CTS
CONNECTION TECHNOLOGY SYSTEMS

FWR5-3105 Series
Residential Gateway

Network Management

User’s Manual

Version 0.92

Trademarks

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

Copyright Statement

FCC Warning

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

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

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

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

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

Revision History

Version	Firmware	Date	Description
0.90	0.99.06	20160831	First Release
0.91	0.99.0N	20170208	Add QoS (Section 3.8) Add WPS (Section 3.5.5) Revise MAC Access Filter (Section 3.5.4)
0.92	0.99.0N	20190308	Add a note of Copy-cfg command.

Table of Contents

1. INTRODUCTION

Thank you for purchasing the WLAN Residential Gateway which is designed to aim at FTTX applications. This WLAN Residential Gateway provides four TP ports for LAN applications, one fiber optic or TP port for WAN, wireless function provides users not only more flexible ways to enjoy bandwidth-intensive services but also more secure internetwork connections by implementing packet or URL filtering policies.

The wireless function of this Gateway conforms to IEEE 802.11n standards that can provide speed rate up to 30Mbps or 300Mbps when used with other 802.11n wireless products (the speed rate varies depends on the model that your purchase). To enhance wireless connections to reach further, the antennas, dispersing the same amount of power in all directions, can be used to receive and deliver stable and high-gain transmissions. The WLAN Residential Gateway also supports WPA/WPA2/WPA-Mixed authentication methods and 64/128-bit data encryption to implement strict security protection so as to prevent your wireless networks from unauthorized uses or possible malicious attacks. Other security mechanisms provided that can protect your network including the uses of disabling SSID broadcast function, MAC filtering, URL filtering, DDoS protection.

The WLAN Residential Gateway is mainly dedicated to the FTTX broadband service providers who look for a way of delivering multiple IP services to the home users. The fiber optic port supports connection distance from 2KM to 20KM or further than 100KM by using multi-mode optical fiber, single-mode optical fiber (SMF), or bi-direction SMF. The transmission distance varies depending on the fiber transceiver that your purchase. For detailed information about fiber transceiver, please refer to Fiber Transceiver Information PDF in Documentation CD-ROM. To easily manage and maintain the device, advanced network settings are configurable via Web-based Management such as Firmware upgrade. The featured NAT and DHCP server functions also allow you to use a hub or switch to establish a private network depending on your personal needs that allows multiple computers to share a single Internet connection.

1.1 Management Options

Management options available in this Residential Gateway are listed below:

- **CLI Management**

- **Web Management**
  Web Management is of course done over the network. Once the Residential Gateway is on the network, you can login and monitor the status remotely or locally by a web browser. Local console-type Web management, especially for the first time use of Residential Gateway to set up the needed IP, can also be done through any of the four 10/100/1000Base-T 8-pin RJ-45 ports located at the front panel of the Residential Gateway. Direct RJ45 LAN cable connection between a PC and Residential Gateway is required for this.

- **SNMP Management** (See Chapter 4. SNMP NETWORK MANAGEMENT for detailed descriptions.)

1.2 Interface Descriptions

Before you start to configure your device, it is very important that the proper cables with the correct pin arrangement are used when connecting the Residential Gateway to other devices such as switch, hub, workstation, etc. The following describes correct cables for each interface type.

- **WAN 100/1000Base-X SFP Port**

  1x 100/1000Base-X SFP Port is located within the back panel of the Residential Gateway. The small form-factor pluggable (SFP) is a compact optical transceiver used in optical data communication applications. It interfaces a network device mother board (for a switch, router or similar device) to a fiber optic or unshielded twisted pair networking cable. It is a popular industry format supported by several fiber optic component vendors.

  SFP transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required optical reach over the available optical fiber type. SFP transceivers are also available with a "copper" cable interface, allowing a host device designed primarily for optical fiber communications to also communicate over unshielded twisted pair networking cable.

  SFP slot for 3.3V mini GBIC module supports hot swappable SFP fiber transceiver. Before connecting the other switches, workstation or Media Converter, make sure both side of the SFP transfer are with the same media type, for example, 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX, and check the fiber-optic cable type matches the SFP transfer model. To connect to 1000Base-SX transceiver, use the multi-mode fiber cable with male duplex LC connector type for one side. To connect to 1000Base-LX transfer, use the single-mode fiber cable with male duplex LC connector type for one side.

- **LAN 10/100/1000Base-TX RJ-45 Ports**

  4x10/100/1000Base-T 8-pin RJ-45 ports are located at the front panel of the Residential Gateway. These RJ-45 ports allow user to connect their traditional copper based Ethernet/Fast Ethernet devices into network. All these ports support auto-negotiation and

MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5 cable may be used.

Since there is no separated RJ-45 Management Console port for this Residential Gateway, however any of these four 10/100/1000Base-T RJ-45 ports can be used temporarily as the RJ-45 Management Console Port for local management. This temporary RJ-45 Management Console Port of the Residential Gateway and a RJ-45 LAN cable for PC connections are required to connect the Residential Gateway and a PC. Through these, the user then can configure and check the Residential Gateway even when the network is down.

1.3 Connecting the Residential Gateway

Before starting to configure the Residential Gateway, you have to connect your devices correctly. When you connect your device correctly, the corresponding LEDs will light up.

- Connect the power adaptor to the power port of the Residential Gateway on the back, and the other end into a wall outlet. The Power LED should be ON.

- The system starts to initiate. After completing the system test, the Status LED will light up.

- **CAUTION:** For the first-time configuration, connect one end of an Ethernet patch cable (RJ-45) to any ports on the front panel and connect the other end of the patch cable (RJ-45) to the Ethernet port on Administrator computer. LAN LED for the corresponding port will light up.

- Connect one end of an Ethernet patch cable (RJ-45) to other LAN ports of the Router and connect the other end of the patch cable (RJ-45) to the Ethernet port on other computers or Ethernet devices to form a small area network. The LAN LED for that port on the front panel will light up.

- Connect the Fiber cable provided from your service provider to the WAN Fiber port on the back panel, the WAN LED will light up and blinking if data are transmitting.

2. Command Line Interface (CLI)

This chapter introduces you how to use Command Line Interface CLI, specifically in:

- Telnet
- Configuring the system
- Resetting the system

2.1 Remote Console Management - Telnet

You can manage the Gateway via Telnet session. However, you must first assign a unique IP address to the Gateway before doing so. Use the Local Console to login the Gateway and assign the IP address for the first time.

Follow these steps to manage the Gateway through Telnet session:

Step 1. Use Local Console to assign an IP address to the Gateway

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

Step 2. Run Telnet

Step 3. Log into the Gateway CLI

Limitations: When using Telnet, keep the following in mind:

Only two active Telnet sessions can access the Gateway at the same time.

2.2 Navigating CLI

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

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

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

2.2.1 General Commands

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

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

logout	Logout from the CLI or terminate Console or Telnet session.	User Mode Privileged Mode

2.2.2 Quick Keys

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

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

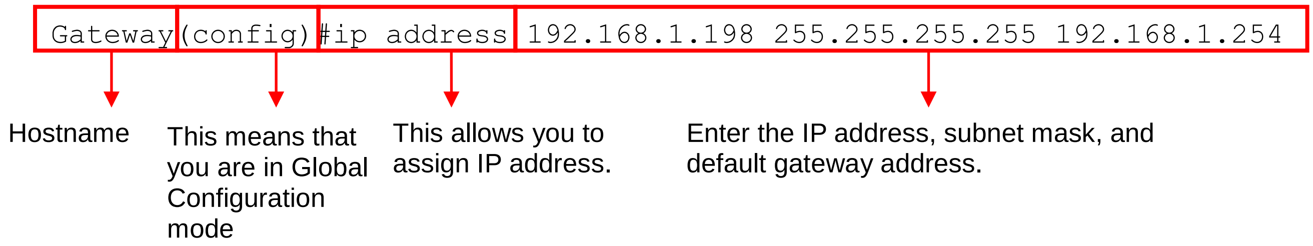
Unfinished command followed by ?	Enter an unfinished command or keyword and press “?” key to complete the command and get command syntax help.
	
	Example: List all available commands starting with the characters that you enter.
	
	`Gateway#h?`
	`help                          Show available commands`
	`history                       Show history commands`

A space followed by ?	Enter a command and then press Spacebar followed by a “?” key to view the next parameter.
Up arrow	Use Up arrow key to scroll through the previous entered commands, beginning with the most recent key-in commands.
Down arrow	Use Down arrow key to scroll through the previous entered commands, beginning with the commands that are entered first.

2.2.3 Command Format

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

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



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

Hostname

This means that you are in Global Configuration mode

This allows you to assign IP address.

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

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

Symbols	Brief Description
>	Currently, the device is in User mode.
#	Currently, the device is in Privileged mode.
(config)#	Currently, the device is in Global Configuration mode.
Syntax	**Brief Description**
[ ]	Reference parameter.
[-s size] [-r repeat] [-t timeout]	These three parameters are used in ping command and are optional, which means that you can ignore these three parameters if they are unnecessary when executing ping command.
[A.B.C.D]	Brackets represent that this is a required field. Enter an IP address or gateway address.
[255.X.X.X]	Brackets represent that this is a required field. Enter the subnet mask.
[port]	Enter one port number.
[port_list]	Enter a range of port numbers or server discontinuous port numbers.
[forced_false | auto]	There are three options that you can choose. Specify one of them.
[1-8191]	Specify a value between 1 and 8191.

[0-7] 802.1p_list
[0-63] dscp_list
	Specify one value, more than one value or a range of values.
	Example 1: specifying one value
	`Gateway(config)#qos 802.1p-map 1 0`
	`Gateway(config)#qos dscp-map 10 3`
	Example 2: specifying three values (separated by commas)
	`Gateway(config)#qos 802.1p-map 1,3 0`
	`Gateway(config)#qos dscp-map 10,13,15 3`
	Example 3: specifying a range of values (separated by a hyphen)
	`Gateway(config)#qos 802.1p-map 1-3 0`
	`Gateway(config)#qos dscp-map 10-15 3`

2.2.4 Login Username & Password

Default Login

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

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

Enable Mode Password

Enable mode is password-protected. When you try to enter Enable mode, a password prompt will appear to request the user to provide the legitimate passwords. Enable mode password is the same as the one entered after login password prompt. By default, no password is required. Therefore, press **Enter** key in password prompt.

