SIMPNIC

S1
IoT Gateway

Network Management

User's Manual

Version 0.9

Revision History

Version	F/W	Date	Description
0.9	1.01.02	2018/09/07	First release

Trademarks

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

Copyright Statement

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.

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.

CTS Contact Information

■ Headquarter/Manufacturer:

Connection Technology Systems Inc.
18F-6, No.79, Sec.1, Xintai 5th Rd.,
XiZhi Dist., New Taipei City 221, Taiwan(R.O.C)
Tel: +886-2-2698-9661
Fax: +886-2-2698-9662
Dir.Line:+886-2-2698-9201
www.ctsystem.com
www.simpnic.com

■ Global Authorized Representatives:

Connection Technology USA Inc.
40538 La Purissima Way, Fremont, CA 94539, USA
Tel: +1-510-509-0304
Sales Direct Line: +1-510-509-0305
E-mail:cts_us@ctsystem.com

Connection Technology Systems Japan
Higobashi Bldg, No3 R201, 1-23-13, Edobori, Nisi-ku, Osaka 550-0002, Japan
Tel: +81-6-6450-8890
E-mail: cts_japan@ctsystem.com

Connection Technology Systems NE AB
August Barks Gata 21,
421 32 Västra Frölunda, Sweden
Tel: +46-31-221980
E-mail: info@ctsystem.se

COMPONET Handels GmbH
Hirschstettner Straße 19-21/Stiege I
A-1220 Wien, Austria
Tel: +43-1-2350-5660
E-mail: office@componet.at

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 routers, switches, hubs, workstations, etc..

10/100/Base-T RJ-45 Port

Depending on the model that you purchased, one 10/100Base-T RJ-45 port is located on the rear panel of the Gateway controller. The RJ-45 port allows users to connect their traditional copper-based Ethernet devices to network. This port supports 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.

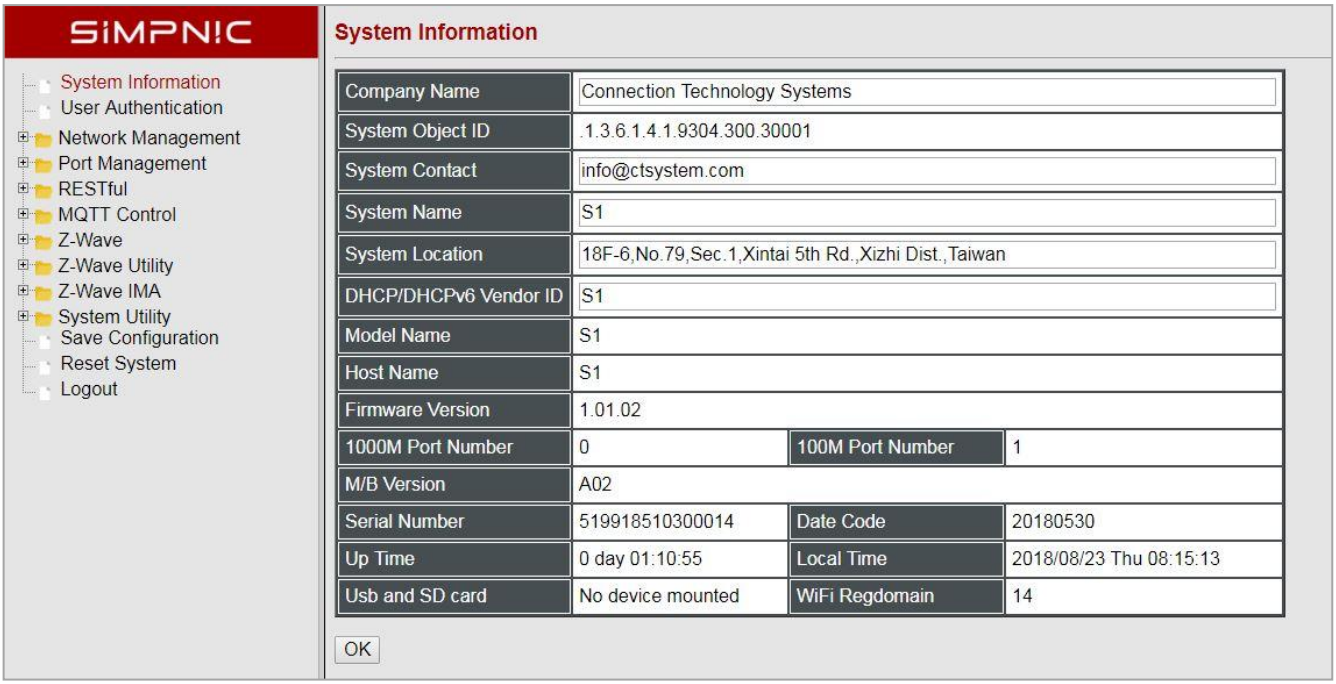
A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for a proper operation of a network with subnets defined.

2. WEB MANAGEMENT

You can manage S1 gateway via a web browser locally. The default IP of this Gateway Controller is set as DHCP mode. Through the connection of the RJ-45 port on the rear panel of S1 using a RJ45 cable with a router, you will be allowed to have an access of S1 with the IP address automatically obtained form this router for the first time. (You can change the IP address of S1 to the desired one later in its **Network Management** menu.)

Initiate a web browser and input the IP address assigned by the connected router to enter S1 system. Once you gain the access, the following login window will appear. Also input the default administrator username ***admin*** and last four letters of (MAC address + UID + serial number) as the default password to login into the main screen page.

After you login successfully, the screen with the Main Menu will show up.



In the Main Menu, there are 10 main functions, including System Information, User Authentication, Network Management, Port Management, RESTful Configuratin, MQTT Control, Z-Wave Configuration, Z-Wave Utility, Z-Wave IMA, System Utility, Save Configuration, Reset System and Logout contained. We will respectively describe their sub-functions in the following sections of this chapter.

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

2. **User Authentication:** View the registered user list. Add a new user or remove an existing user.

3. **Network Management:** Set up or view the Gateway Controller's IP address and related information required for network management applications.

4. **Port Management:** Set up port configuration and view the port status.

5. **RESTful Configuratin:** Configure RESTful API for the communication between the SiMPNiC app and gateway.

6. **MQTT Control:** Set up MQTT Configuration and view MQTT status.

7. **Z-Wave:** Manage Z-Wave network, add/delete Z-Wave sensors, and set up Z-Wave sensor configuration.

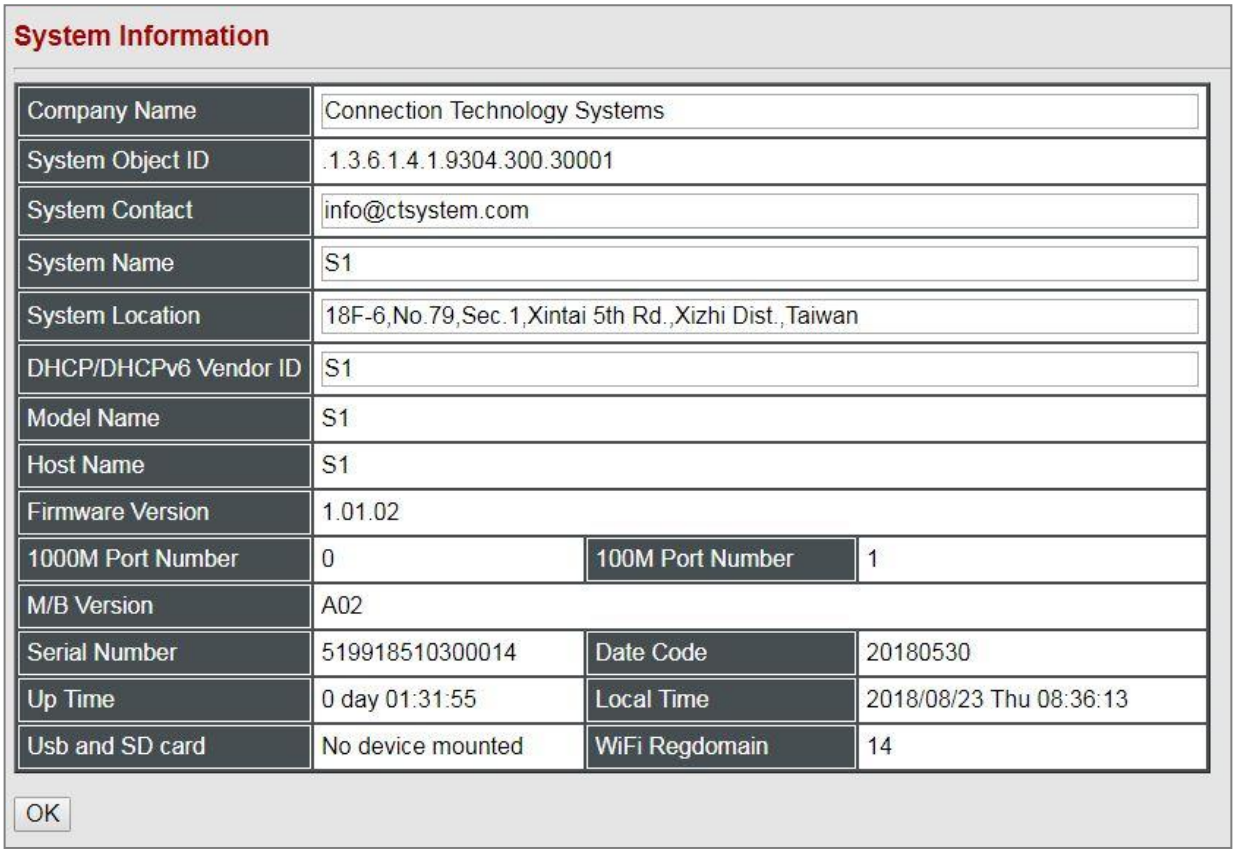
8. **Z-Wave Utility**: For the configuration related to Z-Wave, including save/backup/restore configuration files.

9. **Z-Wave IMA:** Analyze Z-Wave network traffic condition, and set up/delete the route.

10. **System Utility:** Ping, do the firmware upgrade, load the factory default settings, etc..
11. **Save Configuration:** Save all changes into the system.
12. **Reset System:** Reboot the Gateway Controller.
13. **Logout:** Exit the management interface.

2.1 System Information

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



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/DHCPv6 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 supporting 1000Mbps transmission speed.

100M Port Number: The number of ports supporting 100Mbps transmission speed.

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.

Usb and SD card: View-only field that shows the installation status of USB connector and Micro SD connector.

WiFi Regdomain: View-only field that shows the regulatory domain used to reconfigure wireless drivers to make sure that wireless hardware usage complies with local laws set by the FCC, ETSI and other organizations.

2.2 User Authentication

To prevent any unauthorized operations, only registered users are allowed to operate the Gateway Controller. Users who would like to operate the Gateway Controller need to create a user account first.

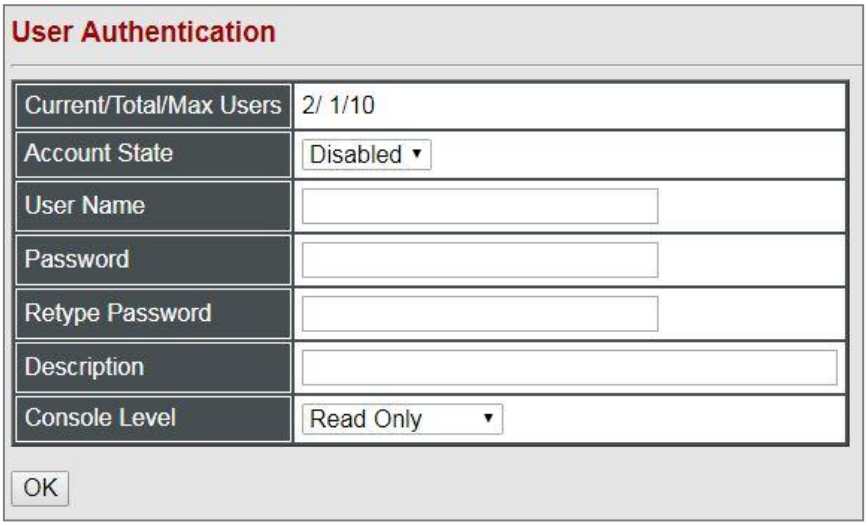
To view or change current registered users, select **User Authentication** from the **Main Menu** and then the following screen page shows up.

Password Encryption: Pull down the menu of **Password Encryption** to disable or enable MD5 (Message-Digest Algorithm). It is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. The default setting is disabled.

Click **New** to add a new user and then the following screen page appears. Up to 10 users can be registered.

Click **Edit** to modify a registered user's settings.

Click **Delete** to remove the selected registered user from the user list.



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

Current: This shows the number of registered user currently.

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

Max: This shows the maximum accounts are available for registration. The maximum number is 10.

Account State: Enable or disable this user account.

User Name: Specify the authorized user login name. Up to 20 alphanumeric characters can be accepted.

Password: Enter the desired user password. Up to 20 alphanumeric characters can be accepted.

Retype Password: Enter the password again for double-checking.

Description: Enter a unique description for this user. Up to 35 alphanumeric characters can be accepted. This is mainly used for reference only.

Console Level: Select the desired privilege level for the management operation from the pull-down menu. Three operation levels of privilege are available in the Gateway Controller:

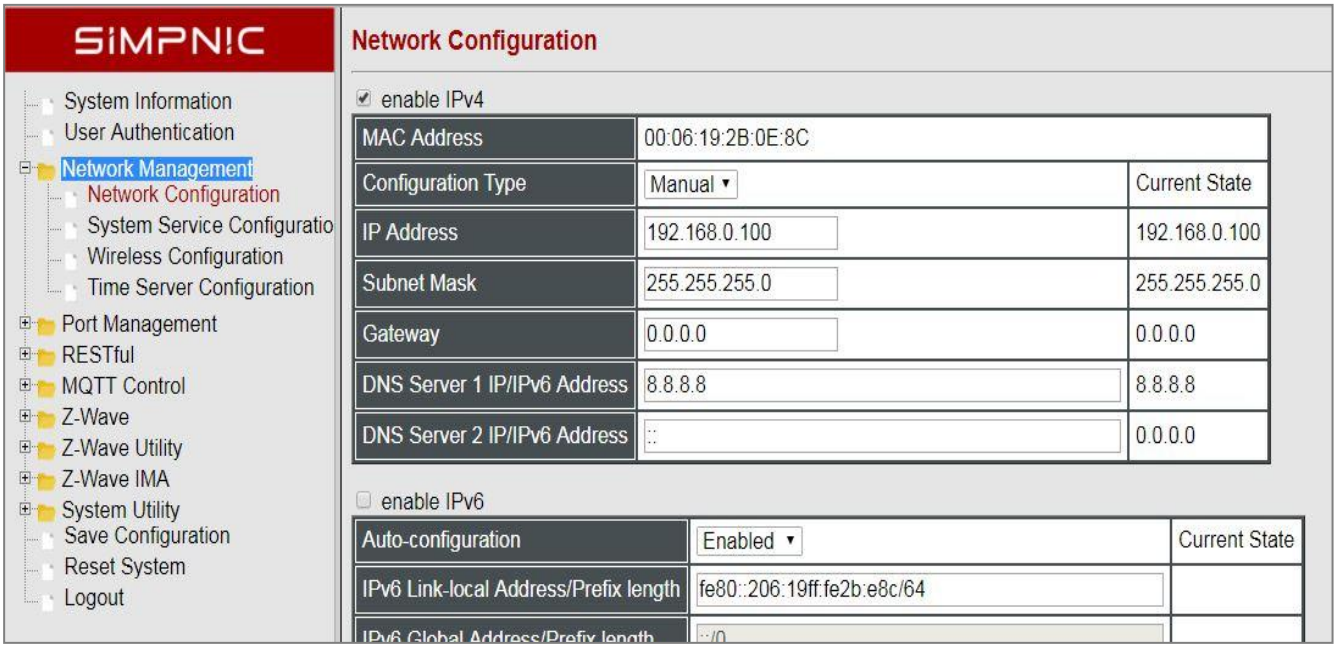
> **Administrator:** Own the full-access right. The user can maintain user account as well as system information, load the factory default settings, and so on.
>
> **Read & Write:** Own the partial-access right. The user is unable to modify user account, system information and items under System Utility menu.
>
> **Read Only:** Allow to view only.

NOTE:

1. To prevent incautious operations, users cannot delete their own account, modify their own user name and change their own account state.
2. The acquired hashed password from backup config file is not applicable for user login on Web interface.
3. We strongly recommend not to alter off-line Auth Method setting in backup configure file.
4. If Auth-Method is enabled and do firmware downgrade, users must reset default config.

2.3 Network Management

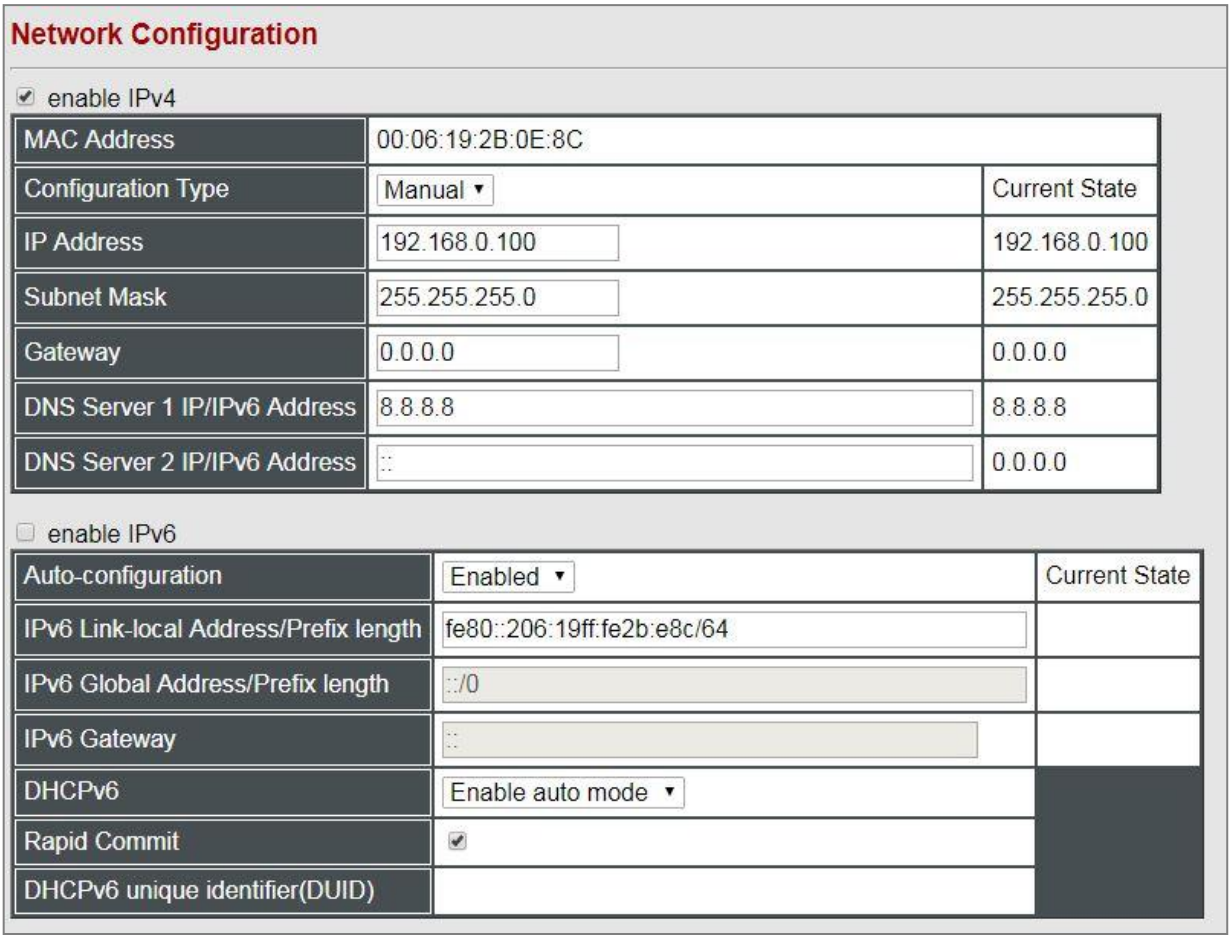
In order to enable network management of the Gateway Controller, proper network configuration is required. To do this, click the folder **Network Management** from the **Main Menu** and then several options will be displayed for your selection.



1. **Network Configuration:** Set up the required IP configuration of the Gateway Controller.
2. **System Service Configuration:** Enable or disable the specified network services.
3. **Wireless Configuration:** Set up wireless configuration of the Gateway Controller.
4. **Time Server Configuration:** Set up the time server's configuration.

2.3.1 Network Configuration

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



Enable IPv4: Click the checkbox in front of **enable IPv4** to enable IPv4 function on the Gateway Controller.

MAC Address: This view-only field shows the unique and permanent MAC address 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, "**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.

IP Address: Enter the unique IP address of 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/IPv6 Address: Specify the IP/IPv6 address of the primary DNS server.

DNS Server 2 IP/IPv6 Address: Specify the IP/IPv6 address of the secondary DNS server.

Current State: This View-only field shows currently assigned IP address (by DHCP or manual), Subnet Mask and Gateway of the Gateway Controller.

Enable IPv6: Click the checkbox in front of **enable IPv6** to enable IPv6 function on the Gateway Controller.

Auto-configuration: Enable Auto-configuration for the Gateway Controller to get IPv6 address automatically or disable it for manual configuration.

IPv6 Link-local Address/Prefix length: The Gateway Controller will form a link-local address from its MAC address and the link-local prefix FE80::/10. This is done by putting the prefix into the leftmost bits and the MAC address (in EUI-64 format) into the rightmost bits, and if there are any bits left in between, those are set to zero.

IPv6 Global Address/Prefix length: This is done in the same fashion as the link-local address, but instead of the link-local prefix FE80:: it will use the prefix supplied by the router and put it together with its identifier (which by default is the MAC address in EUI-64 format).

IPv6 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.

DHCPv6: Enable or disable DHCPv6 function

Disable: Disable DHCPv6.

Enable auto mode: Configure DHCPv6 function in auto mode.

Enable force mode: Configure DHCPv6 function in force mode.

