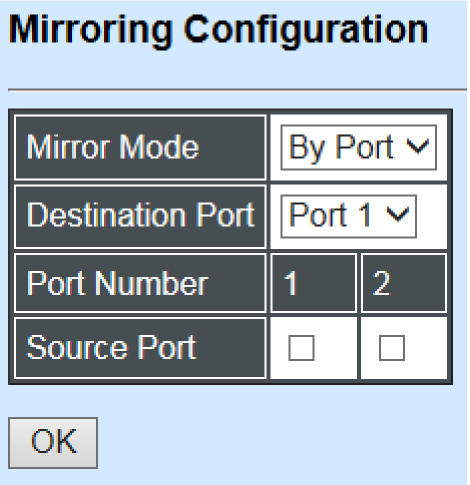
VLAN Mode: To specify VLAN mode for management VLAN. Three options are available, ACCESS, TRUNK, TRUNK NATIVE.

Management Port: To specify port(s) for management.

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.



Mirroring Configuration

Mirror Mode	By Port	
Destination Port	Port 1	
Port Number	1	2
Source Port	□	□

Mirror Mode: Either **disabled** or **By Port**.

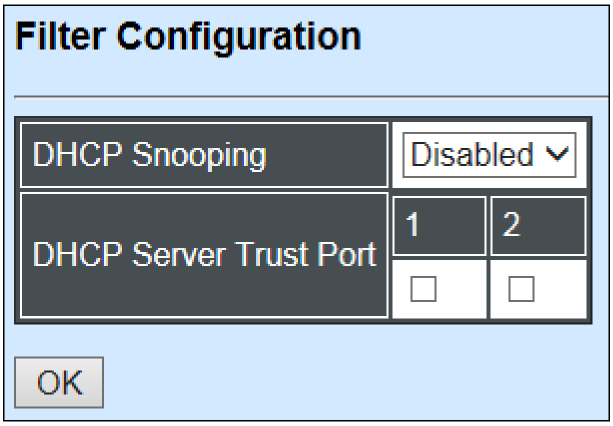
Destination Port: Specify the port to which the traffic will be mirrored to.

Source Port: Specify the port(s) to which the traffic will be mirrored from as a source.

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

3.4.8 Filter Configuration

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



Filter Configuration

DHCP Snooping	Disabled	
DHCP Server Trust Port	1	2
	□	□

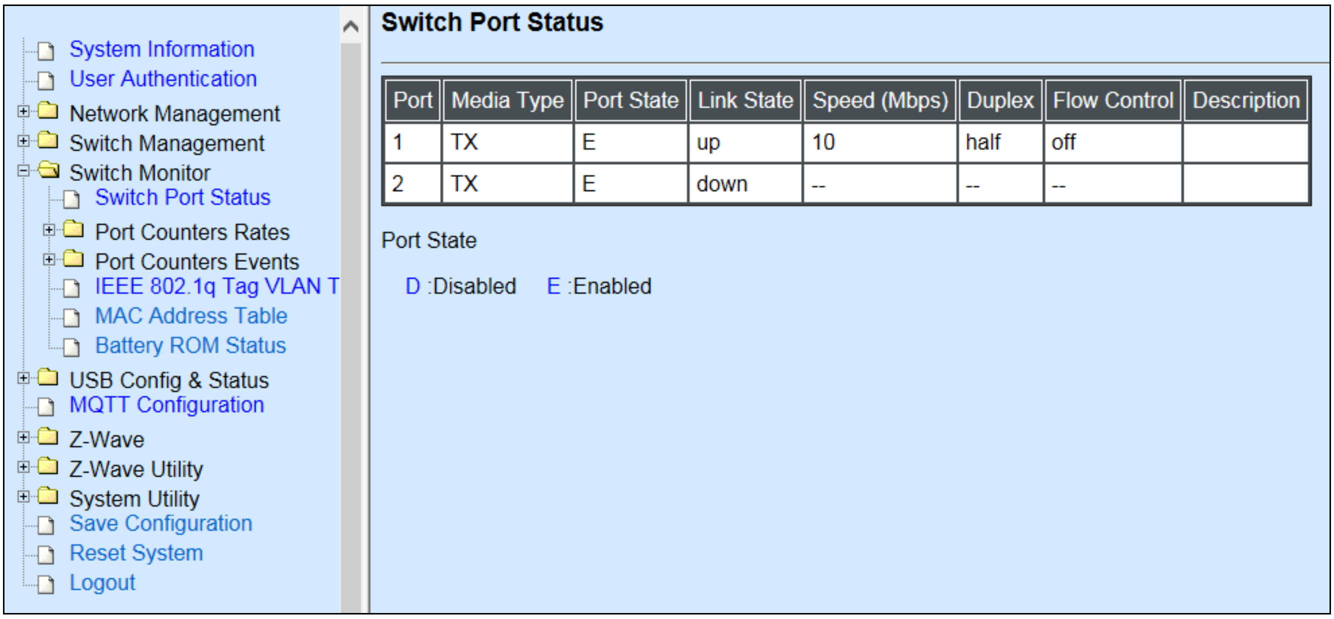
DHCP Snooping: Enable or disable DHCP Snooping function.

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 Gateway Controller. Users may monitor the port link-up status or traffic counters for maintenance or diagnostic purposes. Select the folder **Switch Monitor** from the **Main Menu** and then the following screen page appears.



Switch Port Status

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	E	up	10	half	off	
2	TX	E	down	--	--	--	

Port State

D :Disabled   E :Enabled

1. **Switch Port Status:** 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).

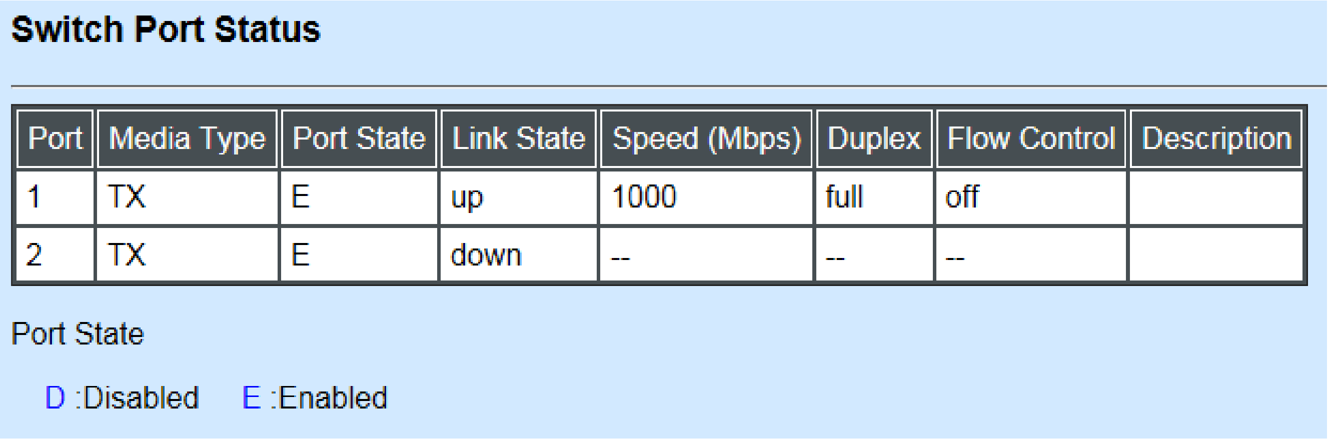
4. **IEEE 802.1q Tag VLAN Table:** View the current IEEE 802.1q Tag VLAN Table.

5. **MAC Address Table:** List current MAC addresses learned by the Gateway Controller.

6. **Battery ROM Status:** The information regarding the battery connected.

3.5.1 Switch Port Status

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



Switch Port Status

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control	Description
1	TX	E	up	1000	full	off	
2	TX	E	down	--	--	--	

Port State

D :Disabled   E :Enabled

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 **E** (Enabled).

Disabled: A port in this state cannot receive and forward packets.

Enabled: 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.

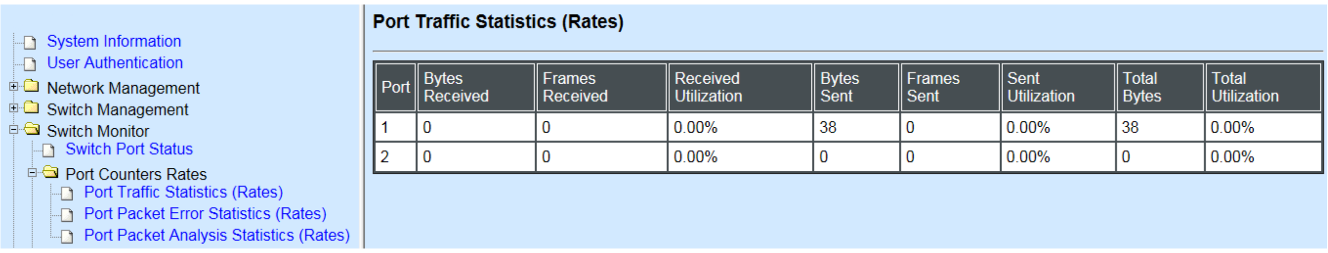
Duplex: The current operation Duplex mode of each port, either Full or Half.

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.



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%	38	0	0.00%	38	0.00%
2	0	0	0.00%	0	0	0.00%	0	0.00%

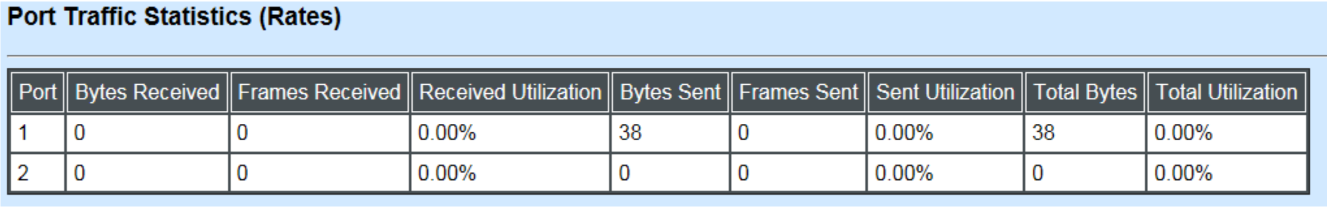
1. **Port Traffic Statistics (Rates):** View the number of bytes received, frames received, bytes sent, frames sent, and total bytes.

2. **Port Packet Error Statistics (Rates):** View the number of CRC errors, undersize frames, oversize frames…etc.

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

3.5.2.1 Port Traffic Statistics (Rates)

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



Port Traffic Statistics (Rates)

Port	Bytes Received	Frames Received	Received Utilization	Bytes Sent	Frames Sent	Sent Utilization	Total Bytes	Total Utilization
1	0	0	0.00%	38	0	0.00%	38	0.00%
2	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.

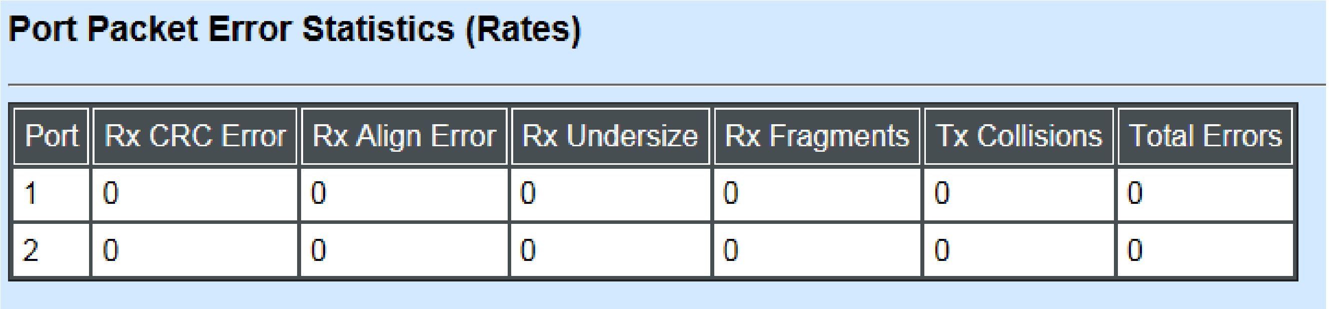
Sent Utilization: The ratio of each port's sending traffic to current port's total bandwidth.

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	Tx Collisions	Total Errors
1	0	0	0	0	0	0
2	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.

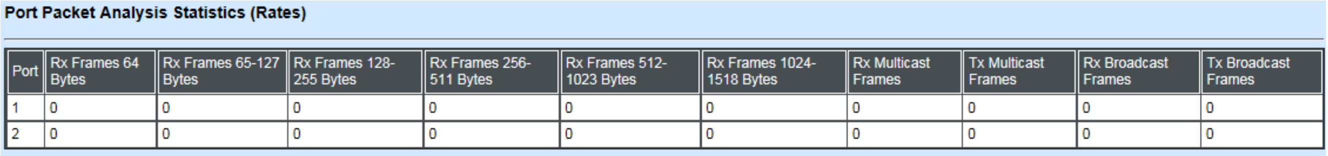
RX Fragments: Fragment frames received.

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 65-127 Bytes	Rx Frames 128-255 Bytes	Rx Frames 256-511 Bytes	Rx Frames 512-1023 Bytes	Rx Frames 1024-1518 Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

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

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

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

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

RX Frames 1024-1518 Bytes: 1024-1518 bytes frames received.

RX Multicast Frames: Good multicast frames received.

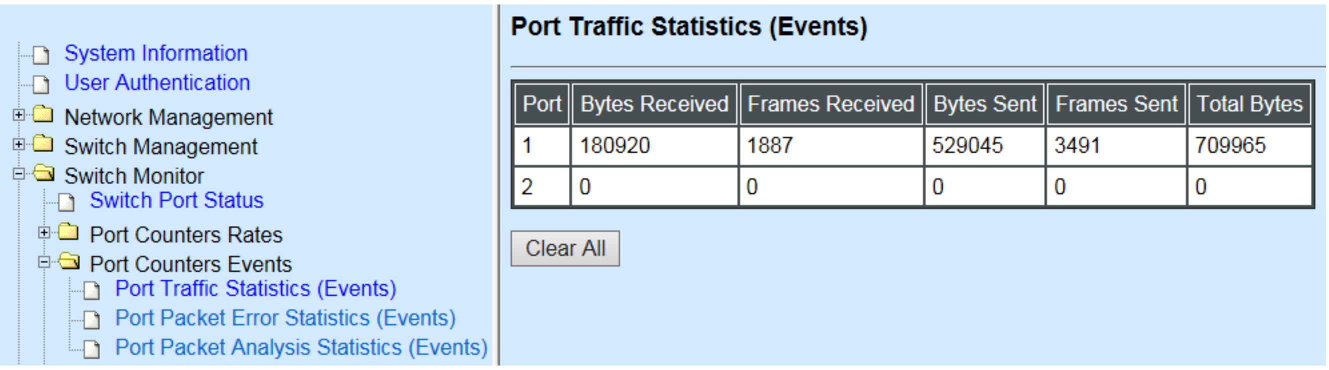
TX Multicast Frames: Good multicast packets sent.

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 Traffic Statistics (Events)

Port	Bytes Received	Frames Received	Bytes Sent	Frames Sent	Total Bytes
1	180920	1887	529045	3491	709965
2	0	0	0	0	0

1. **Port Traffic Statistics (Events):** View the number of bytes received, frames received, bytes sent,

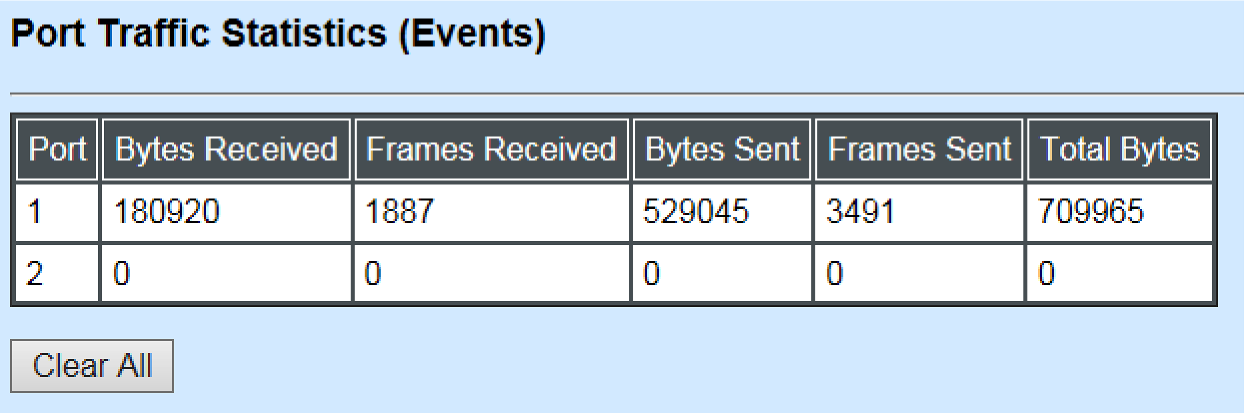
frames sent, and total bytes and clear each row's statistics.

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	180920	1887	529045	3491	709965
2	0	0	0	0	0

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.

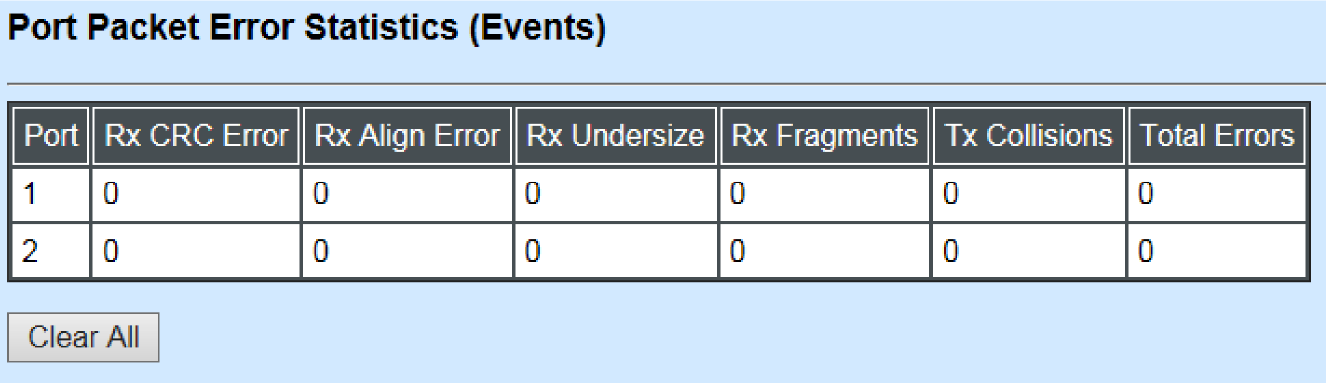
Frames Sent: The total frames sent from current port.

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	Tx Collisions	Total Errors
1	0	0	0	0	0	0
2	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.

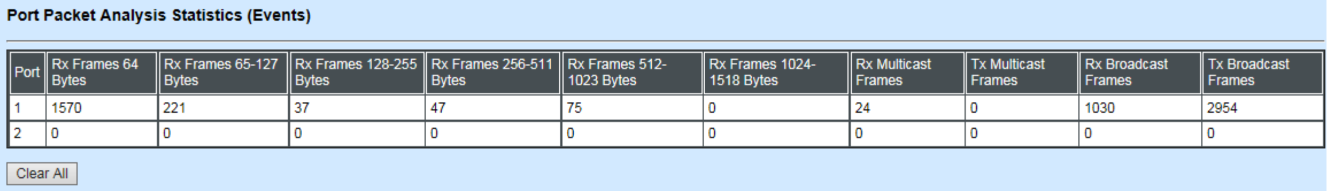
TX Collisions: Total frames collision detected.

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 65-127 Bytes	Rx Frames 128-255 Bytes	Rx Frames 256-511 Bytes	Rx Frames 512-1023 Bytes	Rx Frames 1024-1518 Bytes	Rx Multicast Frames	Tx Multicast Frames	Rx Broadcast Frames	Tx Broadcast Frames
1	1570	221	37	47	75	0	24	0	1030	2954
2	0	0	0	0	0	0	0	0	0	0

RX Frames 64 Bytes: 64 bytes frames received.

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

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

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

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

RX Frames 1024-1518 Bytes: 1024-1518 bytes frames received.

RX Multicast Frames: Good multicast frames received.

TX Multicast Frames: Good multicast packets sent.

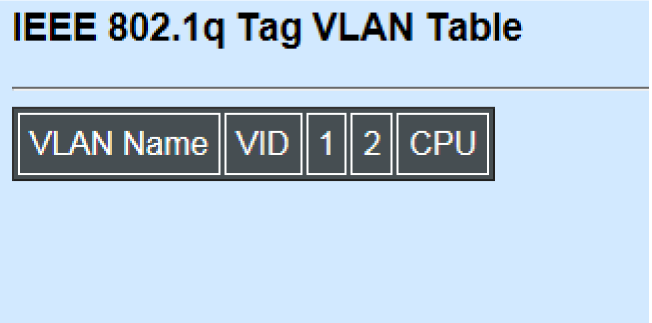
RX Broadcast Frames: Good broadcast frames received.

TX Broadcast Frames: Good broadcast packets sent.

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

3.5.4 IEEE 802.1q Tag VLAN Table

Select **IEEE 802.1q Tag VLAN Table** from the **Switch Monitor** menu and then the following screen page appears.



IEEE 802.1q Tag VLAN Table

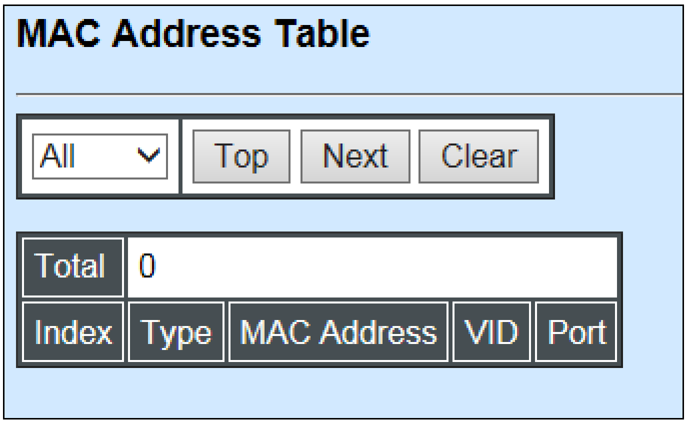
VLAN Name	VID	1	2	CPU

VLAN Name: View-only filed that shows the VLAN name.

VID: View-only filed that shows the VID.

3.5.5 MAC Address Table

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



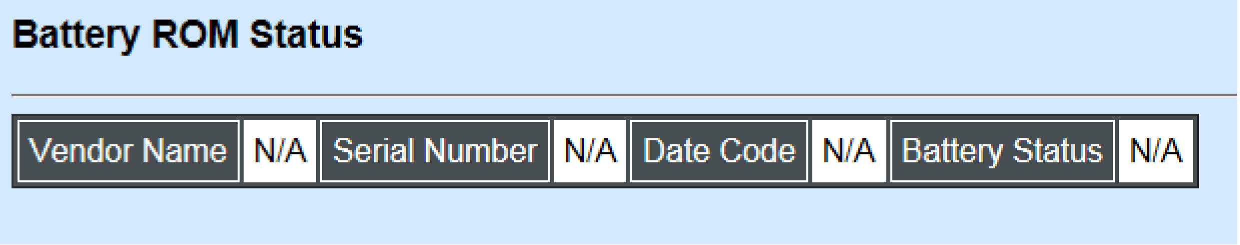
MAC Address Table

Total	0			
Index	Type	MAC Address	VID	Port

The table above shows the MAC addresses learned from each port of the Gateway Controller.

3.5.6 Battery ROM Status

This is to show the information regarding the battery connected. Click the **Battery ROM Status** in **Switch Monitor** folder and then the following screen page appears.



Battery ROM Status

Vendor Name	N/A	Serial Number	N/A	Date Code	N/A	Battery Status	N/A

Vendor Name: The manufacturer who make the battery.

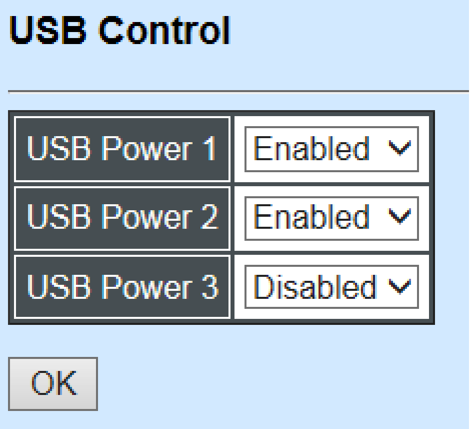
Serial Number: An identification number for the battery.