Forgot Your Login Username & Password

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

2.3 User Mode

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

Command	Description
exit	Quit the User mode or close the terminal connection.
help	Display a list of available commands in User mode.
history	Display the command history.
logout	Logout from the Gateway.
ping	Test whether a specified network device or host is reachable or not.
traceroute	Trace the route to HOST.
enable	Enter the Privileged mode.

2.3.1 Ping Command

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

Command	Parameter	Description
Gateway> ping [A.B.C.D] [-s size (1-65500)bytes] [-r timeout (1-99) secs]	[A.B.C.D]	Enter the IP/IPv6 address that you would like to ping.
	[-s size (1-65500)bytes]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes.

[-t timeout (1-99)secs]		(optional)
	[-r repeat (1-99) times]	Enter the repeat value that how many times should be pinged.
	[-t timeout (1-99) secs]	Enter the timeout value when the specified IP address is not reachable. (optional)

Example
Gateway> ping 8.8.8.8 Gateway> ping 8.8.8.8 –s 128 –t 10

2.3.2 Traceroute Command

Traceroute is used to trach the path between the local host and the remote host. Enter the **traceroute** command in User mode. In this command, you can add an optional max hops value for the number of hops that packets are sent and received.

Command	Parameter	Description
Gateway > traceroute [A.B.C.D | URL] [-h 1-100] hops [-t 1-99] secs	[A.B.C.D | URL]	Enter the IP address that you would like to ping.
	[-h 1-100] hops	Specify max hops between the local host and the remote host
	[-t 1-99] secs	Specify timeout time in second

Example
Gateway > traceroute 8.8.8.8 Gateway> traceroute 8.8.8.8 –h 30

2.4 Privileged Mode

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

Command	Description
configure	Enter Global Configuration mode.
copy-cfg	Restore or backup configuration file via FTP or TFTP server.
disable	Exit Enable mode and return to User Mode.
exit	Exit Enable mode and return to User Mode.
firmware	Allow users to update firmware via FTP or TFTP.
help	Display a list of available commands in Enable mode.
history	Show commands that have been used.
logout	Logout from the Gateway.
ping	Test whether a specified network device or host is reachable or not.
reload	Restart the Gateway.
show	Show a list of commands or show the current setting of each listed command.
traceroute	Trace the route to HOST.
write	Save your configurations to Flash.

2.4.1 Copy-cfg Command

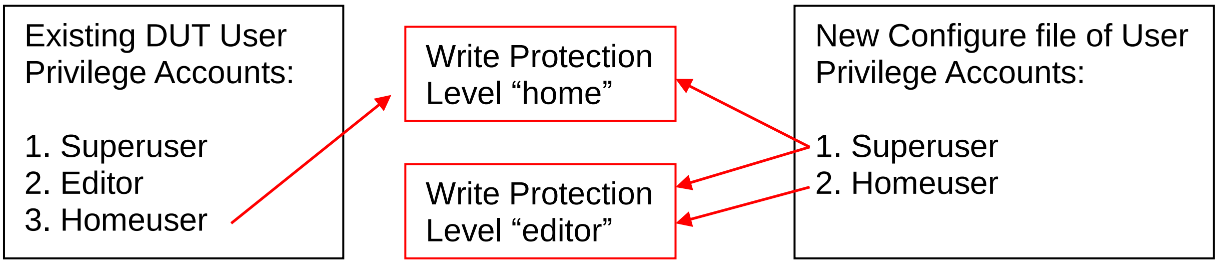
Use “copy-cfg” command to backup a configuration file via FTP or TFTP server and restore the Gateway back to the defaults or to the defaults but keep IP configurations.

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

Command	Parameter	Description
Gateway# copy-cfg from ftp [A.B.C.D] [file name] [user_name] [password]	[A.B.C.D]	Enter the IP/IPv6 address of your FTP server.
	[file name]	Enter the configuration file name that you want to restore.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Gateway# copy-cfg from tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP/IPv6 address of your TFTP server.
	[file name]	Enter the configuration file name that you want to restore.
Example		
Gateway# copy-cfg from ftp 192.168.1.198 HS_0600_file.conf misadmin1 abcxyz Gateway# copy-cfg from tftp 192.168.1.198 HS_0600_file.conf		

Note: For ISP, the default write protection level is set "home" in configuration file on the ground of safety, which means the following functions are unable to be overwritten when executing configure restoration.
1. DDNS
2. Network Setup (LAN-IP, DHCP Server, DHCP Reserved)
3. WiFi (Wireless Setup, Wireless Security)
4. Application (DMZ, Port Forwarding)
5. Security (Firewall, Packet Filter, URL Filter, VPN Pass-Through, UPnP, DDoS)
6. Administration (User Privilege) - Yet if the write protection level is "home", the user privilege level "superuser" and "editor" will be deleted except "homeuser". However, the "homeuser" is copied from either existing DUT or new configure file. It depends on the write protection level.

Assume that we have a setting of existing User Privilege in DUT and a configure file ready to be loaded.


Existing DUT User Privilege Accounts:
1. Superuser
2. Editor
3. Homeuser
Write Protection Level "home"
Write Protection Level "editor"
New Configure file of User Privilege Accounts:
1. Superuser
2. Homeuser

Here is the treatment of User Privilege of configure restoration:
A. Save the existing homeuser configuration in DUT
B. Reset the DUT back to the default setting.
C. Check the write protection level. If the write protection level is "home", it loads DUT's homeuser configure back into DUT.

To overwrite all of configuration, please change the write protection level "home" into "editor".In terms of User Privilege. If the write protection level is "editor", it loads the homeuser of new homeuser configure file into DUT

2. **Backup configuration file to FTP or TFTP server.**

Command	Parameter	Description
Gateway# copy-cfg to ftp [A.B.C.D] [file name] [running | default | startup] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Gateway# copy-cfg to tftp [A.B.C.D] [file_name] [running | default | startup]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file name]	Enter the configuration file name that you want to backup.
	[running | default | startup]	Specify backup config to be running, default or startup
Example		
Gateway# copy-cfg to ftp 192.168.1.198 HS_0600_file.conf running misadmin1 abcxyz Gateway# copy-cfg to tftp 192.168.1.198 HS_0600_file.conf startup		

3. **Restore the Gateway back to default settings.**

Command / Example
Gateway# copy-cfg from default Gateway# reload

4. **Restore the Gateway back to default settings but keep IP configurations.**

Command / Example
Gateway# copy-cfg from default keep-ip Gateway# reload

2.4.2 Firmware Command

To upgrade firmware via TFTP or FTP server.

Command	Parameter	Description
Gateway# firmware upgrade ftp [A.B.C.D] [file_name] [Image-1| Image-2] [user_name] [password]	[A.B.C.D]	Enter the IP address of your FTP server.
	[file name]	Enter the firmware file name that you want to upgrade.
	[Image-1| Image-2]	Choose image-1 or image-2 for the firmware to be upgraded to.
	[user_name]	Enter the username for FTP server login.
	[password]	Enter the password for FTP server login.
Gateway# firmware upgrade tftp [A.B.C.D] [file_name]	[A.B.C.D]	Enter the IP address of your TFTP server.
	[file_name]	Enter the firmware file name that you want to upgrade.

[Image-1| Image-2]	[Image-1| Image-2]	Choose image-1 or image-2 for the firmware to be upgraded to.
Example		
Gateway# firmware upgrade ftp 192.168.1.198 HS_0600_file.bin edgegateway10 abcxyz		
Gateway# firmware upgrade tftp 192.168.1.198 HS_0600_file.bin		

2.4.3 Ping Command

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

Command	Parameter	Description
Gateway> ping [A.B.C.D] [-s size (1-65500)bytes] [-r timeout (1-99) secs] [-t timeout (1-99)secs]	[A.B.C.D]	Enter the IP address that you would like to ping.
	[-s size (1-65500)bytes]	Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes. (optional)
	[-r repeat (1-99) times]	Enter the repeat value that how many times should be pinged.
	[-t timeout (1-99) secs]	Enter the timeout value when the specified IP address is not reachable. (optional)
Example		
Gateway> ping 8.8.8.8 Gateway> ping 8.8.8.8 –s 128 –t 10		

2.4.4 Reload Command

1. **To restart the Gateway.**

Command / Example
Gateway# reload

2. **To specify the image for the next restart before restarting.**

Command / Example
Gateway# reload Image-2 OK! Gateway# reload

2.4.5 Traceroute Command

Command	Parameter	Description
Gateway > traceroute [A.B.C.D | URL] [-h 1-100] hops [-t 1-99] secs	[A.B.C.D | URL]	Enter the IP address that you would like to ping.
	[-h 1-100] hops	Specify max hops between the local host and the remote host
	[-t 1-99] secs	Specify timeout time in second
Example		
Gateway > traceroute 8.8.8.8 Gateway> traceroute 8.8.8.8 –h 30		

2.4.6 Write Command

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

Command / Example
Gateway# write Save Config Succeeded!

2.4.7 Configure Command

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

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

2.4.8 Show Command

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

1. **Display system information**

Enter “show system-info” command in Privileged or Configuration mode, and then the following information will appear.

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

System Object ID: Display the predefined System OID.

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

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

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

DHCP Vendor ID: Enter the Vendor ID used for DHCP relay agent function.

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

Current Boot Image: The image that is currently using.

Configured Boot Image: The image you want to use after reboot.

Image-1 Version: Display the firmware version 1 (image-1) used in this device.