Rapid Commit: Check to enable Rapid Commit which allows the server and client to use a two-message exchange to configure clients, rather than the default four-message exchange,

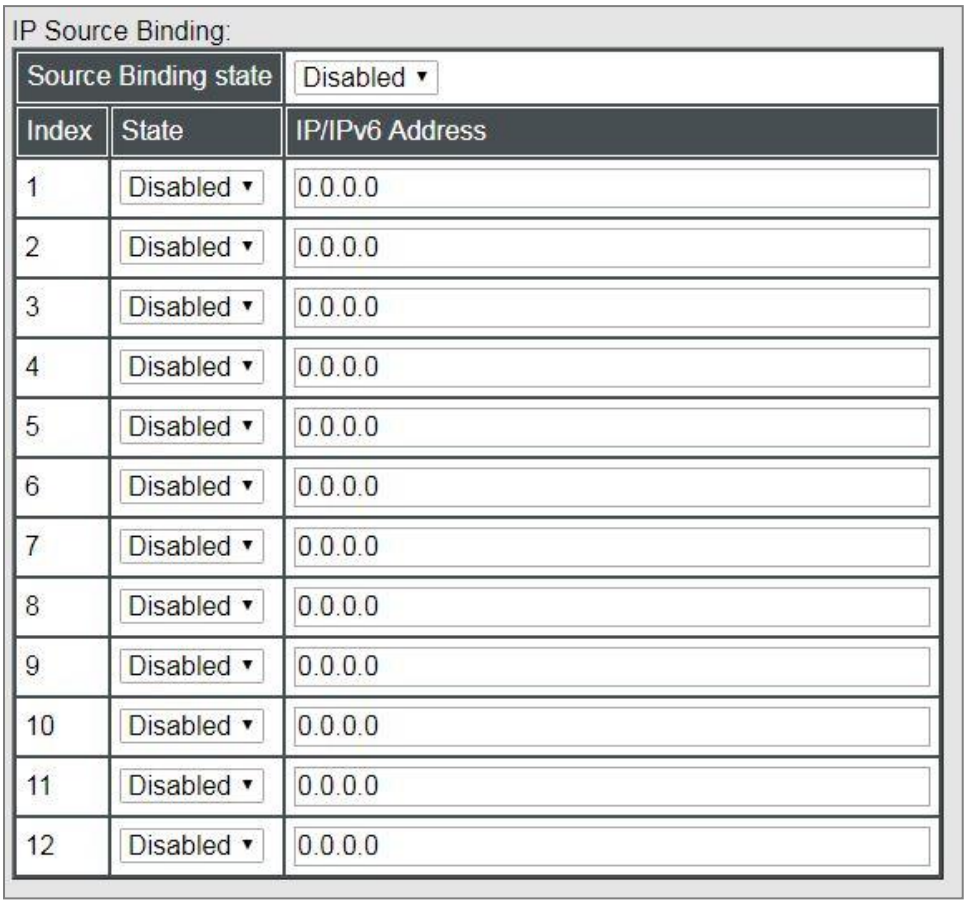
DHCPv6 unique identifier (DUID): View only field shows The DHCP Unique Identifier (DUID).

Current State: This View-only field shows currently assigned IPv6 address (by auto-configuration or manual) and Gateway of the Gateway Controller.

P2P Server: Enable or disable the P2P function.

Current State: Display the connection status bewteen the Gateway Controller and P2P server.

P2P UID: The unique UID used to register to P2P server.



Source Binding state: Globally enable or disable IP source binding.

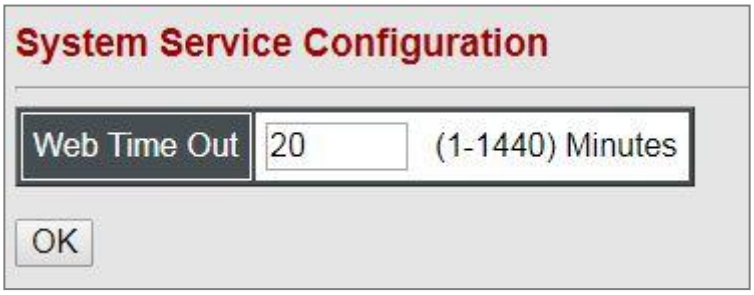
State: Disable or enable the assigned IP address to reach the management.

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 A.

2.3.2 System Service Configuration

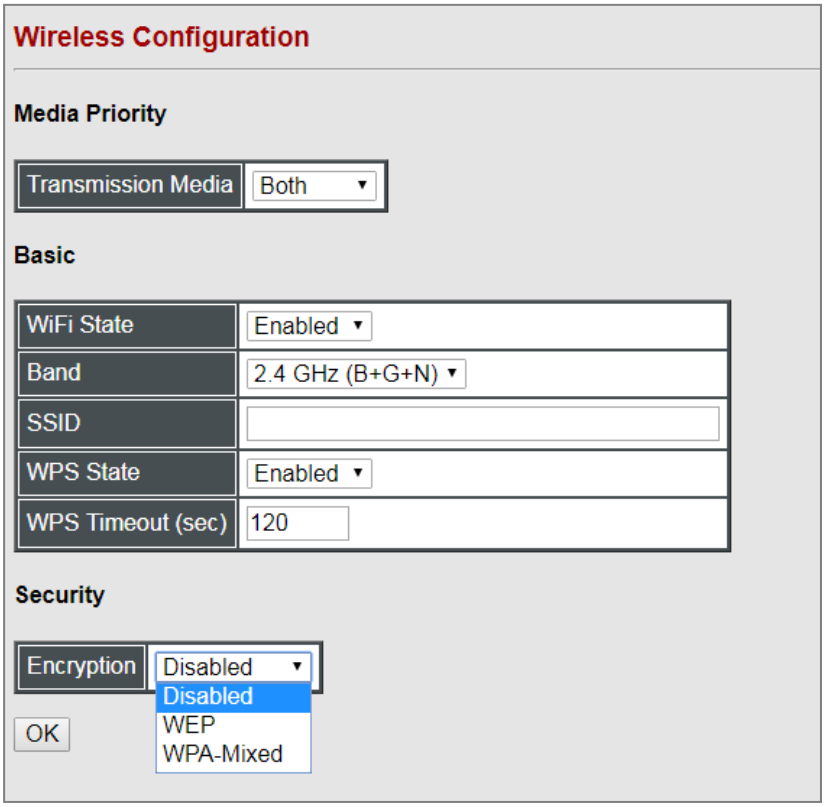
Click the option **System Service Configuration** from the **Network Management** menu and then the following screen page appears.



Web Time Out: Specify the desired time that the Gateway Controller will wait before disconnecting an inactive web session. Valid range:1-1440 minutes. Deault value is 20 minutes. Click **OK**, the new settings will be taken effect immediately.

2.3.3 Wireless Configuration

Click the option **Wireless Configuration** from the **Network Management** menu and then the following screen page appears. In this wireless setting page, the user can control the ON/OFF status of WiFi function of the Gateway Control, set up the 802.11 mode, configure the wireless security and encryption to prevent from unauthorized access and monitoring.



Transmission Media: Include **Wire**, **Wireless** and **Both** three options for the user to be chosen. From the pull-down **Transmission Media** list, you can decide either the wired or wireless connection will be the first priority method of the Gateway Controller when these connections exist at the same time.

Please note that in case **Both** option is chosen, the loop will occur when the Gateway Controller connects to the same router/access porint in the wired and wireless way. It is highly recommend that different router/access porints can be respectively connected by the wired or wireless connection of the Gateway Controller.

WiFi State: Enable or disable the WiFi function for 2.4G bandwidth.

Band: This Gateway Controller is a wireless client that supports IEEE 802.11/b/g/n (2.4 GHz). Click the **Band** pull-down list**,** there are 2.4 GHz(B), 2.4 GHz(G), 2.4 GHz(N), 2.4 GHz(B+G), 2.4 GHz(G+N), and 2.4 GHz(B+G+N) 6 options can be chosen.

SSID: When you would like your Gateway Controller to connect with the available wireless network, you need to input the network name belonging to the router/access point in the field of **SSID** for the purpose of security. This name is also referred to as the SSID.

Encryption: There are 3 encryption modes, including **Disabled**, **WEP**, and **WPA-Mixed** offered for your selection. Please pull down the **Encryption** list and select the encryption mode based on the wireless configuration of router/access point that your Gateway Controller would like to connect for the wireless security. For more details on the setup in these different modes, please refer to the following description.

If **Disabled** option is chosen, the Gateway Controlle can directly connect to the access point/router without inputting any key.

WEP(Wired Equivalent Privacy) is a basic method of encrypting data based on IEEE 802.11 standard for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the encryption key of the connected access point/router.

When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F(a-f)) or ASCII (American Standard Code for Information Interchange - alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network.

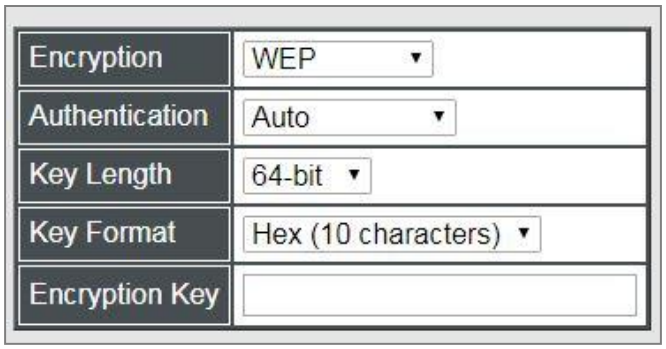
Example,

64-bit hexadecimal keys are exactly 10 characters in length. (12345678FA is a valid string of 10 characters for 64-bit encryption.)

128-bit hexadecimal keys are exactly 26 characters in length. (456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption.)

64-bit ASCII keys are up to 5 characters in length (DMODE is a valid string of 5 characters for 64-bit encryption.)

128-bit ASCII keys are up to 13 characters in length (2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption.)



- **Authentication:** Include Auto, Open System, or Shared Key three options for Gateway Controller's authentication.

- **Key Length:** Include 64-bit or 128-bit encryption type. The must have the same WEP encryption length as the connected access point/router.

- **Key Format:** Select "ASCII" or "Hex" from the pull-down list to set up the key value. ASCII(American Standard Code for Information Interchange) is a code for representing char as numbers from 0-127. Hexadecimal digits consist of the numbers 0-9 and the letters A-F (a-f).

- **Encryption Key:** Enter the password belonging to the access point/router that the Gateway Controller would like to connect.

WPA Mixed is the security mode which permits the Gateway Controller to connect to any access point/router with the WPA or WPA2 encryption. WPA(Wi-Fi Protected Access) is the older standard. It is a kind of encryption which improves the security of WEP; WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. And it provides a stronger wireless security than WPA.

Some older wireless access points/routers only support WPA. So, you have to select the mixed mode to open the WiFi service to this Gateway Controller.

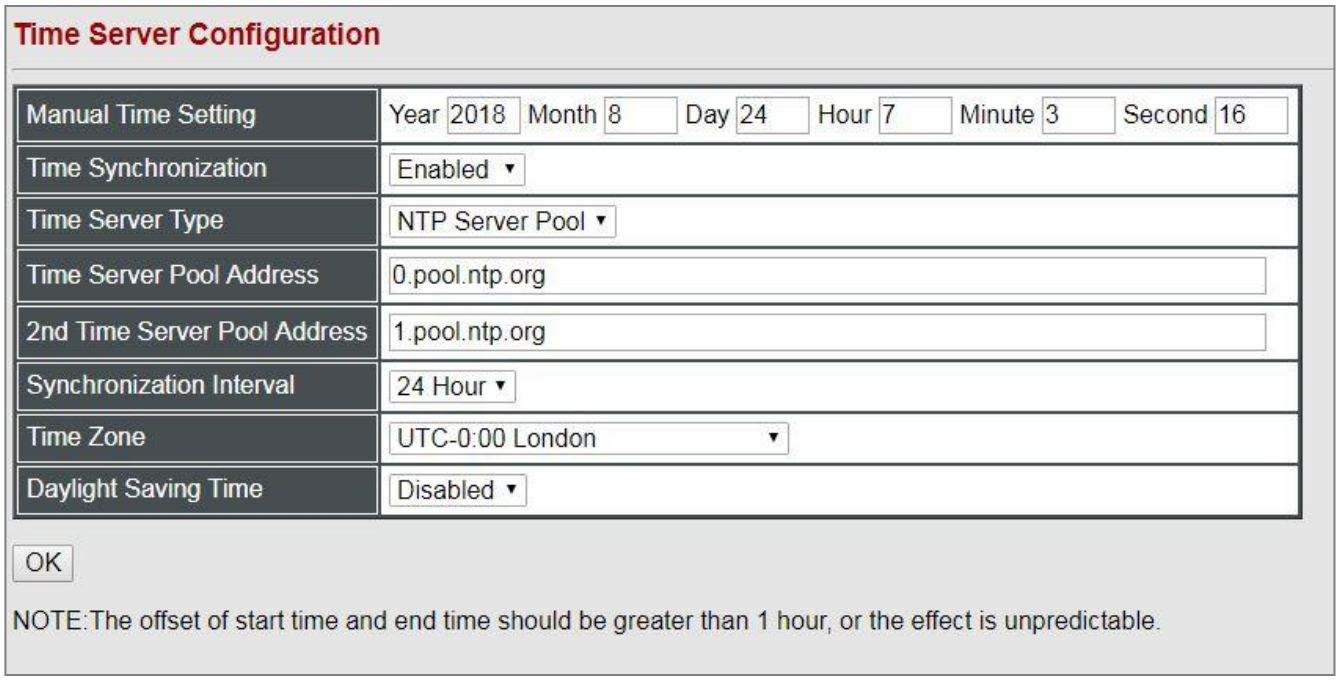
- **Pre-Shared Key Format:** Select **Passphrase** (alphanumeric format) or **Hex(64characters)** (“A-F”, “a-f” and “0-9”) from the pull-down menu.

- **Pre-Shared Key:** Specify the pre-shared alphanumeric key value in the text box. The key value can be between 8 and 63 characters long or 64 HEX characters long. Symbols and spaces can also be accepted.

Click **OK** when wireless settings are completed, the new settings will be taken effect immediately.

2.3.4 Time Server Configuration

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



Manual Time Setting: Specify the system time for the Gateway Controller manually in the field of Year, Month, Day, Hour, Minute and Second accordingly.

Time Synchronization: To enable or disable the time synchronization function.

Time Server Type: Include **NTP Server Pool** and **NTP Server** two options.

Time Server Pool Address: If the “NTP Server Pool” option is selected in Time Server Type, set up the pool address of the first NTP pool server.

2nd Time Server Pool Address: If the “NTP Server Pool” option is selected in Time Server Type, set up the pool address of the secondary NTP time server. When the first NTP time server is down, the Gateway Controller will automatically connect to the secondary NTP pool server.

Time Server Domain Name: If the “NTP Server” option is selected in Time Server Type, set up the IP address of the first NTP time server.

2nd Time Server Domain Name: If the “NTP Server” option is selected in Time Server Type, set up the IP address of the secondary NTP time server. When the first NTP time server is down, the Gateway Controller will automatically connect to the secondary NTP time server.

Synchronization Interval: Set up the time interval to synchronize with the NTP time server.

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

Daylight Saving Time: Include **"Disabled"**, **"recurring"** and **"date"** three options to enable or disable the daylight saving time function. It is a way of getting more daytime hour(s) by setting the time to be hour(s) ahead in the morning.

Daylight Saving Time Date Start: If the "date" option is selected in Daylight Saving Time, click the pull-down menu to select the start date of daylight saving time.

Daylight Saving Time Date End: If the "date" option is selected in Daylight Saving Time, click the pull-down menu to select the end date of daylight saving time.

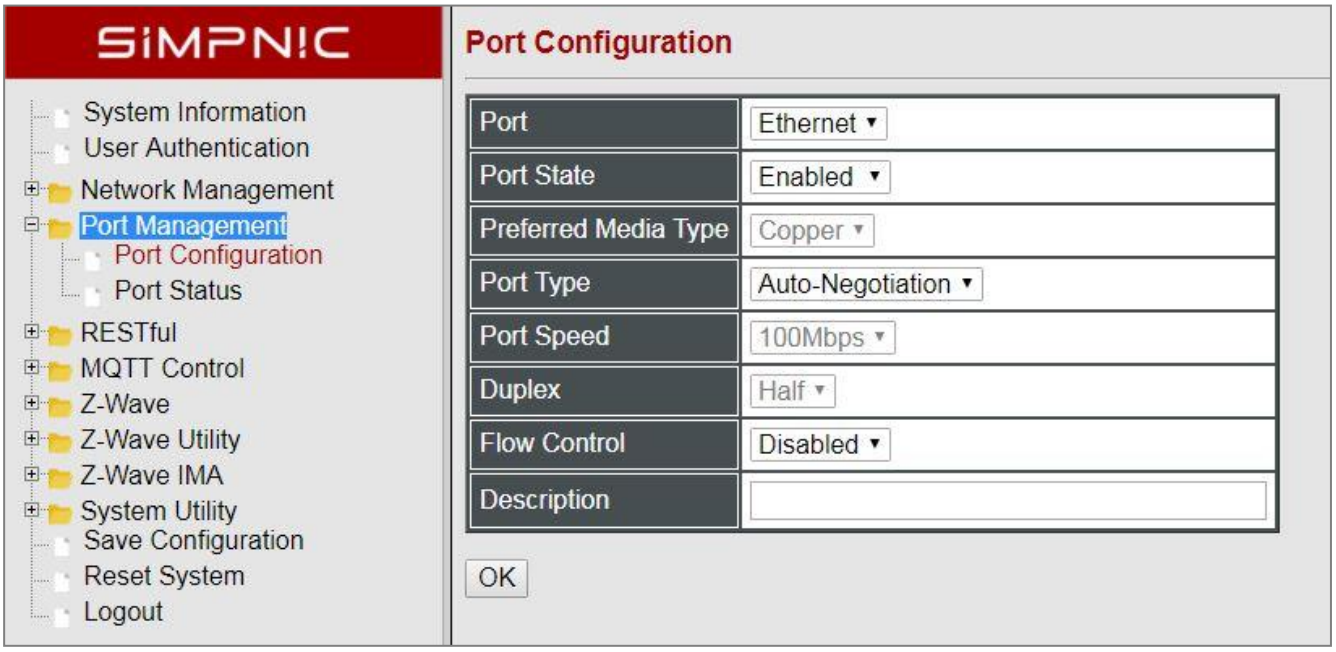
Daylight Saving Time Recurring Star: If the "recurring" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring start date of daylight saving time.

Daylight Saving Time Recurring End: If the "recurring" option is selected in Daylight Saving Time, click the pull-down menu to select the recurring end date of daylight saving time.

NOTE: SNTP is used to get the time from those NTP servers. It is recommended that the time server is in the same LAN with the Gateway Controller or at least not too far away. In this way, the time will be more accurate.

2.4 Port Management

To manage the Gateway Controller and set up the port configuration, click the folder **Port Management** from the **Main Menu** and then two options will be displayed for your selection.

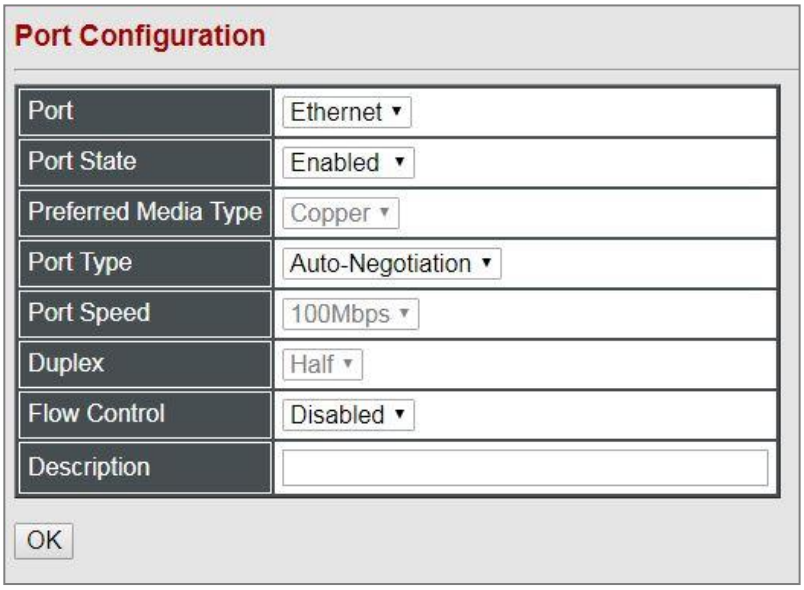


1. **Port Configuration:** Enable or disable port state, flow control, etc. for the Ethernet port of the Gateway Controller.

2. **Port Status:** View the current port state, link state, etc. of the Ethernet port and wireless port of the Gateway Controller.

2.4.1 Port Configuration

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



Port: It lists the Ethernet port of the Gateway Controller.

Port State: Enable or disable the current port state.

Preferred Media Type: View-only field that shows copper is the media type of the Gateway Controller..

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

Port Speed: When you select “Manual” as port type, you can further specify the transmission speed (10Mbps/100Mbps) of the Ethernet port. When you select “Auto-Negotiation” as port type for the Ethernet port, the devices will automatically negotiate with each other and choose the highest performance transmission mode.

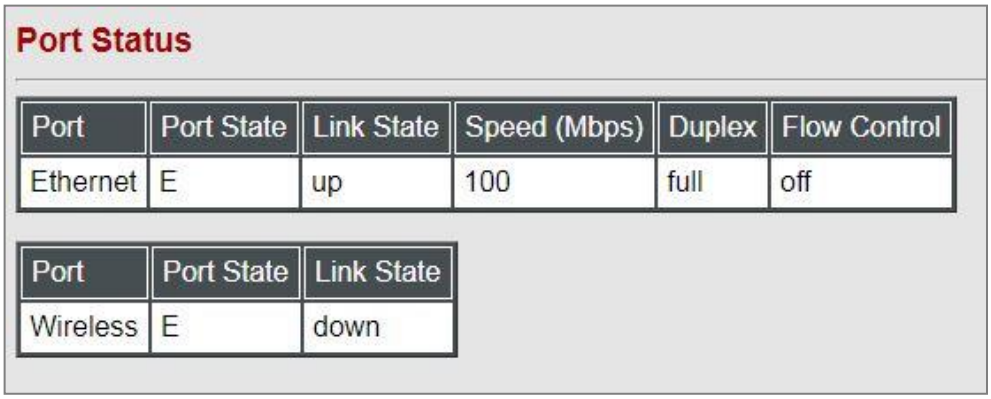
Duplex: In the Ethernet port with 10Mbps/100Mbps port speed and select “Manual” as port type, you can further specify the current operation Duplex mode (full or half duplex) of the port.

Flow Control: Enable or disable the flow control.

Description: Enter a unique description for the port. Up to 35 alphanumeric characters can be accepted.

2.4.2 Port Status

In order to view the real-time port status of the Managed Industrial PoE Ethernet Switch, select **Port Status** from the **Port Management** menu and then the following screen page appears.



Port : Display the Ethernet and wireless ports of the Gateway Controller.

Port State: This shows each port's state which can be **D** (Disabled) or **E** (Enabled).

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

E: Packets can be forwarded.

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

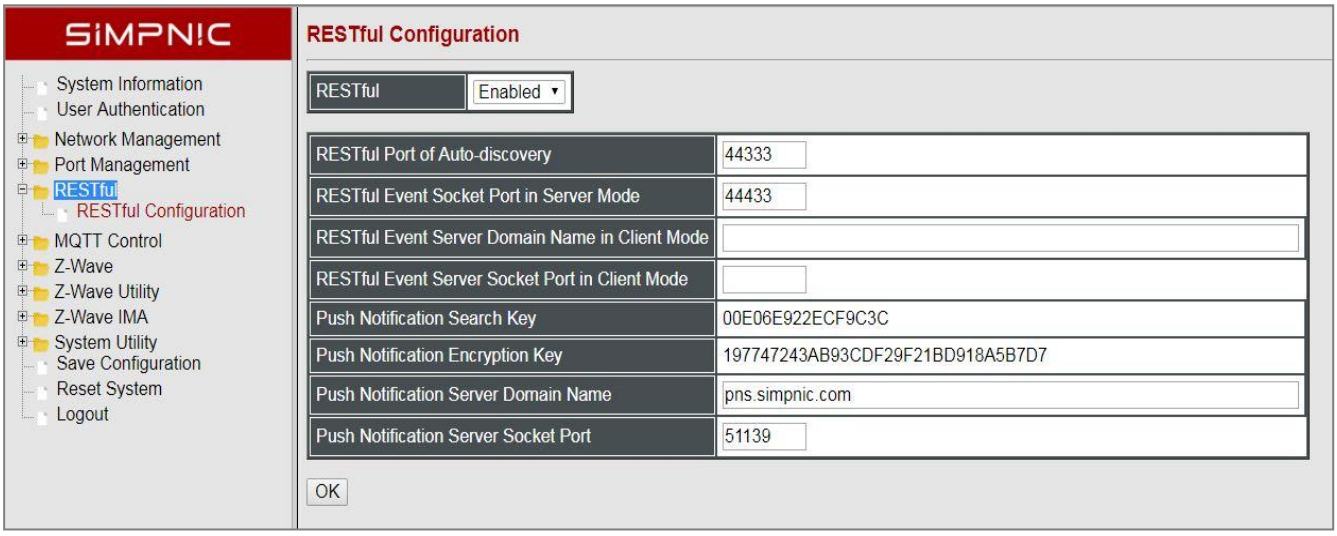
Speed (Mbps): The current operation speed of the port, which can be 10M or 100M.