Date Code: The date of manufacture.

Battery Status: The current status of battery.

3.6 USB Config & Status

It shows the current USB port availability. Click the **USB Control** in **USB Config & Status** folder and then the following screen page appears.



USB Control

USB Power 1	Enabled
USB Power 2	Enabled
USB Power 3	Disabled

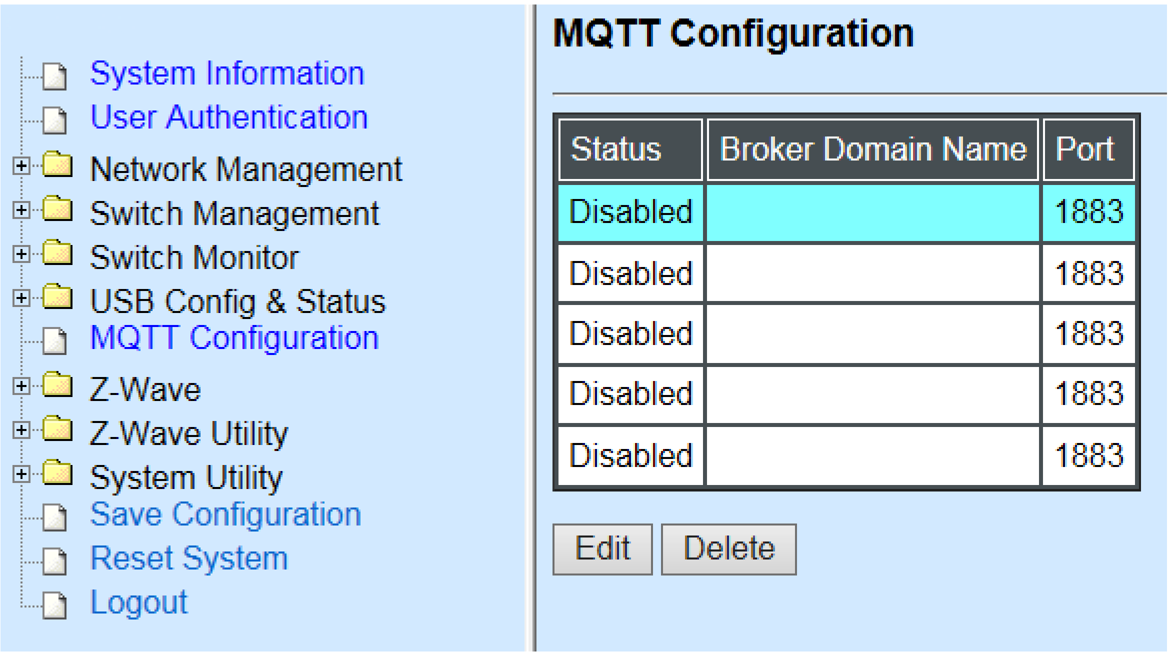
USB Power 1: Click “Enabled” to activate the USB Port 1 or “Disabled” to deactivate it. The default setting is “Enabled”.

USB Power 2: Click “Enabled” to activate the USB Port 2 or “Disabled” to deactivate it. The default setting is “Enabled”.

USB Power 3: Click “Enabled” to activate the USB Port 3 or “Disabled” to deactivate it. The default setting is “Disabled”.

3.7 MQTT Configuration

Message Queue Telemetry Transport (MQTT) is a Client Server publish/subscribe messaging transport protocol. It is light weight, open, simple, and designed so as to be easy to implement. These characteristics make it ideal for use in many situations, including constrained environments such as for communication in Machine to Machine (M2M) and Internet of Things (IoT) contexts where a small code footprint is required and/or network bandwidth is at a premium.

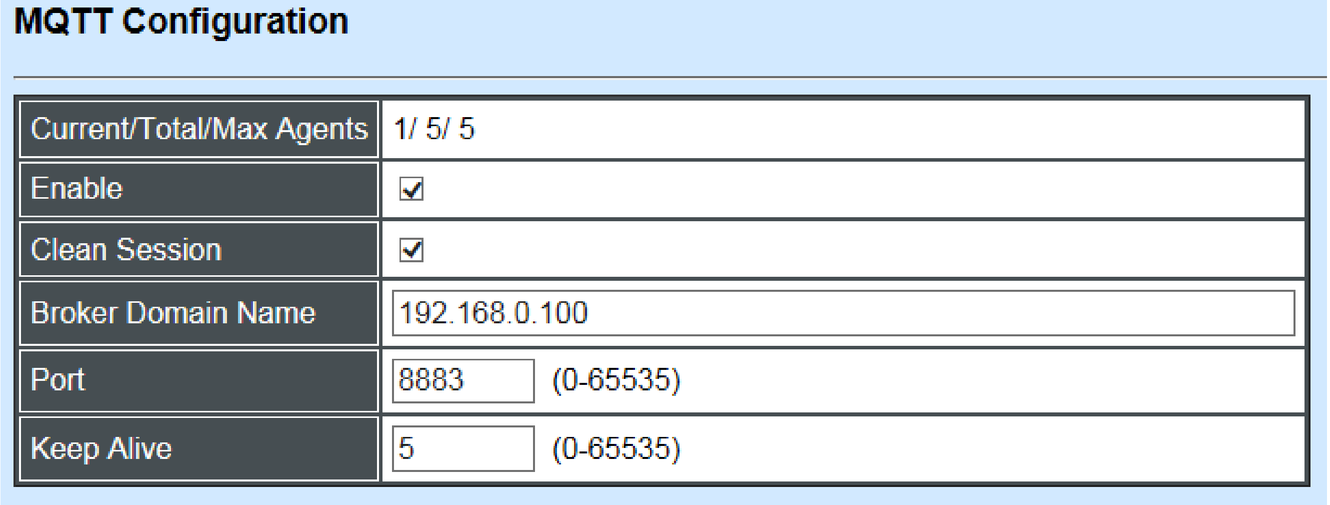


MQTT Configuration

Status	Broker Domain Name	Port
Disabled		1883
Disabled		1883
Disabled		1883
Disabled		1883
Disabled		1883

Click **“Delete”** to erase a setting.

Click **“Edit”** for further settings and the following screen appears.



MQTT Configuration

Current/Total/Max Agents	1/ 5/ 5
Enable	☑
Clean Session	☑
Broker Domain Name	192.168.0.100
Port	8883 (0-65535)
Keep Alive	5 (0-65535)

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

Current: This shows the number of currently registered accounts.

Total: This shows the number of total registered accounts.

Max: This shows the number of maximum number available for registration. The default maximum number is 5.

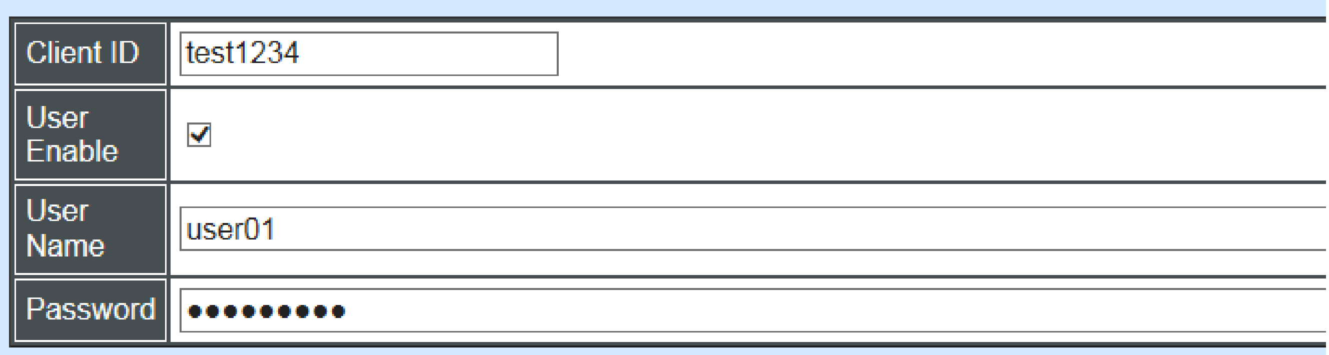
Enable: Check to enable MQTT function or vice versa. The default setting is disable.

Clean Session: The clean session flag indicates the broker, whether the client wants to establish a persistent session or not**.** A persistent session (CleanSession is false) means, that the broker will store all subscriptions for the client and also all missed messages, when subscribing with Quality of Service (QoS) 1 or 2. If clean session is set to true, the broker won't store anything for the client and will also purge all information from a previous persistent session.

Broker Domain Name: Assign a domain name, IP address or website typically, to the broker. The broker is primarily responsible for receiving all messages, filtering them, decide who is interested in it and then sending the message to all subscribed clients.

Port: This refers to a list of Internet socket port numbers used by protocols of the transport layer of the Internet Protocol Suite for the establishment of host-to-host connectivity. The configurable range is 0 ~ 65535.

Keep Alive: The keep alive is a time interval, the clients commits to by sending regular PING Request messages to the broker. The broker response with PING Response and this mechanism will allow both sides to determine if the other one is still alive and reachable. "0" refers to "disable". The default setting is 5.



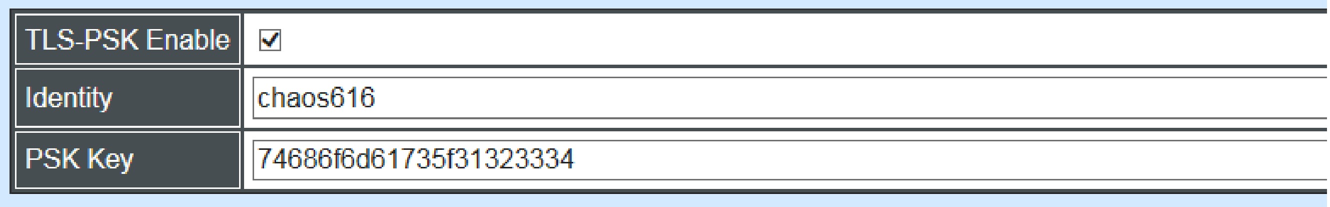
Client ID	test1234
User Enable	☑
User Name	user01
Password	●●●●●●●●●

Client ID: The client identifier (short Client ID) is an identifier of each MQTT client connecting to a MQTT broker. Specify the client identifier name, up to 23 alphanumeric characters

User Enable: Check to activate the account or vice versa.

User Name: Specify the authorized user login name, up to 255 alphanumeric characters

Password: Enter the desired user password, up to 255 alphanumeric characters.



TLS-PSK Enable	☑
Identity	chaos616
PSK Key	74686f6d61735f31323334

TLS-PSK Enable: Transport Layer Security pre-shared key ciphersuites (TLS-PSK) is a set of cryptographic protocols that provide secure communication based on pre-shared keys (PSKs). These pre-shared keys are symmetric keys shared in advance among the communicating parties.

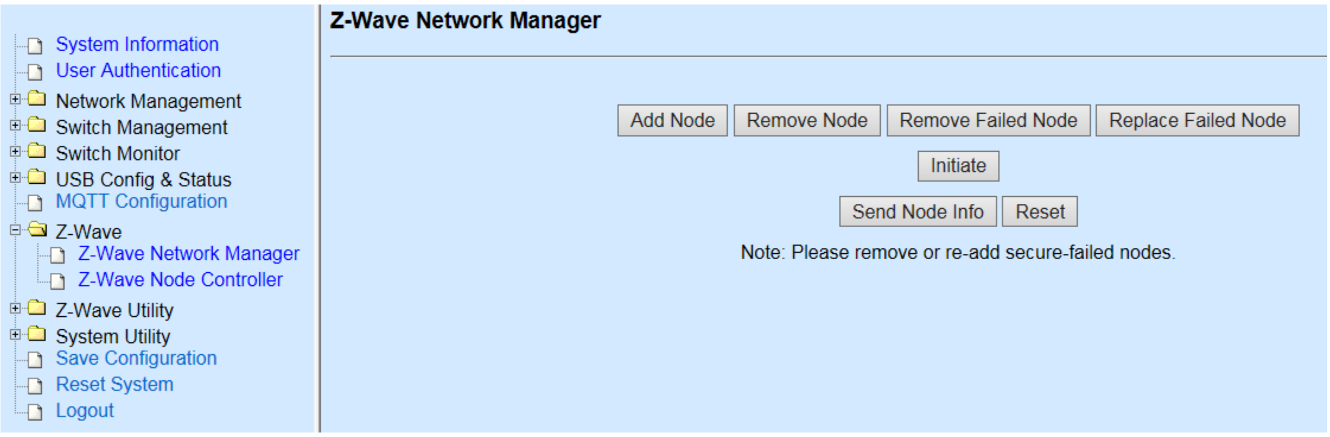
Identity: Specify a name to the Identity, up to 127 alphanumeric characters.

PSK Key: Enter the desired user password, up to 127 alphanumeric characters.

3.8 Z-Wave

Z-Wave is a wireless communications specification designed to allow devices in the home (lighting, access controls, entertainment systems and household appliances, for example) to communicate with one another for the purposes of home automation. The section shows the configuration and displays the status. Click the **Z-Wave** folder and then the following screen page appears.

Note: The controller needs booting up time whenever the controller is reset.It approximately takes 60 seconds. During this period, Z-Wave LED turns off. Make sure the Z-Wave LED status is in green, which represents Z-Wave works in normal operation.

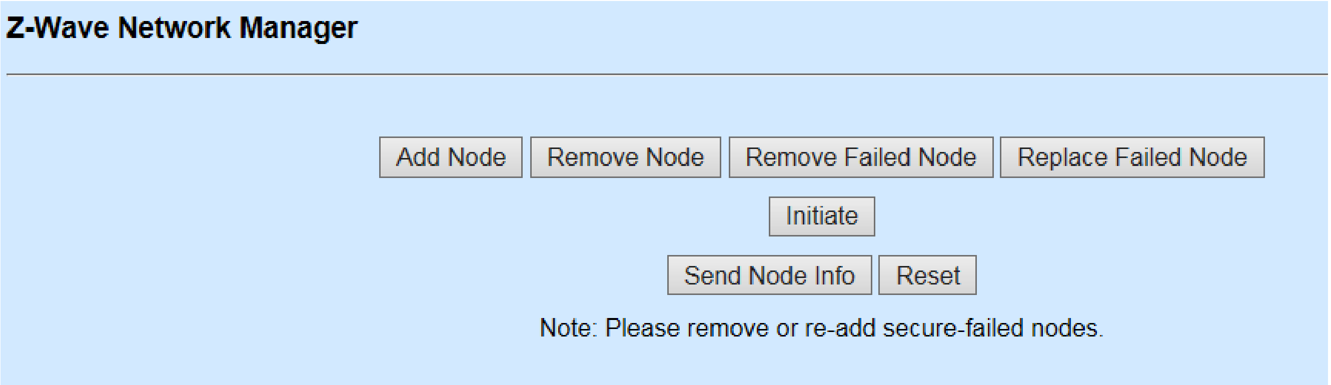


Note: Please remove or re-add secure-failed nodes.

1. Z-Wave Network Manager: To manage controller tasks in Z-Wave network.

2. Z-Wave Node Controller: To manage the devices connected with the controller.

3.8.1 Z-Wave Network Manager



Note: Please remove or re-add secure-failed nodes.

Add Node: Click to turn the controller into Inclusion Mode. Under Inclusion mode, the Gateway Controller is allowed to bring a device into a network. The Inclusion Mode will time out after 120 seconds. It also can be manually stopped using "Abort" button. Once a new device is successfully included, the Inclusion Mode stops.

Note: If a newly-added node is a sleeping node, the initial status of a node would be sleeping once included. The controller makes attempts to set the wake up interval of the node as 2 minutes. However, the node will remain its original wake up interval if the controller fails to change its wake up interval. You may set custom interval mentioned in Section 3.8.4.7. The custom wake up interval would come into effect after the node wakes up and receive the wake up interval you set.

Remove Node: Click to turn the controller into Exclusion Mode. Under Exclusion mode, the controller is allowed to remove a device from a network. The Exclusion Mode will time out after 120 seconds. It also can be manually stopped using "Abort" button. Once a new device is successfully excluded, the Exclusion Mode stops.

Remove Failed Node: The page below displays the list of nodes. Click a node among the list of nodes and click **"Remove Failed Node"** to remove a node that is no longer communicating with the controller. A failed node proves true if the node is removed successfully.
A node can be forced to get removed using **"Send Node Info"** if a node gives no reply to the controller. Click a node among the list of nodes and click **"Send Node Info"**, then click **"Remove Failed Node"**, the node can be removed successfully. The process of Remove Failed Node can be manually stopped using "Abort" button.

Replace Failed Node: Click to replace the failed node with a new node. The controller removes the designated node first and broadcast inclusion request. Thus, a new node can be added to the network. The ID of newly-included node has the same node ID as the failed one. The process of Replace Failed Node can be manually stopped using "Abort" button.

Initiate: Click to accept inclusion, exclusion or replication requests from other controllers. The controller turns into "Learn Mode". The Learn Mode will time out after 60 seconds. Learn Mode stops when the controller is included, excluded or replicated successfully. The process of Learn Mode can be manually stopped using "Abort" button. If you press "Abort" button during communication process, it cause the Z-Wave system to restart, which approximately takes 90 seconds.

Note: Executing the said actions Add Node, Remove Node, Remove Failed Node, Replace Failed Node or Initiate would cause Z-Wave process restart and application busy.

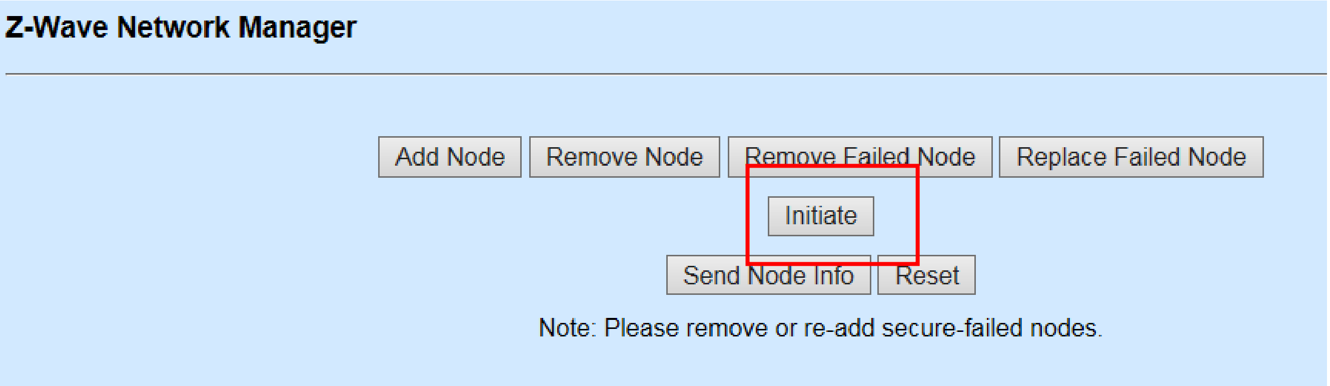
Send Node Info: This is to be used to ask for NIF from all nodes in a network to get known of the capabilities of the node. To get NIF from a device, click any single node in the list of nodes, and click "Send Node Info". To get NIF from all devices in a network, click the node ID of the controller itself in the list of nodes, and click "Send Node Info". This is also used to check if a node is in good connection. A node giving reply of Node Information Frame indicates that the controller is in connection with the node. A node not giving reply of Node Information Frame indicates that the controller is a failed node, sleeping node or out-of-battery node.

Reset: Click to return the controller to factory settings. Note that all connections with included devices and all configurations and settings are lost. This approximately takes 90 seconds to finish the process.

Note: The Z-Wave LED turns blinking green when clicking Add Node, Remove Node, Remove Failed Node or Replace Failed Node. The Z-Wave LED turns off when clicking Initiate or Reset.
If this controller is the primary controller for your network, resetting it will result in the nodes in your network being orphaned and it will be necessary after the reset to exclude and re-include all of the nodes in the network. If this controller is being used as a secondary controller in the network, use this procedure to reset this controller only in the event that the network primary controller is missing or otherwise inoperable.

3.8.1.1 Adding and Removing The Controller in An Existing Network

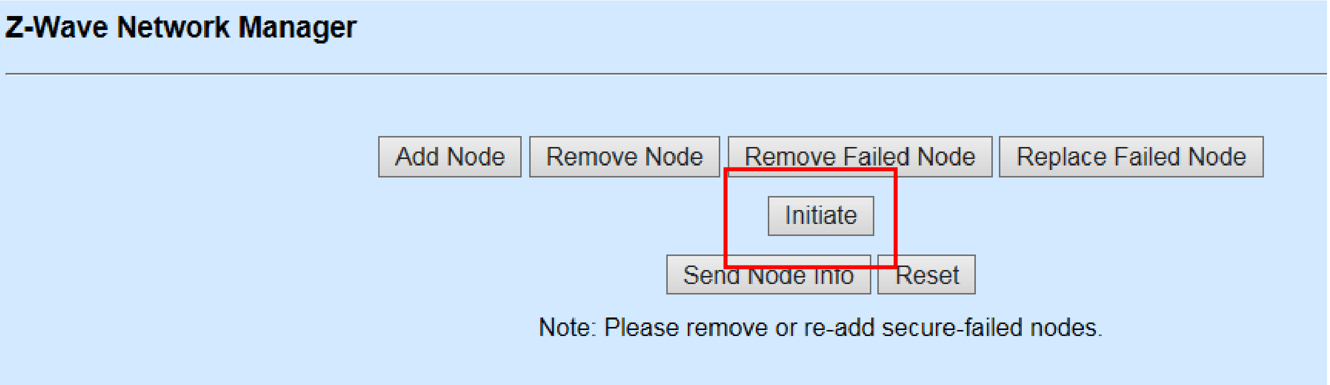
To add the controller to an existing network:
1. Click **"Initiate"** to activate Learn Mode.



Note: Please remove or re-add secure-failed nodes.

2. Wait for inclusion request from another controller.
3. Once the controller is successfully included, the Learn Mode stops.

To remove the controller from an existing network:
1. Click **"Initiate"** to activate Learn Mode.



Note: Please remove or re-add secure-failed nodes.

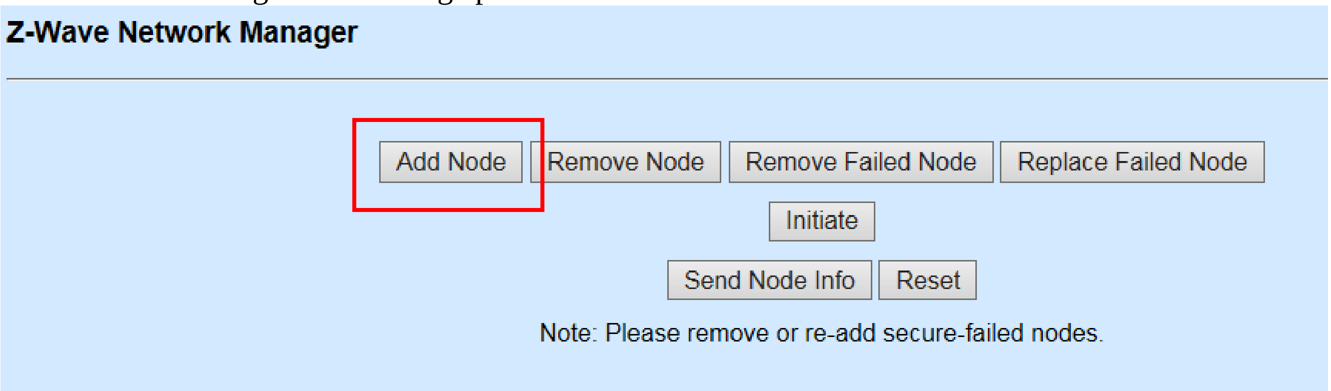
2. Wait for exclusion request from another controller.
3. Once the controller is successfully excluded, the Learn Mode stops.

Note: Make sure that the controller did not include any other device before, otherwise the controller will not be able to access Learn Mode and the Initiate button will become invalid.

3.8.1.2 How to Initiate A Replication of Network Information from The Controller to Another Controller

1. Click "Add Node" to include a controller into our network.
2. Turn the other controller into "Learn Mode".

3. After the other controller is successfully included, click “Add Node” again.
4. Turn the other controller into “Learn Mode” again.
5. The controller begins to exchange protocol data with the other controller in the same network.