Image-2 Version: Display the firmware version 2 (image-2) used in this device.

M/B Version: Display the main board version.

Serial Number: Display the serial number of this Gateway.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

2. Display or verify currently-configured settings

Refer to the following sub-sections. “Interface command”, “IP command”, “User command”, “VLAN command” sections, etc.

3. Display interface information or statistics

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

4. Show default, running and startup configurations

Refer to “show default-setting copmmand”, “show running-config command” and “show start-up-config command” sections.

2.5 Configuration Mode

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

Command	Description
applications	Application global configuration commands.
exit	Exit the configuration mode.
help	Display a list of available commands in Configuration mode.
history	Show commands that have been used.
interface	Select a single interface or a range of interfaces.
ip	Set up the IPv4 address and enable DHCP mode & IGMP snooping.
management	Set up console/telnet/web/SSH access control and timeout value.
no	Disable a command or set it back to its default setting.
ntp	Set up required configurations for Network Time Protocol.
qos	Set up the priority of packets within the Managed Switch.

security	Security global configuration commands.
show	Show a list of commands or show the current setting of each listed command.
snmp-server	SNMP server configuration commands.
system-info	Set up acceptable frame size and address learning, etc.
syslog	Set up required configurations for Syslog server.
user	Create a new user account.
vlan	Set up VLAN mode and VLAN configuration.

2.5.1 Entering Interface Numbers

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

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

2.5.2 No Command

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

2.5.3 Show Command

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

1. Display system information

Enter "show system-info" command in Privileged or Configuration mode, and then the following information will appear.

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

System Object ID: Display the predefined System OID.

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

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

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

Model Name: Display the product’s model name.

Host Name: Display the product’s host name.

DHCP Vendor ID: Enter the Vendor ID used for DHCP relay agent function.

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

M/B Version: Display the main board version.

Serial Number: Display the serial number of this Gateway.

Up Time: Display the up time since last restarting.

Local Time: Display local time.

2. **Display or verify currently-configured settings**

Refer to the following sub-sections. “Interface command”, “IP command”, “User command”, “VLAN command” sections, etc.

3. **Display interface information or statistics**

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

4. **Show default, running and startup configurations**

Refer to “show default-setting copmmand”, “show running-config command” and “show start-up-config command” sections.

2.5.4 Applications Command

1. Set up DMZ function.

Command	Parameter	Description
Gateway(config)# applications dmz		Enable DMZ function. DMZ stands for “Demilitarized Zone”. It is an IP address on the private network of the Residential Gateway. But it is exposed to the Internet

		for special-purpose services. So a host on the private network can be assigned the IP address of the DMZ to provide services to the hosts on the Internet. The network administrator should be cautious of adopting DMZ. If a host is on DMZ, it is not protected by the firewall. And the Residential Gateway will open all ports to expose DMZ to the Internet. This may expose the local network to a variety of security risk.
Gateway(config)# applications destination-ip [A.B.C.D]	[A.B.C.D]	Specify the IP address of the host on the DMZ.
Gateway(config)# applications source-ip [A.B.C.D] [1-254]	[A.B.C.D] [1-254]	Specify an IP address range in the text boxes so the DMZ will be exposed to the IP address in the specified IP address range only.
Gateway(config)# applications source-ip any		Allow any IP address to expose the DMZ to any IP address on the Internet.
No Command		
Gateway(config)# no applications dmz		Disable DMZ function.
Show Command		
Gateway(config)# show applications dmz		Shows the current status of DMZ.

2. Set up Port Forwarding function.

Command	Parameter	Description
Gateway(config)# applications port-forwarding		Enable Port Forwarding function. A host on the private network of the Residential Gateway is invisible from the Internet for it is protected by the firewall. Therefore, when a server is on the private network, its service will be inaccessible from the Internet. To open the service to hosts on the Internet, the network administrator may adopt Port Forwarding feature. Port Forwarding allows an IP address on the private network to be accessed from an IP address on the public network. It will redirect packets from the public network to a specified private IP address if the packets meet the pre-condition of a port forwarding rule.
Gateway(config)# applications port-forwarding apply		Apply all the configured port forwarding settings made.
Gateway(config-port-forwarding-No.)# active		Enable the port forwarding rule.
Gateway(config-port-forwarding-No.)# description [description]	[description]	Specify any remark on the rule up to 20 characters.
Gateway(config-port-forwarding-	[A.B.C.D]	Specify the IP address of the server on

No.)# client-ip [A.B.C.D]		the private network.
Gateway(config-port-forwarding-No.)# local-port [1-65535]	[1-65535]	Specify the port number which the packets are destined to (1~65535).
Gateway(config-port-forwarding-No.)# public-port [1-65535]	[1-65535]	Specify the port number which the packets from the Internet are destined to (1~65535).
Gateway(config-port-forwarding-No.)# protocol [both|tcp|udp]	[both|tcp|udp]	Choose *TCP*, *UDP* or *Both* as your desired protocol.
No Command		
Gateway(config)# no applications port-forwarding		Disable Port Forwarding function.
Gateway(config)# no applications port-forwarding [1-10]	[1-10]	Delete the specified port forwarding rule.
Gateway(config-port-forwarding-No.)# no active		Disable the port forwarding rule.
Gateway(config-port-forwarding-No.)# no description		Clear the remark on the rule.
Gateway(config-port-forwarding-No.)# no client-ip		Clear the IP address of the server on the private network.
Gateway(config-port-forwarding-No.)# no local-port		Return local port to default value 1.
Gateway(config-port-forwarding-No.)# no public-port		Return public port to default value 1.
Gateway(config-port-forwarding-No.)# no protocol		Return protocol to default value “Both”.
Show Command		
Gateway(config)# show applications port-forwarding		Shows the status of port forwarding.
Gateway(config-port-forwarding-No.)# show		Shows the current status of the rule.

2.5.5 Interface Command

Use “interface” command to set up configurations of several discontinuous ports or a range of ports.

1. **Entering interface numbers.**

Command	Parameter	Description
Gateway(config)# interface lan [port_list]	[port_list]	Enter several lan port numbers separated by commas or a range of port numbers. For example: 1,3 or 2-4
Gateway(config)# interface wan [port_list]	[port_list]	Enter several wan port numbers separated by commas or a range of port numbers.
Gateway(config)# interface wlan1		Enter WiFi 5G interface.
Gateway(config)# interface wlan2		Enter WiFi 2.4G interface.

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

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

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

3. **Enable port auto-negotiation.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# combo-mode [copper|fiber]	[copper|fiber]	Specify combo port on copper or fiber port.
No command		
Gateway(config-net-PORT-PORT)# no combo-mode		Disable combo mode.

4. **Set up port duplex mode.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# duplex [full]	[full]	Configure port duplex to **full.**
No command		
Gateway(config-net-PORT-PORT)# no duplex		Configure port duplex to **half.** **Note1 : Only copper ports can be configured as half duplex.** **Note2 : Auto-negotiation needs to be disabled before configuring duplex mode.**

5. **Enable flow control operation.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# flowcontrol		Enable flow control on port(s).
No command		
Gateway(config-net-PORT-PORT)# no flowcontrol		Disable flow control on port(s).

6. **Operation mode selection.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# operation-mode nat		Enable NAT mode. When the Residential Gateway is in this mode, all devices connected to the Residential Gateway from its LAN ports and WLAN are in the private network.
Gateway(config-net-PORT-PORT)# operation-mode bridge		Enable Bridge mode. When the Residential Gateway is in this mode, all devices connected to the Residential Gateway from its LAN ports or WLAN are in the public network.
No command		
Gateway(config-net-PORT-PORT)# no operation-mode		Return to NAT mode.

7. **Shutdown Interface.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# shutdown		Disable interface.
No command		
Gateway(config-net-PORT-PORT)# no shutdown		Enable interface.

8. **Set up port speed.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# speed [1000|100|10]	[1000|100|10]	Set port speed as 1000Mbps, 100Mbps or 10Mbps. **Note1: Speed can only be configured when auto-negotiation is disabled.** **Note2: Fiber ports can not be configured as 10Mbps.**
No command		
Gateway(config-net-PORT-PORT)# no speed		Undo port speed setting.

9. **Set up VLAN parameters per port.**

Command	Parameter	Description
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Configure port PVID.
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan trunk-	[1-4094]	Configure port VID.

vlan [1-4094]		
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan mode access		Configure port as dot-1q access port.
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan mode trunk		Configure port as dot-1q trunk port. This is for LAN and WAN only.
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan mode trunk native		Configure port as dot-1q trunk native port. This is for LAN and WAN only.
No command		
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan access-vlan		Undo configure port PVID.
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan trunk-vlan		Undo configure port VID.
Gateway(config-net-PORT-PORT)# vlan dot1q-vlan mode		Undo VLAN mode configuration.
Gateway(config-net-PORT-PORT)# no vlan dot1q-vlan mode trunk native		Undo VLAN trunk native mode configuration.
Show command		
Gateway(config-net-PORT-PORT)# show interface		Show the current status of each port.
Gateway(config-net-PORT-PORT)# show dot1q-vlan tag-vlan		Show IEEE802.1q tag VLAN table.