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

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

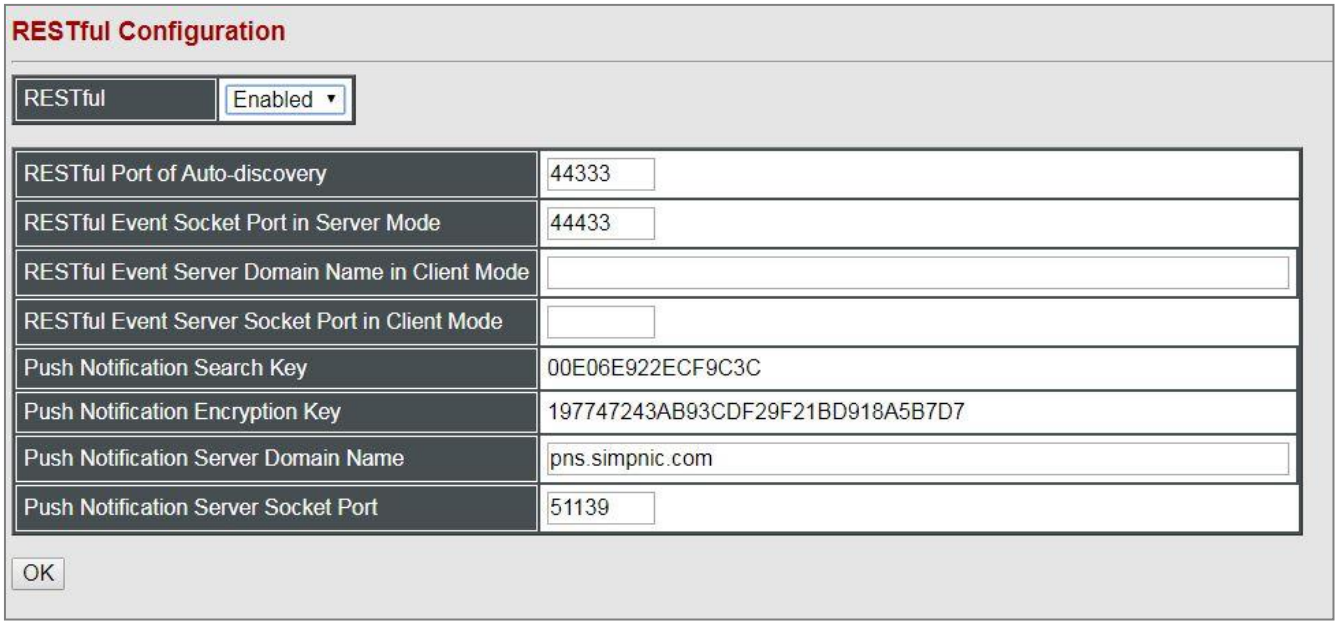
2.5 RESTful

SiMPNiC app communicates with the Gateway Controller through the RESTful API. To configure this API if needed, click the folder **RESTful** from the **Main Menu** and then one option will be displayed.



2.5.1 RESTful Configuration

Click the option **RESTful Configuration** from the **RESTful** menu and then the following screen page appears. We highly recommend not to do any changes on this RESTful setting page to avoid the failure of communication between SiMPNiC app and the Gateway Controller.



RESTful: Enable/disable the RESTful function.

RESTful Port of Auto-discovery: The port number of RESTful Port of Auto-discovery on the restful server.

RESTful Event Socket Port in Server Mode: The port number of RESTful Event Socket Port on the restful server.

RESTful Event Server Domain Name in Client Mode: The IP address or domain name of RESTful Event Server on the restful client.

RESTful Event Server Socket Port in Client Mode: The port number of RESTful Event Server on the restful client.

Push Notification Search Key: The registration key of push notification service.

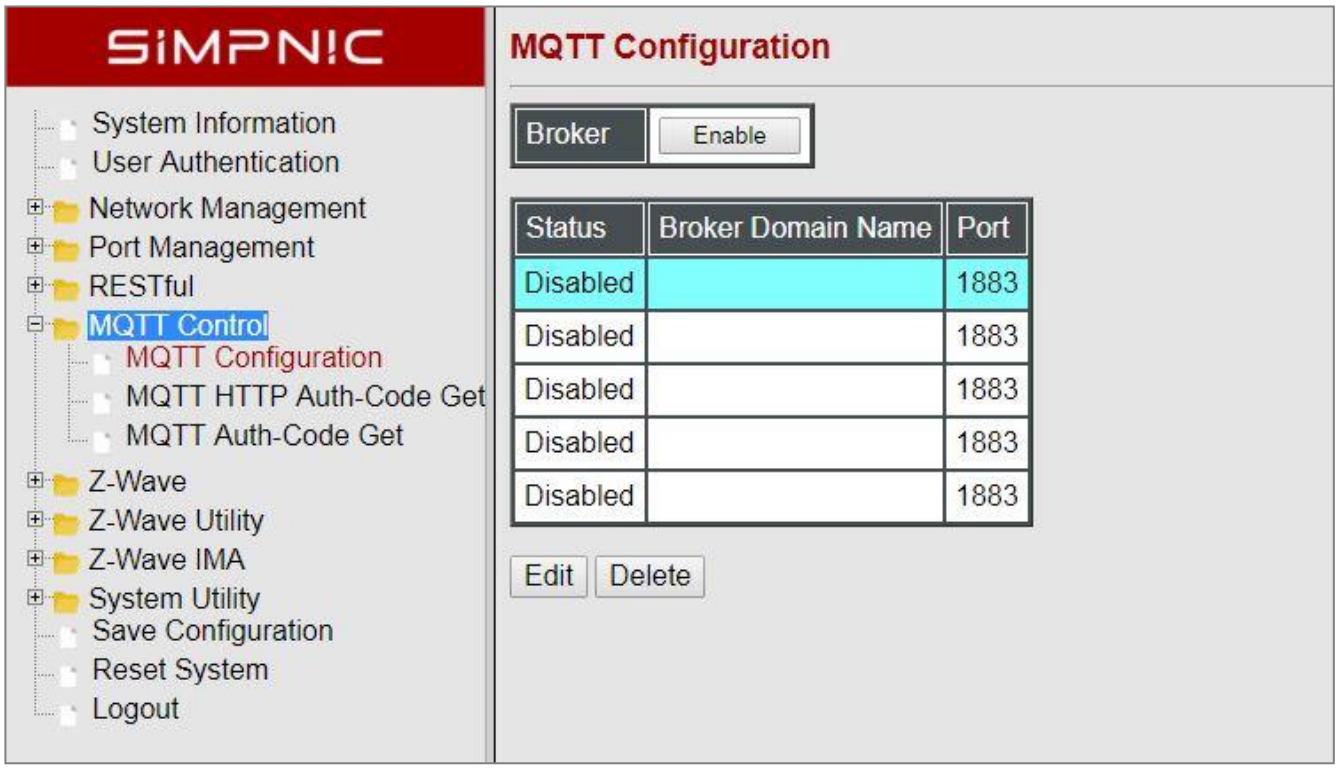
Push Notification Encryption Key: The encryption key of push notification service.

Push Notification Server Domain Name: The IP address or domain name of Push Notification Server.

Push Notification Server Socket Port: The service port number of Push Notification Server.

2.6 MQTT Control

To set up the MQTT connection between the Gateway Controller and external brokers, and view MQTT status, click the folder **MQTT Control** from the **Main Menu** and then some options will be displayed for your selection.



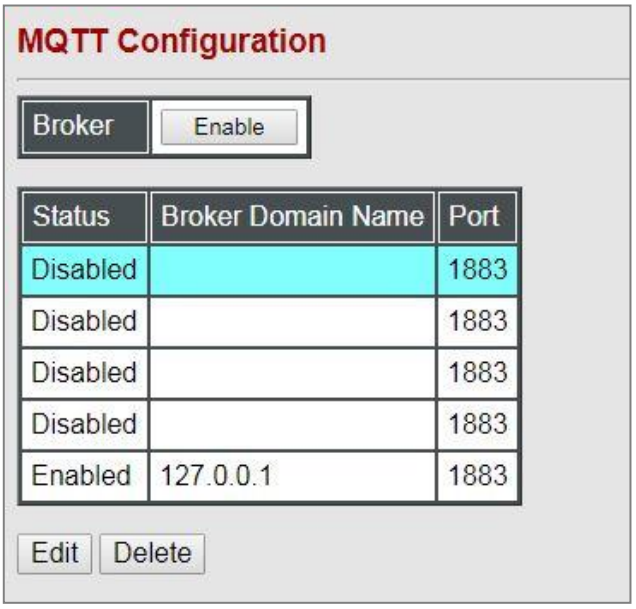
1. **MQTT Configuration:** Enable or disable the built-in MQTT broker function of the Gateway Controller, and edit/delete MQTT connection.

2. **MQTT HTTP Auth-Code Get:** This allows users to upload the CA, CLI-Cert, and CLI_key to the Gateway Controller for the specified broker's authentication.

3. **MQTT Auth-Code Get:** This allows users to upload the CA, CLI-Cert, and CLI_key to the Gateway Controller for the specified broker's authentication via FTP/TFTP.

2.6.1 MQTT Configuration

Message Queuing Telemetry Transport (MQTT) is a 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 the 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.



Broker: Enable or disable MQTT Broker function of the Gateway Controller. Default status is “Disabled”. If you can enable the MQTT broker function by clicking on the **Enable** button, the system will automatically detect the current status of the Gateway Controller and switch the button accordingly, and the Gateway Controller itself will automaicaly build a client connection and listed at the end of the table in this setting page. (See the figure above)

A message broker is an intermediary computer program module that translates a message from the formal messaging protocol of the sender to the formal messaging protocol of the receiver. Message brokers are elements in telecommunication or computer networks where software applications communicate by exchanging formally-defined messages.

The Gateway Controller offers up to 5 sets of MQTT broker connection. Click **Delete** to remove an existing setting or **Edit** for further settings and the following screen appears.

Current/Total/Max Agents	1/ 5/ 5
Enable	☐
Clean Session	☑
Broker Domain Name	
Port	1883 (0-65535)
Keep Alive	60 (0-65535)

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

Current: This shows the number of registered account currently.

Total: This shows the amount of total registered accounts.

Max: This shows the maximum accounts are available for registration. The maximum number is 5.

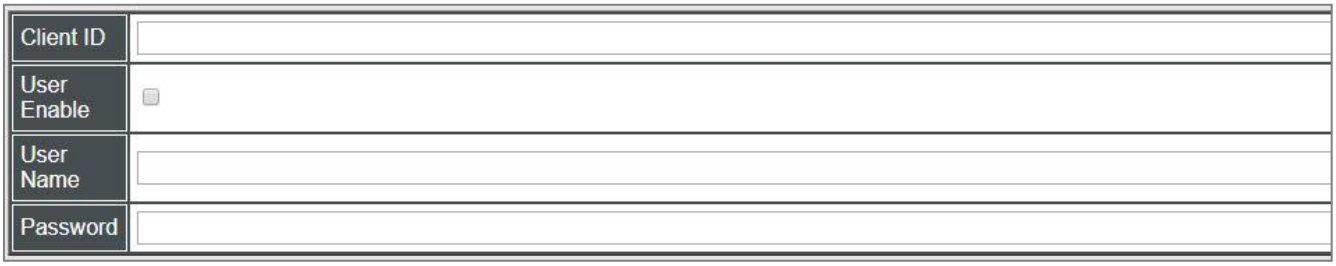
Enable: Check to enable MQTT function or vice versa. The default setting is disable.

Clean Session: The clean session flag indicates the broker, whether the client would like 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. If clean session is enabled by clicking on the checkbox, the broker will not 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 responses 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 60.

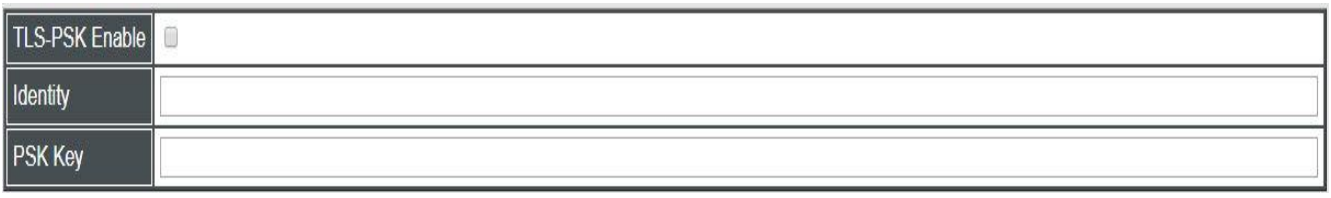


Client ID: The client identifier (short Client ID) is an identifier of each MQTT client connecting to a MQTT broker. Specify the client identifier name, up to 23 alphanumeric characters

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.

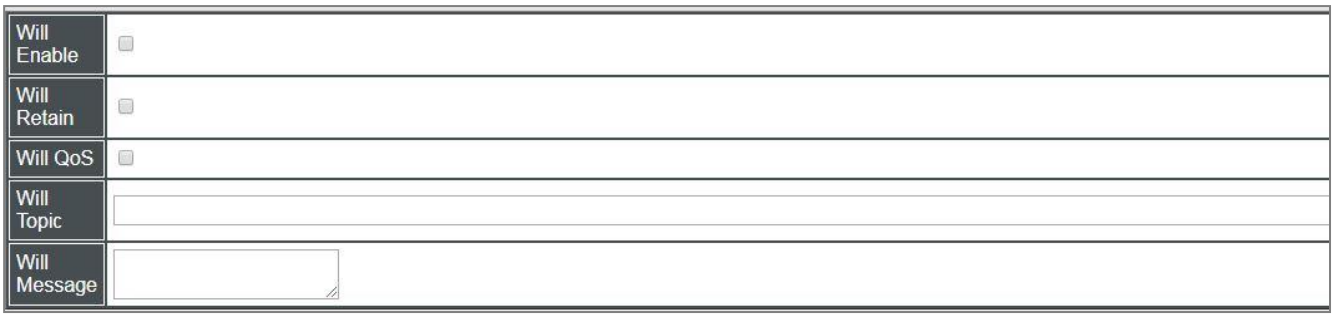


TLS-PSK Enable: Transport Layer Security pre-shared key ciphersuites (TLS-PSK) is a set of cryptographic protocols that provide secure communication based on pre-shared keys (PSKs). These pre-shared keys are symmetric keys shared in advance among the communicating parties.

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

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

TLS-Cert Enable: Enable or disable TLS anthentication with CA.



Will Enable: When Gateway Controller's disconnection occurs, all subscribers will be notified with the Will Message if this function is enabled.

Will Retain: The Will Message will be retained in server if this function is enabled. This function only works when publishing the Will message.

Will QoS: Once this function is enabled, the broker must record the Will Topic that the Gateway Controller subscribes when the Gateway Controller disconnects. The broker also must save the Will message published during this period of time. This Will message will be sent again until the Gateway Controller's connection recovers.

Note: The Gateway Controller applies QoS1 into this function, QoS1 stands that the delivery of the Will message is guaranteed one time at least.

Will Topic: The subject of the Will message.

Will Message: The content of the Will message.

2.6.2 MQTT HTTP Auth-Code Get Configuration

Upload the required CA (Certificate Authority) for the Gateway Controller's authentication when connecting with the specified broker. Select **MQTT HTTP Auth-Code Get** from the **MQTT Control** menu and then the following screen page appears.

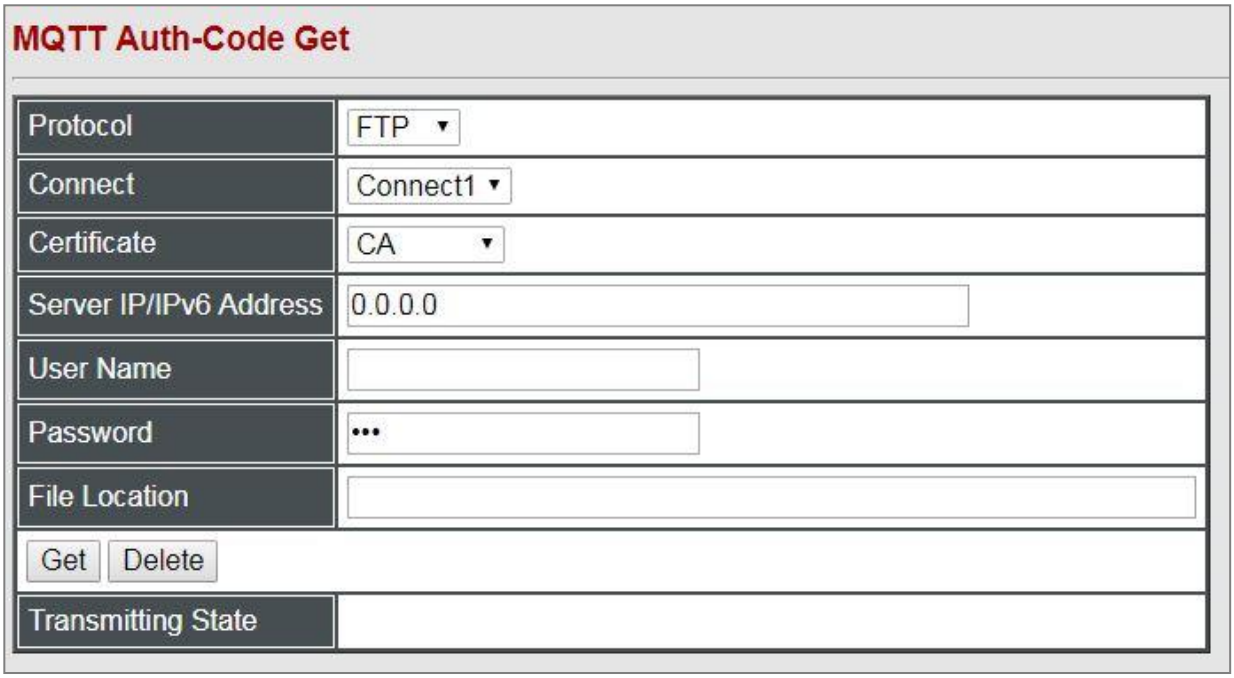
Connect: From the **Connect** pull-down list, choose the desired broker based on the settings of MQTT Configuration.

Certificate: There are three types of the certificate: CA, CLI-Cert and CLI_key. Please note that CA, CLI-Cert, and CLI_key are required when SSL encryption is used in the data transmission.

Auth-Code Get: Click **Choose File** to select the designated file, and then click **Get** to begin uploading the certificate to the Gateway Controller. Click **Delete** to remove the uploaded of CA files for the selected conneciton.

2.6.3 MQTT Auth-Code Get Configuration

The Gateway Controller has both built-in TFTP and FTP clients. Users may update their CA, CLI-Cert, CLI_key to the Gateway Controller. Select **MQTT Auth-Code Get** from the **MQTT Control** menu and then the following screen page appears.



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

Connect: Specify the specific MQTT broker from the pull- down list.

Certificate: Select CA, CLI-Cert or CLI_key required for MQTT broker connection.

Server IP/IPv6 Address: Enter the specific IP/IPv6 address of the FTP/TFTP file server.

User Name: Enter the specific username to access the FTP file server.

Password: Enter the specific password to access the FTP file server.

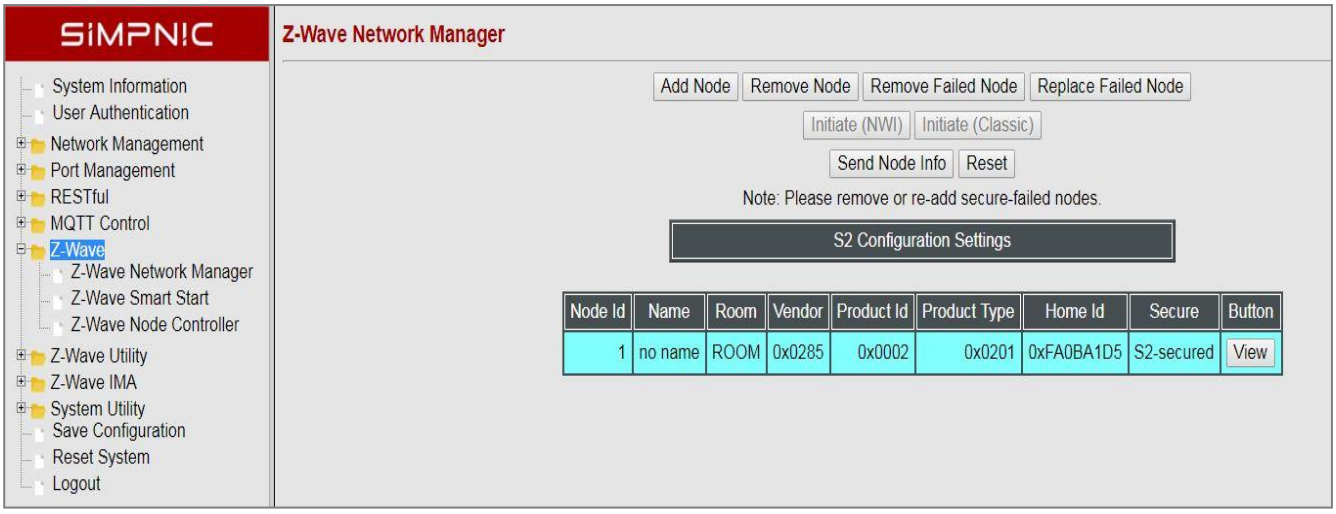
File Location: Enter the specific path and filename within the FTP/TFTP file server.

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

Click **Delete** to remove the uploaded of CA files for the selected conneciton.

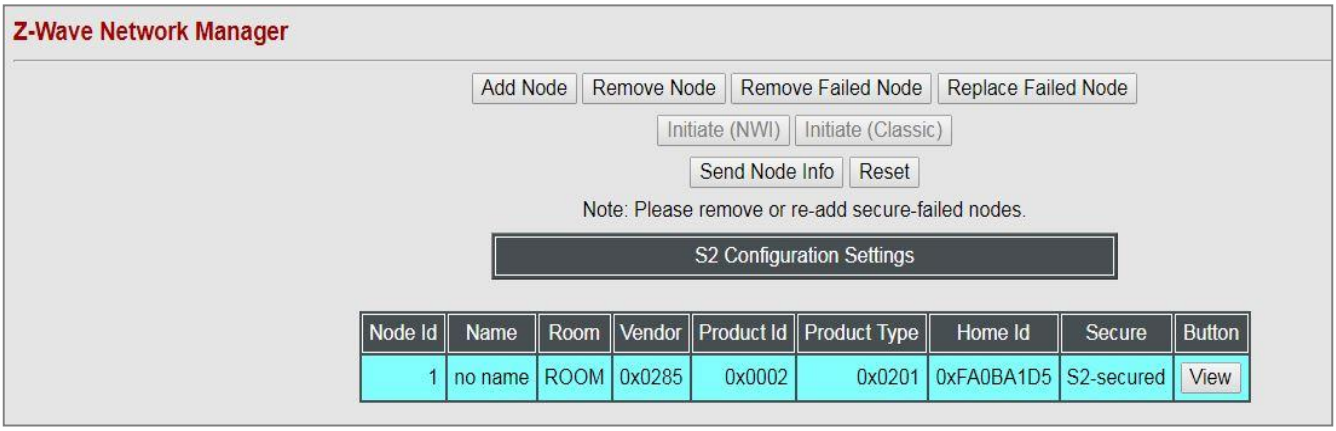
2.7 Z-Wave

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 folder **Z-Wave** from the **Main Menu** and then several options will be displayed for your selection..