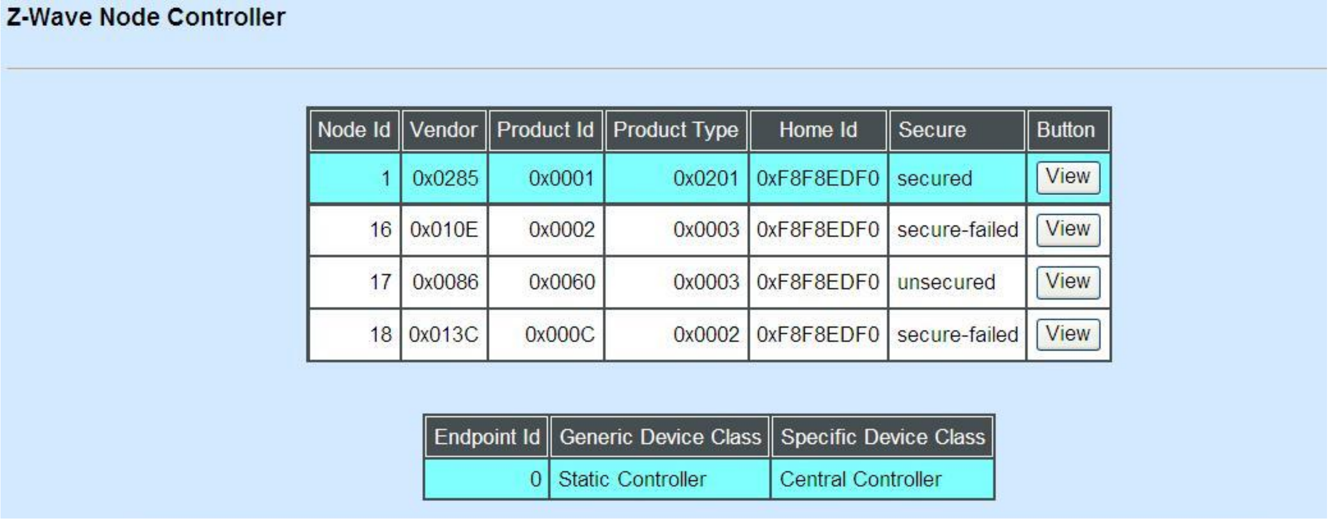


Note: Please remove or re-add secure-failed nodes.

3.8.1.3 Assigning The Controller as an SIS

The controller is included as a Secondary controller by a Primary Controller. If there is no SIS in the network, the Primary controller may assigns this controller as SIS. In this case, the controller will turn into a SIS from Secondary role, which takes approximately 110 seconds.

3.8.2 Z-Wave Node Controller



Node Id	Vendor	Product Id	Product Type	Home Id	Secure	Button
1	0x0285	0x0001	0x0201	0xF8F8EDF0	secured	View
16	0x010E	0x0002	0x0003	0xF8F8EDF0	secure-failed	View
17	0x0086	0x0060	0x0003	0xF8F8EDF0	unsecured	View
18	0x013C	0x000C	0x0002	0xF8F8EDF0	secure-failed	View

Endpoint Id	Generic Device Class	Specific Device Class
0	Static Controller	Central Controller

Node ID: The identification number of each node assigned.

Vendor: A unique ID identifying the manufacturer of the device.

Product Type: A unique ID identifying the actual product type.

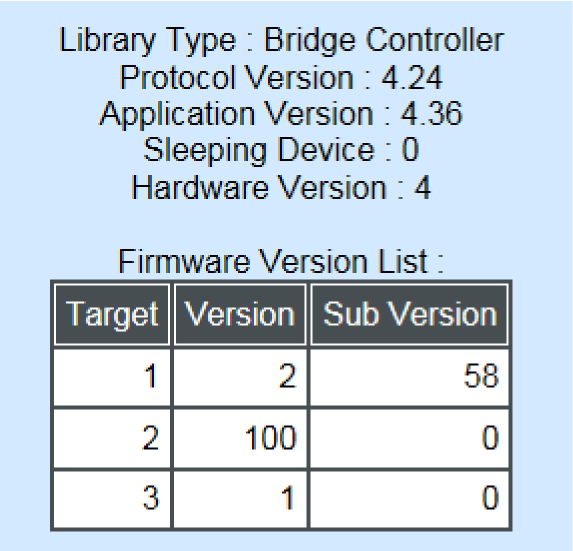
Product ID: A unique ID identifying the actual product.

Home ID: Unique network address of the link layer network.

Secure: Shows security status for each node. The status showing “secured” indicates that the node is a security enabled Z-Wave Plus product and successfully secured. The status showing “unsecured” indicates that the node is not a security enabled Z-Wave Plus product. The status showing “secure-failed” indicates that the node is a security enabled Z-Wave Plus product yet fails to be secured.

Note: It’s recommended that remove secure-failed nodes and re-add them.

Button: Click **“View”** for more information. The following screen appears.



Library Type : Bridge Controller
Protocol Version : 4.24
Application Version : 4.36
Sleeping Device : 0
Hardware Version : 4

Firmware Version List :

Target	Version	Sub Version
1	2	58
2	100	0
3	1	0

Library Type: Several Library Type available as below.

Library Type
Static Controller
Controller
Enhanced Slave
Slave
Installer
Routing Slave
Bridge Controller
Device Under Test (DUT)
AV Remote
AV Device

Protocol Version: Shows Z-Wave module FW version.

Application Version: Shows Z-Wave serial API version.

Sleeping Device: Shows if the device connected is sleeping device. “0” refers to “No”. “1” refers to “Yes”.

Hardware Version: A value which is unique to this particular version of the product

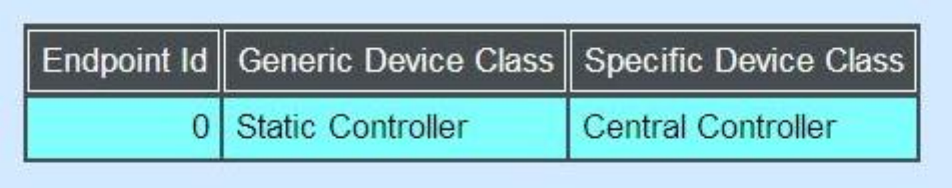
Firmware Version List
Target 1: SDK middleware version.

Target 2: The firmware version. For example, The Version field shows 100 (stand for 1.00) and the Sub Version shows 0. The value of two fields shown can be converted into this format --- 1.00.00.

Target 3: Reserved field for future application

Version: The major version shown.

Sub Version: The minor version shown.



Endpoint Id	Generic Device Class	Specific Device Class
0	Static Controller	Central Controller

Endpoint ID: The identification number of endpoint assigned in a node.

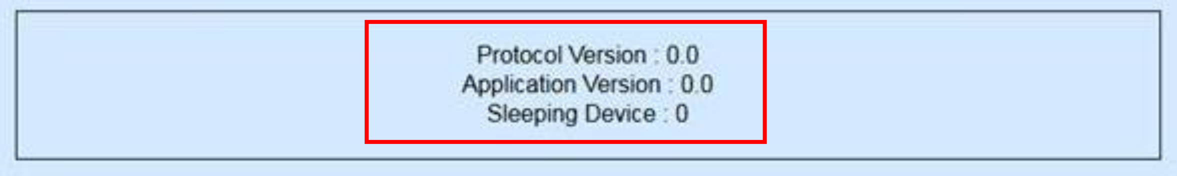
Generic Device Class: The subordinate information of class the sensor belongs to.

Note: If Generic Device Class is unable to be identified, the Generic Device Class column shows "Unknown (0xHH)".

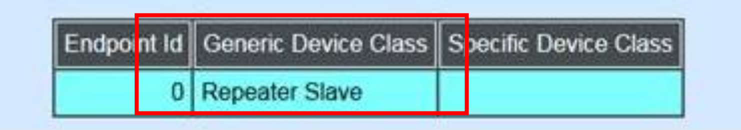
Specific Device Class: The detailed information of class the sensor belongs to.

Note: Somehow the list of nodes may show virtual nodes because bridge library is implemented. Their Protocol & Application Version show "0.0" and Genetic Device Class shows "Repeater Slave". Refer to the given example below.

Note: If Specific Device Class is unable to be identified, the Specific Device Class column shows "Unknown (0xHH)".



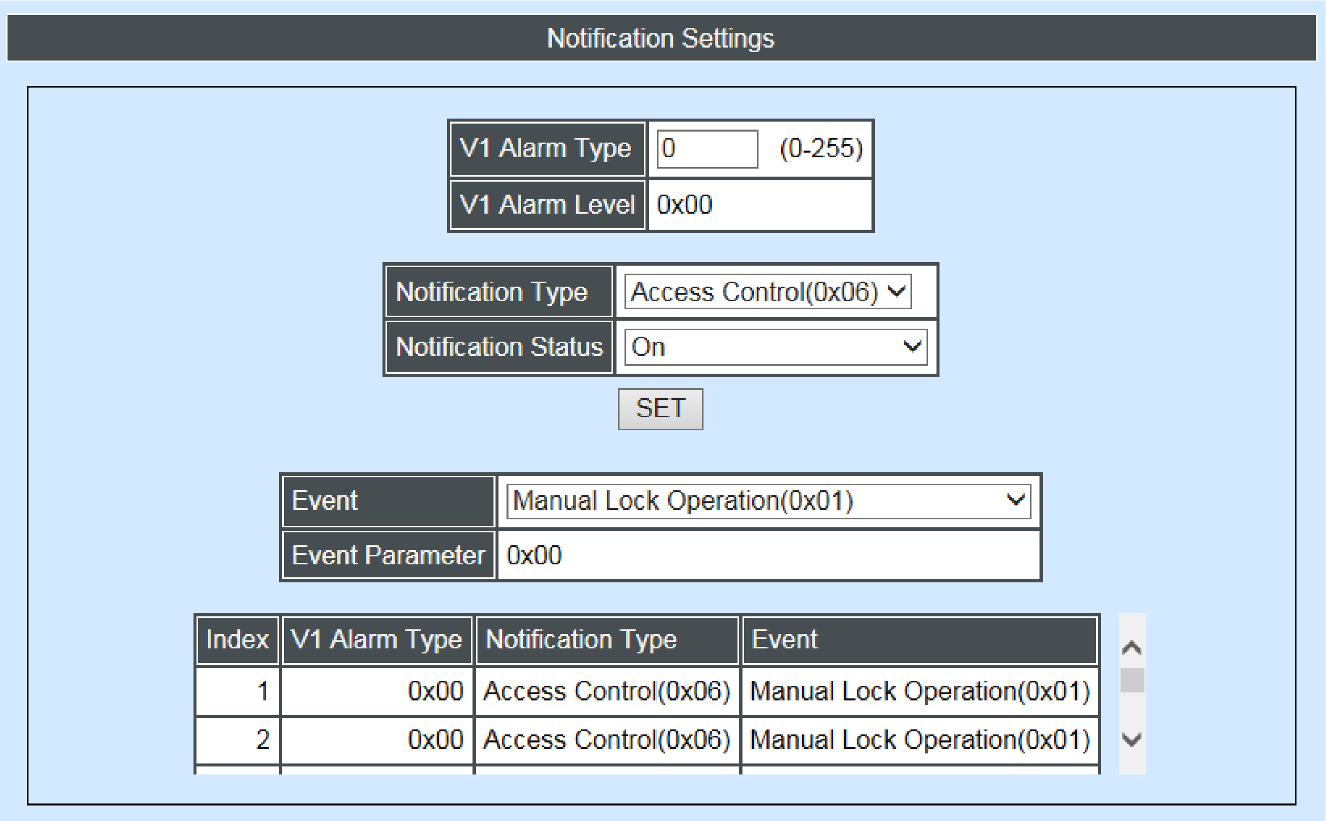
Protocol Version : 0.0
Application Version : 0.0
Sleeping Device : 0



Endpoint Id	Generic Device Class	Specific Device Class
0	Repeater Slave	

3.8.2.1 Notification Settings

This is used to advertise a specific event using a notification sensor.



Notification Settings

V1 Alarm Type	0 (0-255)
V1 Alarm Level	0x00

Notification Type	Access Control(0x06)
Notification Status	On

Event	Manual Lock Operation(0x01)
Event Parameter	0x00

Index	V1 Alarm Type	Notification Type	Event
1	0x00	Access Control(0x06)	Manual Lock Operation(0x01)
2	0x00	Access Control(0x06)	Manual Lock Operation(0x01)

V1 Alarm Type: Specify which alarm is being requested.

V1 Alarm Level: Shows the alarm level that is application specific.

Notification Type: Specify the type of the current report.

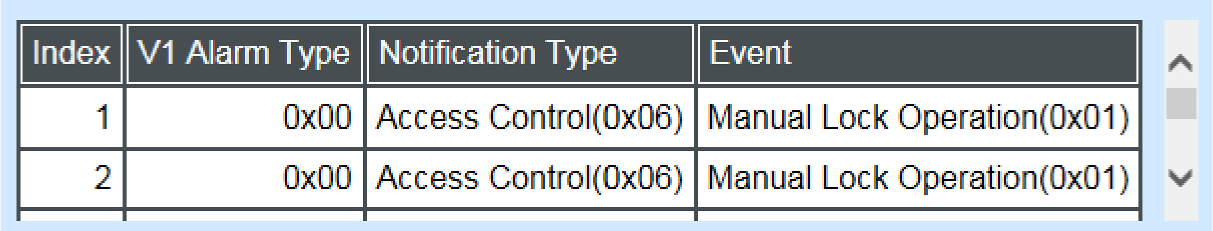
Notification Status: Click drop-down arrow to determine unsolicited messages must be disabled or enabled for the specified Notification Type.

Click "SET" to apply settings

Event: Specify the event of the current report.

Event Parameter: Shows the parameter corresponding the event specified.

The table below shows the Event Log of notification devices connected with the controller.



Index	V1 Alarm Type	Notification Type	Event
1	0x00	Access Control(0x06)	Manual Lock Operation(0x01)
2	0x00	Access Control(0x06)	Manual Lock Operation(0x01)

Index: Shows the number of each Event Log.

V1 Alarm Type: Shows which alarm is being requested.

Notification Type: Shows the type of the current report.

Event: Shows the event of the current report.

The details of notification type & event are shown as below

Notification Type		Event		Event Parameter(s)
Smoke Alarm	0x01	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Smoke detected	0x01	Node Location Report (Node Naming and Location Command Class).
		Smoke detected, Unknown Location	0x02	
		Smoke Alarm Test	0x03	
		Replacement Required	0x04	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
CO Alarm	0x02	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Carbon monoxide detected	0x01	Node Location Report (Node Naming and Location Command Class)
		Carbon monoxide detected, Unknown Location	0x02	
		Carbon monoxide Test	0x03	
		Replacement Required	0x04	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
CO2 Alarm	0x03	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Carbon dioxide detected	0x01	Node Location Report (Node Naming and Location Command Class)
		Carbon dioxide detected, Unknown Location	0x02	
		Carbon dioxide Test	0x03	
		Replacement Required	0x04	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)

Heat Alarm	0x04	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Overheat detected	0x01	Node Location Report (Node Naming and Location Command Class)
		Overheat detected, Unknown Location	0x02	
		Rapid Temperature Rise	0x03	Node Location Report (Node Naming and Location Command Class)
		Rapid Temperature Rise, Unknown Location	0x04	
		Under heat detected	0x05	Node Location Report (Node Naming and Location Command Class)
		Under heat detected, Unknown Location	0x06	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Water Alarm	0x05	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Water Leak detected	0x01	Node Location Report (Node Naming and Location Command Class)
		Water Leak detected, Unknown Location	0x02	
		Water Level Dropped	0x03	Node Location Report (Node Naming and Location Command Class)
		Water Level Dropped, Unknown Location	0x04	
		Replace Water Filter	0x05	
		Water Flow Alarm	0x06	
		Water Pressure Alarm	0x07	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Access Control	0x06	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Manual Lock Operation	0x01	
		Manual Unlock Operation	0x02	
		RF Lock Operation	0x03	
		RF Unlock Operation	0x04	
		Keypad Lock Operation	0x05	User Code Report (User Code Command Class V1)
		Keypad Unlock Operation	0x06	User Code Report (User Code

				Command Class V1)
		Manual Not Fully Locked Operation	0x07	
		RF Not Fully Locked Operation	0x08	
		Auto Lock Locked Operation	0x09	
		Auto Lock Not Fully Operation	0x0A	
		Lock Jammed	0x0B	
		All user codes deleted	0x0C	
		Single user code deleted	0x0D	
		New user code added	0x0E	
		New user code not added due to duplicate code	0x0F	
		Keypad temporary disabled	0x10	
		Keypad busy	0x11	
		New Program code Entered - Unique code for lock configuration	0x12	
		Manually Enter user Access code exceeds code limit	0x13	
		Unlock By RF with invalid user code	0x14	
		Locked by RF with invalid user codes	0x15	
		Window/Door is open	0x16	
		Window/Door is closed	0x17	
		Barrier performing Initialization process	0x40	(1 byte) 0xFF = Performing Process 0x00 = Process Complete 0x01- 0xFE = Reserved
Access Control	0x06	Barrier operation (Open/Close) force has been exceeded.	0x41	
		Barrier motor has exceeded manufacturer’s operational time limit	0x42	(1 byte) 0x00-0x7F = 0sec-127sec 0x80-0xFE = Reserved
		Barrier motor has exceeded physical mechanical limits. (For example: barrier has opened past open limit)	0x43	
		Barrier unable to perform requested operation due to UL requirements	0x44	
		Barrier Unattended operation has been disabled per UL requirements	0x45	
		Barrier failed to perform Requested operation, device malfunction	0x46	
		Barrier Vacation Mode	0x47	(1 byte) 0xFF = Mode Enabled 0x00 = Mode Disabled 0x01-0xFE = Reserved
		Barrier Safety Beam Obstacle	0x48	(1 byte) 0xFF = Obstruction 0x00 = No Obstruction 0x01-0xFE = Reserved

Access Control	0x06	Barrier Sensor Not Detected/ Supervisory Error	0x49	(1 byte) 0x00 = Sensor not defined 0x01-0xFE = Sensor ID
		Barrier Sensor Low Battery Warning	0x4A	(1 byte) 0x00 = Sensor not defined 0x01-0xFE = Sensor ID
		Barrier detected short in Wall Station wires	0x4B	
		Barrier associated with non-Z-wave remote control	0x4C	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Home Security	0x07	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Intrusion	0x01	Node Location Report (Node Naming and Location Command Class, version 1)
		Intrusion, Unknown Location	0x02	
		Tampering, Product covering removed	0x03	
		Tampering, Invalid Code	0x04	
		Glass Breakage	0x05	Node Location Report (Node Naming and Location Command Class, version 1)
		Glass Breakage, Unknown Location	0x06	
		Motion Detection	0x07	Node Location Report (Node Naming and Location Command Class, version 1)
		Motion Detection, Unknown Location	0x08	
		Tampering, Product Moved	0x09	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Power Management	0x08	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Power has been applied	0x01	
		AC mains disconnected	0x02	
		AC mains re-connected	0x03	
		Surge detected	0x04	
		Voltage Drop/Drift	0x05	
		Over-current detected	0x06	
		Over-voltage detected	0x07	
		Over-load detected	0x08	

		Load error	0x09	
		Replace battery soon	0x0A	
		Replace battery now	0x0B	
		Battery is charging	0x0C	
		Battery is fully charged	0x0D	
		Charge battery soon	0x0E	
		Charge battery now!	0x0F	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
System	0x09	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		System hardware failure	0x01	
		System software failure	0x02	
		System hardware failure with manufacturer proprietary failure code	0x03	Manufacturer proprietary system failure codes. Cannot be listed in NIF. MUST be described in product manual.
		System software failure with manufacturer proprietary failure code	0x04	Manufacturer proprietary system failure codes. Cannot be listed in NIF. MUST be described in product manual.
		Heartbeat	0x05	
		Tampering, Product covering removed	0x06	
		Emergency Shutoff	0x07	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Emergency Alarm	0x0A	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Contact Police	0x01	
		Contact Fire Service	0x02	
		Contact Medical Service	0x03	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Clock	0x0B	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Wake Up Alert	0x01	
		Timer Ended	0x02	
		Time Remaining	0x03	Event Parm 1 = hour(s) Event Parm 1 = minute(s) Event Parm 1 = second(s)
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Appliance	0x0C	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Program Started	0x01	
		Program in progress	0x02	
		Program completed	0x03	
		Replace main filter	0x04	
		Failure to set target temperature	0x05	
		Supplying water	0x06	
		Water supply failure	0x07	
		Boiling	0x08	
		Boiling failure	0x09	
		Washing	0x0A	
		Washing Failure	0x0B	
		Rinsing	0x0C	
		Rinsing Failure	0x0D	
		Draining	0x0E	
		Draining Failure	0x0F	
		Spinning	0x10	
		Spinning failure	0x11	
		Drying	0x12	
		Drying failure	0x13	
		Fan failure	0x14	
		Compressor failure	0x15	
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Home Health	0x0D	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Leaving Bed	0x01	
		Sitting on bed	0x02	
		Lying on bed	0x03	
		Posture changed	0x04	
		Sitting on edge of bed	0x05	
		Volatile Organic Compound level	0x06	Even Parm 1(1 byte) = pollution level 0x01=Clean 0x02=Slightly polluted 0x03=Moderately polluted 0x04=Highly polluted
		Unknown Event	0xFE	

Notification Type		Event		Event Parameter(s)
Siren	0x0E	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is

				provided, there are no active events for the specified Notification Type.
		Siren Active	0x01	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Water Valve	0x0F	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Valve Operation	0x01	Event Parm 1 = 0:Off 1:On
		Master Valve Operation	0x02	Event Parm 1 = 0:Off 1:On
		Valve Short Circuit	0x03	
		Master Valve Short Circuit	0x04	
		Valve Current Alarm	0x05	Event Parm 1 = 1: Nodata 2:Below low threshold 3:Above high threshold 4:Max
		Master Valve Current Alarm	0x06	Event Parm 1 = 1: Nodata 2:Below low threshold 3:Above high threshold 4:Max
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Weather Alarm	0x10	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Rain Alarm	0x01	
		Moisture Alarm	0x02	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Irrigation	0x11	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Schedule Started	0x01	Event Parm 1 = <Schedule ID>
		Schedule Finished	0x02	Event Parm 1 = <Schedule ID>
		Valve Table Run Started	0x03	Event Parm 1 = <Valve Table ID>
		Valve Table Run Finished	0x04	Event Parm 1 = <Valve Table ID>
		Device is not Configured	0x05	
		Unknown Event	0xFE	

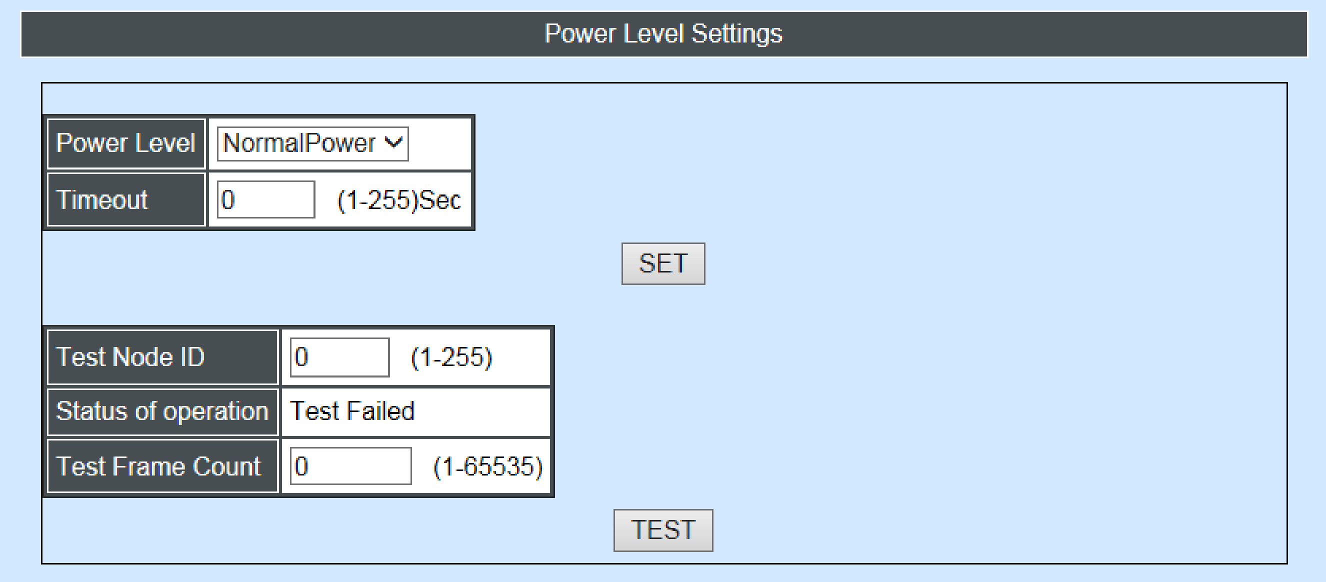
Notification Type		Event		Parameter(s)

Gas Alarm	0x12	Event /Cleared	0x00	- Event identifier for the event which is no more active. - If no Event Parameter is provided, there are no active events for the specified Notification Type.
		Combustible Gas Detected	0x01	Node Location Report (Node Naming and Location Command Class)
		Combustible Gas Detected, Unknown Location	0x02	
		Toxic Gas detected	0x03	Node Location Report (Node Naming and Location Command Class)
		Toxic Gas detected, Unknown Location	0x04	
		Gas Alarm Test	0x05	
		Replacement Required	0x06	
		Unknown Event	0xFE	

Notification Type		Event		Parameter(s)
Request pending notification (Notification Get; pull mode)			0xFF	

3.8.2.2 Power Level Settings

This is used to set the power level indicator value, which should be used by the node when transmitting RF, and the timeout for this power level indicator value before returning the power level defined by the application.