10. Set up WiFi advanced settings. (For WiFi Model Only)

For Bandwidth 5G:

Command	Parameter	Description
Gateway(config)# interface wlan1		Access WiFi bandwidth 5G advanced settings.
Gateway(config)# interface wlan1 apply		Apply all change made on WiFi bandwidth 5G advanced settings.
Gateway(config-wlan1)# aggregation		Enable Aggregation function.
Gateway(config-wlan1)# beacon-interval [20-1024]	[20-1024]	Specify the Beacon Interval threshold in ms ranging between 20-1024. The default value is 100.
Gateway(config-wlan1)# channel [channel_number]	[channel_number]	Specify the channel number from the list shown below: **Channel Number: auto, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128.**

<table>
<tr><td>Gateway(config-wlan1)# channel width [20|40|80]</td><td>[20|40|80]</td><td>Specify the channel width in MHz.</td></tr>
<tr><td>Gateway(config-wlan1)# fragment-threshold [256-2346]</td><td>[256-2346]</td><td>Specify the fragment threshold ranging between 256-2346. The default value is 2346.</td></tr>
<tr><td>Gateway(config-wlan1)# iapp</td><td></td><td>Enable IAPP function.</td></tr>
<tr><td>Gateway(config-wlan1)# ldpc</td><td></td><td>Enable LDPC function.</td></tr>
<tr><td>Gateway(config-wlan1)# multicast-rate [auto|1-44]</td><td>[auto|1-44]</td><td>Specify the number corresponding its data rate respectively as below:
<table>
<tr><td>1:6m</td><td>2:9m</td><td>3:12m</td><td>4:18m</td></tr>
<tr><td>5:24m</td><td>6:36m</td><td>7:48m</td><td>8:54m</td></tr>
<tr><td>9:msc0</td><td>10:msc1</td><td>11:msc2</td><td>12:msc3</td></tr>
<tr><td>13:msc4</td><td>14:msc5</td><td>15:msc6</td><td>16:msc7</td></tr>
<tr><td>17:msc8</td><td>18:msc9</td><td>19:msc10</td><td>20:msc11</td></tr>
<tr><td>21:msc12</td><td>22:msc13</td><td>23:msc14</td><td>24:msc15</td></tr>
<tr><td>25:nss1-msc0</td><td>26:nss1-msc1</td><td>27:nss1-msc2</td><td>28:nss1-msc3</td></tr>
<tr><td>29:nss1-msc4</td><td>30:nss1-msc5</td><td>31:nss1-msc6</td><td>32:nss1-msc7</td></tr>
<tr><td>33:nss1-msc8</td><td>34:nss1-msc9</td><td>35:nss2-msc0</td><td>36:nss2-msc1</td></tr>
<tr><td>37:nss2-msc2</td><td>38:nss2-msc3</td><td>39:nss2-msc4</td><td>40:nss2-msc5</td></tr>
<tr><td>41:nss2-msc6</td><td>42:nss2-msc7</td><td>43:nss2-msc8</td><td>44:nss2-msc9</td></tr>
</table></td></tr>
<tr><td>Gateway(config-wlan1)# multicast-to-unicast</td><td></td><td>Enable Multicast to Unicast function.</td></tr>
<tr><td>Gateway(config-wlan1)# protection</td><td></td><td>Enable Protection function.</td></tr>
<tr><td>Gateway(config-wlan1)# rf-output-power [100|70|50|35|15]</td><td>[100|70|50|35|15]</td><td>Specify the percentage of RF Output Power level, 100%, 70%, 50%, 35% and 15% are available.</td></tr>
<tr><td>Gateway(config-wlan1)# rts-threshold [0-2347]</td><td>[0-2347]</td><td>Specify the RTS threshold ranging between 0-2347. The default value is 2347.</td></tr>
<tr><td>Gateway(config-wlan1)# short-gi</td><td></td><td>Enable Short GI function.</td></tr>
<tr><td>Gateway(config-wlan1)# stbc</td><td></td><td>Enable STBC function.</td></tr>
<tr><td>Gateway(config-wlan1)# tdls channel-switch-prohibited</td><td></td><td>Enable TDLS Channel Switch Prohibited function.</td></tr>
<tr><td>Gateway(config-wlan1)# tdls prohibited</td><td></td><td>Enable TDLS Prohibited function.</td></tr>
<tr><td>Gateway(config-wlan1)# tx-breamforming</td><td></td><td>Enable Tx Beamforming function.</td></tr>
</table>

Gateway(config-wlan1)# wlan-partition		Enable WLAN Partition function.
Gateway(config-wlan1)# wps		Enable WPS function.
No Command		
Gateway(config-wlan1)# no aggregation		Disable Aggregation function.
Gateway(config-wlan1)# no beacon-interval		Return Beacon Interval to default value.
Gateway(config-wlan1)# no channel		Return channel number to default value.
Gateway(config-wlan1)# no channel width		Return channel width to default value.
Gateway(config-wlan1)# no fragment-threshold		Return fragment threshold to default value.
Gateway(config-wlan1)# no iapp		Disable IAPP function.
Gateway(config-wlan1)# no ldpc		Disble LDPC function.
Gateway(config-wlan1)# no multicast-rate		Return multicast rate to default value
Gateway(config-wlan1)# no multicast-to-unicast		Disable Multicast to Unicast function.
Gateway(config-wlan1)# no protection		Disable Protection function.
Gateway(config-wlan1)# no rf-output-power		Return RF output power to default value.
Gateway(config-wlan1)# no rts-threshold		Return RTS threshold to default value.
Gateway(config-wlan1)# no short-gi		Disable Short GI function.
Gateway(config-wlan1)# no stbc		Disable STBC function.
Gateway(config-wlan1)# no tdls channel-switch-prohibited		Disable TDLS Channel Switch Prohibited function.
Gateway(config-wlan1)# no tdls prohibited		Disable TDLS Prohibited function.
Gateway(config-wlan1)# no tx-breamforming		Disable Tx-Beamforming function.
Gateway(config-wlan1)# no wlan-partition		Disable WLAN Partition function.
Gateway(config-wlan1)# wps		Disable WPS function.
Show Command		
Gateway(config)# show interface wlan1		Shows the current advanced status of WiFi 5G.

For Bandwidth 2.4G:

<table>
<tr><th>Command</th><th>Parameter</th><th>Description</th></tr>
<tr><td>Gateway(config)# interface wlan2</td><td></td><td>Access WiFi bandwidth 2.4G advanced settings.</td></tr>
<tr><td>Gateway(config)# interface wlan2 apply</td><td></td><td>Apply all change made on WiFi bandwidth 2.4G advanced settings.</td></tr>
<tr><td>Gateway(config-wlan2)# aggregation</td><td></td><td>Enable Aggregation function.</td></tr>
<tr><td>Gateway(config-wlan2)# beacon-interval [20-1024]</td><td>[20-1024]</td><td>Specify the Beacon Interval threshold in ms ranging between 20-1024. The default value is 100.</td></tr>
<tr><td>Gateway(config-wlan2)# control-sideband [upper|lower]</td><td>[upper|lower]</td><td>The extra bandwidth will be available when the channel bandwidth is 40MHz. If you select <i><u>Upper</u></i>, the extra bandwidth will be extended in the upper sideband. (<i>This field is only available when the network mode is 2.4 GHz (N), 2.4 GHz (G+N), or 2.4 GHz (B+G+N).</i>)</td></tr>
<tr><td>Gateway(config-wlan2)# channel [channel_number]</td><td>[channel_number]</td><td>Specify the channel number from the list shown below:

<b>Channel Number: auto, 5-13</b></td></tr>
<tr><td>Gateway(config-wlan2)# coexist</td><td></td><td>Enable Coexist function.</td></tr>
<tr><td>Gateway(config-wlan2)# channel width [20|40|80]</td><td>[20|40|80]</td><td>Specify the channel width in MHz.</td></tr>
<tr><td>Gateway(config-wlan2)# fragment-threshold [256-2346]</td><td>[256-2346]</td><td>Specify the fragment threshold ranging between 256-2346. The default value is 2346.</td></tr>
<tr><td>Gateway(config-wlan2)# iapp</td><td></td><td>Enable IAPP function.</td></tr>
<tr><td>Gateway(config-wlan2)# ldpc</td><td></td><td>Enable LDPC function.</td></tr>
<tr><td>Gateway(config-wlan2)# multicast-rate [auto|1-44]</td><td>[auto|1-44]</td><td>Specify the number corresponding its data rate respectively as below:
<table>
<tr><td>1:6m</td><td>2:9m</td><td>3:12m</td><td>4:18m</td></tr>
<tr><td>5:24m</td><td>6:36m</td><td>7:48m</td><td>8:54m</td></tr>
<tr><td>9:msc0</td><td>10:msc1</td><td>11:msc2</td><td>12:msc3</td></tr>
<tr><td>13:msc4</td><td>14:msc5</td><td>15:msc6</td><td>16:msc7</td></tr>
<tr><td>17:msc8</td><td>18:msc9</td><td>19:msc10</td><td>20:msc11</td></tr>
<tr><td>21:msc12</td><td>22:msc13</td><td>23:msc14</td><td>24:msc15</td></tr>
<tr><td>25:nss1-msc0</td><td>26:nss1-msc1</td><td>27:nss1-msc2</td><td>28:nss1-msc3</td></tr>
<tr><td>29:nss1-msc4</td><td>30:nss1-msc5</td><td>31:nss1-msc6</td><td>32:nss1-msc7</td></tr>
<tr><td>33:nss1-msc8</td><td>34:nss1-msc9</td><td>35:nss2-msc0</td><td>36:nss2-msc1</td></tr>
<tr><td>37:nss2-msc2</td><td>38:nss2-msc3</td><td>39:nss2-msc4</td><td>40:nss2-msc5</td></tr>
<tr><td>41:nss2-msc6</td><td>42:nss2-msc7</td><td>43:nss2-msc8</td><td>44:nss2-msc9</td></tr>
</table></td></tr>
</table>

Gateway(config-wlan2)# multicast-to-unicast		Enable Multicast to Unicast function.
Gateway(config-wlan2)# preamble-type [long|short]	[long|short]	Specify Preamble Type, either Long Preamble or Short Preamble.
Gateway(config-wlan2)# protection		Enable Protection function.
Gateway(config-wlan2)# rf-output-power [100|70|50|35|15]	[100|70|50|35|15]	Specify the percentage of RF Output Power level, 100%, 70%, 50%, 35% and 15% are available.
Gateway(config-wlan2)# rts-threshold [0-2347]	[0-2347]	Specify the RTS threshold ranging between 0-2347. The default value is 2347.
Gateway(config-wlan2)# short-gi		Enable Short GI function.
Gateway(config-wlan2)# stbc		Enable STBC function.
Gateway(config-wlan2)# tdls channel-switch-prohibited		Enable TDLS Channel Switch Prohibited function.
Gateway(config-wlan2)# tdls prohibited		Enable TDLS Prohibited function.
Gateway(config-wlan2)# tx-breamforming		Enable Tx Beamforming function.
Gateway(config-wlan2)# wlan-partition		Enable WLAN Partition function.
Gateway(config-wlan2)# wps		Enable WPS function.
No Command		
Gateway(config-wlan2)# no aggregation		Disable Aggregation function.
Gateway(config-wlan2)# no beacon-interval		Return Beacon Interval to default value.
Gateway(config-wlan2)# control-sideband		Return sideband to default value.
Gateway(config-wlan2)# no channel		Return channel number to default value.
Gateway(config-wlan2)# no coexist		Disable Coexist function.
Gateway(config-wlan2)# no channel width		Return channel width to default value.
Gateway(config-wlan2)# no fragment-threshold		Return fragment threshold to default value.
Gateway(config-wlan2)# no iapp		Disable IAPP function.
Gateway(config-wlan2)# no ldpc		Disble LDPC function.