1. **Z-Wave Network Manager:** To manage Gateway Controller tasks in Z-Wave network.
2. **Z-Wave Smart Start:** To add or remove the DSK of the sensors.
3. **Z-Wave Node Controller:** To manage the sensors connected with the Gateway Controller.

2.7.1 Z-Wave Network Manager



Add Node: Click **Add Node** to turn the Gateway Controller into the Include mode. Under the Inclusion mode, the Gateway Controller is allowed to bring a sensor into a network. The Inclusion Mode will time out after 120 seconds. It also can be manually stopped using **Abort** button. Once a new sensor 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 Gateway 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 Gateway Controller fails to change its wake up interval. You may set custom interval mentioned in Section 2.7.2.7. 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 **Remove Node** to turn the Gateway Controller into the Exclude mode. Under the Exclusion mode, the Gateway 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. A node can be forced to get removed using **Send Node Info** if a node gives no reply to the Gateway Controller. Click **Send Node Info**, and then specify the failed node showing **d**(down), **a**(abnormal), **i**(isolated),and/or **b**(battery low) in the field of Node Id. This fialed node can be removed successfully by clicking **Remove Failed Node**. The process of Remove Failed Node can be manually stopped using **Abort** button.

Replace Failed Node: Click **Replace Failed Node** to replace the failed node with a new node. The Gateway Controller removes the designated node first and broadcasts 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 (NWI): Be provided for testing only.

Initiate (Classic): Be provided for testing only.

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.

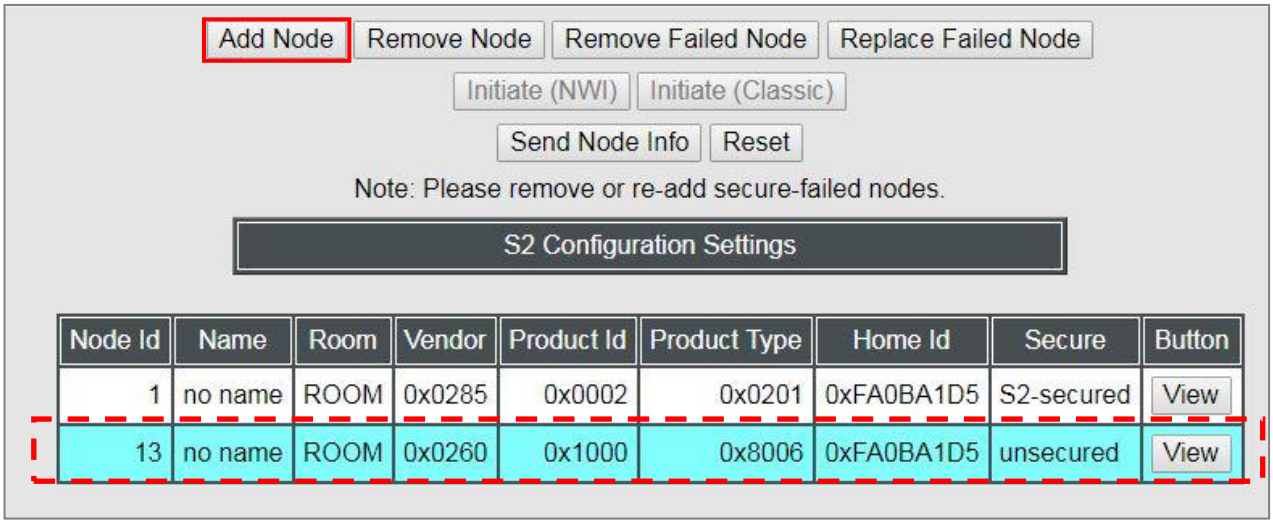
Send Node Info: This is to be used to ask for NIF from all nodes in a network to get known of the capabilities of the node. To get NIF from a sensor, click any single node on the list of nodes, and click **Send Node Info**. This is also used to check if a node is in good connection. A node giving reply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

Reset: Click **Reset** to reset the Gateway Controller back to the factory default settings. Please note that all connections with included sensors and all configurations and settings are lost. This approximately takes 90 seconds to finish the process.

2.7.1.1 Add and Remove the Sensors to/from an Existing Z-Wave Network

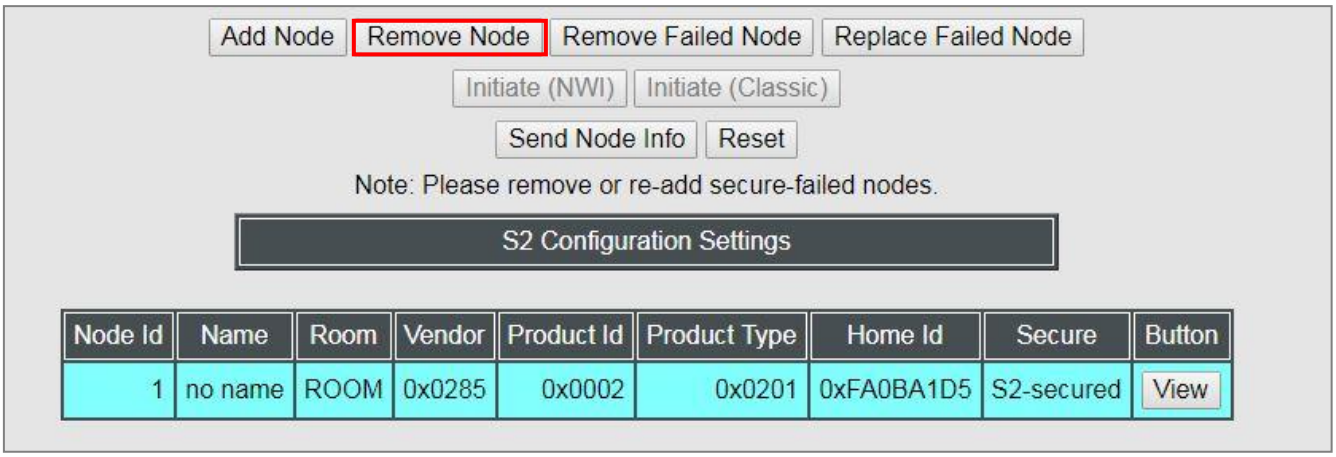
To add the controller to an existing network:

1. Click **Add Node** on the Z-Wave Network Manager setting page.
2. Wait for inclusion request from the sensor.
3. Once the sensor is successfully included, the Gateway Controller will return to the Z-Wave Network Manager setting page and this sensor will be on the list of nodes.(See the figure below.)



To remove the controller from an existing network:

1. Click **Remvoe Node** on the Z-Wave Network Manager setting page.
2. Wait for exclusion request from the sensor.
3. Once the sensor is successfully excluded, the Gateway Controller will return to the Z-Wave Network Manager setting page and this sensor will be deleted from the list of nodes. (See the figure below.)



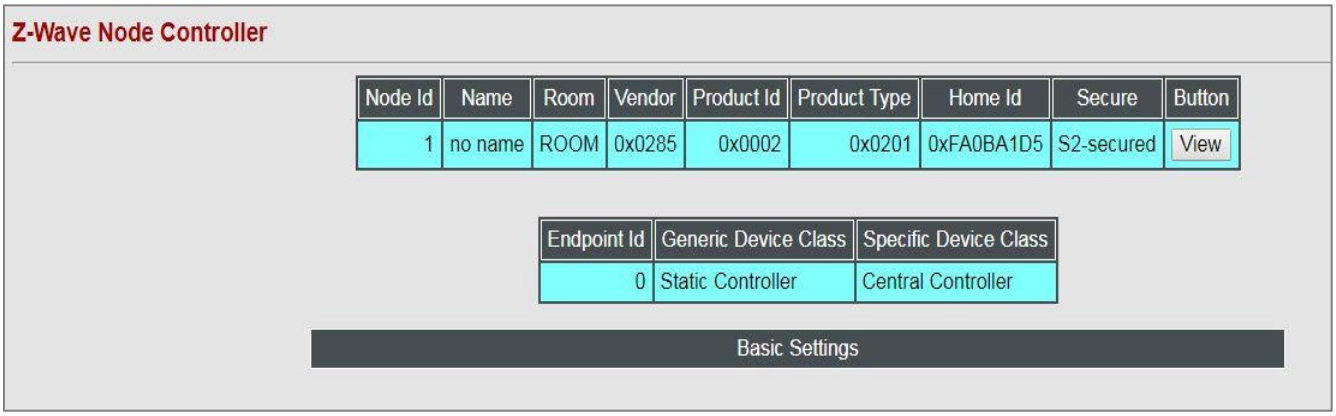
2.7.1.2 Remove Failed Node from an Existing Z-Wave Network

1. Click **Send Node Info** to refresh the list of nodes.
2. Specify the failed node on the list .
3. Click **Remove Failed Node** on the Z-Wave Network Manager setting page.
4. Once the sensor is successfully excluded, the Gateway Controller will return to the Z-Wave Network Manager setting page and this sensor will be deleted from the list of nodes.

2.7.1.3 Replace Failed Node from an Existing Z-Wave Network

1. Click **Send Node Info** to refresh the list of nodes.
2. Specify the failed node on the list.
3. Click **Replace Failed Node** on the Z-Wave Network Manager setting page.
4. Once the sensor is successfully excluded, the Gateway Controller will return to the Z-Wave Network Manager setting page and this sensor will be deleted from the list of nodes.
5. The Gateway Controller will automatically enter the Include mode to add another new sensor.
6. Once this new sensor is successfully included, it begins to exchange protocol data with the other sensor in the same network.

2.7.2 Z-Wave Node Controller



Node ID: The identification number of each node assigned.

Name: The name of the sensor (Node ID 1 is for the Gateway Controller only)

Room: The room name of the sensor groups.

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

Product ID: A unique ID identifying the actual product.

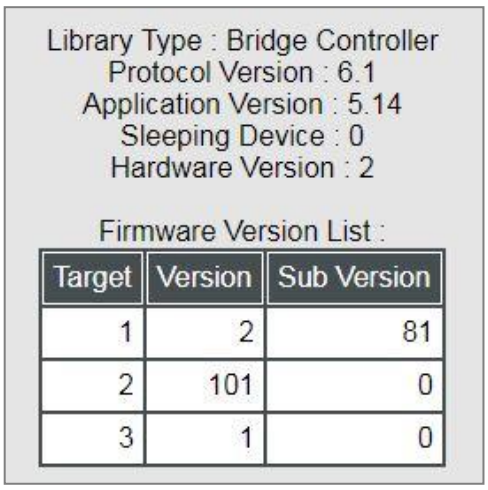
Product Type: A unique ID identifying the actual product type.

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 is recommended that remove secure-failed nodes and re-add them.

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



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.

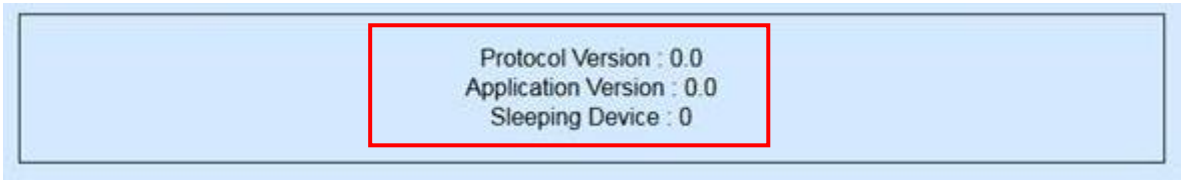
Generic Device Class: The subordinate information of class the sensor belongs to.

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.

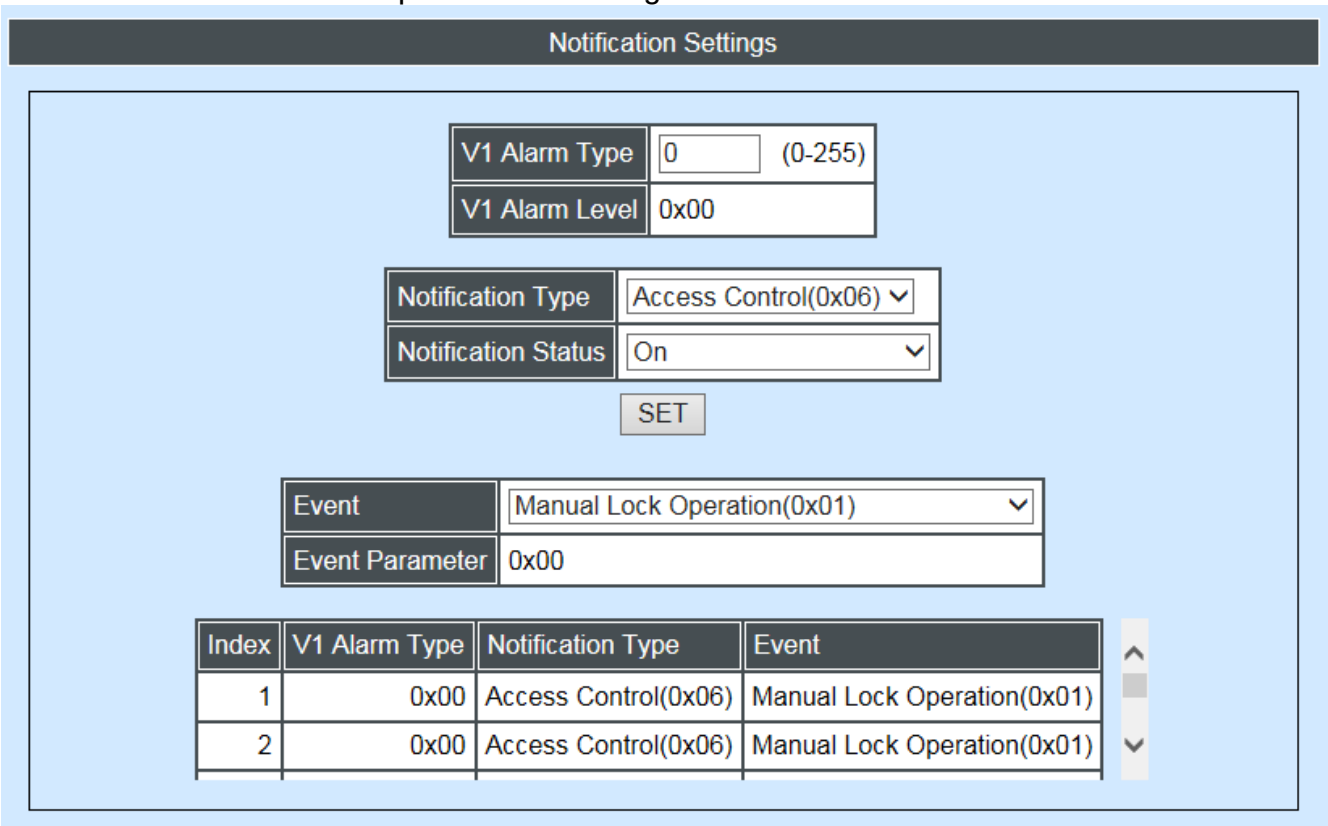
Note: Somehow the list of nodes may show virtual nodes because bridge library is implemented. Their Protocol & Application Version show “0.0” and Genetic Device Class shows “Repeater Slave”. Refer to the given example below.

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



2.7.2.1 Notification Settings

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



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.

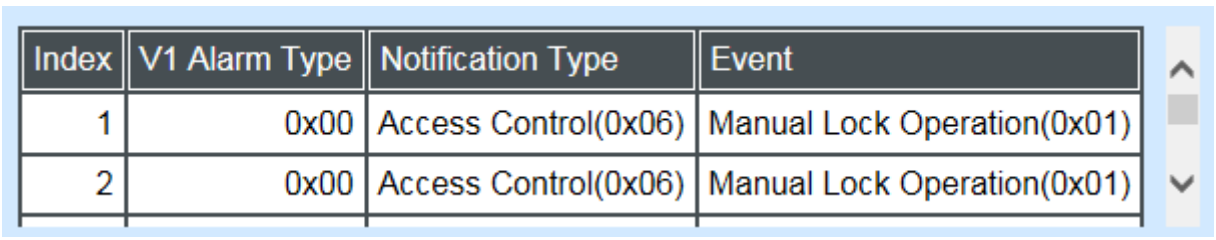
Notification Status: Click drop-down arrow to determine unsolicited messages must be disabled or enabled for the specified Notification Type.

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

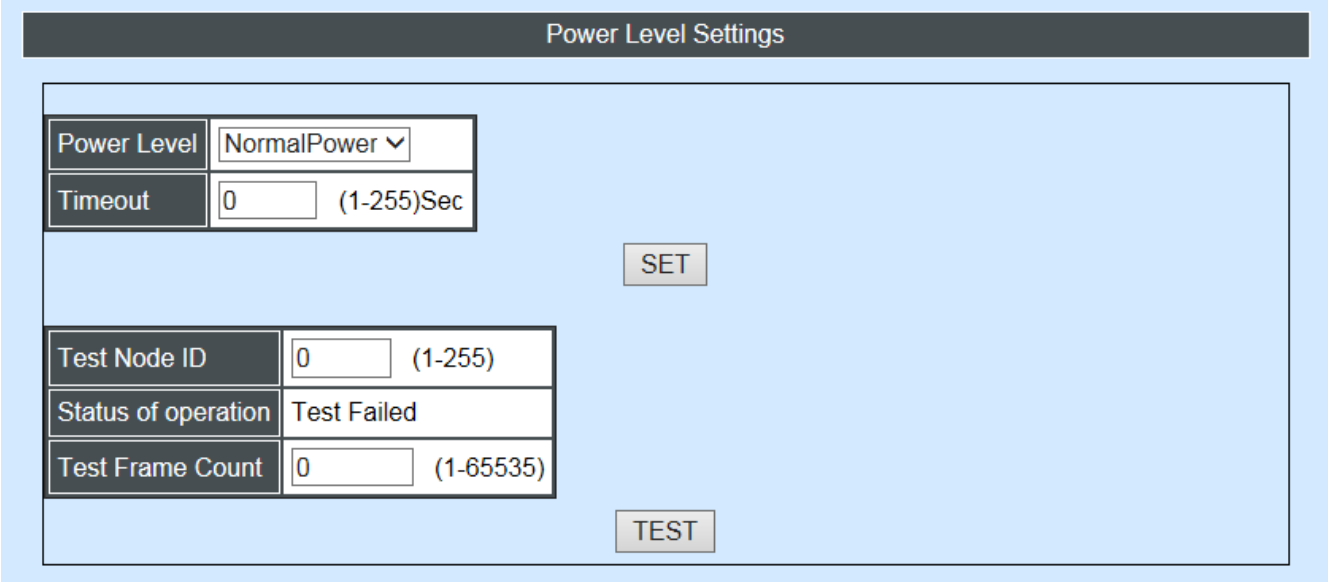
				events for the specified Notification Type.
		Schedule Started	0x01	Event Parm 1 = <Schedule ID>
		Schedule Finished	0x02	Event Parm 1 = <Schedule ID>
		Valve Table Run Started	0x03	Event Parm 1 = <Valve Table ID>
		Valve Table Run Finished	0x04	Event Parm 1 = <Valve Table ID>
		Device is not Configured	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	

2.7.2.2 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: 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.

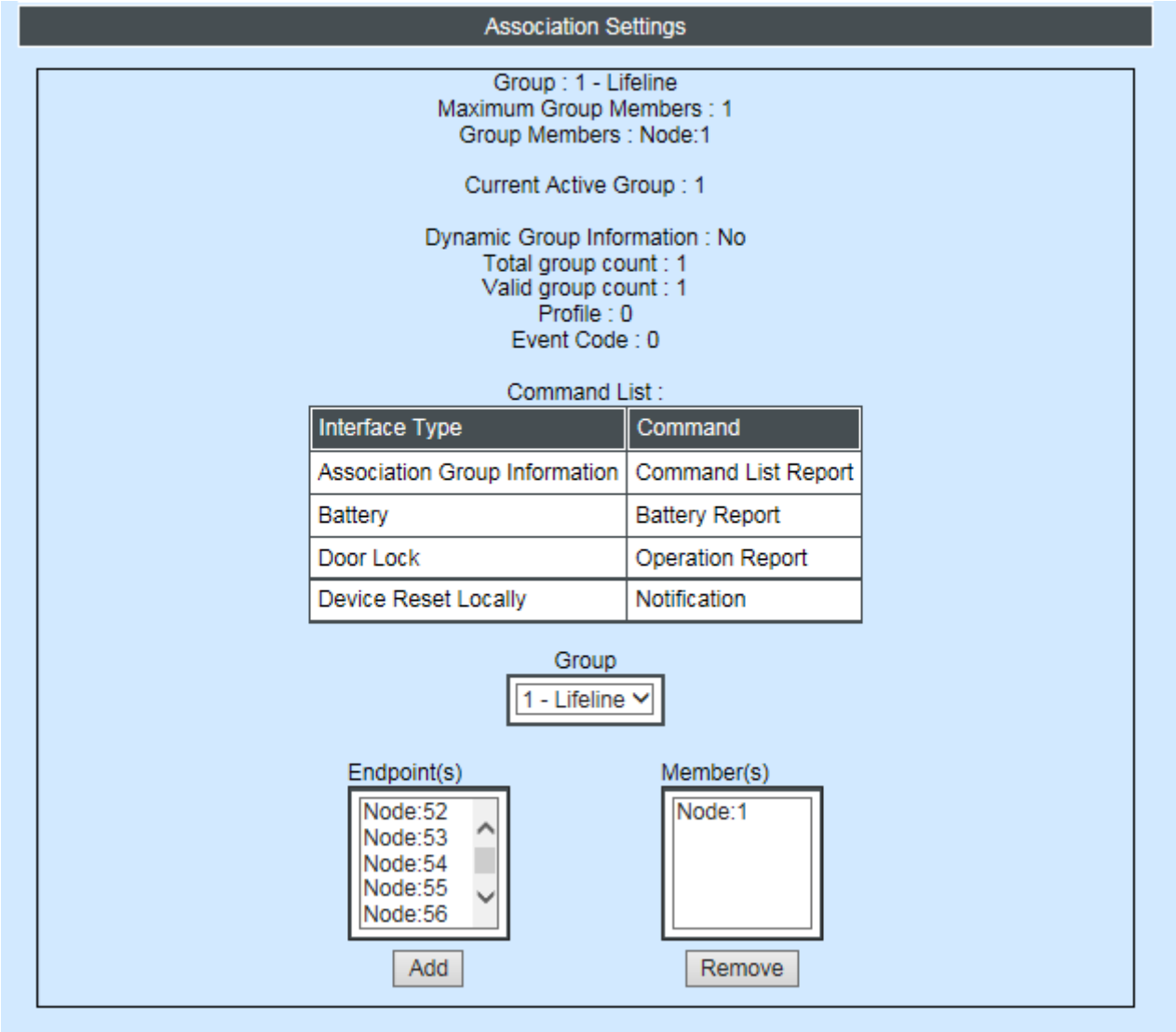
Test Node ID: Type the test node ID that needs testing. The valid value is 1~255

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.

2.7.2.3 Association Settings

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



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.