Power Level Settings

Power Level	NormalPower
Timeout	0 (1-255)Sec

Test Node ID	0 (1-255)
Status of operation	Test Failed
Test Frame Count	0 (1-65535)

Power Level: The power level indicator value to set.
Valid levels are: NormalPower, minus1dBm, minus2dBm, minus3dBm, minus4dBm, minus5dBm, minus6dBm, minus7dBm, minus8dBm and minus9dBm.

Timeout value is ignored if Power level is set to NormalPower.

Timeout: The time in seconds the node should keep the Power level before resetting to NormalPower level. Valid values are 1-255 resulting in timeouts from 1 second to 255 seconds.

The test section is used to instruct the destination node to transmit a number of test frames to the specified node ID with the RF power level specified.

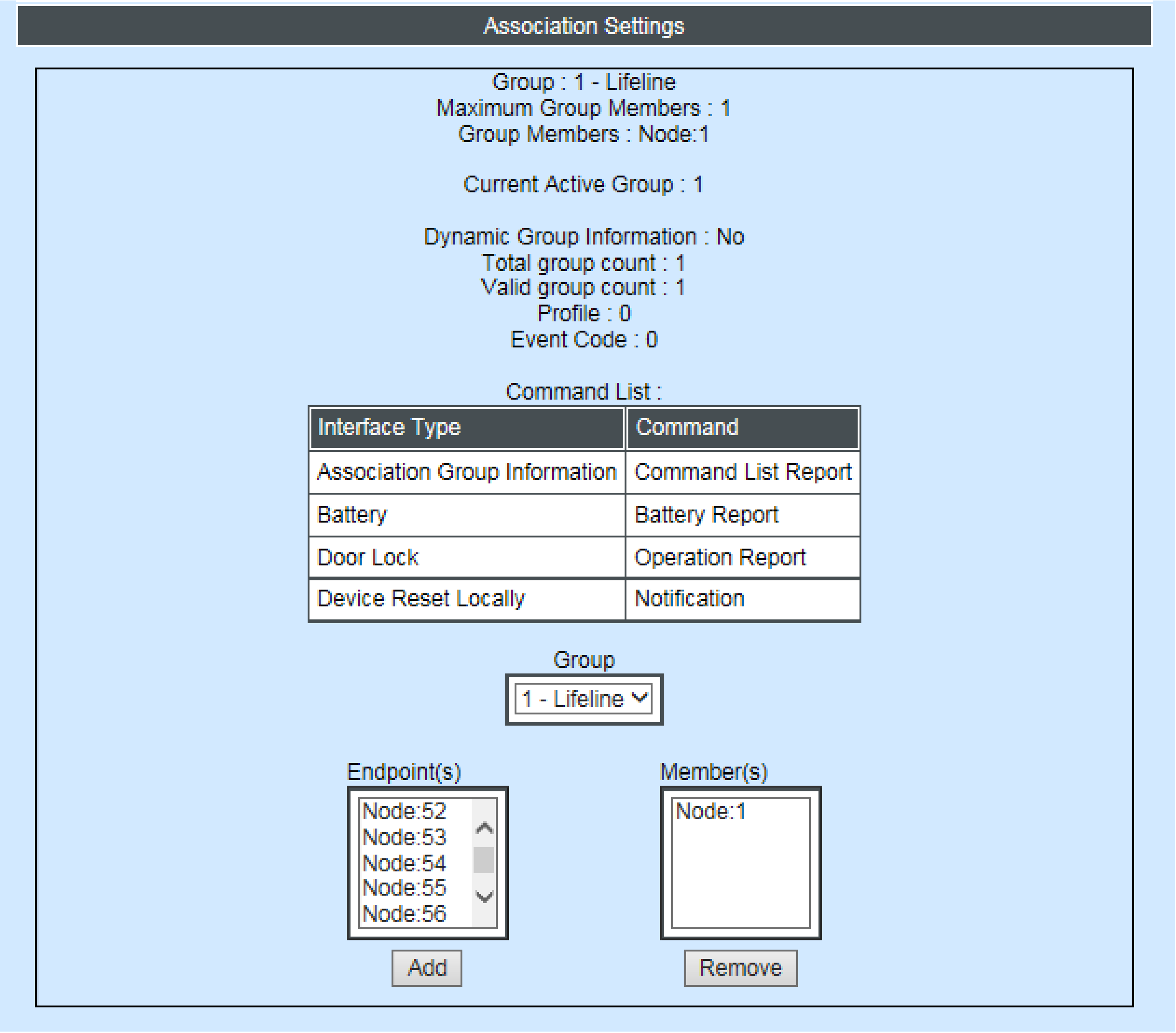
Test Node ID: Type the test node ID that needs testing. The valid value is 1~255

Status of Operation: Shows the current status of test operation.

Test Frame Count: It contains the number of test frames to transmit to the test node ID. Valid test frame count range is 1-65535.

3.8.2.3 Association Settings

This is used to allow a device to show the capabilities of each association group supported by a given application resource.



Association Settings

Group : 1 - Lifeline
Maximum Group Members : 1
Group Members : Node:1

Current Active Group : 1

Dynamic Group Information : No
Total group count : 1
Valid group count : 1
Profile : 0
Event Code : 0

Command List :

Interface Type	Command
Association Group Information	Command List Report
Battery	Battery Report
Door Lock	Operation Report
Device Reset Locally	Notification

Group: 1 - Lifeline

Endpoint(s): Node:52, Node:53, Node:54, Node:55, Node:56

Member(s): Node:1

Group: The name of the group given.

Maximum Group Members: The devices that can be added to the group at most.

Group Members: The current members that are added to the group.

Current Active Group: The available is from 1~255.

Dynamic Group Information: Shows if the Z-Wave Gateway device performs periodic cache refresh for this node.

Total Group Count: The total number of groups in the device.

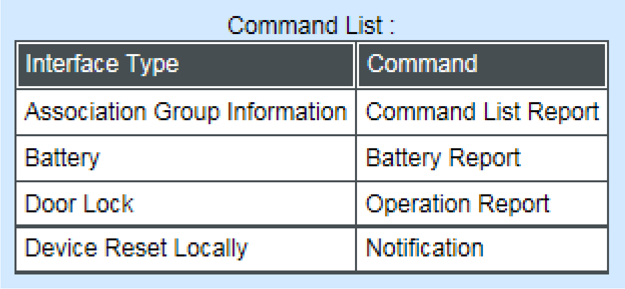
Valid Group Count: The valid number of groups in the device.

Profile: The profile defines the scope of events which triggers the transmission of commands to members of the actual association group.

Event Code: Reserved field for future application.

Command List

It shows the commands that may be sent from the association group.

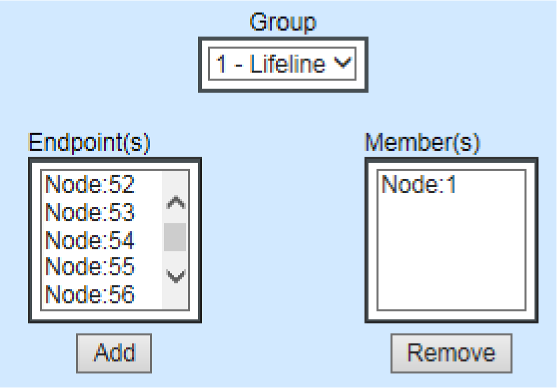


Command List :

Interface Type	Command
Association Group Information	Command List Report
Battery	Battery Report
Door Lock	Operation Report
Device Reset Locally	Notification

Interface Type: The list of command class.

Command: The subordinate command that belongs to the corresponding command class.



Group: 1 - Lifeline

Endpoint(s): Node:52, Node:53, Node:54, Node:55, Node:56

Member(s): Node:1

To add or remove members in a group, you may use the following items.

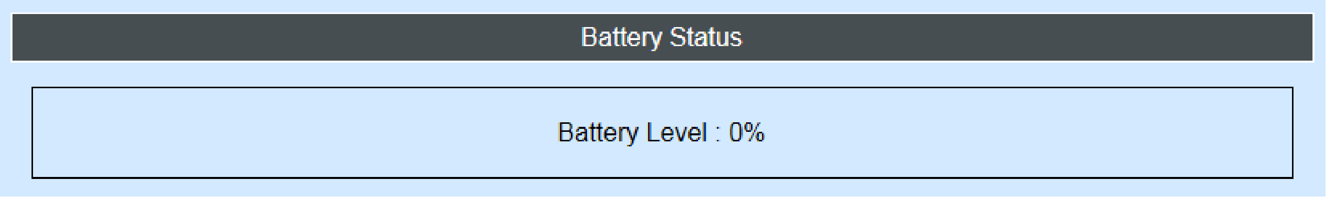
Group: Click drop-down arrow to choose the group you want to configure.

Member(s): To remove members in a group, choose any node under Member(s) and click “Remove”

Endpoint(s): To add members in a group, choose any node under Endpoint(s) and click “Add”

3.8.2.4 Battery Status

This is used to show the battery status of a battery operated device.



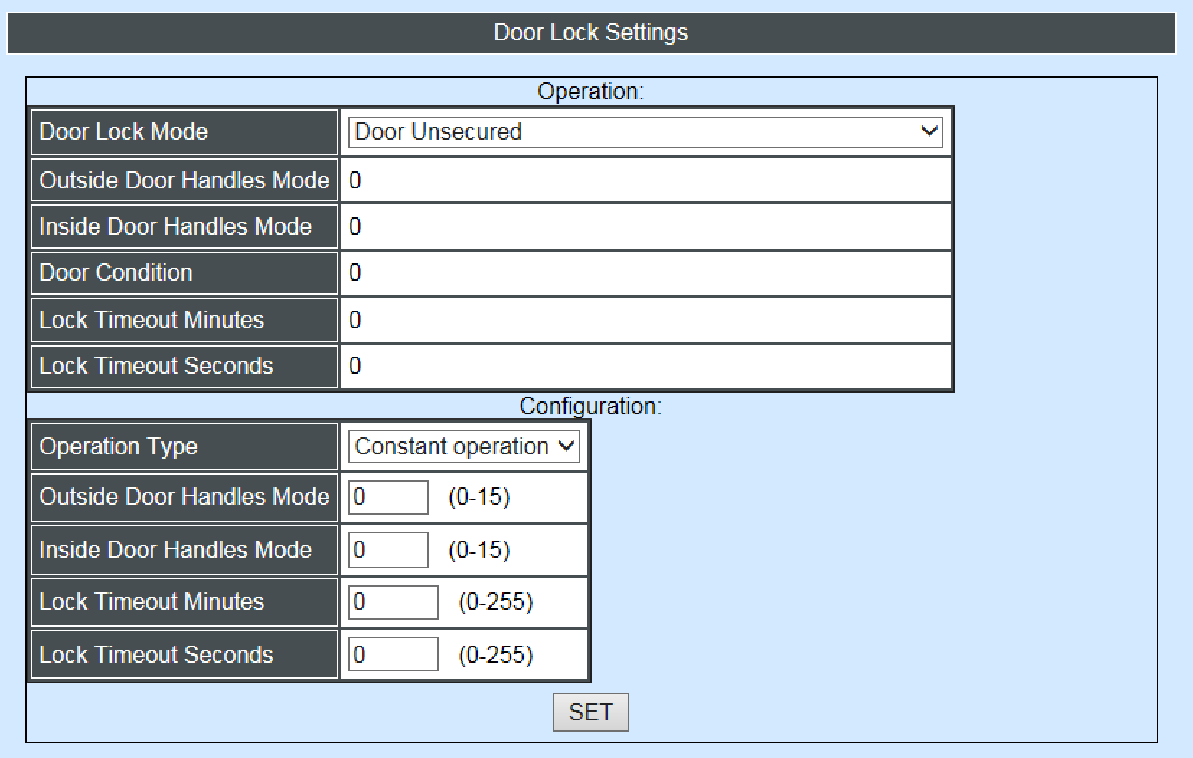
Battery Status

Battery Level : 0%

Battery Level: The percentage scale ranging from 0 to 100%. 0% indicates the battery is totally out of energy and 100% indicates fully-charged.

3.8.2.5 Door Lock Settings

This is used to operate and configure a door lock device.



Door Lock Settings

Operation:

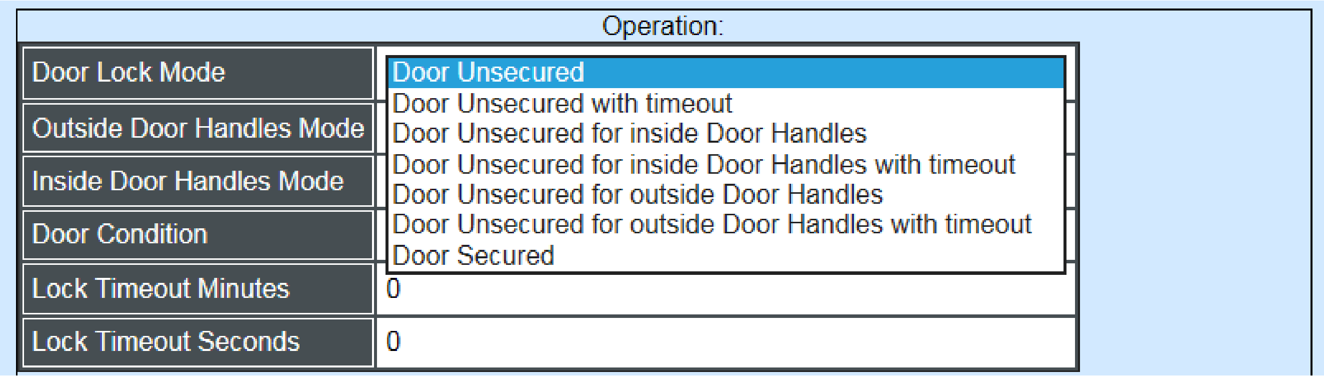
Door Lock Mode	Door Unsecured
Outside Door Handles Mode	0
Inside Door Handles Mode	0
Door Condition	0
Lock Timeout Minutes	0
Lock Timeout Seconds	0

Configuration:

Operation Type	Constant operation
Outside Door Handles Mode	0 (0-15)
Inside Door Handles Mode	0 (0-15)
Lock Timeout Minutes	0 (0-255)
Lock Timeout Seconds	0 (0-255)

Operation

Door Lock Mode: Click drop-down arrow and specify the operation mode of the door lock device. Several modes are available: Door Unsecured, Door Unsecured with timeout, Door Unsecured for inside Door Handles, Door Unsecured for inside Door Handles with timeout, Door Unsecured for outside Door Handles, Door Unsecured for outside Door Handles with timeout and Door Secured.



Operation:

Door Lock Mode	Door Unsecured Door Unsecured with timeout Door Unsecured for inside Door Handles Door Unsecured for inside Door Handles with timeout Door Unsecured for outside Door Handles Door Unsecured for outside Door Handles with timeout Door Secured
Outside Door Handles Mode	
Inside Door Handles Mode	
Door Condition	
Lock Timeout Minutes	0
Lock Timeout Seconds	0

Outside Door Handles Mode: The status of each individual outside door handle.

Inside Door Handles Mode: The status of each individual inside door handle.

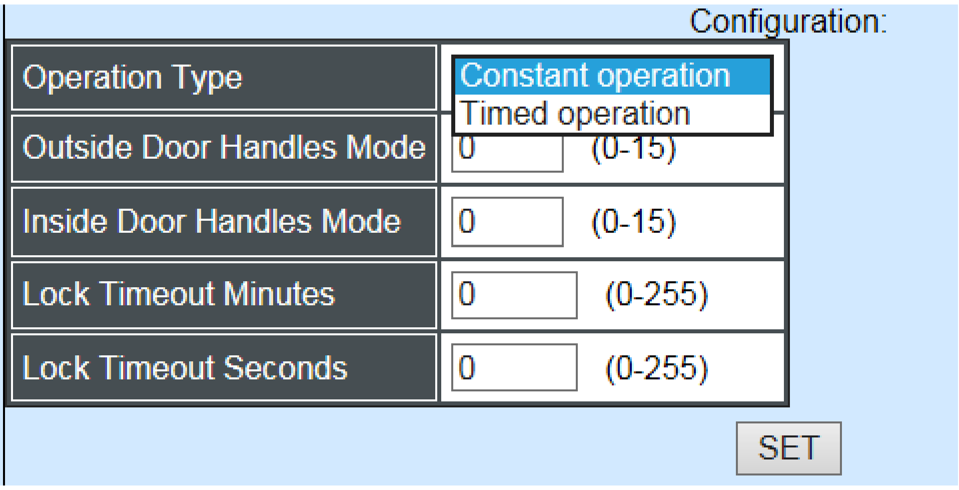
Door Condition: The status of the door lock components.

Lock Timeout Minutes: The remaining time in minute before the door lock will automatically be locked again.

Lock Timeout Seconds: The remaining time in second before the door lock will automatically be locked again.

Configuration

Operation Type: Constant operation and Timed operation are selectable. Constant operation indicates that door will be unsecured until set back to secured mode by command. Timed operation indicates that the device fallback to secured mode after timeout has expired. When timed operation is chosen, the Lock Timeout Minutes and Lock Timeout Seconds fields must be set to valid values.



Configuration:

Operation Type	Constant operation Timed operation
Outside Door Handles Mode	0 (0-15)
Inside Door Handles Mode	0 (0-15)
Lock Timeout Minutes	0 (0-255)
Lock Timeout Seconds	0 (0-255)

Outside Door Handles Mode: Set up the mode of each individual outside door handle. The available value is 0~15.

Inside Door Handles Mode: Set up the mode of each individual inside door handle. The available value is 0~15.

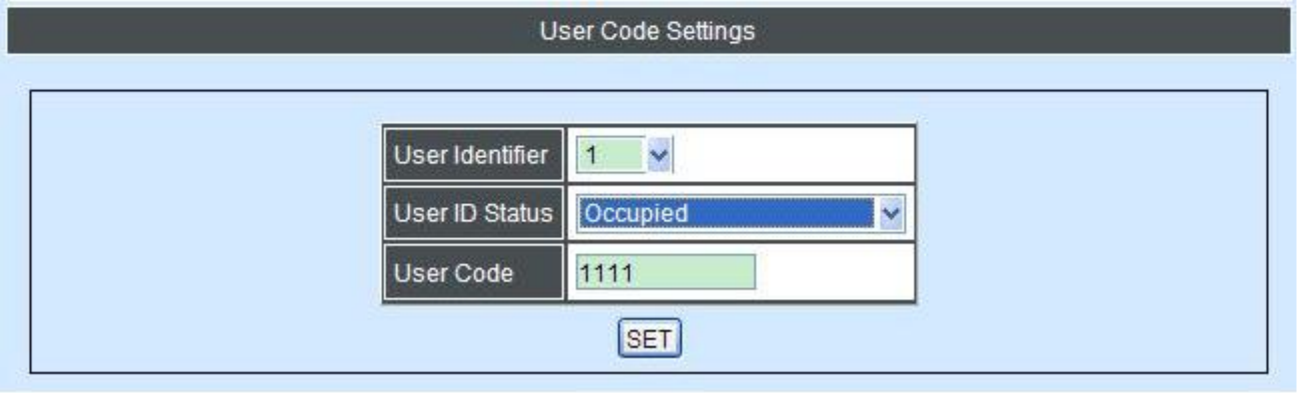
Lock Timeout Minutes: Set up the time in minute that a door lock must wait before automatically being locked again. The range is 0~255 in minute.

Lock Timeout Seconds: Set up the time in second that a door lock must wait before automatically being locked again. The range is 0~255 in second.

Click "SET" to apply settings.

3.8.2.6 User Code Settings

This is used to supply an enabled Door Lock Device with a command class to manage user codes.



User Code Settings

User Identifier	1
User ID Status	Occupied
User Code	1111

User Identifier: This is used to recognize the user identity. Click drop-down arrow and choose the user ID you want to configure.

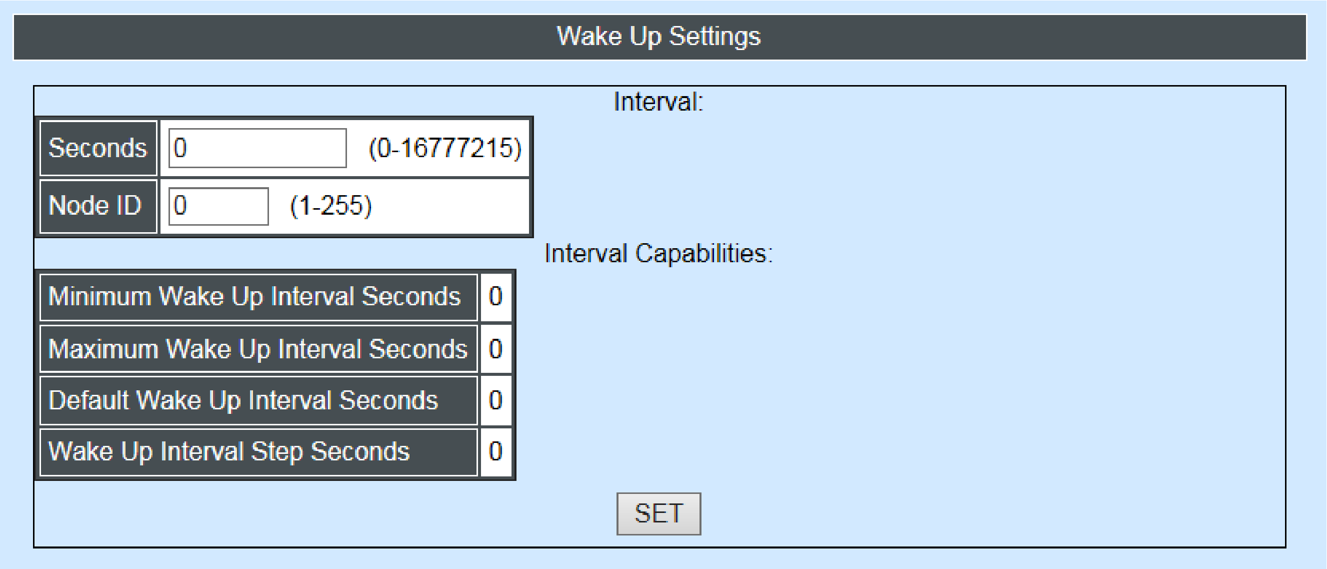
User ID Status: Shows the state of the User Identifier. Click drop-down arrow and the following status shows – Available, Occupied, Reserved by administrator and Status not available.

User Code: Type the user code in the box. Minimum code length is 4 and maximum 10 ASCII digits.

Click "SET" to apply the settings.

3.8.2.7 Wake Up Settings

This is used to allow a battery-powered device to notify another device (always listening), that it is awake and ready to receive any queued commands and read back of the Wake up interval capabilities in a node.



Wake Up Settings

Interval:

Seconds	0	(0-16777215)
Node ID	0	(1-255)

Interval Capabilities:

Minimum Wake Up Interval Seconds	0
Maximum Wake Up Interval Seconds	0
Default Wake Up Interval Seconds	0
Wake Up Interval Step Seconds	0

Interval

Seconds: Set up the wake up interval in second of a device. Valid value is 0~16777215 in second.

Note: If a newly-added node is a sleeping node, the initial status of a node would be sleeping once included. The controller makes attempts to set the wake up interval of the node as 2 minutes. However, the node will remain its original wake up interval if the controller fails to change its wake up interval. You may set custom interval. The custom wake up interval would come into effect only after the node wakes up and receive the wake up interval you set.