Gateway(config-wlan2)# no multicast-rate		Return multicast rate to default value
Gateway(config-wlan2)# no multicast-to-unicast		Disable Multicast to Unicast function.
Gateway(config-wlan2)# no preamble-type		Return Preamble Type to default value.
Gateway(config-wlan2)# no protection		Disable Protection function.
Gateway(config-wlan2)# no rf-output-power		Return RF output power to default value.
Gateway(config-wlan2)# no rts-threshold		Return RTS threshold to default value.
Gateway(config-wlan2)# no short-gi		Disable Short GI function.
Gateway(config-wlan2)# no stbc		Disable STBC function.
Gateway(config-wlan2)# no tdls channel-switch-prohibited		Disable TDLS Channel Switch Prohibited function.
Gateway(config-wlan2)# no tdls prohibited		Disable TDLS Prohibited function.
Gateway(config-wlan2)# no tx-breamforming		Disable Tx-Beamforming function.
Gateway(config-wlan2)# no wlan-partition		Disable WLAN Partition function.
Gateway(config-wlan2)# no wps		Disable WPS function.
Show Command		
Gateway(config)# show interface wlan2		Shows the current advanced status of WiFi 2.4G.

11. Set up WiFi basic & security settings. (For WiFi Model Only)

For Bandwidth 5G:

<table>
<tr><th>Command</th><th>Parameter</th><th>Description</th></tr>
<tr><td>Gateway(config)# interface wlan1</td><td></td><td>Access WiFi bandwidth 5G settings.</td></tr>
<tr><td>Gateway(config)# interface wlan1ssid [1-4]</td><td>[1-4]</td><td>Specify the SSID you want to configure.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# active</td><td></td><td>Enable the WiFi service set.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# broadcast</td><td></td><td>Have the SSID disclose in public.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# datarate [auto|1-44]</td><td>[auto|1-44]</td><td>Specify the number corresponding its data rate respectively as below:<table>
<tr><td>1:6m</td><td>2:9m</td><td>3:12m</td><td>4:18m</td></tr>
<tr><td>5:24m</td><td>6:36m</td><td>7:48m</td><td>8:54m</td></tr>
<tr><td>9:msc0</td><td>10:msc1</td><td>11:msc2</td><td>12:msc3</td></tr>
</table></td></tr>
</table>

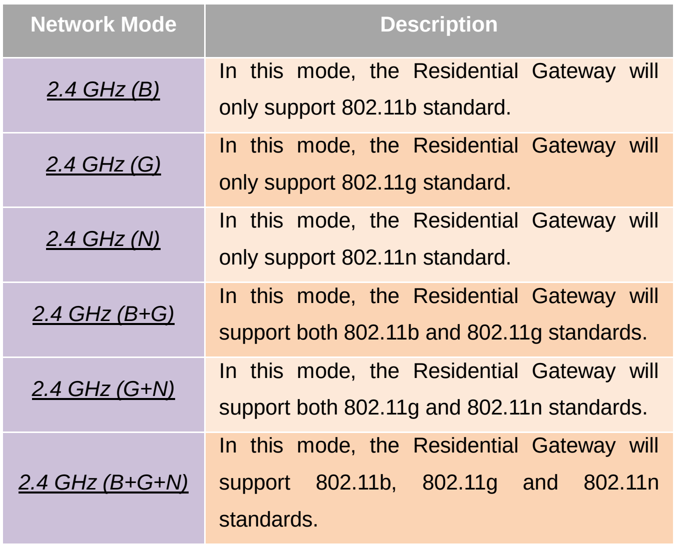
<table>
<tr><td></td><td></td><td><table>
<tr><td>13:msc4</td><td>14:msc5</td><td>15:msc6</td><td>16:msc7</td></tr>
<tr><td>17:msc8</td><td>18:msc9</td><td>19:msc10</td><td>20:msc11</td></tr>
<tr><td>21:msc12</td><td>22:msc13</td><td>23:msc14</td><td>24:msc15</td></tr>
<tr><td>25:nss1-msc0</td><td>26:nss1-msc1</td><td>27:nss1-msc2</td><td>28:nss1-msc3</td></tr>
<tr><td>29:nss1-msc4</td><td>30:nss1-msc5</td><td>31:nss1-msc6</td><td>32:nss1-msc7</td></tr>
<tr><td>33:nss1-msc8</td><td>34:nss1-msc9</td><td>35:nss2-msc0</td><td>36:nss2-msc1</td></tr>
<tr><td>37:nss2-msc2</td><td>38:nss2-msc3</td><td>39:nss2-msc4</td><td>40:nss2-msc5</td></tr>
<tr><td>41:nss2-msc6</td><td>42:nss2-msc7</td><td>43:nss2-msc8</td><td>44:nss2-msc9</td></tr>
</table></td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# dot1x</td><td></td><td>Enable 802.1x Authentication for the WLAN with a RADIUS server.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# dot1x radius-server-ip [A.B.C.D]</td><td>[A.B.C.D]</td><td>Specify the IP address of the RADIUS server in the text box.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# dot1x radius-server-password [password]</td><td>[password]</td><td>Specify the password which the RADIUS server will verify, up to 30 characters.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# dot1x radius-server-port [1812-65535]</td><td>[1812-65535]</td><td>Specify the port number for the RADIUS server. The default value is 1812.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# operation-mode [nat|bridge]</td><td>[nat|bridge]</td><td>Specify the operation mode for the service set, either NAT or Bridge mode.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# restrict rx [0-1000]</td><td>[0-1000]</td><td>Specify the limit in Mbps for data reception.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# restrict tx [0-1000]</td><td>[0-1000]</td><td>Specify the limit in Mbps for data transmission.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# security encryption action [disable|wep|wpa-mixed|wpa2]</td><td>[disable|wep|wpa-mixed|wpa2]</td><td>Specify the encryption method.
WEP stands for “Wired Equivalent Privacy”. It is a basic encryption method based on IEEE 802.11 standard.
<i><u>WPA</u></i> stands for “Wi-Fi Protected Access”. It is a kind of encryption which improves the security of WEP. It adopts two security-enhanced types to encrypt data — <i><u>TKIP</u></i> (Temporal Key Integrity Protocol) and <i><u>AES</u></i> (Advanced Encryption Standard). <i><u>AES</u></i> is a stronger encryption method than <i><u>TKIP</u></i>. <i><u>WPA2</u></i> is based on 802.11i. And it provides a stronger wireless security than <i><u>WPA</u></i>.
<i><u>WPA Mixed</u></i> is the security mode which permits the coexistence of WPA and WPA2 clients on a WLAN. When the wireless security is set in this</td></tr>
</table>

		mode, the wireless client device can connect to the Residential Gateway with WPA/TKIP or WPA2/AES. Some older wireless client devices only support WPA/TKIP. So you have to select the mixed mode to open the WiFi service to this device.
Gateway(config-wlan1-ssid-No.)# security encryption wep authentication [open-system|shared-key|auto]	[open-system|shared-key|auto]	The three available authentication options are *Open System*, *Shared Key* and *Auto*. If you select *Open System*, anyone can request authorization and sends an ID to the Residential Gateway. If the Residential Gateway recognizes the ID, wireless client can connect to the Residential Gateway. *Shared Key* requires wireless clients to have the same key positions as the Residential Gateway.
Gateway(config-wlan1-ssid-No.)# security encryption wep key [key]	[key]	Specify the alphanumeric password for the WLAN.
Gateway(config-wlan1-ssid-No.)# security encryption wep key format [ascii|hex]	[ascii|hex]	Select **ASCII (5 characters)** or **HEX (10 characters)** the format of the key.
Gateway(config-wlan1-ssid-No.)# security encryption wep key [64|128]	[64|128]	Select **64 bits** or **128 bits** from the pull-down menu. The wireless client devices must have the same WEP encryption length as the Residential Gateway.
Gateway(config-wlan1-ssid-No.)# security encryption wpa-mixed authentication-mode [radius|shared-key]	[radius|shared-key]	Select *Enterprise (RADIUS) or Personal (Shared Key)* as the authentication mode.
Gateway(config-wlan1-ssid-No.)# security encryption wpa-mixed key [key]	[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 used.
Gateway(config-wlan1-ssid-No.)# security encryption wpa-mixed key format [passphrase|hex]	[passphrase|hex]	Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* (“A-F”, “a-f” and “0-9”).
Gateway(config-wlan1-ssid-No.)# security encryption wpa2 authentication-mode [radius|shared-key]	[radius|shared-key]	Select *Enterprise (RADIUS) or Personal (Shared Key)* as the authentication mode.
Gateway(config-wlan1-ssid-No.)# security encryption wpa2 key [key]	[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 used.
Gateway(config-wlan1-ssid-No.)# security encryption wpa2 key format [passphrase|hex]	[passphrase|hex]	Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* (“A-F”, “a-f” and “0-9”).
Gateway(config-wlan1-ssid-No.)# security mac-filter action [allow | deny |	[allow | deny | disable]	Select *Disable* to deactivate the MAC access filter feature. Select *Allow* to open the WiFi service of the