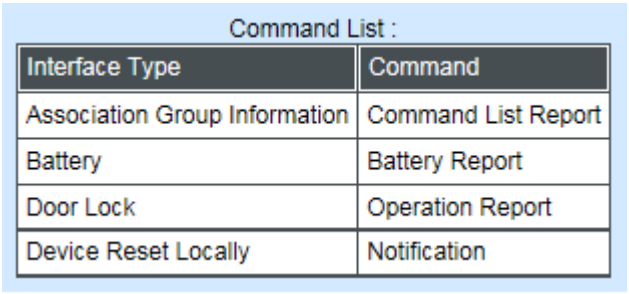
Total Group Count: The total number of groups in the device.

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.

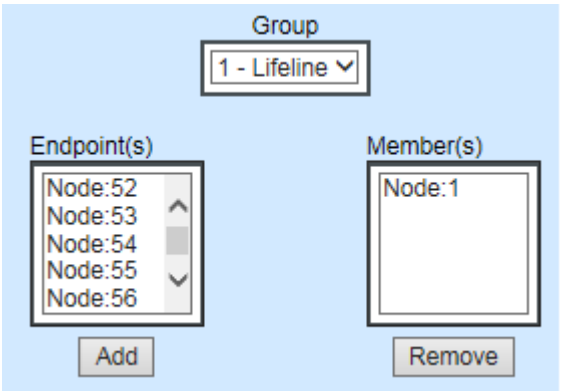
Command List
It shows the commands that may be sent from the association group.


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.



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

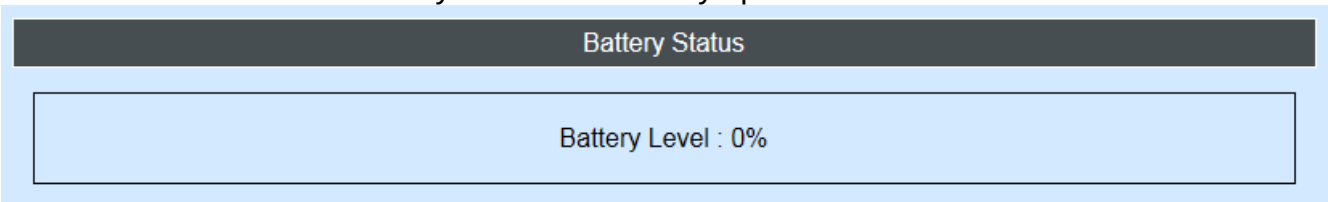
Group: Click drop-down arrow to choose the group you want to configure.

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”

2.7.2.4 Battery Status

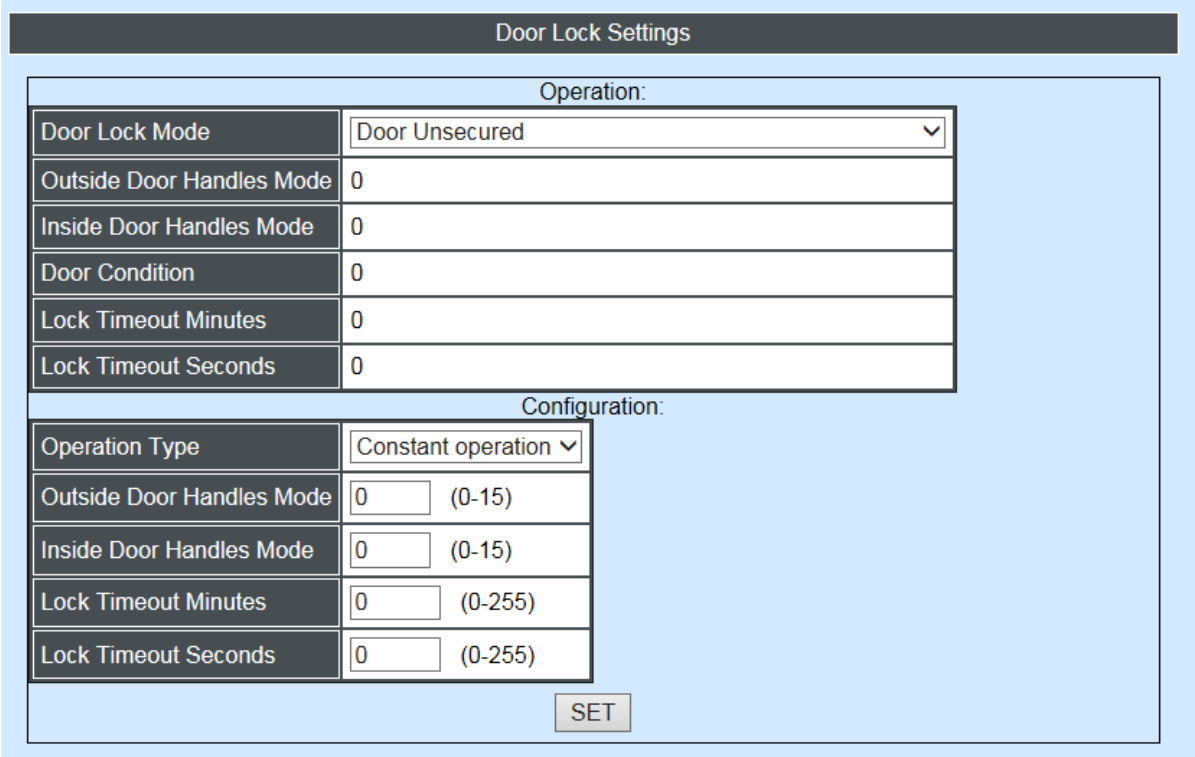
This is used to show the battery status of a battery operated device.



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

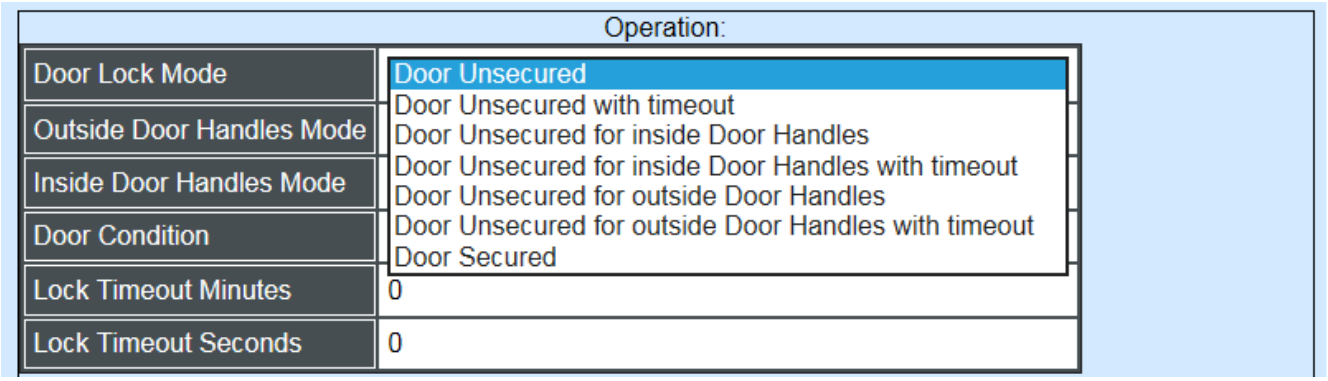
2.7.2.5 Door Lock Settings

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



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.



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

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

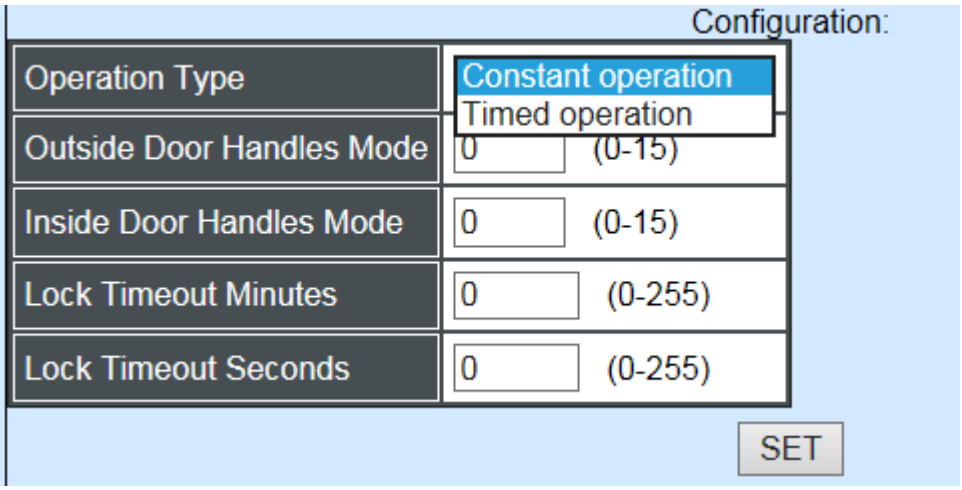
Door Condition: The status of the door lock components.

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.



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.

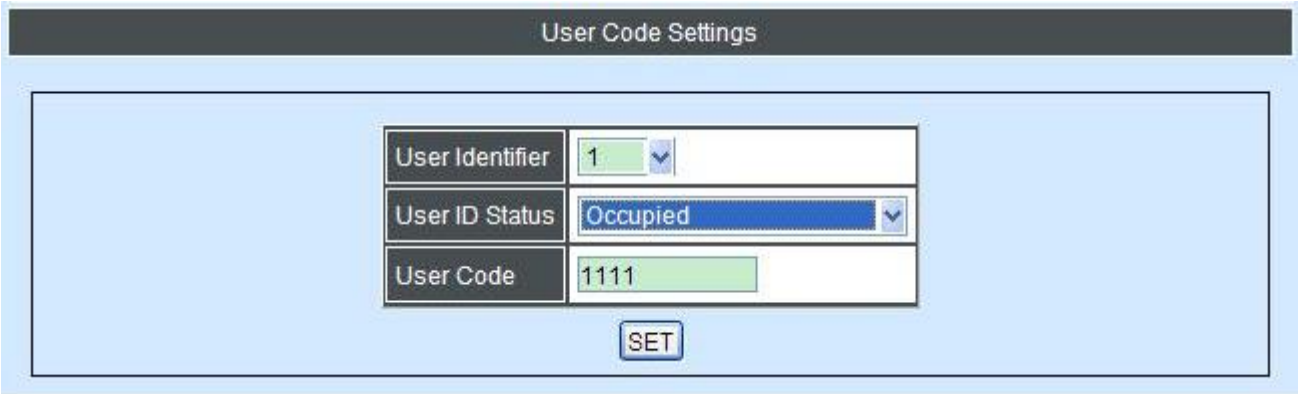
Lock Timeout Minutes: Set up the time in minute that a door lock must wait before automatically being locked again. The range is 0~255 in minute.

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 the new settings.

2.7.2.6 User Code Settings

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



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

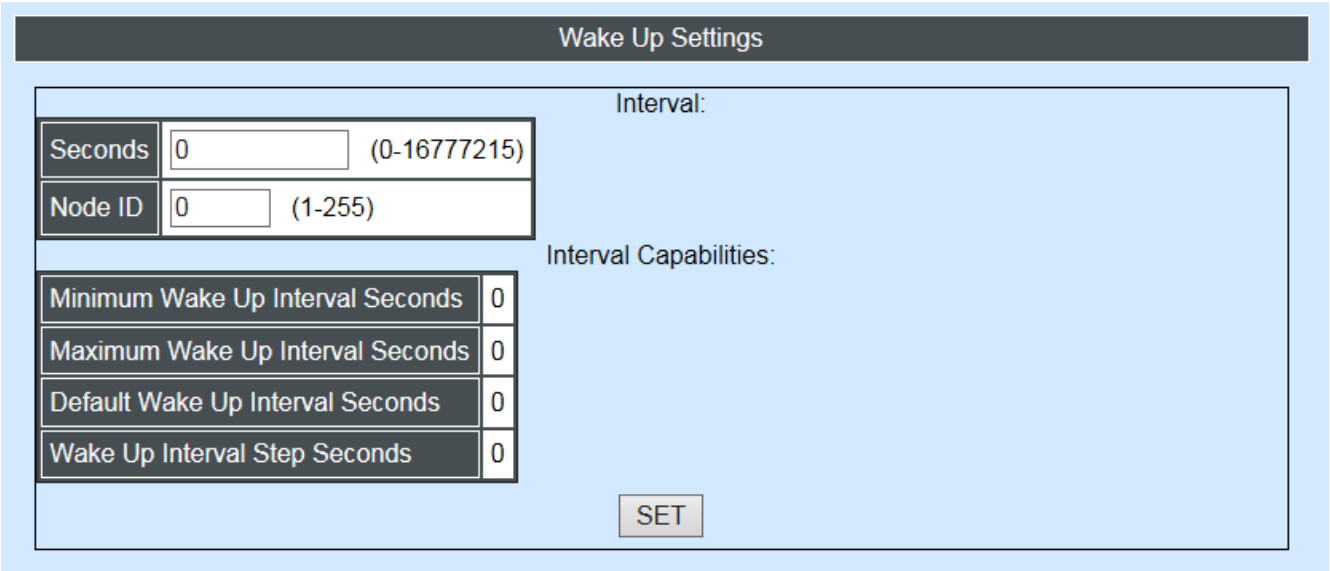
User ID Status: Shows the state of the User Identifier. Click drop-down arrow and the following status shows –Available, Occupied, Reserved by administrator and Status not available.

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

Click **SET** to apply the new settings.

2.7.2.7 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.



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.

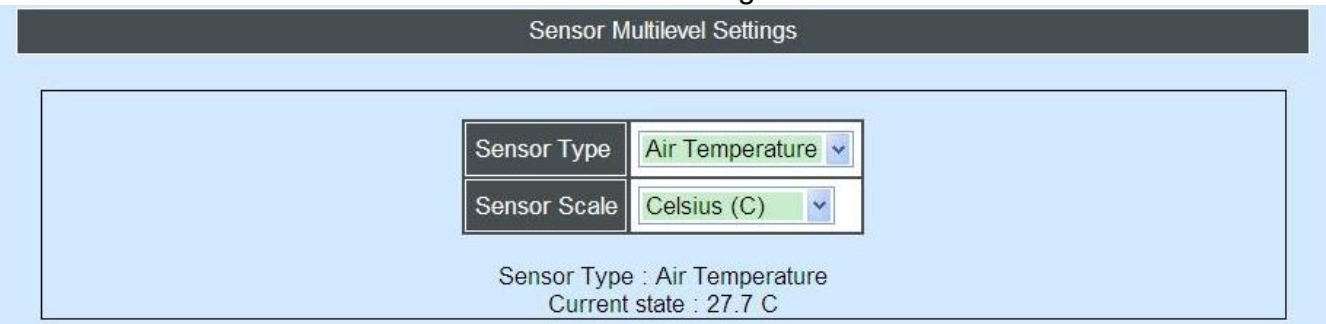
Maximum Wake Up Interval Seconds: Shows the maximum wake up interval in second a battery-operated device supports.

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.

2.7.2.8 Sensor Multilevel Settings

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



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 (Ωm)

Sensor Type	Sensor Scale
Electrical Conductivity	siemens per metre($S \cdot m^{-1}$)
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)

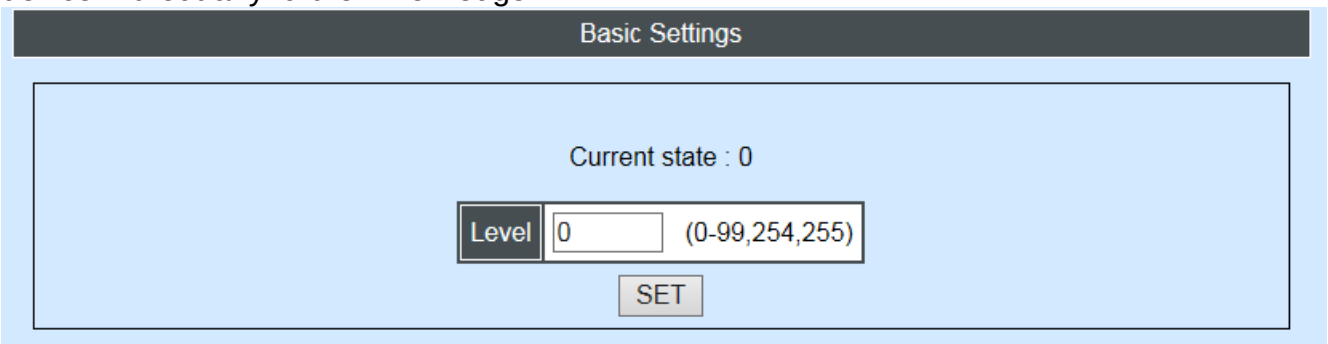
Carbon Monoxide CO-level	mol/m^3 (mole per cubic meter)
Soil Humidity	Percentage value

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.

2.7.2.9 Basic Settings

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



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

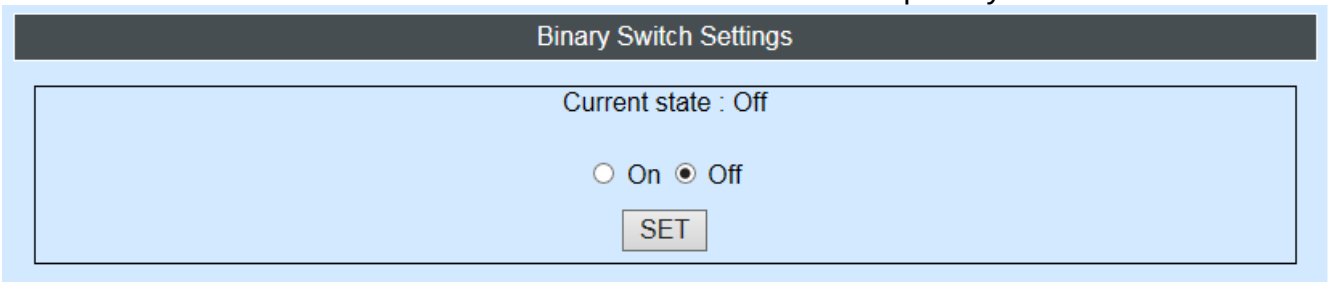
The details of value are shown as below:

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.

2.7.2.10 Binary Settings

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

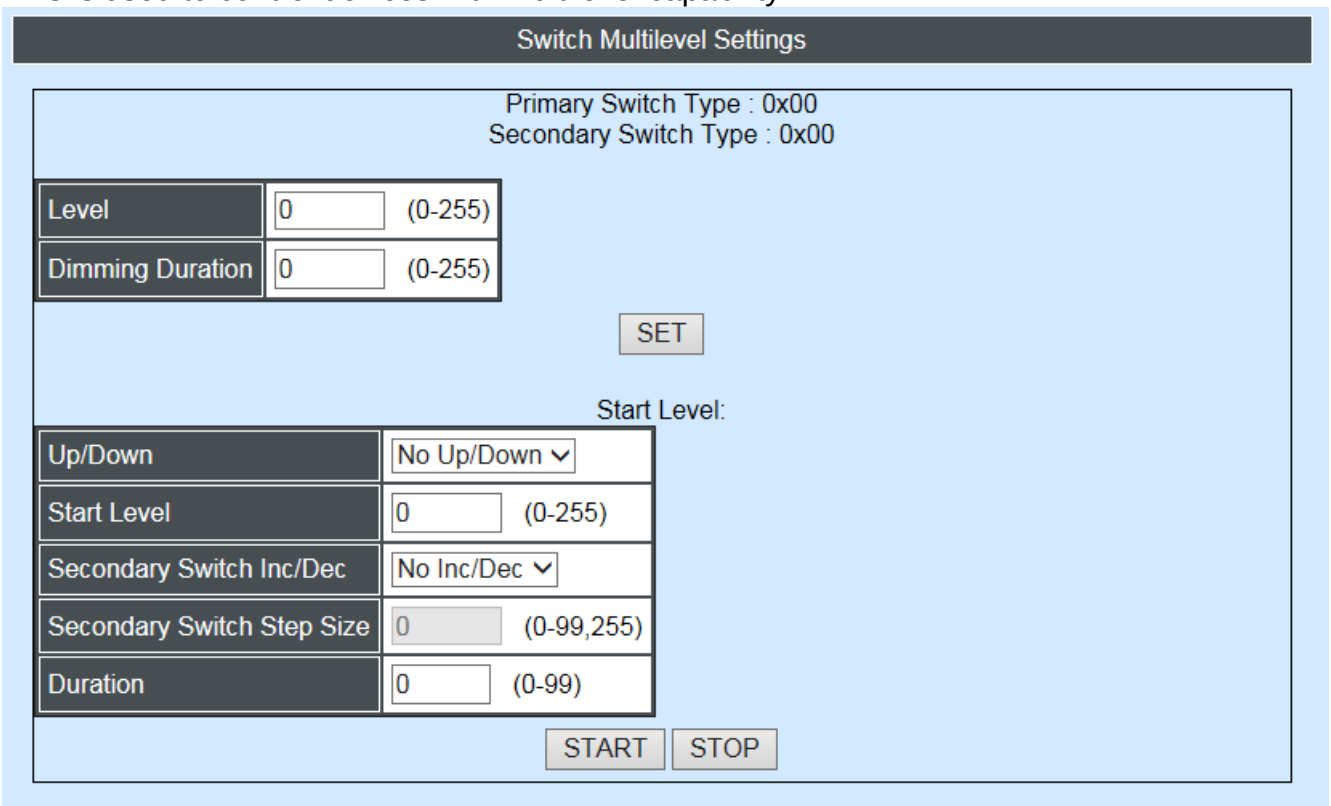


Click On(Enable) or Off(Disable) for a device.

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

2.7.2.11 Switch Multilevel Settings

This is used to control devices with multilevel capability.



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.

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.

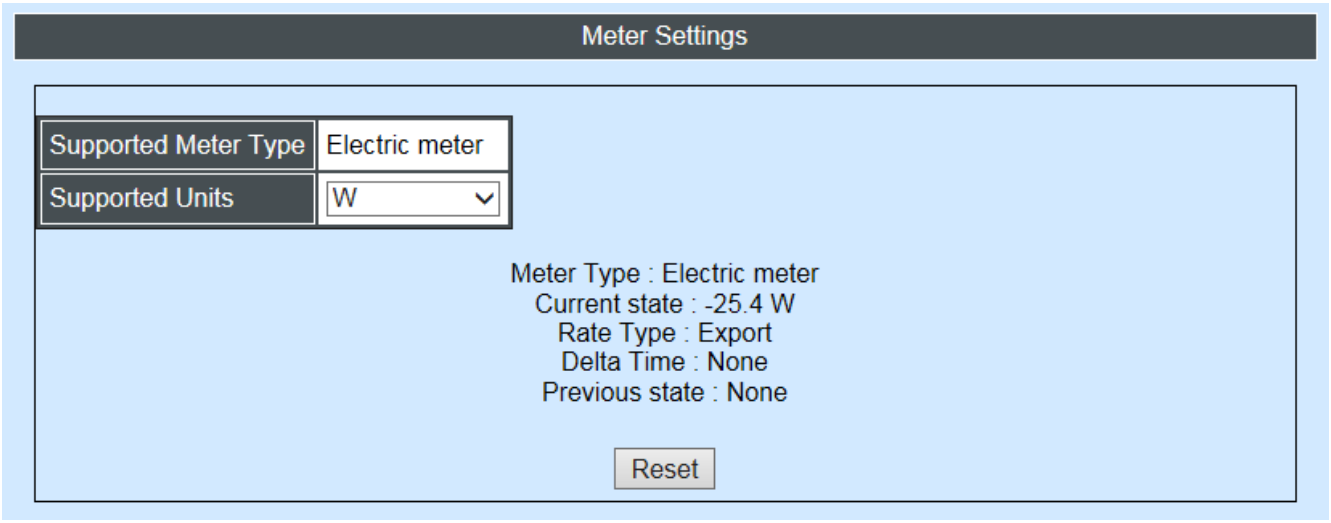
Secondary Switch Step Size: Specify the value 0~99 or 255.