Node ID: The node ID of the device which is to receive the Wake Up Notification Command.

Interval Capabilities

Minimum Wake Up Interval Seconds: Shows the minimum wake up interval in second a battery-operated device supports.

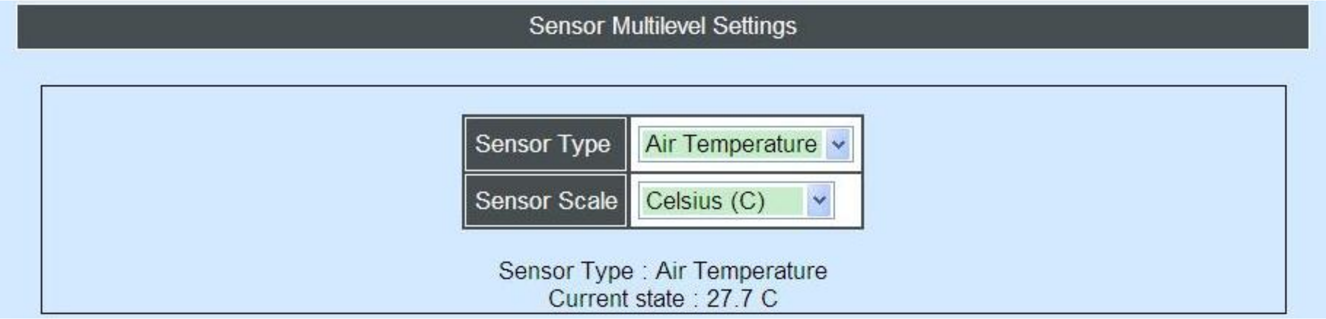
Maximum Wake Up Interval Seconds: Shows the maximum wake up interval in second a battery-operated device supports.

Default Wake Up Interval Seconds: Shows the default wake up interval a battery-operated device supports.

Wake Up Interval Step Seconds: Shows the resolution of possible wake up intervals, which a battery-operated device supports.

3.8.2.8 Sensor Multilevel Settings

This is used to allow a sensor device to issue readings to another device.


Sensor Multilevel Settings

Sensor Type: Air Temperature
Sensor Scale: Celsius (C)

Sensor Type : Air Temperature
Current state : 27.7 C

Sensor Type: Specify what type of sensor this command originates from. Click the drop-down arrow and pick designated one.

Sensor Scale: To indicate what unit the sensor uses. Click the drop-down arrow and pick designated one.

The details of sensor type and scale are shown below:

Sensor Type	Sensor Scale
Air Temperature	Celsius (C)
	Fahrenheit (F)
General Purpose	Percentage value
	Dimensionless value
Luminance	Percentage Value
	Lux
Power	Watt
	Btu/h
Humidity	Percentage
	Absolute humidity (g/m^3)
Velocity	m/s
	Mph
Direction	0 to 360 degrees 0= no wind, 90= east, 180= south, 270= west, and 360= north
Atmospheric Pressure	kPa(kilopascal)
	Inches of Mercury
Barometric Pressure	kPa(kilopascal)
	Inches of Mercury
Solar Radiation	W/m^2
Dew Point	Celsius(C)
	Fahrenheit(F)
Rain Rate	mm/h (millimeter/hour)
	in/h (inch/hour)
Tide Level	m (Meter)
	Feet
Weight	Kg
	Pounds
Voltage	V
	mV
Current	A
	mA

Sensor Type	Sensor Scale

Carbon Dioxide CO_2-level	Ppm (Parts/million)
Air Flow	m3/h (cubic meter/hour)
	cfm (cubic feet/minute)
Tank capacity	l (liter)
	m^3 (cubic meter)
	gallons
Distance	m (meter)
	cm
	feet
Angle Position	Percentage Value
	Degrees relative to north pole of standing eye view
	Degrees relative to south pole of standing eye view
Rotation	rpm (revolutions per minute)
	Hz (Hertz)
Water Temperature	Celsius (C)
	Fahrenheit (F)
Soil Temperature	Celsius (C)
	Fahrenheit (F)
Seismic Intensity	Mercalli
	European Macroseismic
	Liedu
	Shindo
Seismic Magnitude	Local (M_L)
	Moment (M_W)
	Surface wave (M_S)
	Body wave (M_B)
Ultraviolet	UV index
Electrical Resistivity	ohm rate (Ω m)

Sensor Type	**Sensor Scale**
Electrical Conductivity	siemens per metre(S·m−1)
Loudness	Absolute loudness
	A-weighted decibels (dBA)
Moisture	Percentage value
	Volume water content (m^3/m^3)
	Impedance (kΩ)
	Water activity (a_w)
Frequency	Hz- MUST be used until 4.294967295 GHz
	KHz- MUST be used until 4.294967295 GHz
Time	Second(s)
Target Temperature	Celsius(C)
	Fahrenheit(F)
Particulate Matter 2.5	mol/m^3 (mole per cubic meter)
	Absolute $\mu g/m^3$
Formaldehyde CH_2O-level	mol/m^3 (mole per cubic meter)
Radon Concentration	bq/m^3 (Becquerel/cubic meter)
	pCi/L (picocuries/liter)
Methane Density CH_4	mol/m^3 (mole per cubic meter)
Volatile Organic Compound	mol/m^3 (mole per cubic meter)
Carbon Monoxide CO-level	mol/m^3 (mole per cubic meter)
Soil Humidity	Percentage value

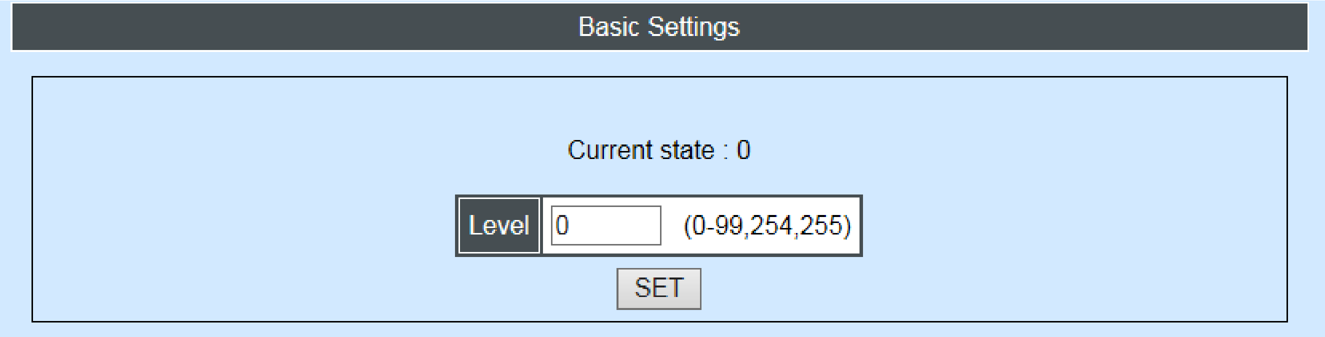
Sensor Type	**Sensor Scale**

Soil Reactivity	pH(acidity)
Soil Salinity	mol/m^3 (mole per cubic meter)
Heart Rate	Bpm(beats/minute)
Blood Pressure	Systolic mmHg(Upper #)
	Diastolic(lower#)
Muscle Mass	Kg
Fat Mass	Kg
Bone Mass	Kg
Total Body Water, TBW	Kg
Basic Metabolic Rate, BMR	J(joule)
Body Mass Index, BMI	BMI Index
Acceleration, X-axis	m/s^2
Acceleration, Y-axis	m/s^2
Acceleration, Z-axis	m/s^2
Smoke Density	Percentage value
Water Flow	l/h (liter/hour)
Water Pressure	kPa(kilopascal)
RF Signal Strength	RSSI(Percentage value)
	dBm

Click “SET” to apply settings. After that, Current state shows up according to the type picked.

3.8.2.9 Basic Settings

This is used to allow a controlling device to operate the primary functionality of a supporting device without any further knowledge.



Basic Settings

Current state : 0

Level 0 (0-99,254,255)

Level: This is used to set a value in a supporting device.

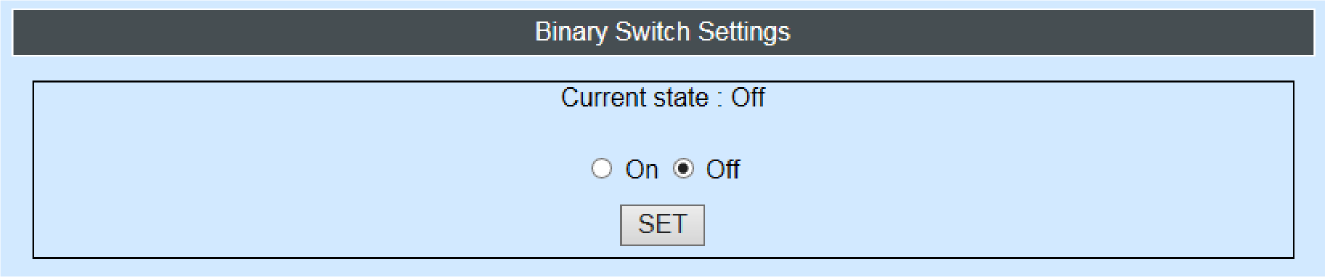
The details of value are shown as below:

Value	Level	State
0 (0x00)	0%	Off
1..99 (0x01..0x63)	1..100%	On
254 (0xFE)	Unknown	Unknown
255 (0xFF)	100%	On

Current State: The current value configured.

3.8.2.10 Binary Settings

This is used to control devices with On/Off or Enable/Disable capability.



Binary Switch Settings

Current state : Off

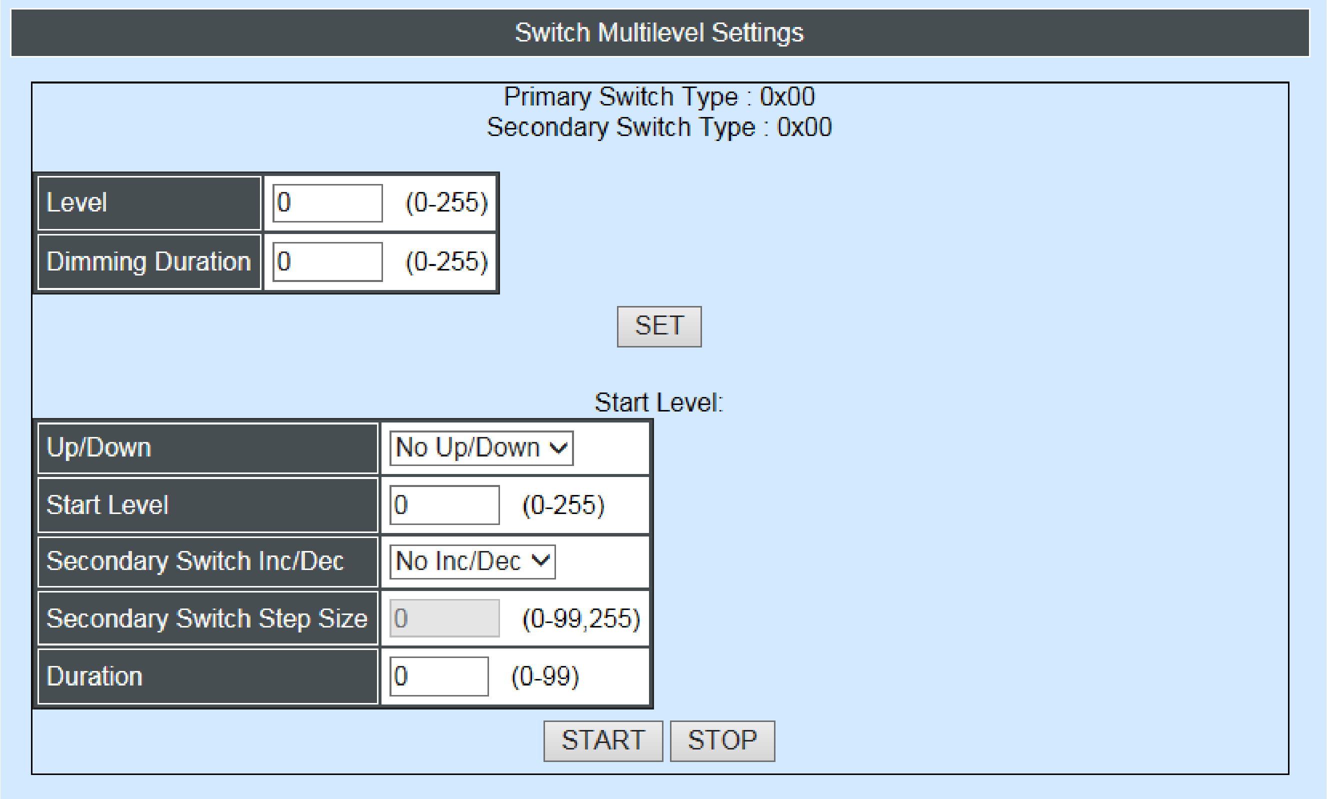
○ On ● Off

Click On(Enable) or Off(Disable) for a device.

Current State: Shows the current state is set “On” or “Off”.

3.8.2.11 Switch Multilevel Settings

This is used to control devices with multilevel capability.



Switch Multilevel Settings

Primary Switch Type : 0x00
Secondary Switch Type : 0x00

Level	0	(0-255)
Dimming Duration	0	(0-255)

Start Level:

Up/Down	No Up/Down	
Start Level	0	(0-255)
Secondary Switch Inc/Dec	No Inc/Dec	
Secondary Switch Step Size	0	(0-99,255)
Duration	0	(0-99)

Primary Switch Type: It shows the primary device functionality.

Secondary Switch Type: It shows the secondary device functionality.

The details of Switch Type are shown as below:

Switch Type Value	0x00 (Direction/Endpoint A)	0x63/0xFF (Direction/Endpoint B)
0x00	Undefined / Not supported (Secondary only)	
0x01	Off	On
0x02	Down	Up

0x03	Close	Open
0x04	Counter-Clockwise	Clockwise
0x05	Left	Right
0x06	Reverse	Forward
0x07	Pull	Push
0x08-0x1F	Reserved	

Level: This is used to set a value in a supporting device.

The details of value are shown as below:

Value	Level	State
0 (0x00)	0%	Off
1..99 (0x01..0x63)	Lowest non-zero level .. 100%	On
…	Reserved	Reserved
255 (0xFF)	Restore most recent (non-zero) level.	On

Dimming Duration: Specify the time that the transition should take from the current value to the new target value.

Start Level

Up/Down: This is used for manipulating the primary device functionality. “Up” is to increase level for Primary Switch Type. “Down” is to decrease level for Primary Switch Type. No Up/Down is to maintain current level for Primary Switch Type. Click drop-down arrow and pick the designated one.

Start Level: Specify the initial level of the level change.

Secondary Switch Inc/Dec: This used for controlling the secondary device functionality. “Increment” is to Increase level for Secondary Switch Type. “Decrement” is to decrease level for Secondary Switch Type. “No Inc/Dec” is to maintain current level for Secondary Switch Type. Click drop-down arrow and pick the designated one.

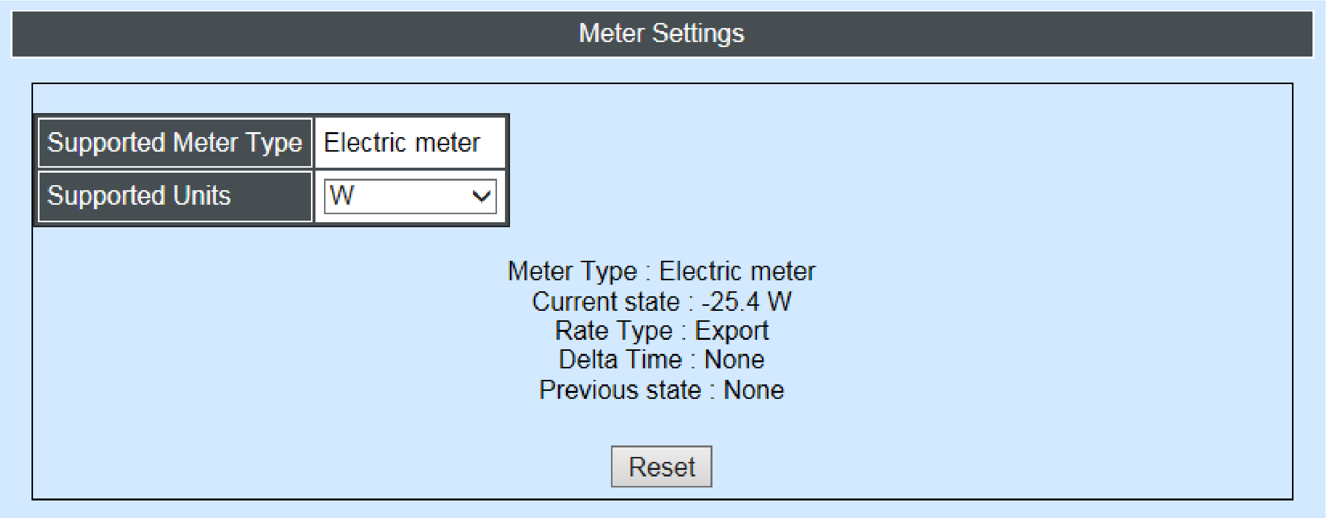
Secondary Switch Step Size: Specify the value 0~99 or 255.

Duration: The dimming rate to use must be calculated to match a transition from 0 to 99 during the time specified by the Duration box.

Click “START” to send “Multilevel Switch Start Level Change Command” based on the configured parameter.
Click “STOP” stop the command in process.

3.8.2.12 Meter Settings

This is intended for Z-Wave enabled devices capable of reporting energy measurements in addition to any main functionality or features e.g. an appliance module reporting the current consumption of the connected load.



Supported Meter Type	Electric meter
Supported Units	W

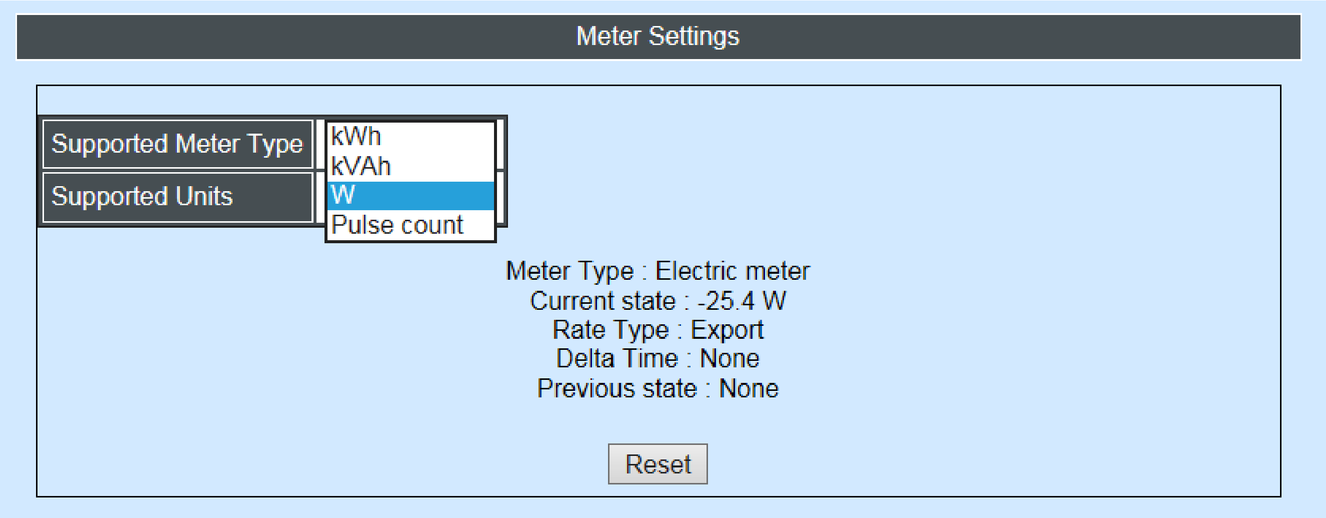
Meter Type : Electric meter
Current state : -25.4 W
Rate Type : Export
Delta Time : None
Previous state : None

Supported Meter Type: Shows what type of metering device originates from.

Supported Units: The unit available for the Meter Type used.

The supported meters and units are shown as below:

Meter Type	Unit
Electric Meter	kWh
	KVAh
	W
	Pulse Count
	A
	Power Factor
Gas Meter	Cubic Meters
	Cubic Feet
	Pulse Count
Water Meter	Cubic Meters
	Cubic Feet
	US Gallons
	Pulse Count



Meter Settings

Supported Meter Type	kWh kVAh W Pulse count
Supported Units	

Meter Type : Electric meter
Current state : -25.4 W
Rate Type : Export
Delta Time : None
Previous state : None

Meter Type: Shows the current meter type.

Current State: Shows the current status of the energy measured.

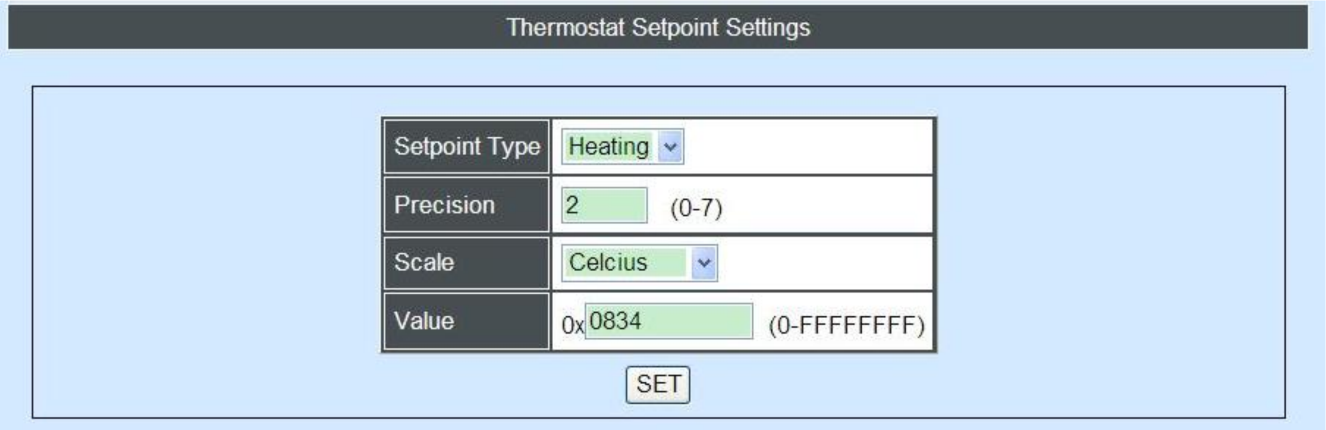
Rate Type: Shows if it is import or export values to be read. The Rate Type shown “Import” is an indication that the Meter Value is a consumed measurement. In contrary when the Rate Type is shown “Export” the indication of the Meter Value is a produced measurement.

Delta Time: Shows the elapsed time in seconds between the ‘Meter Value’ and the ‘Previous Meter Value’ measurements.

Previous State: Shows the previous status of the device.

3.8.2.13 Thermostat Setpoint Settings

This is used for setpoint handling.



Thermostat Setpoint Settings

Setpoint Type	Heating
Precision	2 (0-7)
Scale	Celcius
Value	0x 0834 (0-FFFFFFFF)

Setpoint Type: Click drop-down box and choose the designated type. Several types are available --- Heating, Cooling, Furnace, Dry Air, Moist Air, Auto Changeover, Energy Save Heating, Energy Save Cooling, Away Heating, Away Cooling and Full Power.

Precision: Specifies the precision of the setpoint value. The value must indicate the number of decimals. As an example, the decimal value 1025 with precision 2 must be interpreted as 10.25.

Scale: Click drop-down box to choose the unit used for temperature. Celsius and Fahrenheit are available.

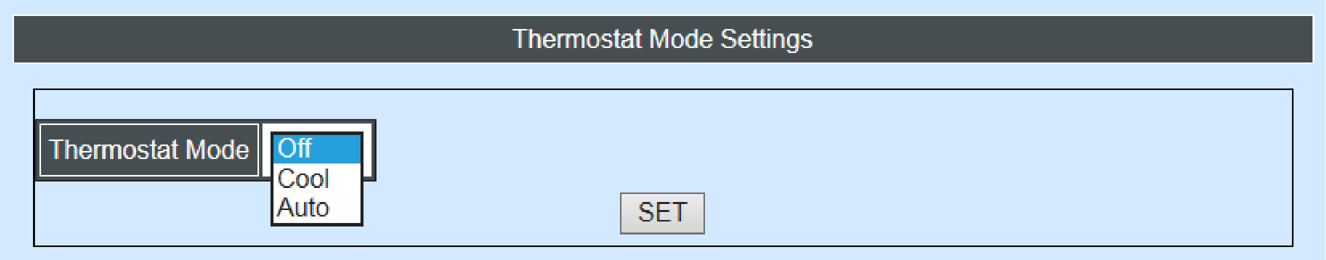
Value: Specify the actual setpoint value.