disable]		Residential Gateway only to the wireless clients in the list. Select *Deny* to open the WiFi service of the Residential Gateway to any wireless clients except those in the list.
Gateway(config-wlan1-ssid-No.)# rule [1-20]	[1-20]	Choose a rule entry you want to configure.
Gateway(config-wlan1-ssid-No.-mac-filter-rule-No.)# description [description]	[description]	Specify description for the rule, up to 20 characters.
Gateway(config-wlan1-ssid-No.-mac-filter-rule-No.)# mac-address [aa:bb:cc:dd:ee:ff]	[aa:bb:cc:dd:ee:ff]	Specify MAC filter address.
Gateway(config-wlan1-ssid-No.)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify access VLAN ID for the SSID.
Gateway(config-wlan1-ssid-No.)# wmm		Enable Wireless Multimedia function. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.
No Command		
Gateway(config-wlan1-ssid-No.)# no active		Disable the WiFi service set.
Gateway(config-wlan1-ssid-No.)# no band		Reset wireless operation band to default.
Gateway(config-wlan1-ssid-No.)# no broadcast		Have the SSID hidden in public.
Gateway(config-wlan1-ssid-No.)# no datarate		Return datarate value to default.
Gateway(config-wlan1-ssid-No.)# no dot1x		Disable 802.1x Authentication for the WLAN with a RADIUS server.
Gateway(config-wlan1-ssid-No.)# no name		Return SSID to default value.
Gateway(config-wlan1-ssid-No.)# no operation-mode		Return operation mode to default.
Gateway(config-wlan1-ssid-No.)# no security encryption		Disable configured wireless encryption.
Gateway(config-wlan1-ssid-No.)# no vlan dot1q-vlan access-vlan		Return access VLAN ID for the SSID to default value.
Gateway(config-wlan1-ssid-No.)# no wmm		Disable Wireless Multimedia function.
Gateway(config-wlan1-ssid-No.)# no security mac-filter action		Disable to deactivate the MAC access filter feature.
Gateway(config-wlan1-ssid-No.)# no security mac-filter rule [1-20]	[1-20]	Clear information of the specific rule number.
Gateway(config-wlan1-ssid-No.-mac-filter-rule-No.)# no	[description]	Clear description.

description		
Gateway(config-wlan1-ssid-No.-mac-filter-rule-No.)# no mac-address	[aa:bb:cc:dd:ee:ff]	Clear MAC filter address.
Show Command		
Gateway(config-wlan1-ssid-No.)# show		Shows the current status of the SSID.
Gateway(config-wlan1-ssid-No.-mac-filter-rule-No.)# show		Display the SSID's current status of MAC filter configuration.

For Bandwidth 2.4G:

<table>
<tr><th>Command</th><th>Parameter</th><th>Description</th></tr>
<tr><td>Gateway(config)# interface wlan2</td><td></td><td>Access WiFi bandwidth 2.4G settings.</td></tr>
<tr><td>Gateway(config)# interface wlan2ssid [1-4]</td><td>[1-4]</td><td>Specify the SSID you want to configure.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# active</td><td></td><td>Enable the WiFi service set.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# [b|g|n|bg|gn|bgn]</td><td>[b|g|n|bg|gn|bgn]</td><td>Select one of the following modes for your wireless network.

<table>
<tr><th>Network Mode</th><th>Description</th></tr>
<tr><td>2.4 GHz (B)</td><td>In this mode, the Residential Gateway will only support 802.11b standard.</td></tr>
<tr><td>2.4 GHz (G)</td><td>In this mode, the Residential Gateway will only support 802.11g standard.</td></tr>
<tr><td>2.4 GHz (N)</td><td>In this mode, the Residential Gateway will only support 802.11n standard.</td></tr>
<tr><td>2.4 GHz (B+G)</td><td>In this mode, the Residential Gateway will support both 802.11b and 802.11g standards.</td></tr>
<tr><td>2.4 GHz (G+N)</td><td>In this mode, the Residential Gateway will support both 802.11g and 802.11n standards.</td></tr>
<tr><td>2.4 GHz (B+G+N)</td><td>In this mode, the Residential Gateway will support 802.11b, 802.11g and 802.11n standards.</td></tr>
</table></td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# broadcast</td><td></td><td>Have the SSID disclose in public.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# datarate [auto|1-44]</td><td>[auto|1-44]</td><td>Specify the number corresponding its data rate respectively as below:
<table>
<tr><td>1:6m</td><td>2:9m</td><td>3:12m</td><td>4:18m</td></tr>
<tr><td>5:24m</td><td>6:36m</td><td>7:48m</td><td>8:54m</td></tr>
<tr><td>9:msc0</td><td>10:msc1</td><td>11:msc2</td><td>12:msc3</td></tr>
<tr><td>13:msc4</td><td>14:msc5</td><td>15:msc6</td><td>16:msc7</td></tr>
<tr><td>17:msc8</td><td>18:msc9</td><td>19:msc10</td><td>20:msc11</td></tr>
<tr><td>21:msc12</td><td>22:msc13</td><td>23:msc14</td><td>24:msc15</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><td>25:nss1-msc0</td><td>26:nss1-msc1</td><td>27:nss1-msc2</td><td>28:nss1-msc3</td></tr>
<tr><td>29:nss1-msc4</td><td>30:nss1-msc5</td><td>31:nss1-msc6</td><td>32:nss1-msc7</td></tr>
<tr><td>33:nss1-msc8</td><td>34:nss1-msc9</td><td>35:nss2-msc0</td><td>36:nss2-msc1</td></tr>
<tr><td>37:nss2-msc2</td><td>38:nss2-msc3</td><td>39:nss2-msc4</td><td>40:nss2-msc5</td></tr>
<tr><td>41:nss2-msc6</td><td>42:nss2-msc7</td><td>43:nss2-msc8</td><td>44:nss2-msc9</td></tr>
</table></td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# dot1x</td><td></td><td>Enable 802.1x Authentication for the WLAN with a RADIUS server.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# dot1x radius-server-ip [A.B.C.D]</td><td>[A.B.C.D]</td><td>Specify the IP address of the RADIUS server in the text box.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# dot1x radius-server-password [password]</td><td>[password]</td><td>Specify the password which the RADIUS server will verify, up to 30 characters.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# dot1x radius-server-port [1812-65535]</td><td>[1812-65535]</td><td>Specify the port number for the RADIUS server. The default value is 1812.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# operation-mode [nat|bridge]</td><td>[nat|bridge]</td><td>Specify the operation mode for the service set, either NAT or Bridge mode.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# restrict rx [0-1000]</td><td>[0-1000]</td><td>Specify the limit in Mbps for data reception.</td></tr>
<tr><td>Gateway(config-wlan1-ssid-No.)# restrict tx [0-1000]</td><td>[0-1000]</td><td>Specify the limit in Mbps for data transmission.</td></tr>
<tr><td>Gateway(config-wlan2-ssid-No.)# security encryption action [disable|wep|wpa-mixed|wpa2]</td><td>[disable|wep|wpa-mixed|wpa2]</td><td>Specify the encryption method.

WEP stands for “Wired Equivalent Privacy”. It is a basic encryption method based on IEEE 802.11 standard.

<i>WPA</i> stands for “Wi-Fi Protected Access”. It is a kind of encryption which improves the security of WEP. It adopts two security-enhanced types to encrypt data － <i>TKIP</i> (Temporal Key Integrity Protocol) and <i>AES</i> (Advanced Encryption Standard). <i>AES</i> is a stronger encryption method than <i>TKIP</i>. <i>WPA2</i> is based on 802.11i. And it provides a stronger wireless security than <i>WPA</i>.

<i>WPA Mixed</i> is the security mode which permits the coexistence of WPA and WPA2 clients on a WLAN. When the wireless security is set in this mode, the wireless client device can connect to the Residential Gateway with WPA/TKIP or WPA2/AES. Some older wireless client devices</td></tr>
</table>

		only support WPA/TKIP. So you have to select the mixed mode to open the WiFi service to this device.
Gateway(config-wlan2-ssid-No.)# security encryption wep authentication [open-system|shared-key|auto]	[open-system|shared-key|auto]	The three available authentication options are *Open System*, *Shared Key* and *Auto*. If you select *Open System*, anyone can request authorization and sends an ID to the Residential Gateway. If the Residential Gateway recognizes the ID, wireless client can connect to the Residential Gateway. *Shared Key* requires wireless clients to have the same key positions as the Residential Gateway.
Gateway(config-wlan2-ssid-No.)# security encryption wep key [key]	[key]	Specify the password for the WLAN.
Gateway(config-wlan2-ssid-No.)# security encryption wep key format [ascii|hex]	[ascii|hex]	Select **ASCII (5 characters)** or **HEX (10 characters)** the format of the key.
Gateway(config-wlan2-ssid-No.)# security encryption wep key [64|128]	[64|128]	Select **64 bits** or **128 bits** from the pull-down menu. The wireless client devices must have the same WEP encryption length as the Residential Gateway.
Gateway(config-wlan2-ssid-No.)# security encryption wpa-mixed authentication-mode [radius|shared-key]	[radius|shared-key]	Select *Enterprise (RADIUS) or Personal (Shared Key)* as the authentication mode.
Gateway(config-wlan2-ssid-No.)# security encryption wpa-mixed key [key]	[key]	Specify the pre-shared 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 used.
Gateway(config-wlan2-ssid-No.)# security encryption wpa-mixed key format [passphrase|hex]	[passphrase|hex]	Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* (“A-F”, “a-f” and “0-9”).
Gateway(config-wlan2-ssid-No.)# security encryption wpa2 authentication-mode [radius|shared-key]	[radius|shared-key]	Select *Enterprise (RADIUS) or Personal (Shared Key)* as the authentication mode.
Gateway(config-wlan2-ssid-No.)# security encryption wpa2 key [key]	[key]	Specify the pre-shared 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 used.
Gateway(config-wlan2-ssid-No.)# security mac-filter action [allow | deny | disable]	[allow | deny | disable]	Select *Disable* to deactivate the MAC access filter feature. Select *Allow* to open the WiFi service of the Residential Gateway only to the wireless clients in the list. Select *Deny* to open the WiFi service of the Residential Gateway to any wireless clients except those in the list.
Gateway(config-wlan2-ssid-No.)# rule [1-20]	[1-20]	Choose a rule entry you want to configure.