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** to stop the command in process.

2.7.2.12 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.

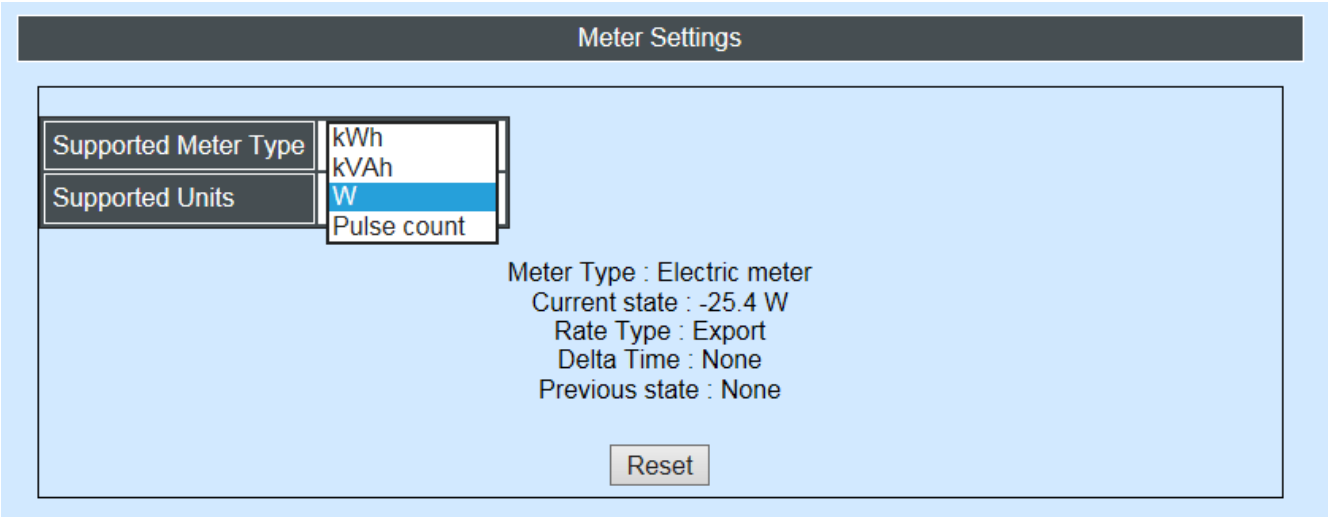


Supported Meter Type: Shows what type of metering device originates from.

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 Type: Shows the current meter type.

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

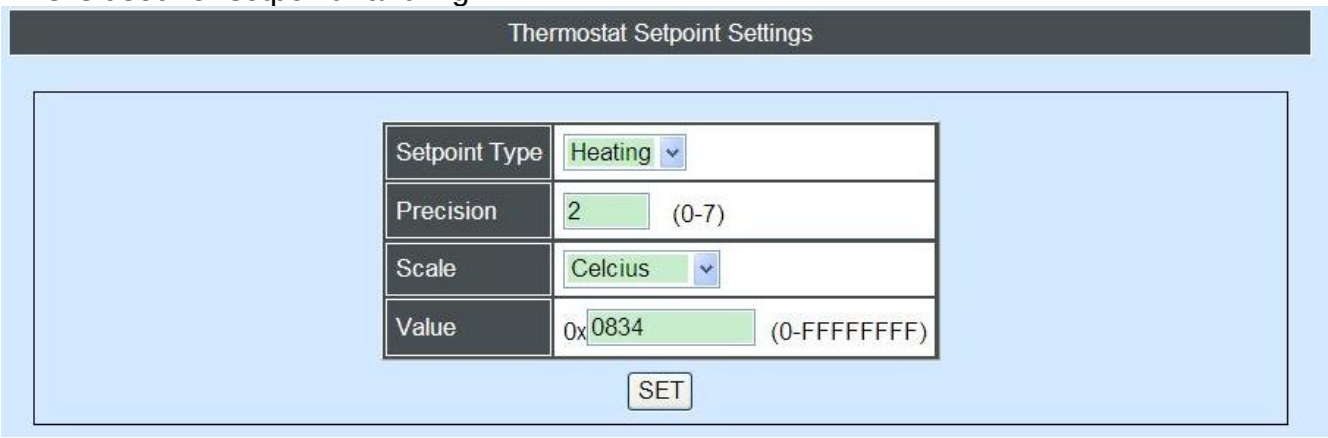
Rate Type: Shows if it is import or export values to be read. The Rate Type shown “Import” is an indication that the Meter Value is a consumed measurement. In contrary when the Rate Type is shown “Export” the indication of the Meter Value is a produced measurement.

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.

2.7.2.13 Thermostat Setpoint Settings

This is used for setpoint handling.



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.

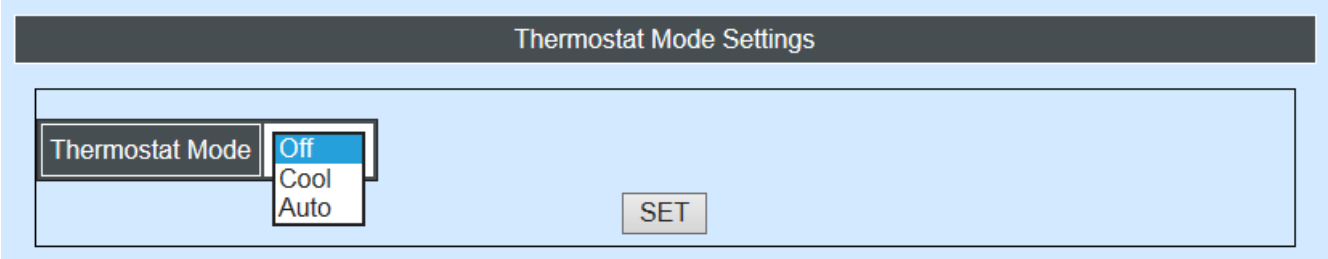
Value: Specify the actual setpoint value.

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

2.7.2.14 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:

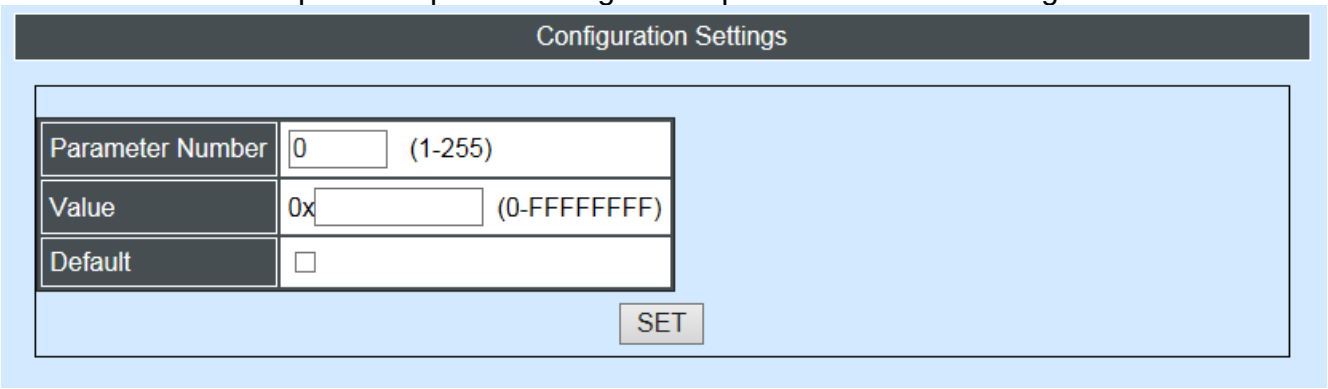
Thermostat Mode	Description
OFF	System is OFF.
HEAT	Continuous heating only.
COOL	Continuous cooling only.
AUTO	The system will automatically switch between heating and cooling when the temperature exceeds the HEAT and COOL set point types.
AUXILIARY	Auxiliary/Emergency Heat. A heat pump (especially 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 new settings.

2.7.2.15 Configuration Settings

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



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

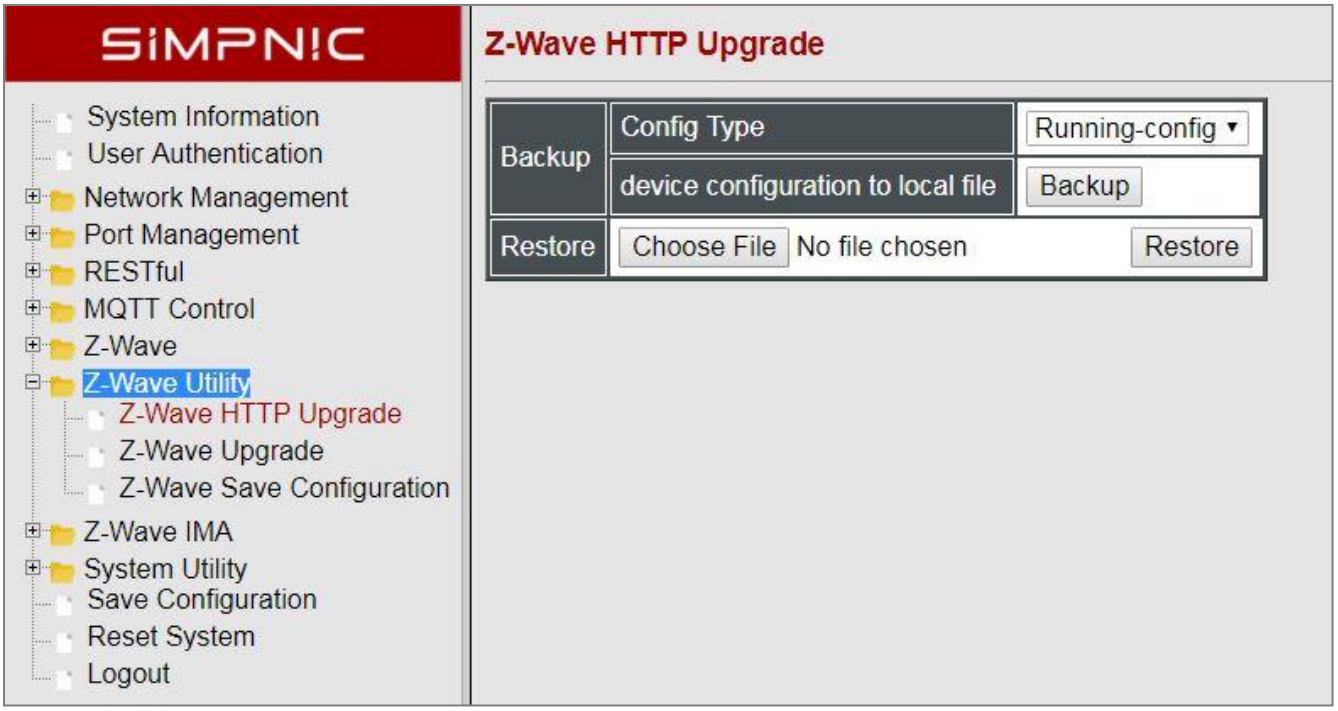
0x00	0		0x0000	0		0x00000000	0
0xFF	-1		0xFFFF	-1		0xFFFFFFFF	-1
0xFE	-2		0xFFFE	-2		0xFFFFFFFE	-2
0x80	-128		0x8000	-32768		0x80000000	-2147483648

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 the new settings.

2.8 Z-Wave Utility

This is used to upgrade, backup or save Z-Wave configuration. Click the folder **Z-Wave Utility** from the **Main Menu** and then some options will be displayed for your selection.



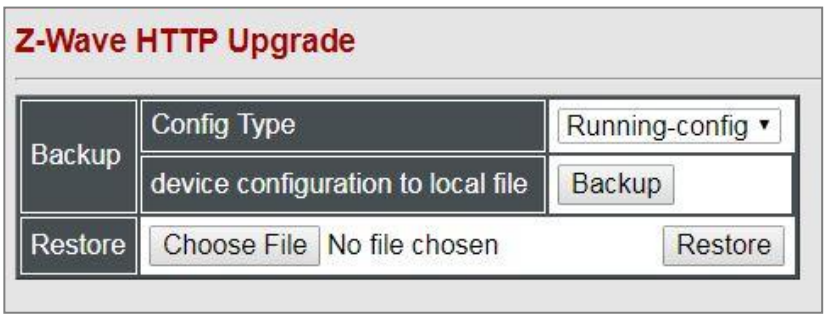
1. Z-Wave HTTP Upgrade: To save or restore their Z-Wave configuration off-line.

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.

2.8.1 Z-Wave HTTP Upgrade

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



Config Type: There are 2 types of Config Type: Running-config and Start-up-config:

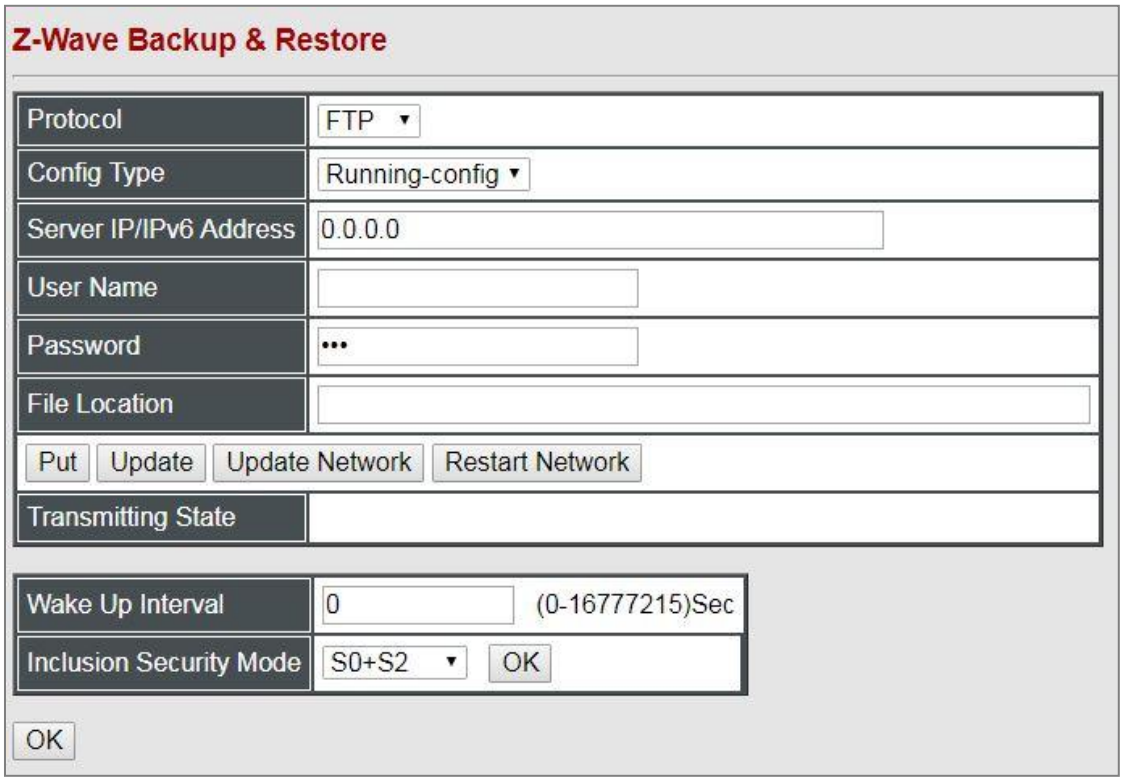
- **Running-config:** Back up the data you're processing
- **Start-up-config: Back up the data same as last saved data.**

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

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

2.8.2 Z-Wave Upgrade

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



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.

Server IP/IPv6 Address: Enter the specific IP/IPv6 address of the FTP/TFTP file server.

User Name: Enter the specific username to access the FTP file server.

Password: Enter the specific password to access the FTP file server.

File Location: Enter the specific path and filename within the FTP/TFTP file server..

Update Network: Click to update Z-Wave network.

Restart Network: Click to restart Z-Wave network.

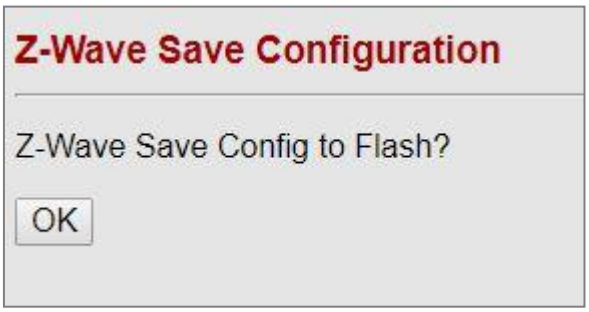
Wake Up Interval: Specify the interval in second to wake up sleeping devices. The default value is 0.

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.

2.8.3 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 Utility** menu and then the following screen page appears.

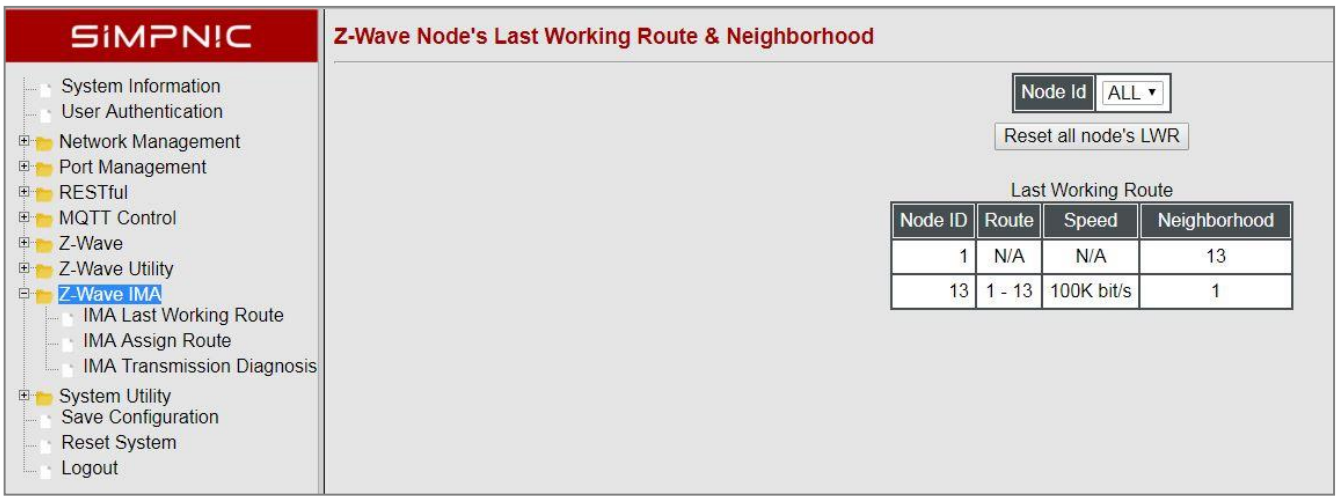


Click **OK** to save the current Z-Wave configuration.

2.9 Z-Wave IMA

The Gateway Controller provides, a powerful diagnostic tool, the Z-Wave Installation and Maintenance Application (IMA) network health monitor.

The Z-Wave IMA allows a technician to locally or remotely survey the Z-Wave signal quality at every node in the system. With Z-Wave IMA, it can speed up the installation and help ensure robust performance of the smart home system. When service is needed, service providers, installers and dealers can use this mesh network health information to diagnose problems in a home or office. Sometimes the technicians have no need to visit, thus, it can save much time and money for service providers as well as installers of home automation and home security systems.



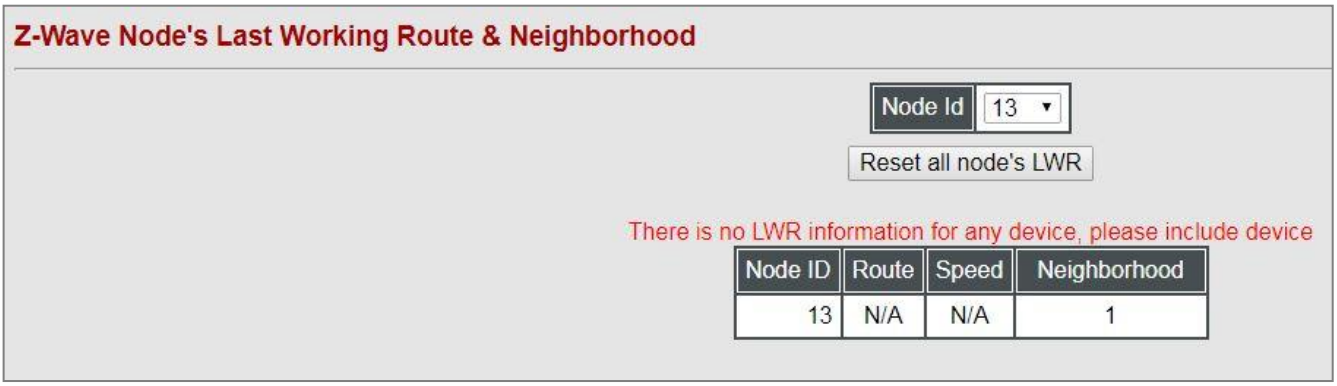
IMA Last Working Route: View the current status nodes that the Gateway Controller includes .

IMA Assign Route: Set up the static route for the Gateway Controller.

IMA Transmission Diagnosis: Diagnose and analyze the real-time conditions of each nodes that the Gateway Controller includes .

2.9.1 IMA Last Working Route(LWR)

In order to view the real-time nodes' status, including node ID, route, speed and neighborhood among the Z-wave network of the Gateway Controller, please select **IMA Last Working Route** from the **Z-Wave IMA** menu and then the following screen page appears.



Node ID: Either **All** or a single node ID can be selected from the pull-down list to view the node information of all nodes or the specified node .

Reset all node's LWR: Clear the current route of the Gateway Controller to all nodes. Thus, the Gateway Controller will then send packets in a direct way to all nodes.

Route: Display the route in which the Gateway Controller sends the packets to the specific node. "1" stands for the Gateway Controller itself. Up to 4 nodes can be the repeater to assist the forwarding of packets.

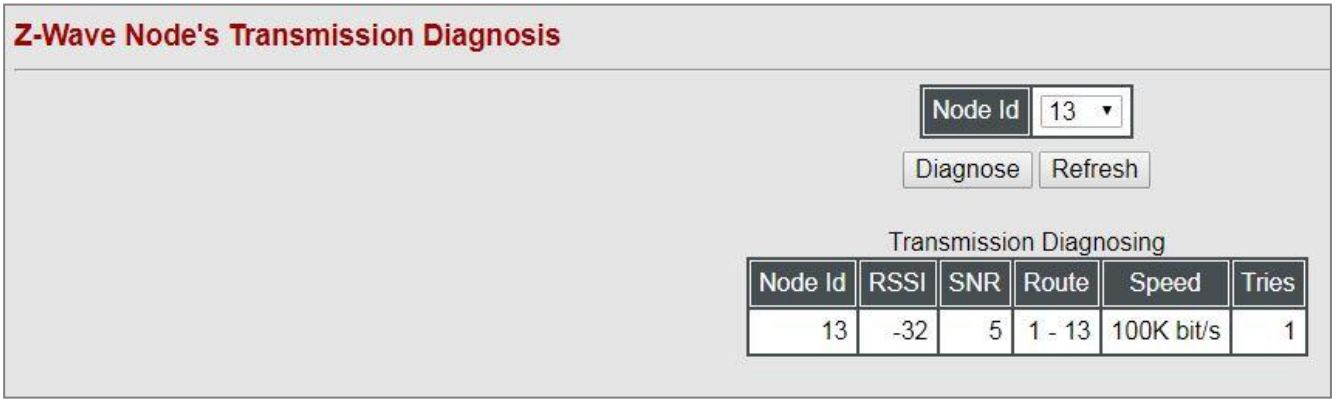
Speed: Display the speed at which the Gateway Controller sends the packet to the specific node. There are three types of speed, including 100K bit/s 40K bit/s and 9.6K bit/s.