The example of value is shown as below:

Raw value (hex)	Signed 8 bit representation (decimal)		Raw value (hex)	Signed 16 bit representation (decimal)		Raw value (hex)	Signed 32 bit representation (decimal)
0x7F	127		0x7FFF	32767		0x7FFFFFFF	2147483647
0x02	2		0x0002	2		0x00000002	2
0x01	1		0x0001	1		0x00000001	1
0x00	0		0x0000	0		0x00000000	0
0xFF	-1		0xFFFF	-1		0xFFFFFFFF	-1
0xFE	-2		0xFFFE	-2		0xFFFFFFFE	-2
0x80	-128		0x8000	-32768		0x80000000	-2147483648

3.8.2.14 Thermostat Mode Settings

This is used to control a thermostat.



Thermostat Mode: Click drop-down arrow to show the modes.

The details of modes are shown below:

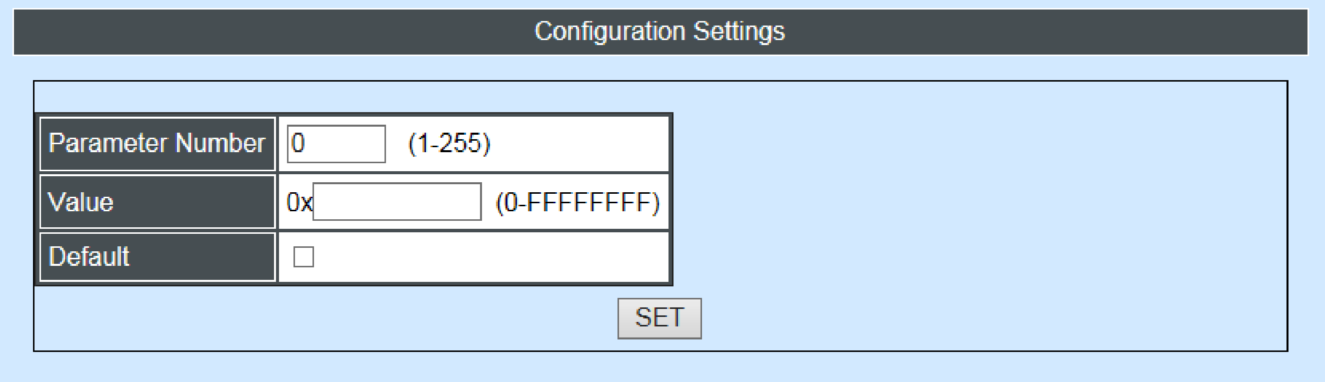
Thermostat Mode	Description
OFF	System is OFF.
HEAT	Continuous heating only.
COOL	Continuous cooling only.
AUTO	The system will automatically switch between heating and cooling when the temperature exceeds the HEAT and COOL set point types.
AUXILIARY	Auxiliary/Emergency Heat. A heat pump (especially air exchange types) is not efficient when the outside temperature is below 35 degrees Fahrenheit (~0 degrees centigrade). Thus, the thermostat may be put into auxiliary heat mode simply to use a more efficient secondary heat source when there are no failures of the compressor or heat pump unit itself.
RESUME (ON)	The system MUST resume to last active mode. The Thermostat Mode Report command MUST NOT advertise this Mode identifier.
FAN	Fan only - cycle fan to circulate air.
FURNACE	Cycle fan to circulate air - heating or cooling will be activated according to

	the FURNACE set point.
DRY	Dehumidification - The system will cycle cooling in relation to the room and the DRY set point temperature in order to remove moisture from ambient.
MOIST	Humidification - Moist Air, heating or cooling will be activated according to the MOIST set point.
AUTO CHANGEOVER	Auto Changeover - heating or cooling will be activated according to the AUTO CHANGEOVER set point.
ENERGY HEAT	Energy Saving Heating (usually lower than normal set point) - heating will be activated according to the ENERGY HEAT set point.
ENERGY COOL	Energy Saving Cooling (usually higher than normal set point) - cooling will be activated according to the ENERGY COOL set point.
AWAY	Away mode, e.g. preventing water from freezing in forced water systems - heating or cooling will be activated when temperature exceeds the AWAY HEAT and/or AWAY COOL set points.
FULL POWER	SPEED UP / FULL POWER heating or cooling mode will be activated when temperature exceeds FULL POWER set point.

Click “SET” to apply settings.

3.8.2.15 Configuration Settings

This is used to allow product specific configuration parameters to be changed.



Configuration Settings

Parameter Number	0 (1-255)
Value	0x (0-FFFFFFFF)
Default	□

Parameter Number: Specify the actual configuration parameter. Valid value is 1~255.

Value: This box carries the value to be automatically assigned by Parameter Number.

The example of value is shown below:

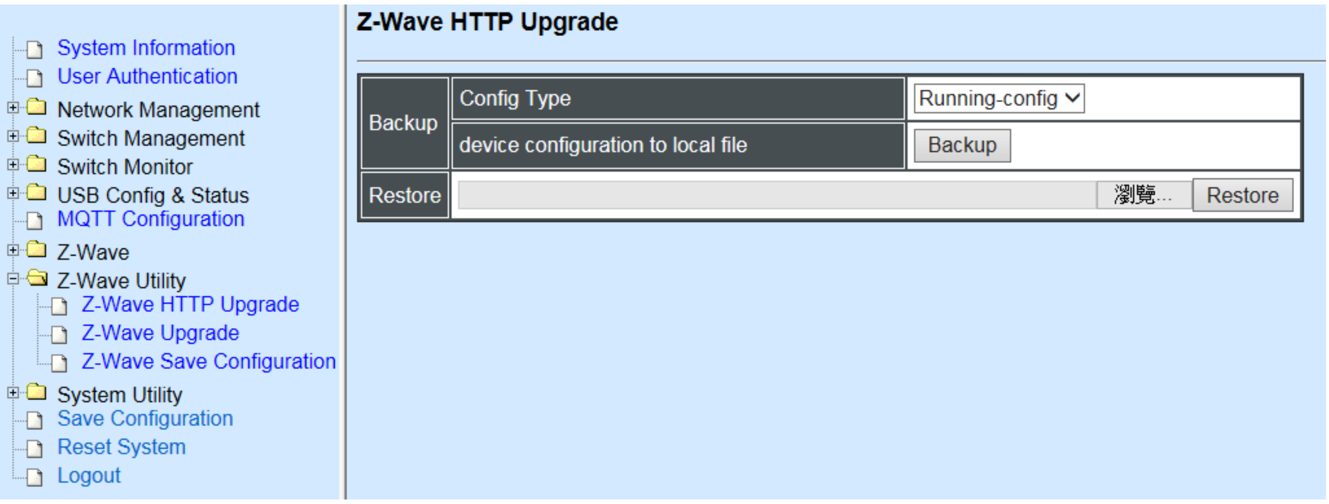
Raw value (hex)	Signed 8 bit representation (decimal)		Raw value (hex)	Signed 16 bit representation (decimal)		Raw value (hex)	Signed 32 bit representation (decimal)
0x7F	127		0x7FFF	32767		0x7FFFFFFF	2147483647
0x02	2		0x0002	2		0x00000002	2
0x01	1		0x0001	1		0x00000001	1
0x00	0		0x0000	0		0x00000000	0
0xFF	-1		0xFFFF	-1		0xFFFFFFFF	-1
0xFE	-2		0xFFFE	-2		0xFFFFFFFE	-2
0x80	-128		0x8000	-32768		0x80000000	-2147483648

Default: This is used to specify if the default value is to be restored for all configuration parameters. Check the box to have the default factory settings must be restored for all Parameter Numbers. If the box is checked, the Parameter Number and the Value fields must be ignored. Uncheck to have the specified Parameter Number must assume the value specified by the Value field.

Click “SET” to apply settings.

3.9 Z-Wave Utility

This is used to upgrade, backup or save Z-Wave configuration. Select Z-Wave Utility folder and the following screen page appears.



Z-Wave HTTP Upgrade

Backup	Config Type	Running-config
	device configuration to local file	Backup
Restore	瀏覽... Restore	

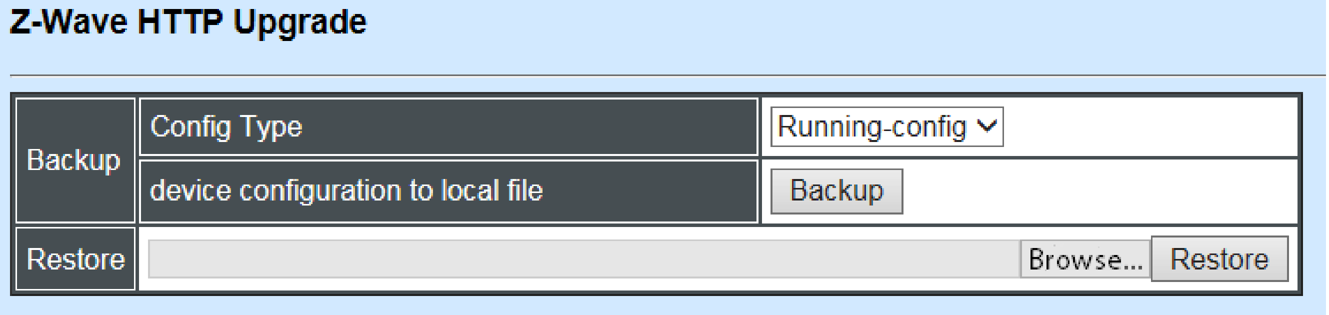
1. Z-Wave HTTP Upgrade: To save or restore their Z-Wave configuration off-line.

2. Z-Wave Upgrade: Users may save or restore their configuration on-line using FTP or TFTP server.

3. Z-Wave Save Configuration: To save configuration first before resetting the Gateway Controller.

3.9.1 Z-Wave HTTP Upgrade

Users may save or restore their Z-Wave configuration off-line. Select **Z-Wave HTTP Upgrade** from the **Z-Wave Config & Status** menu and then the following screen page appears.



Z-Wave HTTP Upgrade

Backup	Config Type	Running-config
	device configuration to local file	Backup
Restore	Browse... Restore	

Config Type

There are three types of Config Type: Running-config and Start-up-config

Running-config: Back up the data you’re processing

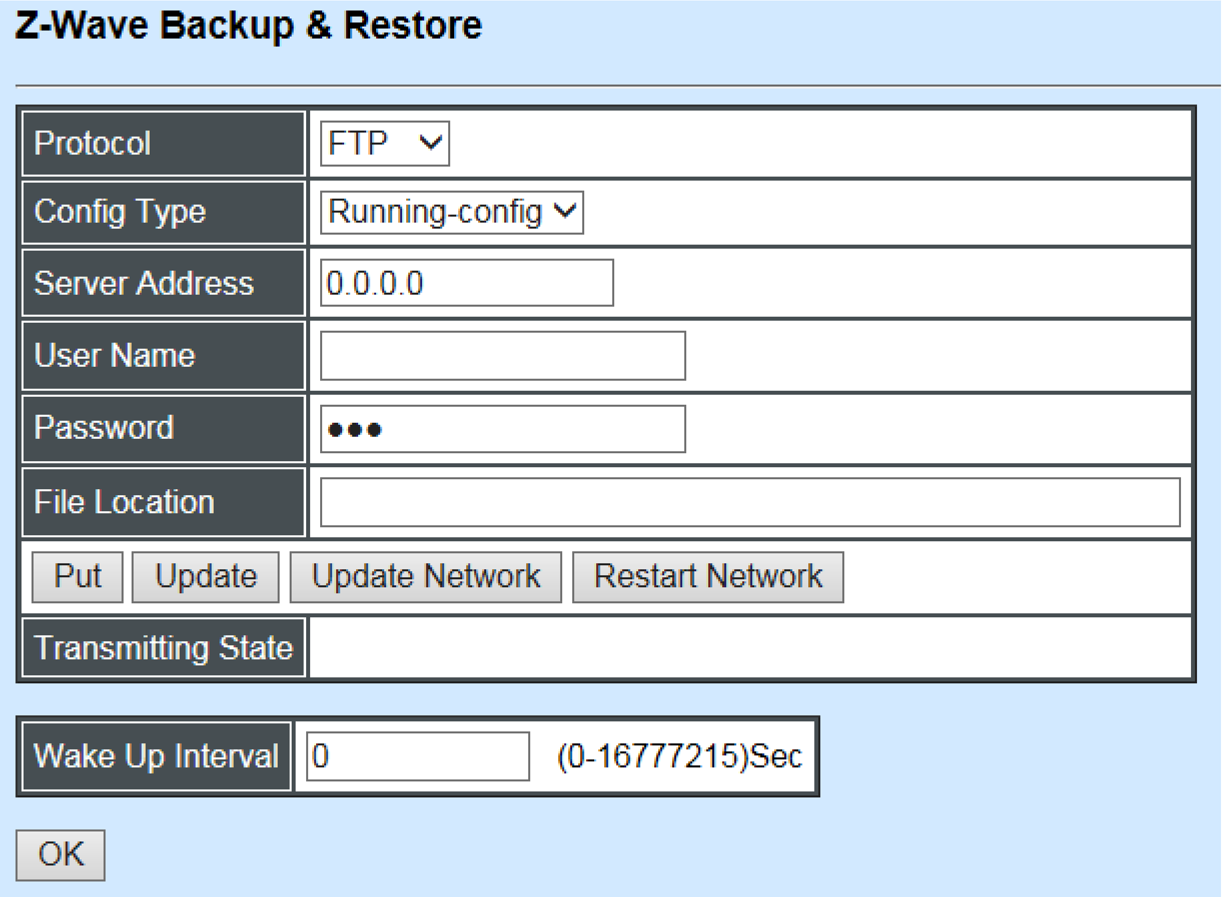
Start-up-config: Back up the data same as last saved data.

Device Configuration to Local File: Click **Backup** and define the route where you intend to save data.

Restore: Click **Browse**, select the designated data and then click **Restore**.

3.9.2 Z-Wave Upgrade

The Gateway Controller has both built-in TFTP and FTP clients. Users may save or restore their configuration on-line. Select **Upgrade** from the **Z-Wave Config & Status** menu and then the following screen page appears.



Z-Wave Backup & Restore

Protocol	FTP
Config Type	Running-config
Server Address	0.0.0.0
User Name	
Password	●●●
File Location	
Transmitting State	

Wake Up Interval	0	(0-16777215)Sec

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

Config Type: Choose “Running-config” or “Start-up-config” which the config file will be saved or restored to

Running-config: Back up the data you’re processing

Start-up-config: Back up the data same as last saved data.

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.

Update Network: Click to update Z-Wave network.

Restart Network: Click to restart Z-Wave network.

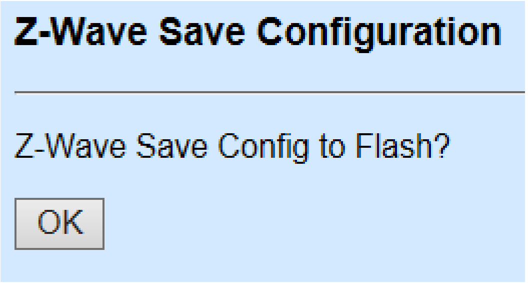
Wake Up Interval: Specify the interval in second to wake up sleeping devices. The default value is 0.

Click **Put** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

Select **Update** then press **Enter** to instruct the Gateway Controller to update existing firmware/configuration to the latest firmware/configuration received. After a successful update, a message will pop up. The Gateway Controller will need a reset to make changes effective.

3.9.3 Z-Wave Save Configuration

In order to save configuration setting permanently, users need to save configuration first before resetting the Gateway Controller. Select **Z-Wave Save Configuration** from the **Z-Wave Config & Status** menu and then the following screen page appears.



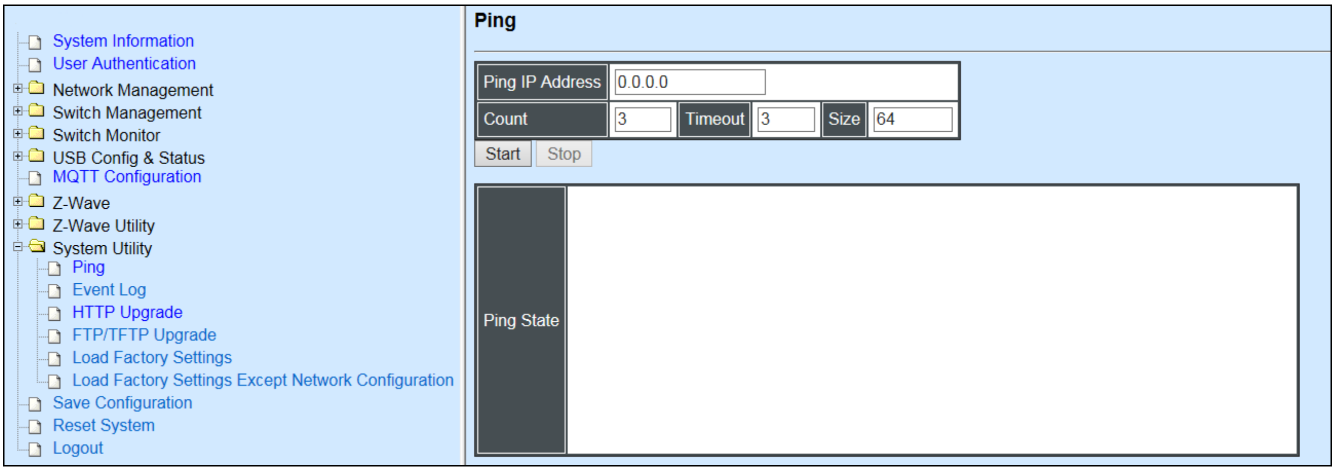
Z-Wave Save Configuration

Z-Wave Save Config to Flash?

Click **"OK"** to save current Z-Wave configuration.

3.10 System Utility

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



Ping

Ping IP Address	0.0.0.0				
Count	3	Timeout	3	Size	64

1. **Ping:** Ping can help you test the network connectivity between the Gateway Controller and the host. You can also specify count s, timeout and size of the Ping packets.

2. **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.

3. **HTTP Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Gateway Controller.

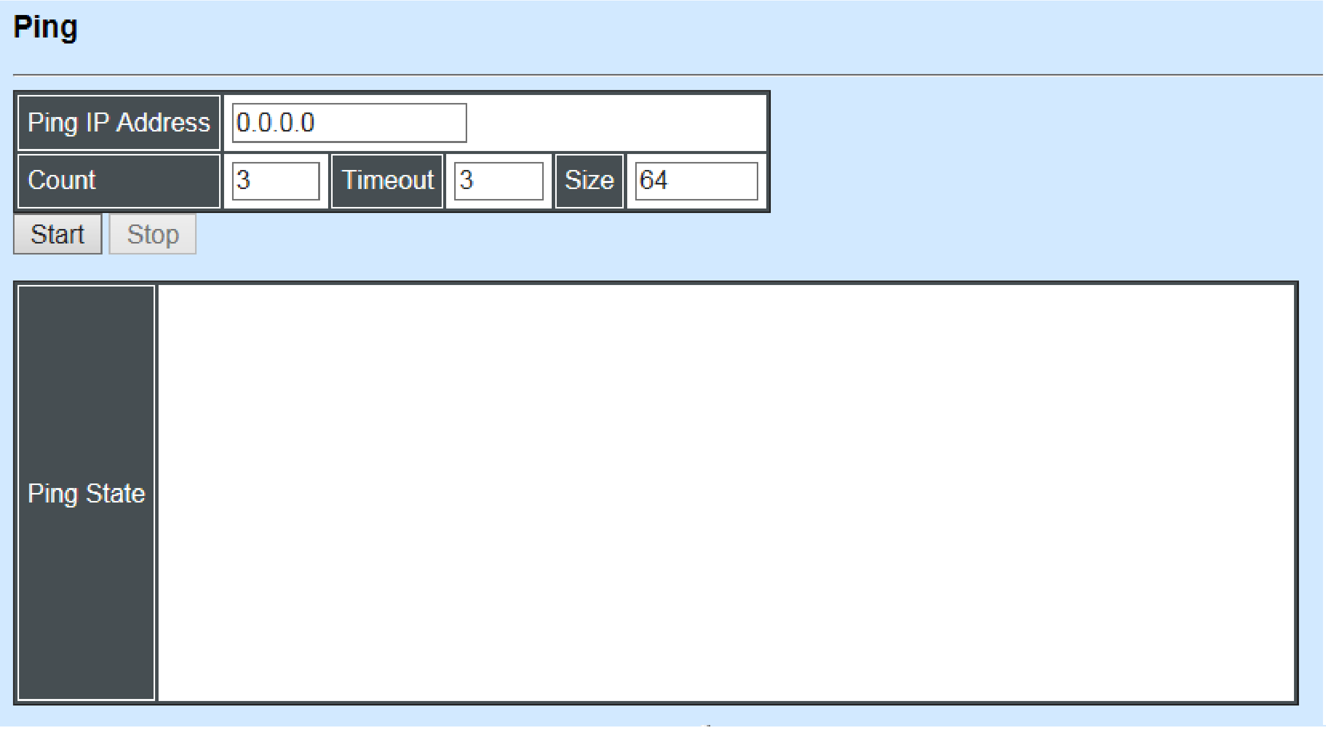
4. **FTP/TFTP Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

5. **Load Factory Setting:** 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.

6. **Load Factory Setting 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.

3.10.1 Ping

Ping can help you test the network connectivity between the Managed Switch and the host. Select **Ping** from the **System Utility** menu and then the following screen page appears.



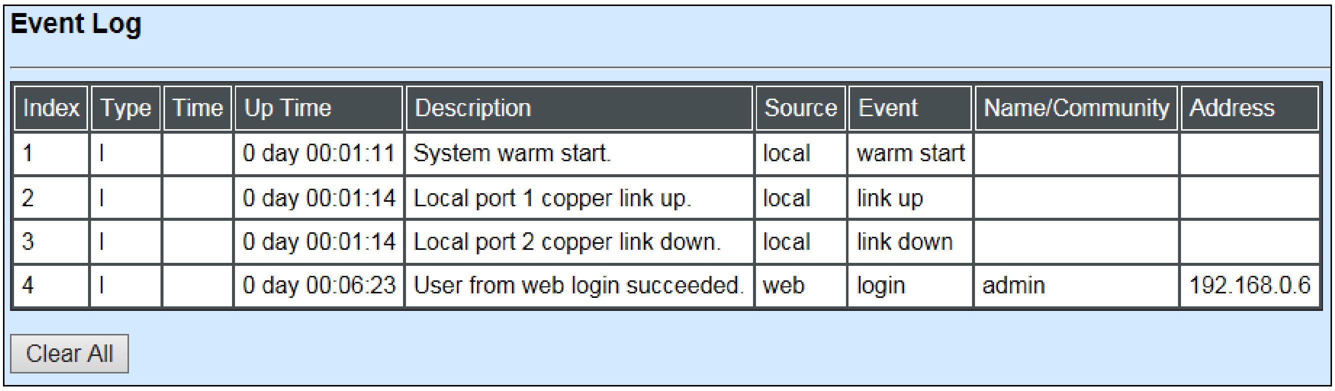
Ping

Ping IP Address	0.0.0.0				
Count	3	Timeout	3	Size	64

You can also specify count s, timeout and size of the Ping packets.
Click **Start** to start the Ping process.

3.10.2 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.