Gateway(config-wlan2-ssid-No.-mac-filter-rule-No.)# description [description]	[description]	Specify description for the rule, up to 20 characters.
Gateway(config-wlan2-ssid-No.-mac-filter-rule-No.)# mac-address [aa:bb:cc:dd:ee:ff]	[aa:bb:cc:dd:ee:ff]	Specify MAC filter address.
Gateway(config-wlan2-ssid-No.)# security encryption wpa2 key format [passphrase|hex]	[passphrase|hex]	Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* ("A-F", "a-f" and "0-9").
Gateway(config-wlan2-ssid-No.)# vlan dot1q-vlan access-vlan [1-4094]	[1-4094]	Specify access VLAN ID for the SSID.
Gateway(config-wlan2-ssid-No.)# wmm		Enable Wireless Multimedia function. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.
No Command		
Gateway(config-wlan2-ssid-No.)# no active		Disable the WiFi service set.
Gateway(config-wlan2-ssid-No.)# no band		Reset wireless operation band to default.
Gateway(config-wlan2-ssid-No.)# no broadcast		Have the SSID hidden in public.
Gateway(config-wlan2-ssid-No.)# no datarate		Return datarate value to default.
Gateway(config-wlan2-ssid-No.)# no dot1x		Disable 802.1x Authentication for the WLAN with a RADIUS server.
Gateway(config-wlan2-ssid-No.)# no name		Return SSID to default value.
Gateway(config-wlan2-ssid-No.)# no operation-mode		Return operation mode to default.
Gateway(config-wlan2-ssid-No.)# no security encryption		Disable configured wireless encryption.
Gateway(config-wlan2-ssid-No.)# no vlan dot1q-vlan access-vlan		Return access VLAN ID for the SSID to default value.
Gateway(config-wlan2-ssid-No.)# no wmm		Disable Wireless Multimedia function.
Gateway(config-wlan2-ssid-No.)# no security mac-filter action		Disable to deactivate the MAC access filter feature.
Gateway(config-wlan2-ssid-No.)# no security mac-filter rule [1-20]	[1-20]	Clear information of the specific rule number.
Gateway(config-wlan2-ssid-No.-mac-filter-rule-No.)# no description	[description]	Clear description.
Gateway(config-wlan2-ssid-No.-mac-filter-rule-No.)# no	[aa:bb:cc:dd:ee:ff]	Clear MAC filter address.

mac-address		
Show Command		
Gateway(config-wlan2-ssid-No.)# show		Shows the current status of the SSID.
Gateway(config-wlan2-ssid-No.-mac-filter-rule-No.)# show		Display the SSID's current status of MAC filter configuration.

2.5.6 IP Command

1. **Set up DDNS service.**

DDNS stands for "Dynamic Domain Name Service". It allows a host to bind with a permanent domain name so the host can be found on the internet with this domain name. With DDNS, the network administrator can access the Residential Gateway with a permanent domain name even if it is often assigned different IP addresses by DHCP. And users on the Internet can access the server (such as the web service) on the private network by the domain name of the Residential Gateway. They do not have to access the server by an IP address which is usually not as easy to remember as a domain name.

IP command	Parameter	Description
Gateway(config)# ip ddns		Enable the DDNS service.
Gateway(config)# ip ddns [dyndns|noip.org]	[dyndns|noip.org]	Select a registration server to which you already registered a domain name.
Gateway(config)# ip ddns host-name		Enter the DDNS URL assigned by the DDNS server.
Gateway(config)# ip ddns password		Enter the password provided by the DDNS server.
Gateway(config)# ip ddns username		Specify the username provided by the DDNS server.
No command		
Gateway(config)# no ip ddns		Return DDNS to be disabled.
Gateway(config)# no ip ddns host-name		Clear the host name.
Gateway(config)# no ip ddns password		Clear the password.
Gateway(config)# no ip ddns username		Clear the username.
Show command		
Gateway(config)#show ip ddns		Show the current DDNS configurations or verify the DDNS settings.

2. **Set up an IP address of the Gateway or configure the Gateway to get an IP address automatically from DHCP server.**

IP command	Parameter	Description
Gateway(config)# ip lan-ip [A.B.C.D] [255.X.X.X]	[A.B.C.D]	Enter the desired IP address for your Gateway.
	[255.X.X.X]	Enter subnet mask of your IP address.
Gateway(config)# ip dhcp server		Enable DHCP mode.

No command	
Gateway(config)#no lan-ip address	Remove the Gateway’s IP address.
Gateway(config)# no ip dhcp server	Disable DHCP mode.
Show command	
Gateway(config)#show ip address	Show the current IP configurations or verify the configured IP settings.
IP command example	
Gateway(config)# ip lan-ip address 192.168.1.198 255.255.255.0	Set up the Gateway’s IP to 192.168.1.198, subnet mask to 255.255.255.0
Gateway(config)# ip dhcp server	Get an IP address automatically.

3. Configure DHCP advanced function

IP command	Parameter	Description
Gateway(config)# ip dhcp server domain-name [domain-name]	[domain-name]	Specify the domain name of the Residential Gateway up to 30 characters.
Gateway(config)# ip dhcp server ip-lease-time [1-14400]	[1-14400]	Specify the lease time in minute. This is a time period in which the DHCP clients can keep their IP addresses since the last time in which they receive the DHCP acknowledgement packet from the Residential Gateway.
Gateway(config)# ip dhcp server start-ip [A.B.C.D] [pools]	[A.B.C.D]	Specify an IP address from which the Residential Gateway will start to assign the IP addresses to the DHCP clients on the private network.
	[pools]	Specify the maximum number of IP addresses which the Residential Gateway can assign to the DHCP clients.
Gateway(config)# ip dhcp server ip-mac-binding address-reservation apply		Apply all the configuration of DHCP reservation made.
Gateway(config)# ip dhcp server ip-mac-binding address-reservation [1-20]	[1-20]	Specify the entry number of DHCP reservation.
Gateway(config-address-reservation-No.)# description [description]	[description]	This is a brief description for this entry.
Gateway(config-address-reservation-No.)# ip-address [A.B.C.D]	[A.B.C.D]	This is an IP address which you want to reserve for a specific DHCP client.
Gateway(config-address-reservation-No.)# ip-address [aa:bb:cc:dd:ee:ff]	[aa:bb:cc:dd:ee:ff]	This is the MAC address of the DHCP client which you want to bundle with the IP address in ***IP*** field.
No command		
Gateway(config)# no ip dhcp server domain-name [domain-name]		Remove DHCP domain name.
Gateway(config)# no ip dhcp server ip-lease-time		Return the lease time to default value.

Gateway(config)# ip dhcp server start-ip	Return the initial IP and maximum number of IP addresses to default value.
Gateway(config-address-reservation-No.)# no description	Clear the description for the DHCP reservation
Gateway(config-address-reservation-No.)# no ip-address	Clear the binding client IP address.
Gateway(config-address-reservation-No.)# no mac-address	Clear the binding client MAC address.
Show command	
Gateway(config)#show ip dhcp server	Show the current IP configurations or verify the configured IP settings.
Gateway(config-address-reservation-No.)# show	Show the reservation table of the entry.

4. Configure IGMP function

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

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

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

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

Command	Parameter	Description
Gateway(config)# ip igmp snooping		When enabled, the Gateway will monitor network traffic and determine which hosts to receive multicast traffic.
Gateway(config)# ip igmp snooping immediate-leave		Enable immediate leave function.
No command		
Gateway(config)# no ip igmp snooping		Disable IGMP/MLD Snooping function.
Gateway(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Show command		
Gateway(config)#show ip igmp snooping		Show current IGMP/MLD snooping status including immediate leave function.

Gateway(config)#show ip igmp snooping groups		Show IGMP/MLD group table.
Gateway(config)#show ip igmp snooping status		Show IGMP/MLD Snooping status.

5. Configure Routing

Command	Parameter	Description
Gateway(config)# ip route static		Enable static route function. A static route is a pre-determined pathway that packets can travel to reach a specific destination network.
Gateway(config)# ip route static [1-20]	[1-20]	Specify the index number of static route.
Gateway(config-static-route-no.)# active		Enable the static route specified.
Gateway(config-static-route-no.)# address [A.B.C.D] [255.x.x.x] [A.B.C.D]	[A.B.C.D]	Specify the destination IP address of the static route
	[255.x.x.x]	Specify the subnet mask of the destination network of the static route.
	[A.B.C.D]	Specify the IP address of a gateway through which this static route will send the packets to the destination network.
Gateway(config-static-route-no.)# address [wan | lan]	[wan | lan]	Specify an interface of the Residential Gateway from which the static route will forward the packets to the destination network.
Gateway(config-static-route-no.)# metric [1-15]	[1-15]	Specify metric value. Metric is the cost of a route to a destination network.
No command		
Gateway(config)# no ip igmp snooping		Disable IGMP/MLD Snooping function.
Gateway(config)# no ip igmp snooping immediate-leave		Disable immediate leave function.
Show command		
Gateway(config)#show ip igmp snooping		Show current IGMP/MLD snooping status including immediate leave function.