Neighborhood: Display the ID of nodes which are near the specific node.

NOTE: If the node is a failed one, its values of the route and speed parameters will be N/A, and its node ID will display **d**(down) on the nodes list in Z-Wave → Z-Wave Network Manager setting page.

2.9.2 IMA Transmission Diagnosis

IMA Transmission Diagnosis allows users to monitor the real-time transmission status between the specified node and the Gateway Controller. Users may monitor the node's Z-Wave network traffic for maintenance or diagnostic purposes. Select **IMA Transmission Diagnosis** from the **Z-Wave IMA** menu and then the following screen page appears.



Node Id: Either **All** or a single node ID can be selected from the pull-down list to proceed IMA transmission diagnosis for all nodes or the specific node.

Diagnose: Click the "**Diagnose**" button to send the analysis packets to the specified node.

Refresh: Click the "**Refresh**" button to update the latest transmission information, including RSSI, SNR, Route, Speed and Tries for all nodes or the specified node.

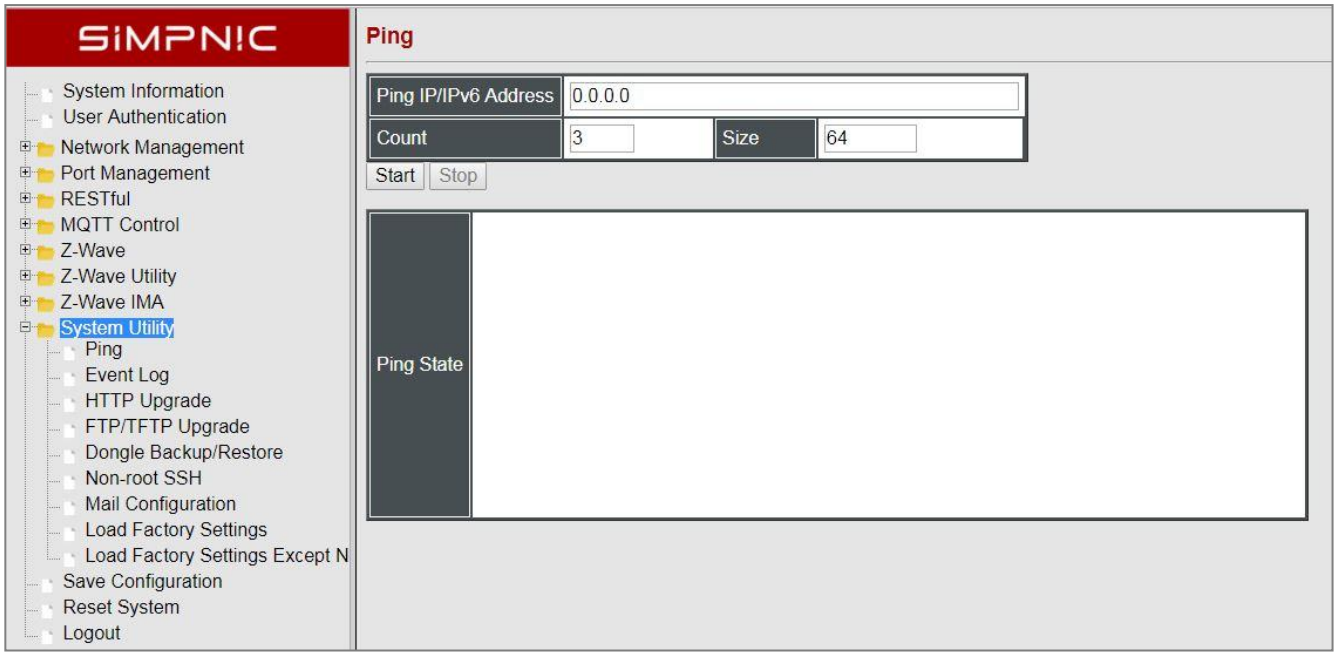
RSSI (Received Signal Strength Indication): It indicates that the strength of the signal received. From the value of this parameter, you can judge the quality of the connection to decide whether the strength of broadcast transmission needs to be increased or not. The closer the value is to 0, the better the connection quality is.

SNR: The abbreviation of signal-to-noise ratio, is also referred to as S/N. SNR is a measure used to compare the level of a desired signal with the same level of background noise. SNR is defined as the ratio of signal power to the noise power, often expressed in dB. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise. The bigger the value becomes, the better the signal quality is.

Tries：The times of sending the analysis packets, which also can be used to judge the network condition. The bigger the value becomes, the worse the connection quaility between the specified node and the Gateway Controller.

2.10 System Utility

System Utility allows users to easily operate and maintain the system. Select the folder **System Utility** from the **Main Menu** and then the following screen page appears.



1. **Ping:** Ping can help you test the network connectivity between the Gateway Controller and the host. You can also specify counts 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.

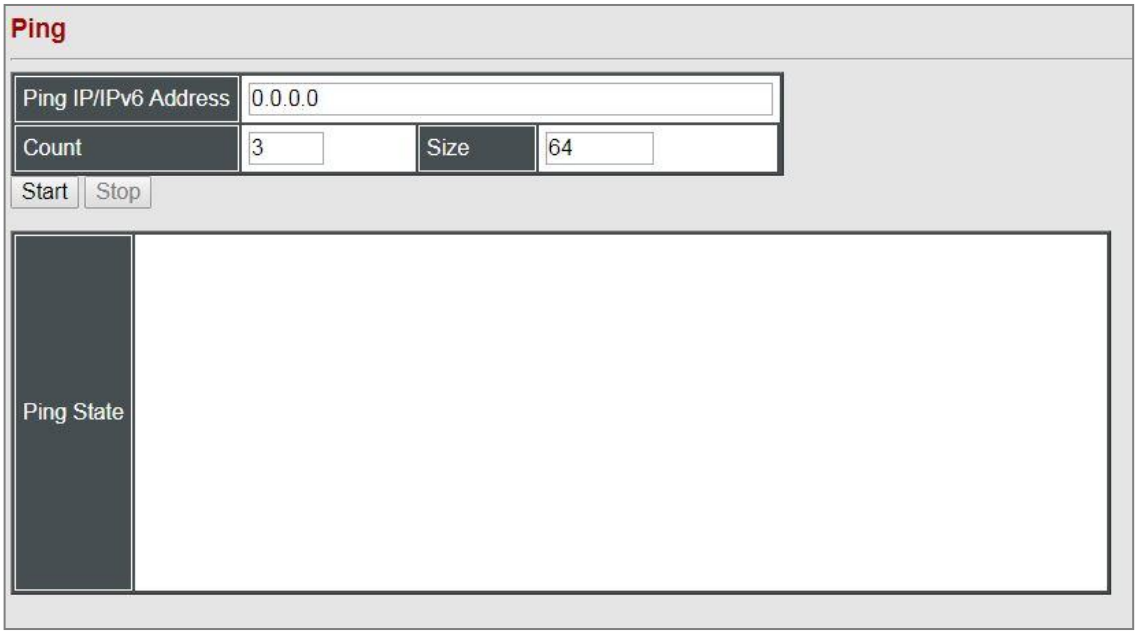
4. **FTP/TFTP Upgrade:** This allows users to update the latest firmware, save current configuration or restore previous configuration to the Managed Switch.

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.

2.10.1 Ping

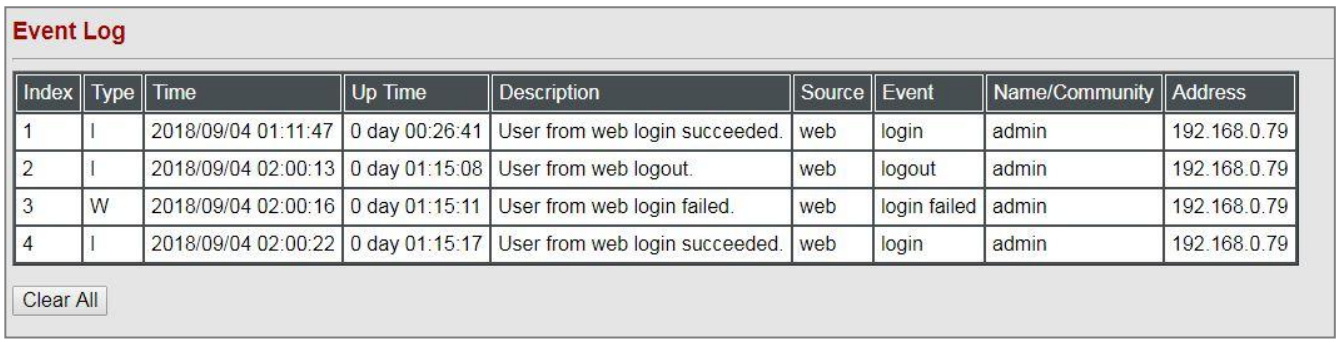
Ping can help you test the network connectivity between the Managed Switch and the host. Select **Ping** from the **System Utility** menu and then the following screen page appears.



Enter the IP/IPv6 address of the host you would like to ping. You can also specify count and size of the Ping packets. Click **Start** to start the Ping process or **Stop** to pause this Ping process.

2.10.2 Event Log

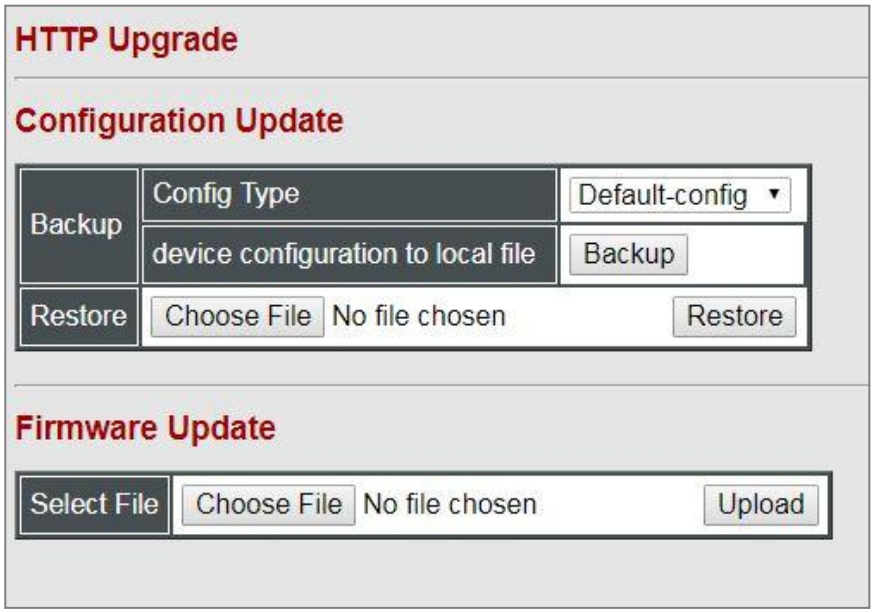
Event log keeps a record of user login and logout timestamp information. Select **Event Log** from the **System Utility** menu and then the following screen page appears.



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

2.10.3 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.



Configuration Update:

There are 2 types of Config Type: Default-config and Start-up-config

- **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.

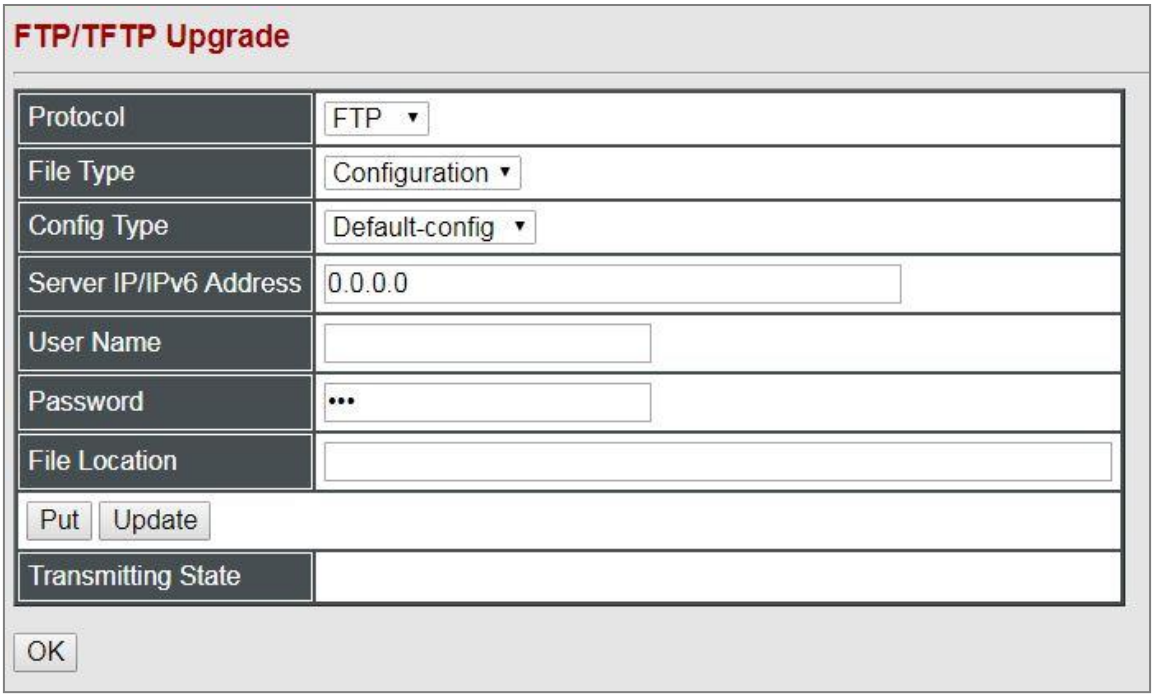
Restore: Click **Choose File**, select the designated data and then click **Restore**.

Firmware Update:

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

2.10.4 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 **FTP/TFTP Upgrade** from the **System Utility** menu and then the following screen page appears.



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

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

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

Server IP/IPv6 Address: Enter the specific address of the FTP/TFTP file server.

User Name: Enter the specific username to access the FTP file server.

Password: Enter the specific password to access the FTP file server.

File Location: Enter the specific path and filename within the FTP/TFTP 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.

2.10.5 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.

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

2.10.6 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.

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

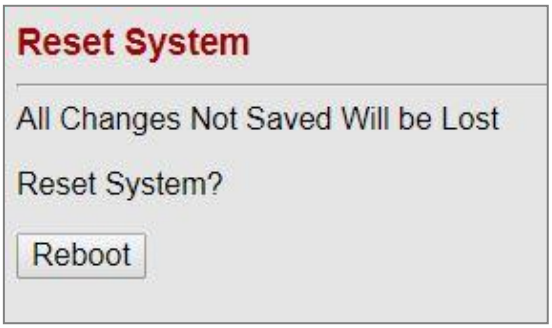
2.11 Save Configuration

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.

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

2.12 Reset System

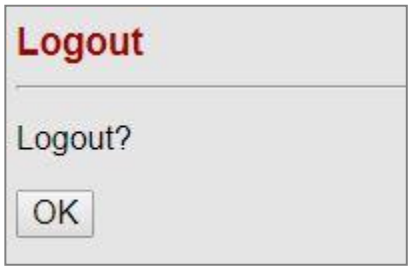
After any configuration changes, **Reset System** can make changes effective. Select **Reset System** from the **Main menu** and then the following screen page appears.



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

2.13 Logout

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



Click the **OK** button to log out.

APPENDIX A: DHCP Auto-Provisioning Setup

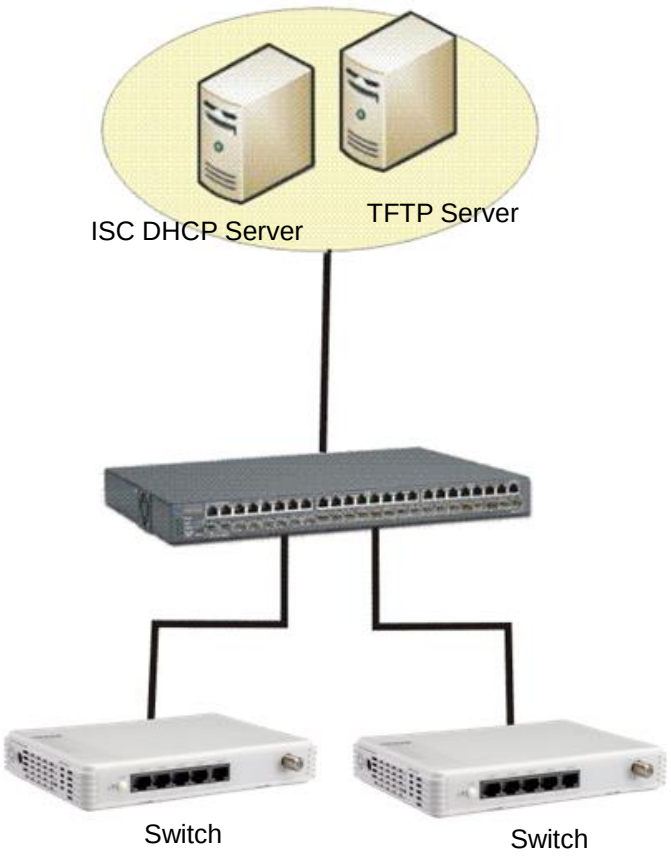
Networking devices, such as switches or gateways, with DHCP Auto-provisioning function allow you to automatically upgrade firmware and configuration at startup process. Before setting up DHCP Server for auto-upgrade of firmware and configuration, please make sure the device that you purchased supports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

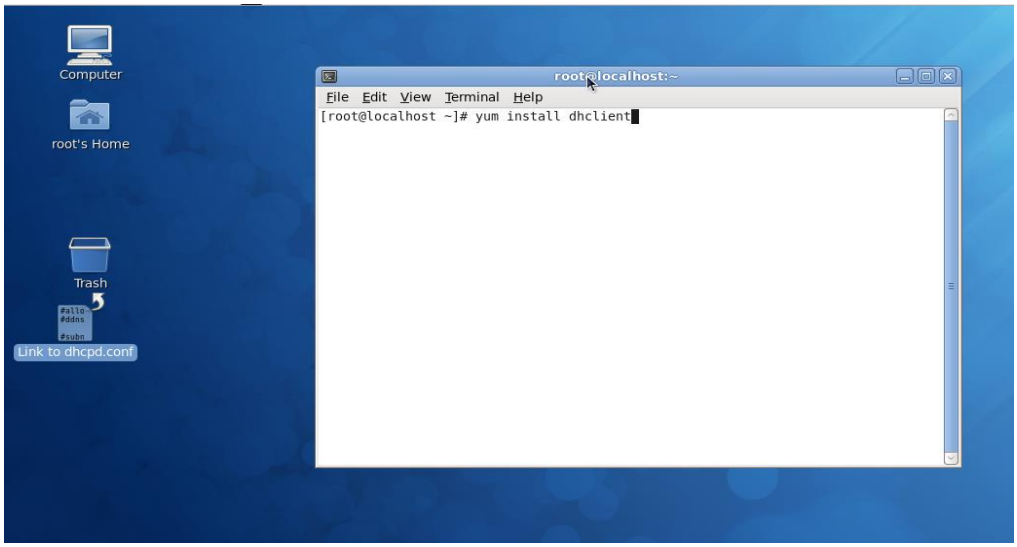
DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. To make auto-provisioning function work properly, you need to prepare ISC DHCP server, File server (TFTP or FTP) and the switching device. See below for a possible network topology example.



Topology Example

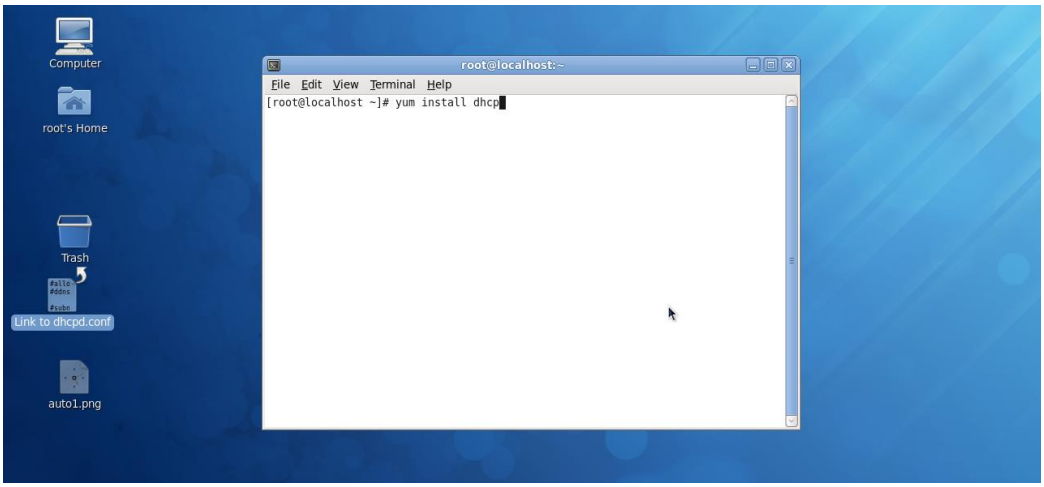
Step 2. Set Up Auto Provision Server

- **Update DHCP client**



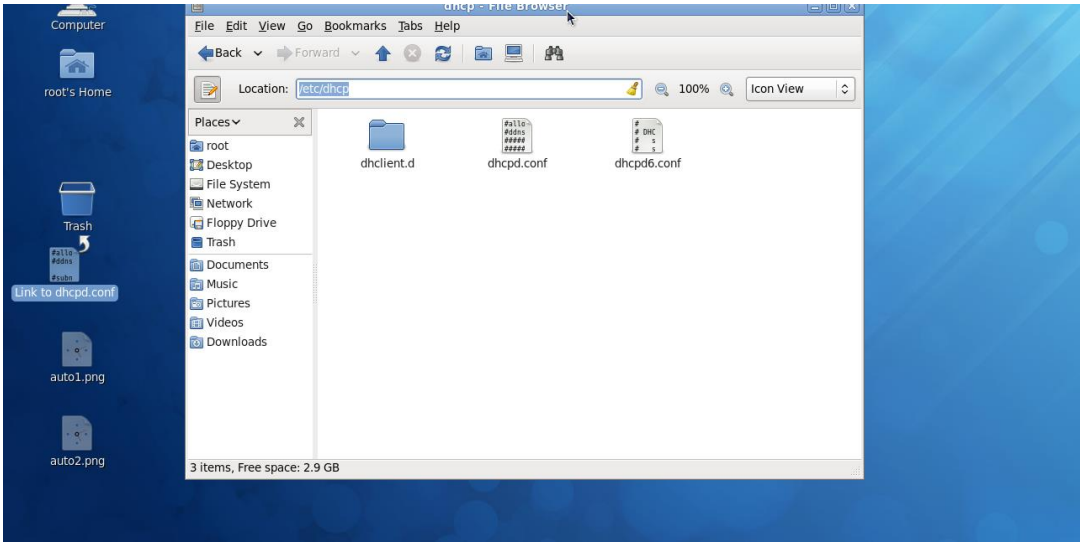
Linux Fedora 12 supports "yum" function by default. First of all, update DHCP client function by issuing "yum install dhclient" command.

- **Install DHCP server**



Issue "yum install dhcp" command to install DHCP server.