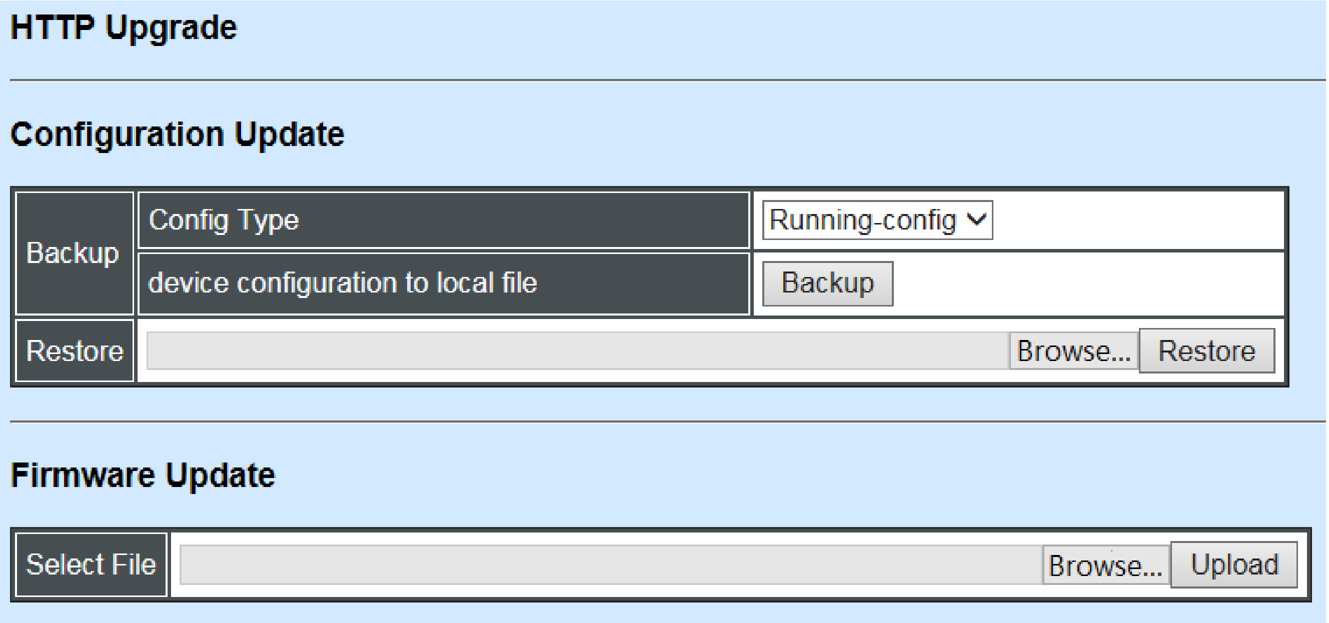
Event Log

Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:01:11	System warm start.	local	warm start		
2	I		0 day 00:01:14	Local port 1 copper link up.	local	link up		
3	I		0 day 00:01:14	Local port 2 copper link down.	local	link down		
4	I		0 day 00:06:23	User from web login succeeded.	web	login	admin	192.168.0.6

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

3.10.3 HTTP Upgrade

Users may save or restore their configuration and update their Firmware off-line. Select **HTTP Upgrade** from the **System Utility** menu and then the following screen page appears.



HTTP Upgrade

Configuration Update

Backup	Config Type	Running-config
	device configuration to local file	Backup
Restore		Browse... Restore

Firmware Update

Select File	Browse... Upload

To backup or restore data, click **HTTP Upgrade**

Config Type

There are three types of Config Type: Running-config, Default-config and Start-up-config

Running-config: Back up the data you're processing

Default-config: Back up the data same as factory setting.

Start-up-config: Back up the data same as last saved data.

Device Configuration to Local File: Click **Backup** and define the route where you intend to save data.

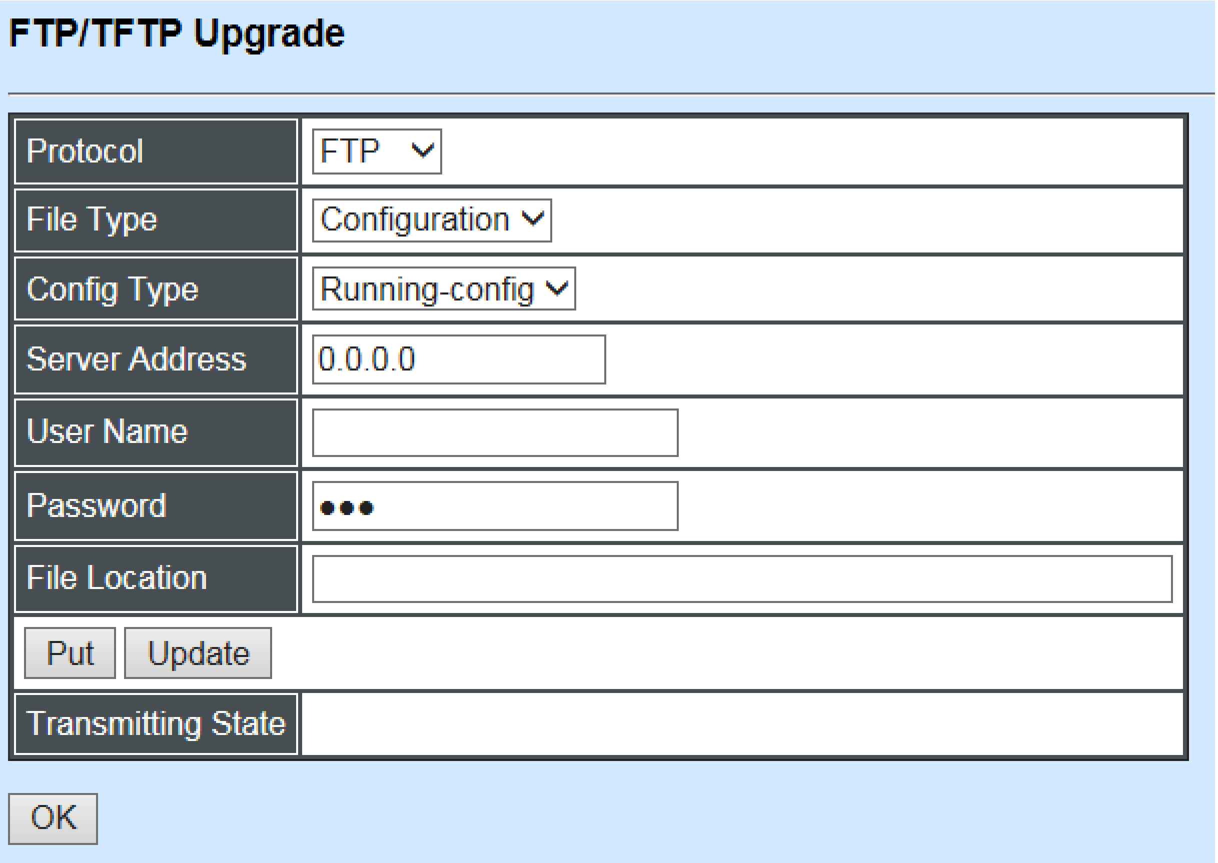
Restore: Click **Browse**, select the designated data and then click **Restore**.

Firmware Update

Select File: Click browse, select the desired file and click **Upload.**

3.10.4 FTP/TFTP Upgrade

The Gateway Controller has both built-in TFTP and FTP clients. Users may save or restore their configuration and update their Firmware on-line. Select **Upgrade** from the **System Utility** menu and then the following screen page appears.



FTP/TFTP Upgrade

Protocol	FTP
File Type	Configuration
Config Type	Running-config
Server Address	0.0.0.0
User Name	
Password	●●●
File Location	
Put Update	
Transmitting State	

OK

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

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

Config Type: Choose "Running-config", "Default-config" or "Start-up-config" which the config file will be saved or restored to

Server Address: Enter the specific 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.
Click **OK** to start the download process and receive files from the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind the user.

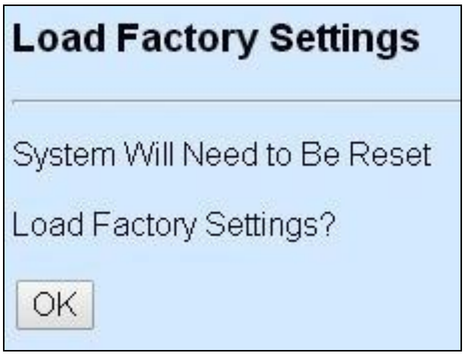
Click **Put** to start the upload process and transmit files to the server. A transmitting progress will be displayed during file transfer. Once completed, a process-completed message will pop up to remind users.

Select **Update** then press **Enter** to instruct the Gateway Controller to update existing firmware/configuration to the latest firmware/configuration received. After a successful update, a message will pop up. The Gateway Controller will need a reset to make changes effective.

3.10.5 Load Factory Settings

Load Factory Settings will set all configurations of the Gateway Controller 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.



Load Factory Settings

System Will Need to Be Reset

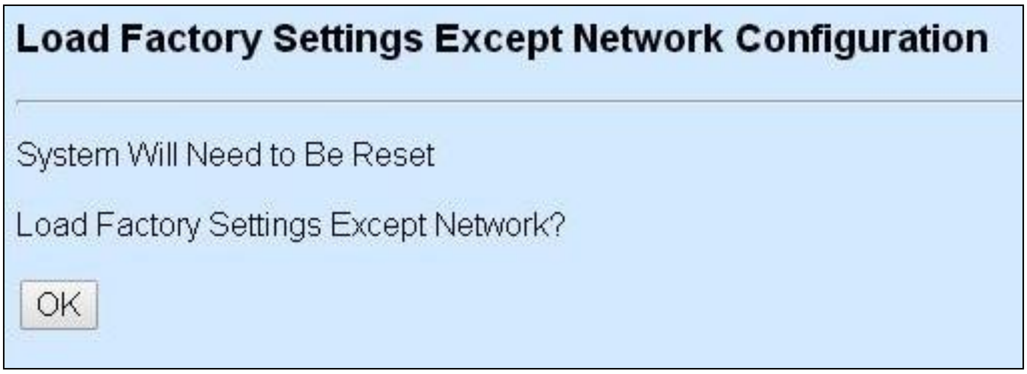
Load Factory Settings?

Click the **“OK”** button to restore the Gateway Controller back to the defaults.

3.10.6 Load Factory Settings Except Network Configuration

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

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



Load Factory Settings Except Network Configuration

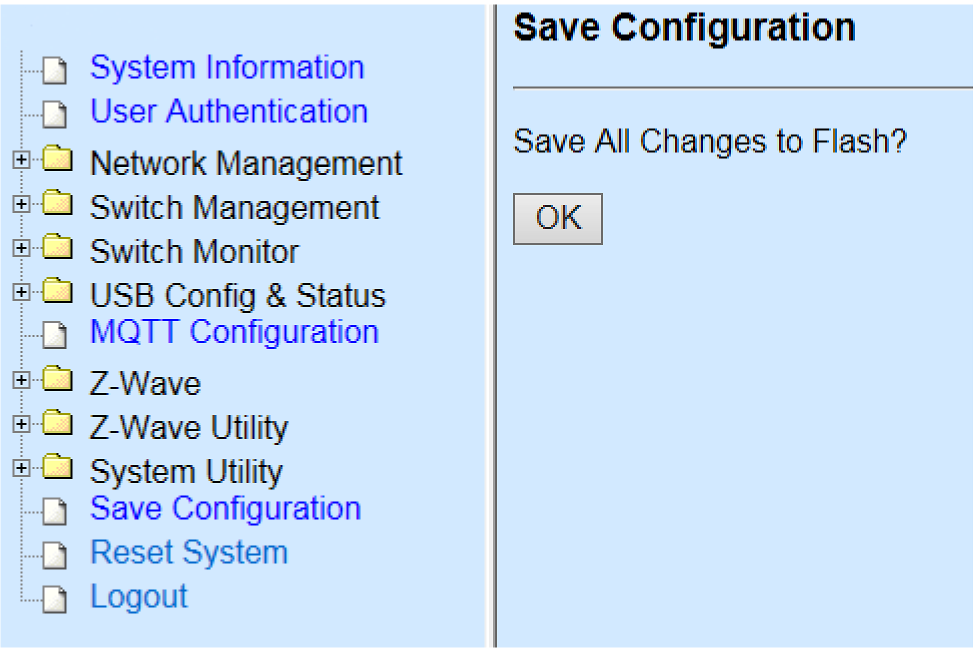
System Will Need to Be Reset

Load Factory Settings Except Network?

Click the **"OK"** button to restore the Gateway Controller back to the defaults excluding network configurations.

3.11 Save Configuration

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



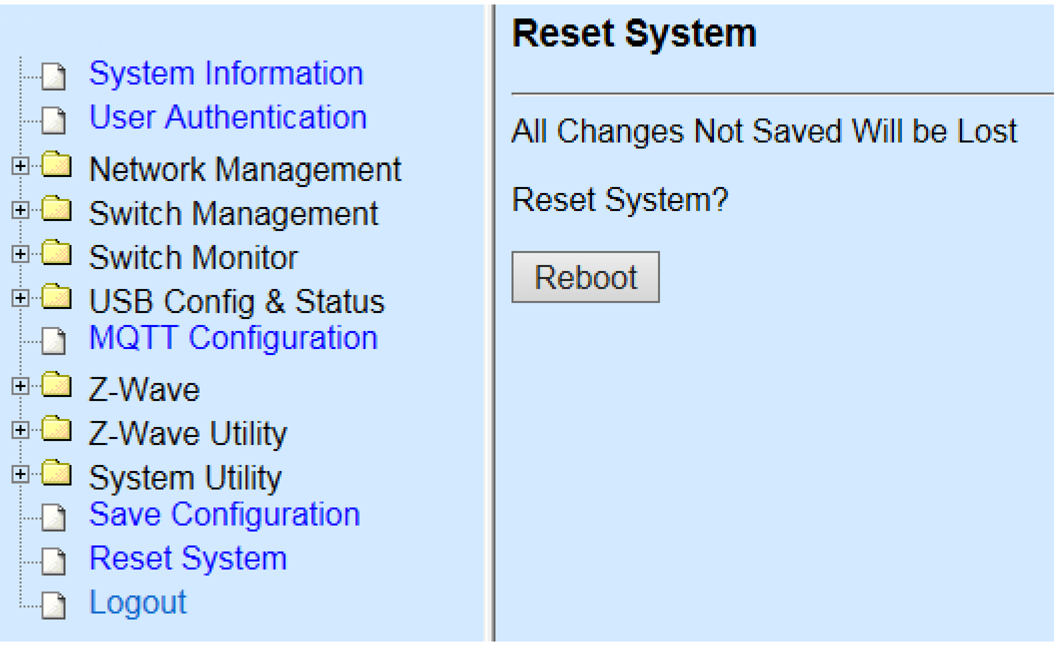
Save Configuration

Save All Changes to Flash?

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

3.12 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.



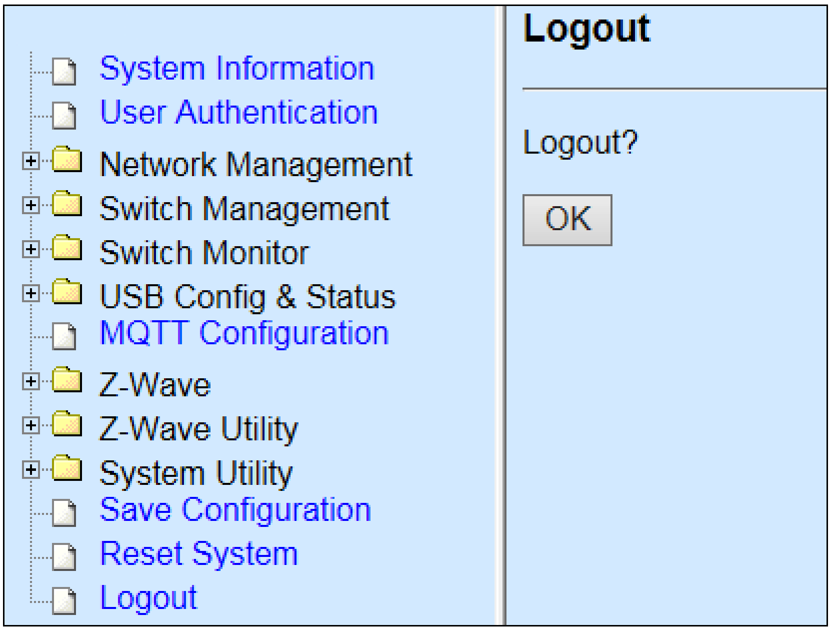
All Changes Not Saved Will be Lost

Reset System?

Click the **“Reboot”** button to restart the Gateway Controller.

3.13 Logout

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



Logout?

Click **“OK”** to log out.

APPENDIX A: DHCP Auto-Provisioning Setup

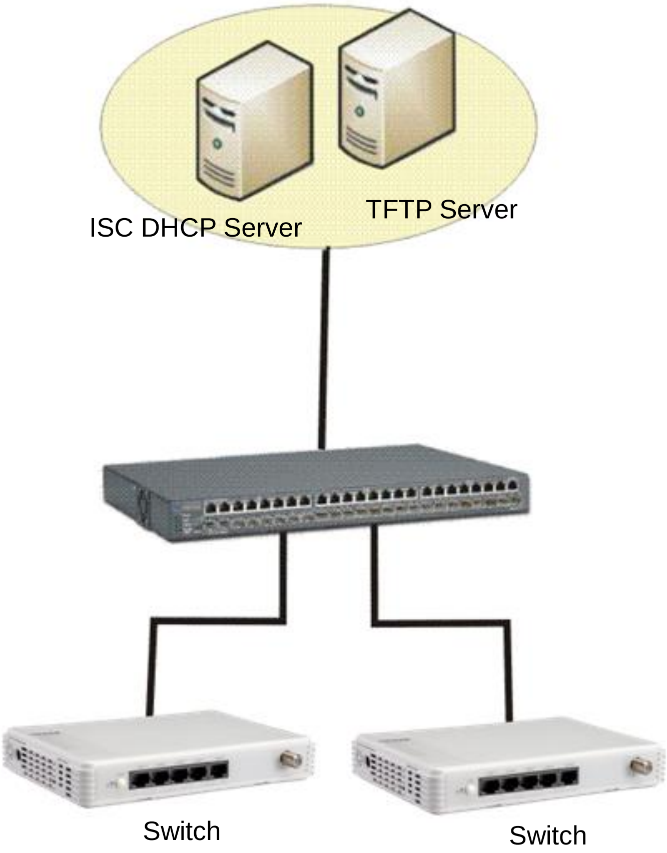
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the device that you purchased supports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

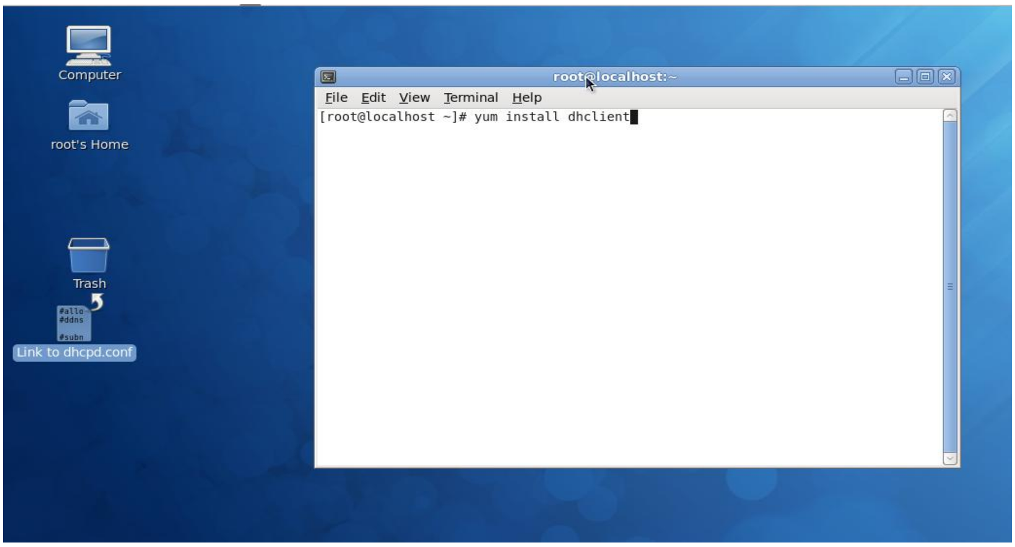
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

Step 2. Set Up Auto Provision Server

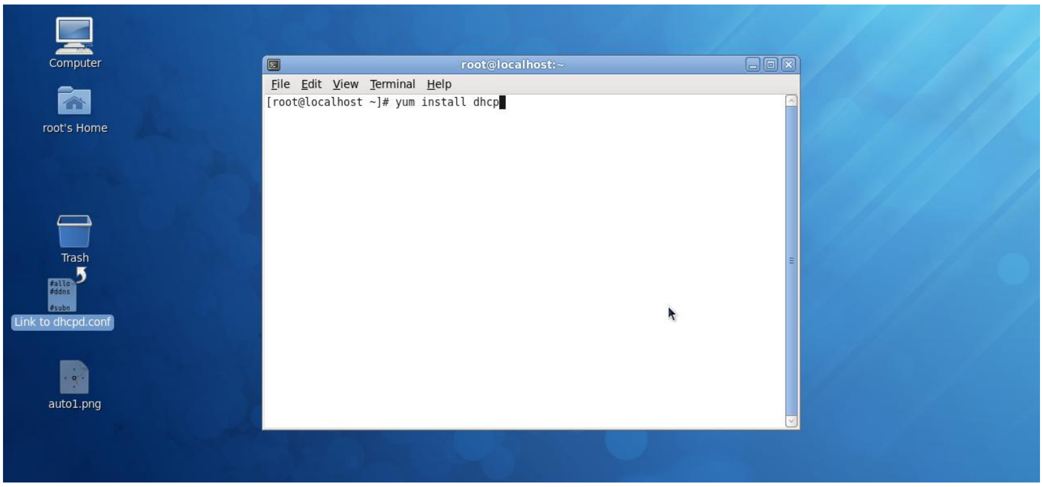
- **Update DHCP client**



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

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

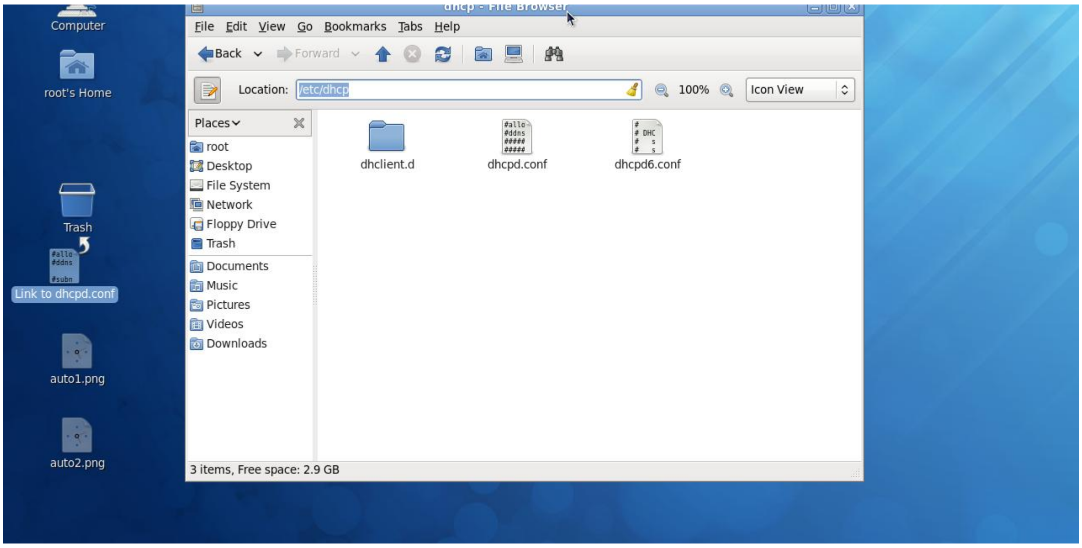
- **Install DHCP server**



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

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

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

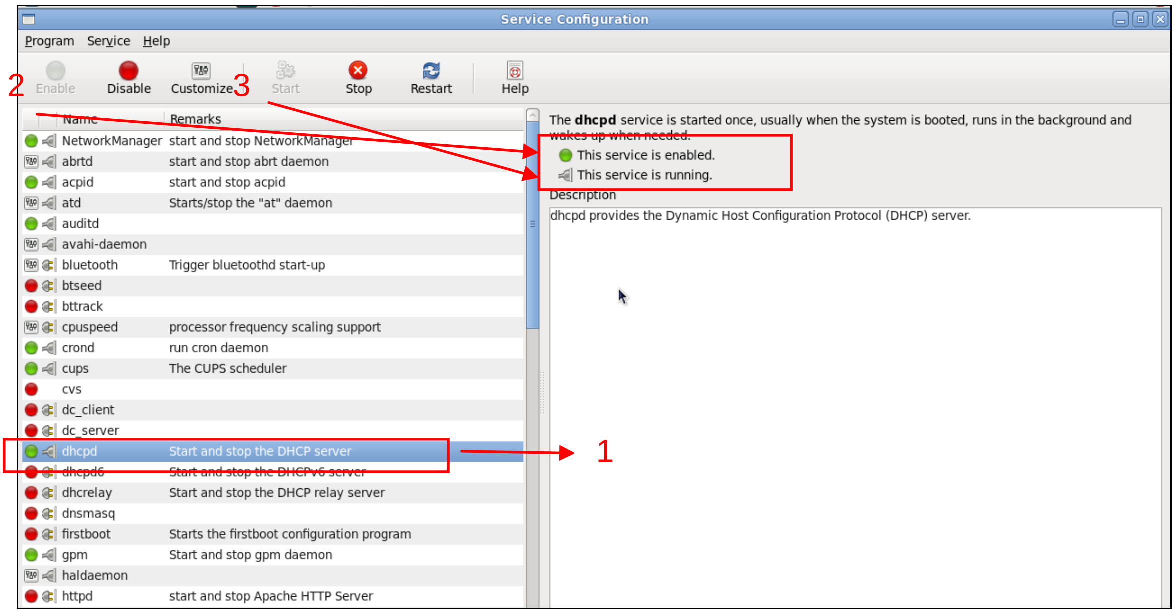


3 items, Free space: 2.9 GB

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

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

- **Enable and run DHCP service**



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

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

This service is enabled.