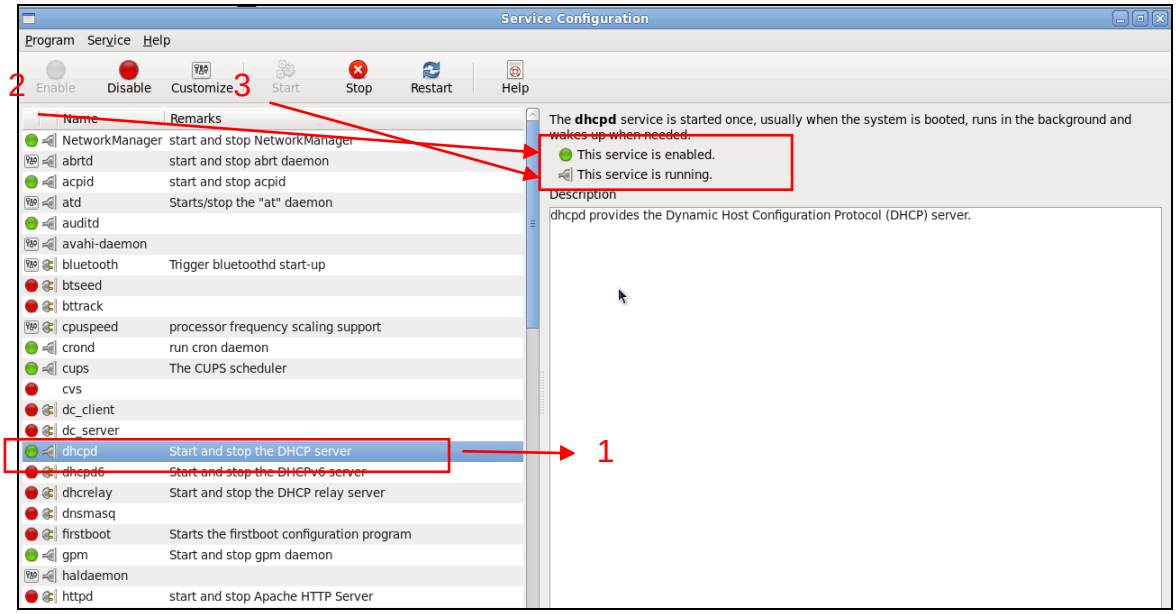
- **Copy dhcpd.conf to /etc/dhcp/ directory**



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

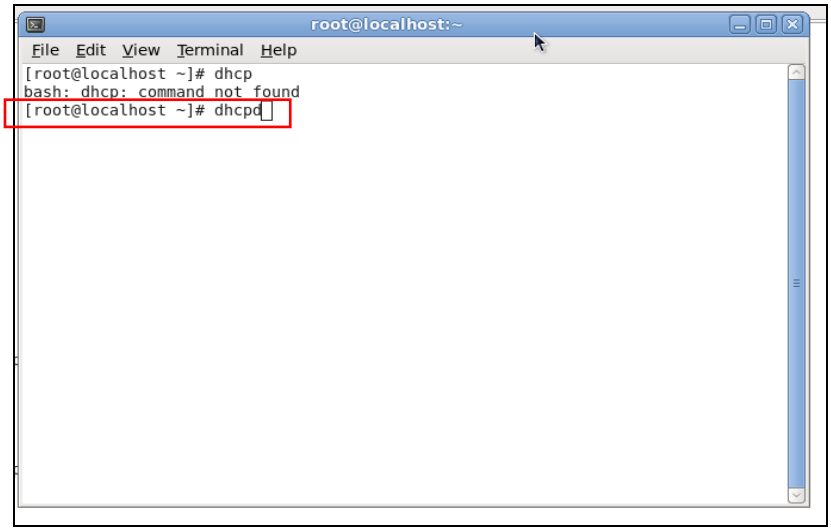
Please note that each vendor has its own way to define auto-provisioning. Make sure to use the file provided by the vendor.

- **Enable and run DHCP service**



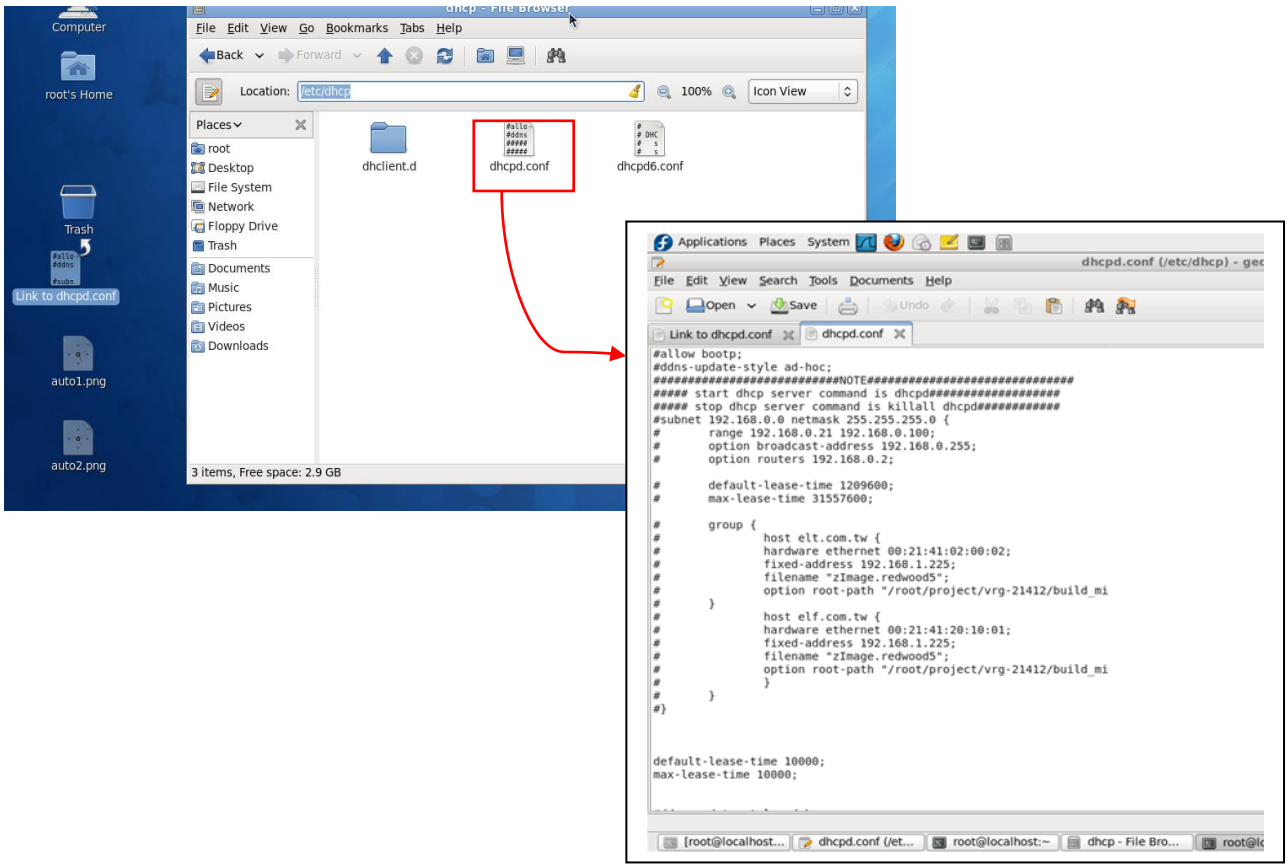
1. Choose dhcpd.
2. Enable DHCP service.
3. Start running DHCP service.

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



Step 3. Modify dhcpd.conf File

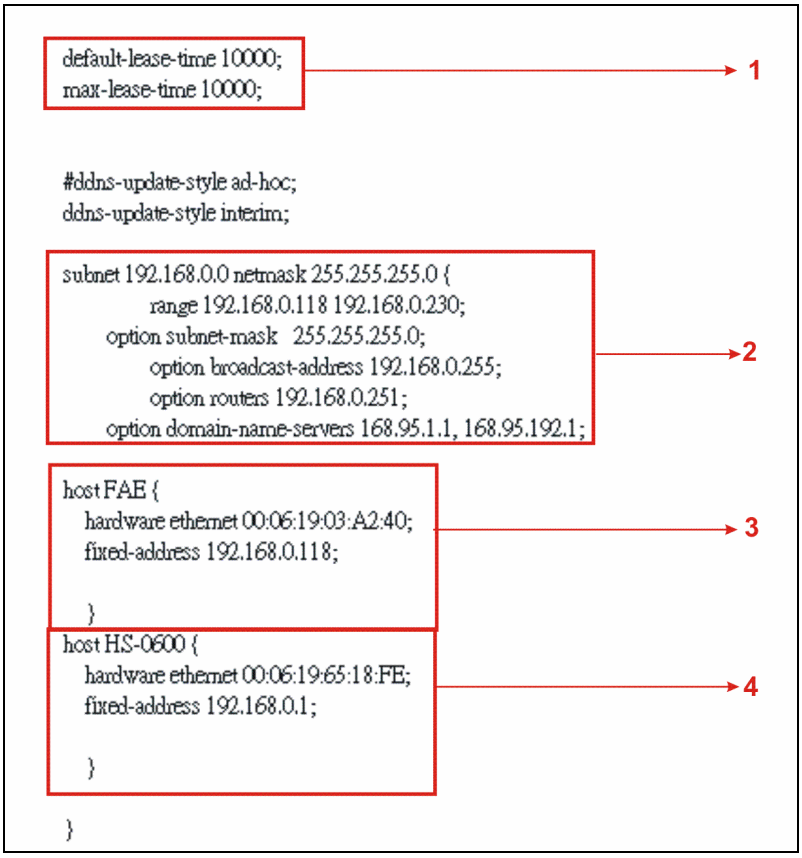
- **Open dhcpd.conf file in /etc/dhcp/ directory**



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

Modify dhcpd.conf file

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



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

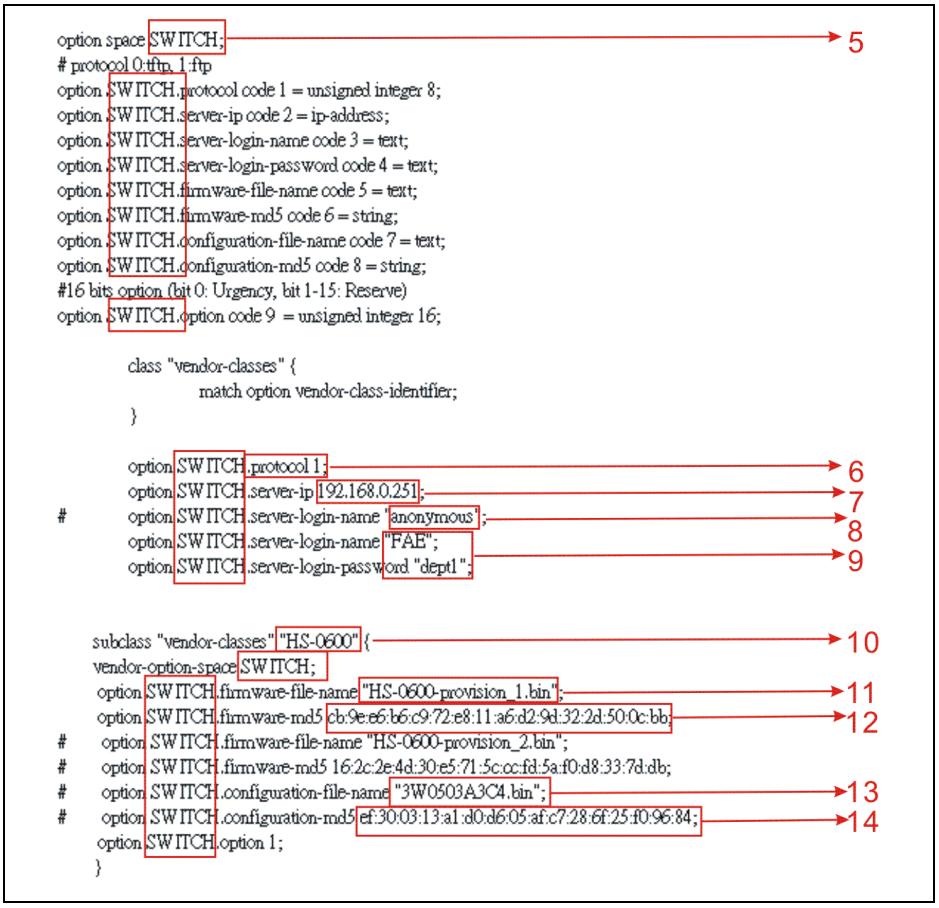
   Default lease time: If a client does not request a specific IP lease time, the server will assign a default lease time value.

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

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

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

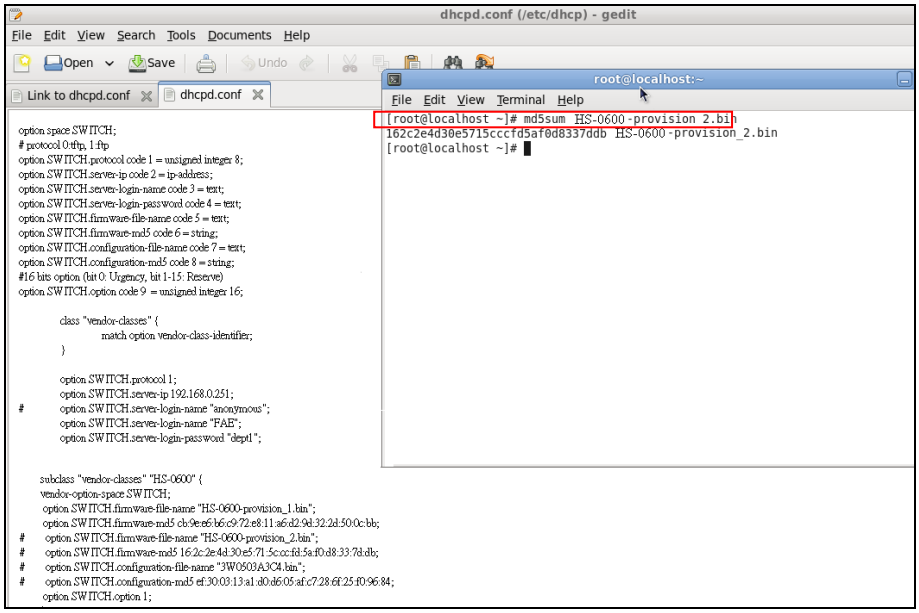
4. Map a host's MAC address to a fixed IP address. Use the same format to create multiple MAC-to-IP address bindings.



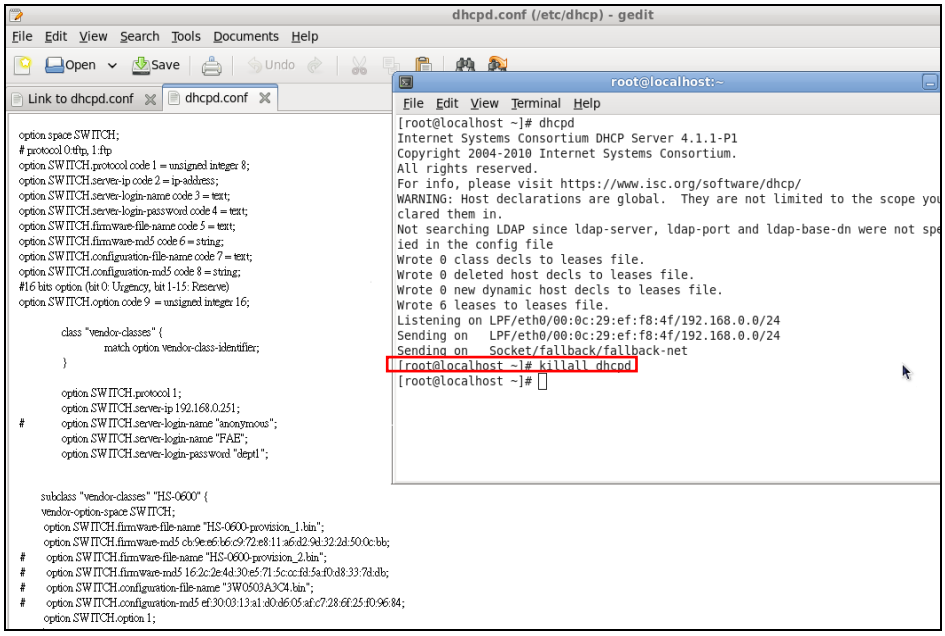
5. This value is configurable and can be defined by users.
6. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
7. Specify the FTP or TFTP IP address.
8. Login TFTP server anonymously (TFTP does not require a login name and password).
9. Specify FTP Server login name and password.
10. Specify 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.

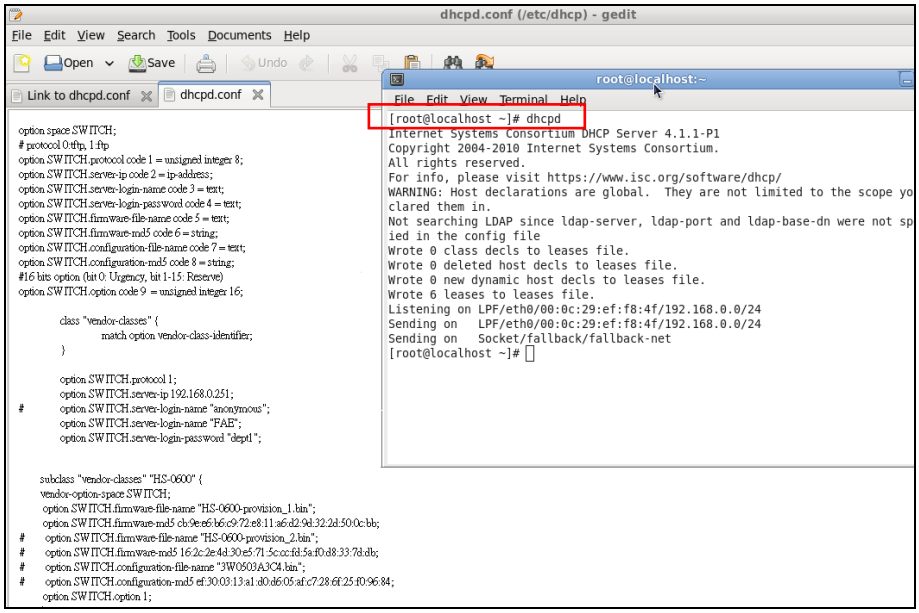
NOTE 1: *The text beginning with a pound sign (#) will be ignored by the DHCP server. For example, in the figure shown above, firmware-file-name "HS-0600-provision_2.bin" and firmware-md5 (line 5 & 6 from the bottom) will be ignored. If you want DHCP server to process these two lines, remove pound signs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



- **Restart DHCP service**





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

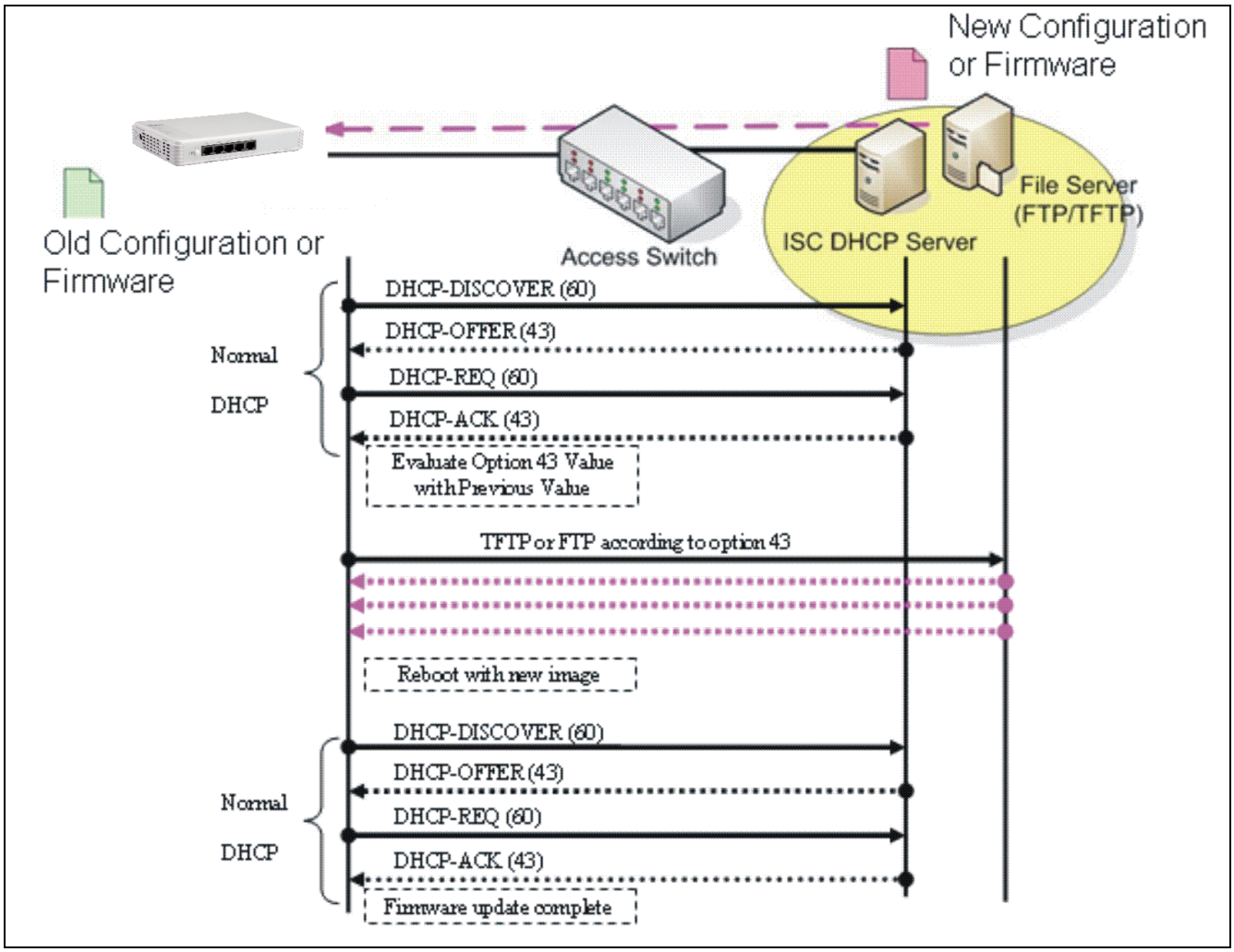
The TFTP/FTP File server should include the following items:

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 2.7.3 Node Controller.

Section	Title	Command Class
2.7.3.1	Notification Settings	Notification Command Class V.7
2.7.3.2	Power Level Settings	Power Level Command Class V.1
2.7.3.3	Association Settings	Association Command Class V.2 Association Group Information Command Class V.1
2.7.3.4	Battery Status	Battery Command Class V.1
2.7.3.5	Door Lock Settings	Door Lock Command Class V.1
2.7.3.6	User Code Settings	User Code Command Class V.1
2.7.3.7	Wake Up Settings	Wake Up Command Class V.2
2.7.3.8	Sensor Multilevel Settings	Multilevel Sensor Command Class V.9
2.7.3.9	Basic Settings	Basic Command Class V.1
2.7.3.10	Binary Settings	Binary Switch Command Class V.1
2.7.3.11	Switch Multilevel Settings	Multilevel Switch Command Class V.3
2.7.3.12	Meter Settings	Meter Command Class V.3
2.7.3.13	Thermostat Setpoint Settings	Thermostat Setpoint Command Class V.1
2.7.3.14	Thermostat Mode Settings	Thermostat Mode Command Class V.1
2.7.3.15	Configuration Settings	Configuration Command Class V.1

FCC Warning

- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.
- This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter
- For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible
- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits 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 the dealer or an experienced radio/TV technician for help.