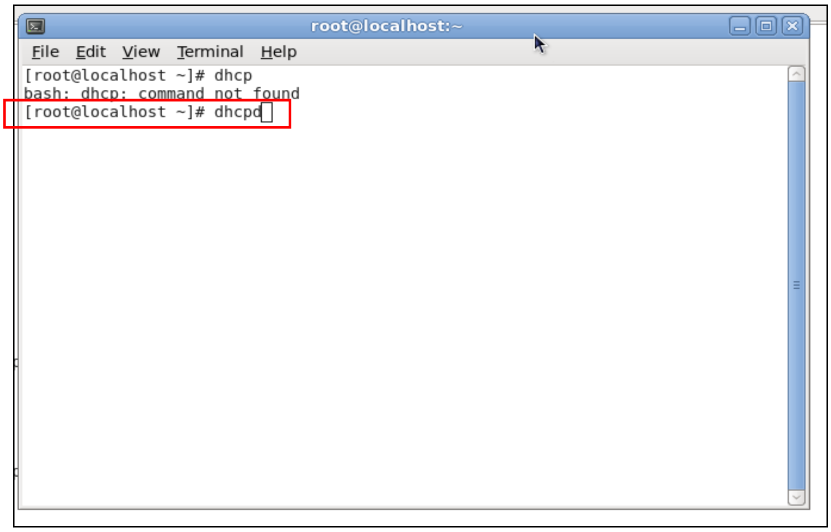
This service is running.

Description

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

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

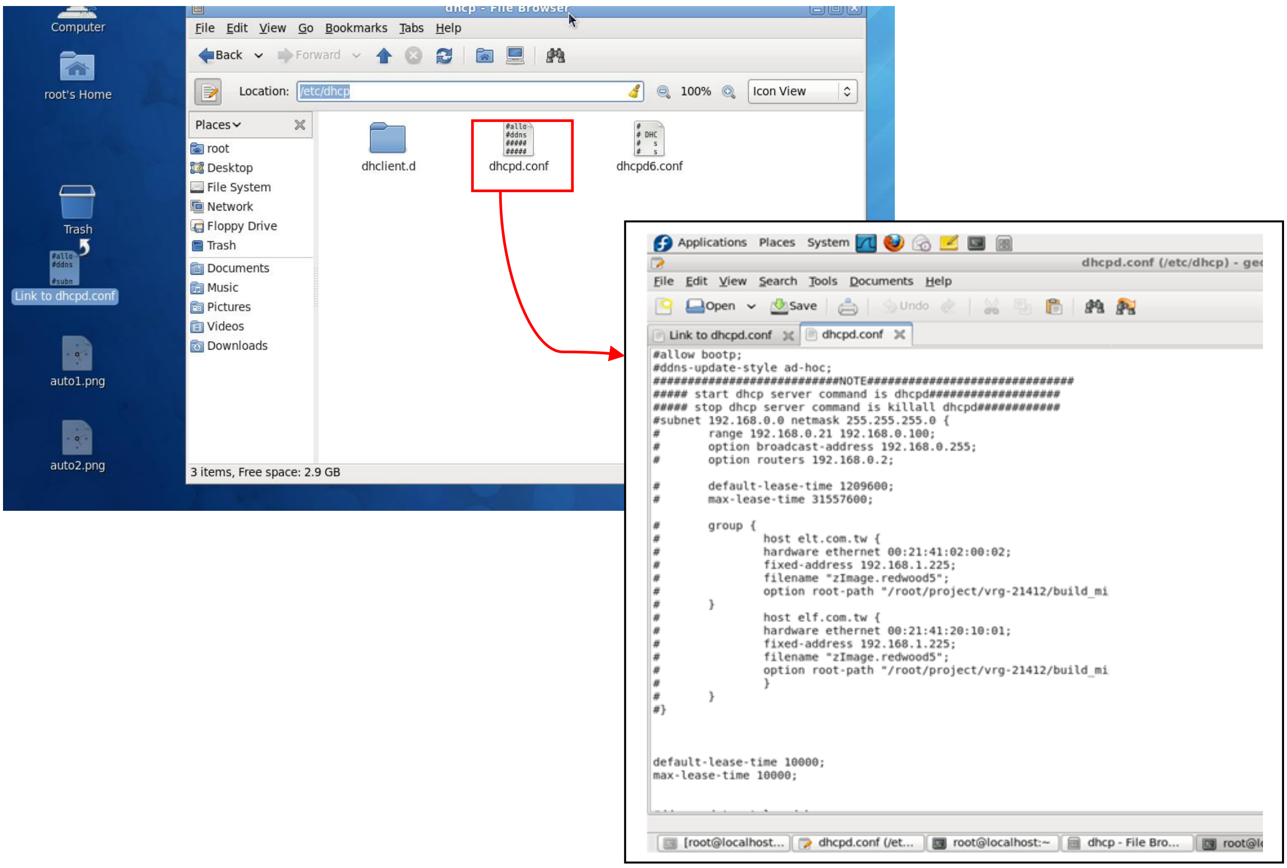
NOTE: *DHCP service can also be enabled using CLI. Issue "dhcpd" command to enable DHCP service.*



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

Step 3. Modify dhcpd.conf File

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

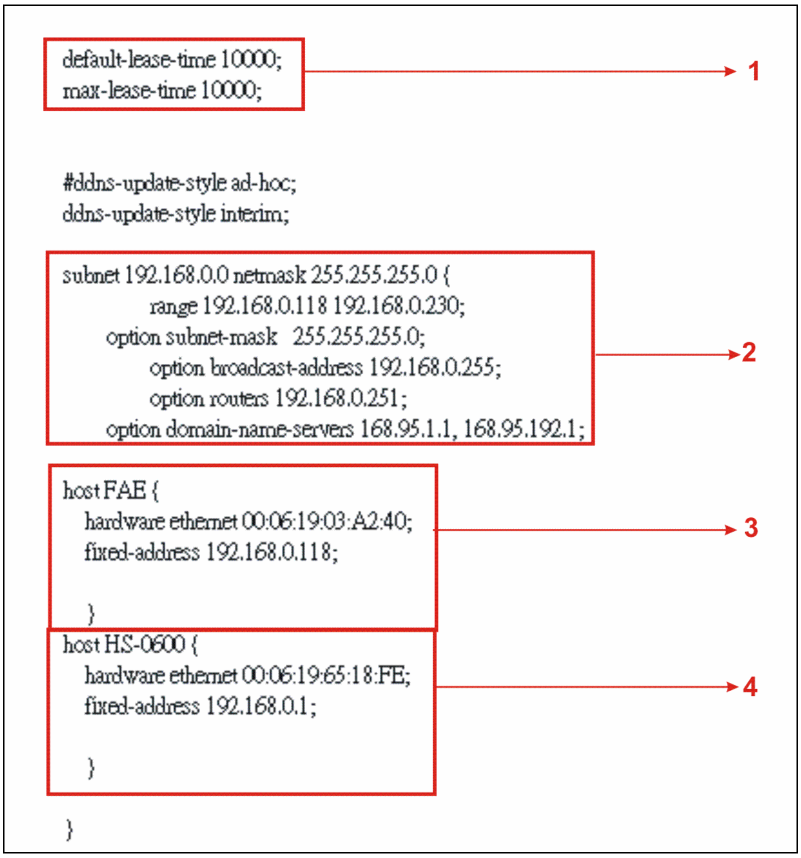


```
#allow bootp;
#ddns-update-style ad-hoc;
###########################NOTE##############################
##### start dhcp server command is dhcpd###################
##### stop dhcp server command is killall dhcpd############
#subnet 192.168.0.0 netmask 255.255.255.0 {
#       range 192.168.0.21 192.168.0.100;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

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

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


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

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

● Modify dhcpd.conf file

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



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


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

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

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

  }

}
```

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

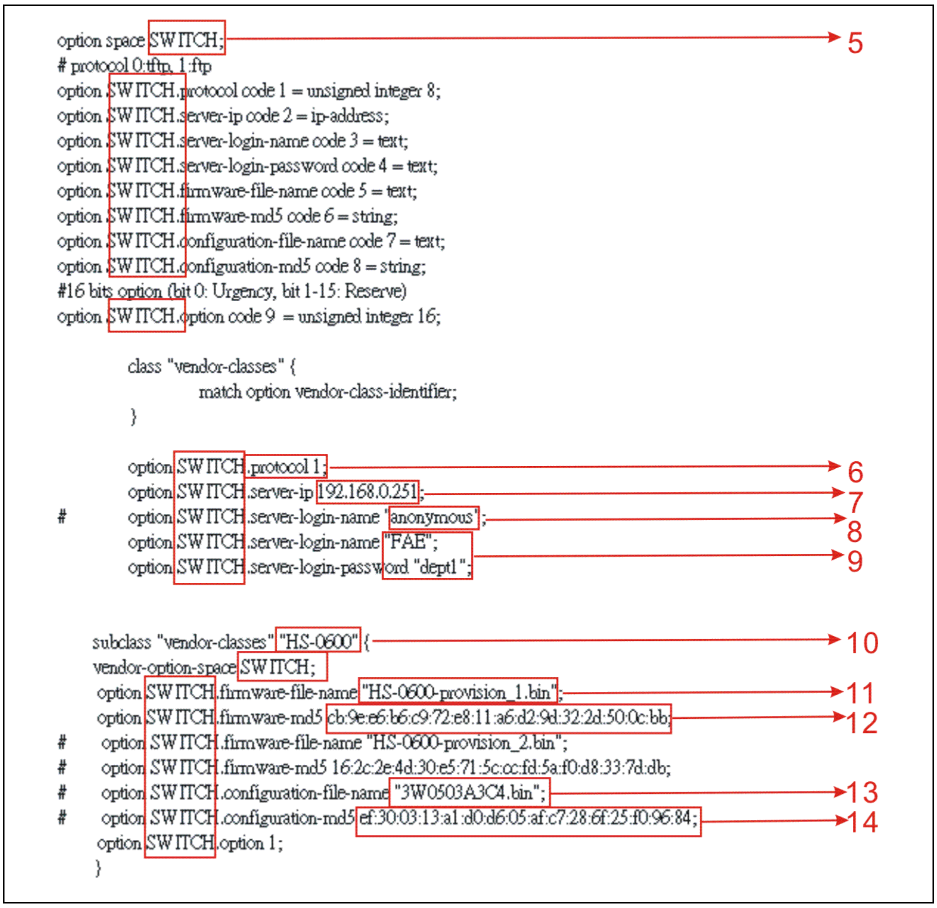
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

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

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

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

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

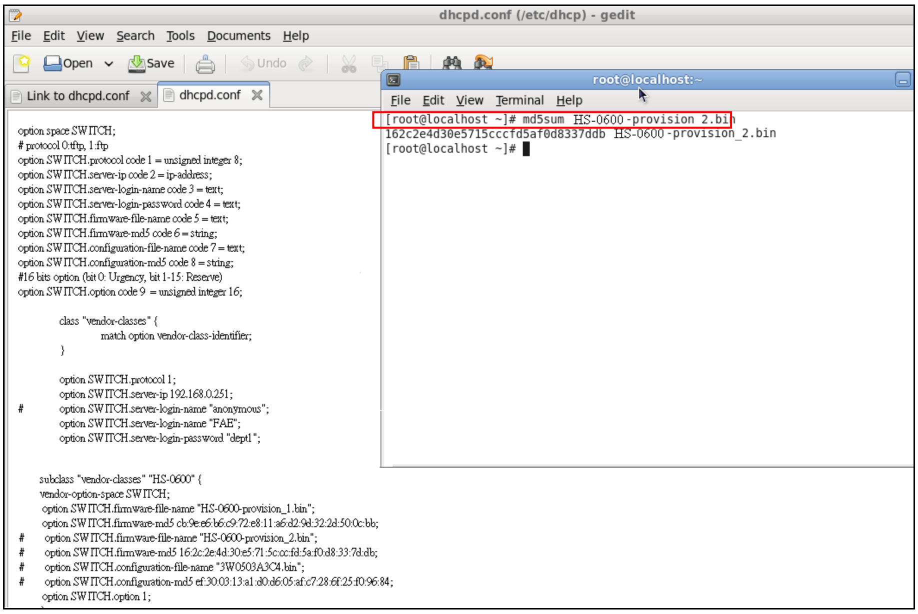


```
option space SWITCH;
# protocol 0:tftp, 1:ftp
option SWITCH.protocol code 1 = unsigned integer 8;
option SWITCH.server-ip code 2 = ip-address;
option SWITCH.server-login-name code 3 = text;
option SWITCH.server-login-password code 4 = text;
option SWITCH.firmware-file-name code 5 = text;
option SWITCH.firmware-md5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

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

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


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

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

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

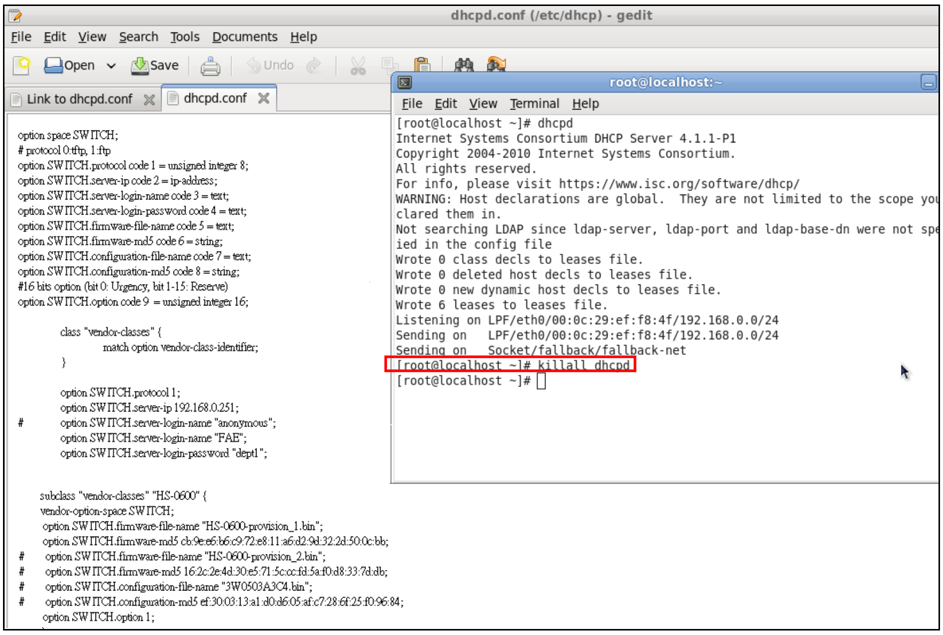
NOTE 2: *You can use either free software program or Linux default md5sum function to get MD5 checksum for firmware image and configuration file.*


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

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

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

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


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

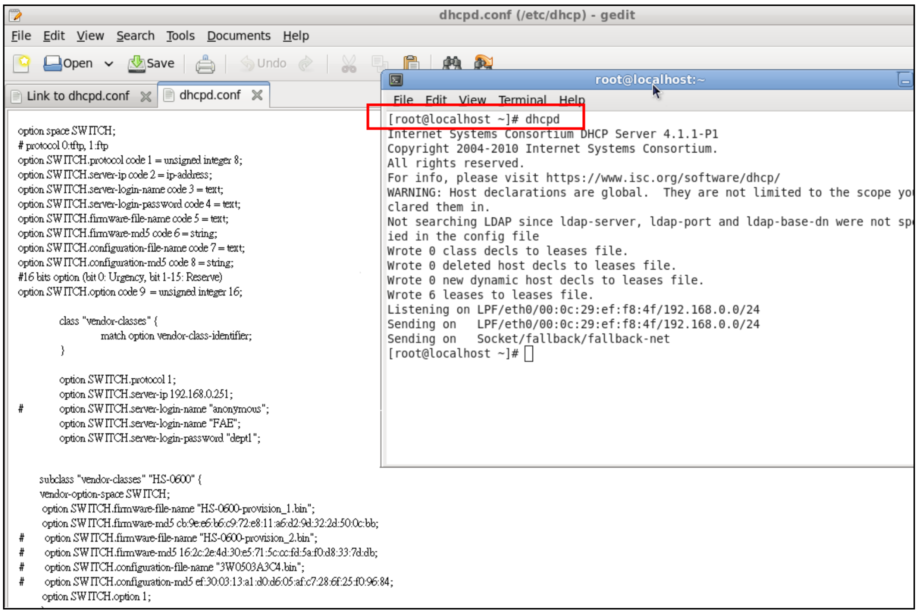
```
[root@localhost ~]# md5sum HS-0600-provision 2.bin
162c2e4d30e5715cccfd5af0d8337ddb HS-0600-provision_2.bin
[root@localhost ~]# 
```

- **Restart DHCP service**


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

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

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

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


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

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


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

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

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

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


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

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

Every time 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 device 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

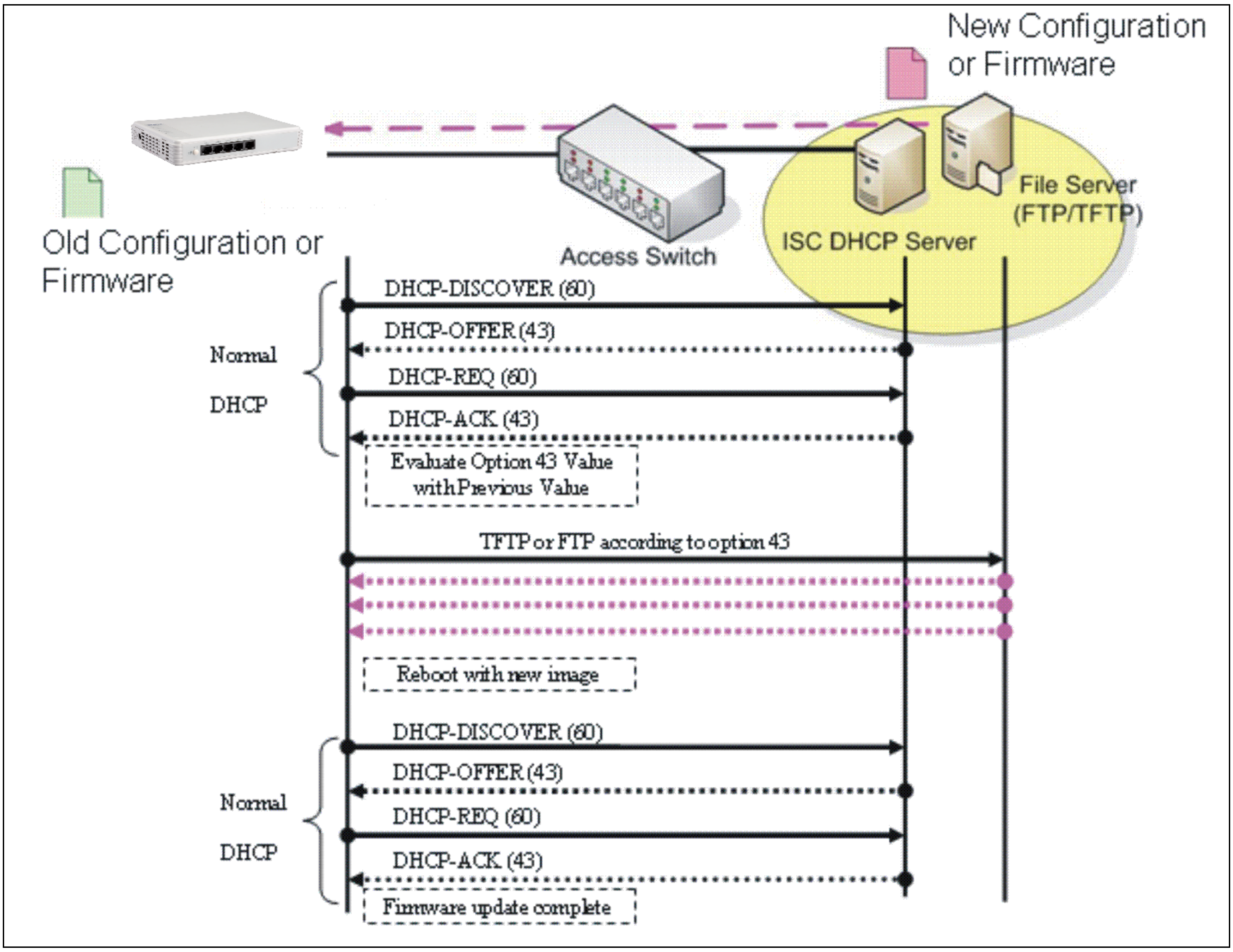
The TFTP/FTP File server should include the following items:

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.



APPENDIX B: Free RADIUS readme

The advanced RADIUS Server Set up for **RADIUS Authentication** is described as below.

When free RADIUS client is enabled on the device,

> On the server side, it needs to put this file "**dictionary.sample**" under the directory **/raddb**, and modify these three files - "**users**", "**clients.conf**" and "**dictionary**", which are on the disc shipped with this product.

* Please use any text editing software (e.g. Notepad) to carry out the following file editing works.

In the file "**users**",

> Set up user name, password, and other attributes.

In the file "**clients.conf**",

> Set the valid range of RADIUS client IP address.

In the file "**dictionary**",
Add this following line -

> **$INCLUDE dictionary.sample**

APPENDIX C: Z-Wave Terminology

Z-Wave Functionality	Documentation Terminology	Description
Inclusion	Add	The process of adding a node to the Z-Wave network
Exclusion	Remove	The process of removing a node from the Z-Wave network
Replication	Copy	The process of copying network information from one to another
Static Controller	Static Controller	A Z-Wave device capable of managing the network on a fixed location on normal operation.
Secure Environment	Secure Environment	For sensitive applications like door lock control Z-.Wave offers an enhanced encryption wrapping defined in the command class Security.
Static Update Controller ID Server (SIS)	Static Update Controller ID Server (SIS)	The central database of nodes and ids.
Primary Controller	Primary Controller	If a SIS does not exist, one controller becomes the primary controller that is only able to include new devices.
Secondary Controller	Secondary Controller	If a SIS exists, all other controllers than the primary controller are named secondary.
Association	Association	A control relationship between a controlling device and a controlled device.
Association Group	Association Group	The list of devices controller by association.
Node Information Frame	Node Information Frame	A special wireless message issued by a Z-Wave device that shows its capabilities and functions.

APPENDIX D: Control Command Class Table

This section is to demonstrate which commands are used in Section 3.8.4 Node Controller.

Section	Title	Command Class
3.8.4.1	Notification Settings	Notification Command Class V.7
3.8.4.2	Power Level Settings	Power Level Command Class V.1
3.8.4.3	Association Settings	Association Command Class V.2 Association Group Information Command Class V.1
3.8.4.4	Battery Status	Battery Command Class V.1
3.8.4.5	Door Lock Settings	Door Lock Command Class V.1
3.8.4.6	User Code Settings	User Code Command Class V.1
3.8.4.7	Wake Up Settings	Wake Up Command Class V.2
3.8.4.8	Sensor Multilevel Settings	Multilevel Sensor Command Class V.9
3.8.4.9	Basic Settings	Basic Command Class V.1
3.8.4.10	Binary Settings	Binary Switch Command Class V.1
3.8.4.11	Switch Multilevel Settings	Multilevel Switch Command Class V.3
3.8.4.12	Meter Settings	Meter Command Class V.3
3.8.4.13	Thermostat Setpoint Settings	Thermostat Setpoint Command Class V.1
3.8.4.14	Thermostat Mode Settings	Thermostat Mode Command Class V.1
3.8.4.15	Configuration Settings	Configuration Command Class V.1