6. Configure WAN Interface

Command	Parameter	Description
Gateway(config)# ip wan-interface apply		Apply all WAN interface configuration and all VLAN configuration.
Gateway(config)# ip wan-interface data [1]	[1]	Specify the number of WAN data interface. The data interface is the default WAN Interface of the Residential Gateway. It is open to remote management from the IP specified using management command when the management interface is not created on the Residential Gateway.
Gateway(config-data-1)# active		Enable the WAN interface entry specified.

Gateway(config-data-1)# connection-type [dhcp | static-ip]	[dhcp | static-ip]	Specify the way of IP distribution, either DHCP or static IP mode.
Gateway(config-data-1)# dhcp mtu [68-1500]	[68-1500]	Specify the DHCP MTU for optimal performance.
Gateway(config-data-1)# dns		Enable DNS automatically.
Gateway(config-data-1)# dns server-1 [A.B.C.D]	[A.B.C.D]	If you choose to set the DNS manually, please specify the IP address of the primary DNS server of this interface. (This parameter is only available for the data interface.)
Gateway(config-data-1)# dns server-2 [A.B.C.D]	[A.B.C.D]	If you choose to set the DNS manually, please specify the IP address of the primary DNS server of this interface. (This parameter is only available for the data interface.)
Gateway(config-data-1)# dns server-3 [A.B.C.D]	[A.B.C.D]	If you choose to set the DNS manually, please specify the IP address of the primary DNS server of this interface. (This parameter is only available for the data interface.)
Gateway(config-data-1)# ping-access		Allow the WAN interface to reply the ICMP echo requests which it receives from the public network.
Gateway(config-data-1)# static-ip [A.B.C.D]	[A.B.C.D]	Specify an IP address to assign the interface an IP address.
Gateway(config-data-1)# static-ip mtu [68-1500]	[68-1500]	Specify the maximal size of Ethernet packets which the Residential Gateway will transmit. MTU stands for “Maximum Transmission Unit.”
Gateway(config-data-1)# vlan-id [1-4094]	[1-4094]	Specify a VLAN ID for the WAN interface. And the WAN interface will add this VLAN ID to the egress untagged packets. (This parameter is only available when the WAN information is Data, Management)
Gateway(config)# ip wan-interface management [1]	[1]	Specify the number of WAN management interface. The Management Interface enables the network administrator to remotely log in the Residential Gateway via the Management Interface’s IP address if the source IP address is allowed using management command. And if the Management Interface is not created on the Residential Gateway, the network administrator can remotely log in the Residential Gateway via the data Interface’s IP address. The difference between the two scenarios is illustrated in the following diagram.
Gateway(config-management-1)# active		Enable the WAN interface entry specified.
Gateway(config- management -1)# connection-type [dhcp |	[dhcp | static-ip]	Specify the way of IP distribution, either DHCP or static IP mode.

static-ip]		
Gateway(config- management -1)# dhcp mtu [68-1500]	[68-1500]	Specify the DHCP MTU for optimal performance.
Gateway(config- management -1)# ping-access		Allow the WAN interface to reply the ICMP echo requests which it receives from the public network.
Gateway(config- management -1)# static-ip [A.B.C.D] [255.x.x.x] [A.B.C.D]	[A.B.C.D]	Specify an IP address to assign the interface an IP address.
	[255.x.x.x]	Specify a subnet mask for this interface.
	[A.B.C.D]	Specify the IP address of a gateway or a router which can deliver the packets which leave the Residential Gateway from this interface to the other network.
Gateway(config- management -1)# static-ip mtu [68-1500]	[68-1500]	Specify the maximal size of Ethernet packets which the Residential Gateway will transmit. MTU stands for “Maximum Transmission Unit.”
Gateway(config- management -1)# vlan-id [1-4094]	[1-4094]	Specify a VLAN ID for the WAN interface. And the WAN interface will add this VLAN ID to the egress untagged packets. (This parameter is only available when the WAN information is Data, Management)
No command		
Gateway(config-data/management-1)# no active		Disable the WAN interface entry specified.
Gateway(config-data/management -1)# no connection-type		Return connection type to default setting
Gateway(config-data/management -1)# no dhcp		Return DHCP connection to default setting
Gateway(config-data-1)# no dns		Return DNS server to default setting.
Gateway(config-data/management -1)# no ping-access		Disable Ping access function.
Gateway(config-data/management -1)# no static-ip		Return Static IP connection to default setting
Gateway(config-data/management -1)# no vlan-id		Return VLAN ID to default setting.
Show command		
Gateway(config-data/management -1)# show		Show current WAN DATA interface status.

2.5.7 Management Command

Command	Parameter	Description
Gateway(config)# management access-		Permit the computers to manage the Residential Gateway from its LAN ports.

control lan		
Gateway(config)# management access-control lan telnet		Gain the Telnet management access on LAN port.
Gateway(config)# management access-control lan web		Gain the Web management access on LAN port.
Gateway(config)# management access-control lan snmp		Gain the SNMP management access on LAN port.
Gateway(config)# management access-control source-binding [A.B.C.D] [1-254]	[A.B.C.D] [1-254]	Specify a range of IP addresses to enable these IP addresses to manage the Residential Gateway from the WAN port
Gateway(config)# management access-control source-binding any		The Residential Gateway can be managed from its WAN port by any remote IP address.
Gateway(config)# management access-control wan		Permit the computers to manage the Residential Gateway from its WAN ports.
Gateway(config)# management access-control wan snmp		Gain the SNMP management access on WAN port.
Gateway(config)# management access-control wan telnet		Gain the Telnet management access on WAN port.
Gateway(config)# management access-control wan web		Gain the Web management access on WAN port.
Gateway(config)# management dhcp-autoprovision		Enable DHCP auto-provision function.
Gateway(config)# management web http-port [HTTP_Port]	[HTTP_Port]	Specify the Internet socket port number used by protocols of the transport layer of the Internet Protocol Suite for the establishment of host-to-host connectivity. The default value is 80.
Gateway(config)# management cwmp-agent		Enable CPE WAN Management Protocol function.
Gateway(config)# management cwmp-agent apply		Submit your settings after you finish configuring CWMP.
Gateway(config)# management cwmp-agent connection-request password [password]	[password]	Specify the password for Connection Request Server.
Gateway(config)# management cwmp-agent connection-request username [username]	[username]	Specify the username for Connection Request Server.

Gateway(config)# management cwmp-agent management-server password [password]	[password]	Specify the password for Auto Configuration Server.
Gateway(config)# management cwmp-agent management-server username [username]	[username]	Specify the username for Auto Configuration Server.
Gateway(config)# management cwmp-agent management-server url [url]	[url]	Specify HTTP address of the Auto Configuration Server.
Gateway(config)# management cwmp-agent parameter-change notify		Enable or disable Periodic Information function. It defines the time interval that a piece of information will be sent after a communication session is done. ***Note:*** If a communication session has been incomplete for long time, the time interval will start counting at the beginning of communication session.
Gateway(config)# management cwmp-agent parameter-change notify interval [1-86400]		Specify the time in second after which a piece of information will be sent again. The default value is 60.
No command		
Gateway(config)# no management access-control lan		Deny the computers to manage the Residential Gateway from its LAN ports.
Gateway(config)# no management access-control lan snmp		Deny the SNMP management access on LAN port.
Gateway(config)# no management access-control lan telnet		Deny the Telnet management access on LAN port.
Gateway(config)# no management access-control lan web		Deny the Web management access on LAN port.
Gateway(config)# no management access-control source-binding		Clear configured IP address.
Gateway(config)# no management access-control wan		Deny the computers to manage the Residential Gateway from its WAN ports.
Gateway(config)# no management access-control wan snmp		Deny the SNMP management access on WAN port.
Gateway(config)# no management access-control wan telnet		Deny the Telnet management access on WAN port.

Gateway(config)# no management access-control wan web		Deny the Web management access on WAN port.
Gateway(config)# no management access-control web http-port		Return HTTP Port to default value.
Gateway(config)# no management cwmp-agent		Disable CPE WAN Management Protocol function.
Gateway(config)# no management cwmp-agent connection-request password		Clear the password for Connection Request Server.
Gateway(config)# no management cwmp-agent connection-request username		Clear the username for Connection Request Server.
Gateway(config)# no management cwmp-agent management-server password		Clear the password for Auto Configuration Server.
Gateway(config)# no management cwmp-agent management-server username		Clear the username for Auto Configuration Server.
Gateway(config)# no management cwmp-agent management-server url		Clear HTTP address of the Auto Configuration Server.
Gateway(config)# no management cwmp-agent parameter-change notify		Disable or disable Periodic Information function.
Gateway(config)# no management cwmp-agent parameter-change notify interval		Return the time interval to default value.
Show Command		
Gateway(config)# Show management access-control		Show the current status of management access.
Gateway(config)# Show management cwmp-agent		Show the current status of CWMP.

2.5.8 NTP Command

Command	Parameter	Description
Gateway(config)# ntp		Enable the Gateway to synchronize the clock with a time server.
Gateway(config)# ntp daylight-saving [recurring | date]	[recurring | date]	Enable daylight saving with recurring mode. Recurring is to use calendar algorithm to define daylight saving time.

		Date is to use annual date to define daylight saving time.
Gateway(config)# ntp offset [Mm,w,d,hh:mm-Mm,w,d,hh:mm]	[Mm,w,d,hh:mm-Mm,w,d,hh:mm]	Offset setting for daylight saving function of recurring mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) Hh=0-23, mm=0-59, Days=1-365**
Gateway(config)# ntp offset [Days,hh:mm-Days,hh:mm]	[Days,hh:mm-Days,hh:mm]	Offset setting for daylight saving function of date mode. **Mm=1-12, w=1-5, d=0-6(0=Sun, 6=Sat) Hh=0-23, mm=0-59, Days=1-365**
Gateway(config)# ntp server ip		Get the access to NTP server using IP address.
Gateway(config)# ntp server ip [A.B.C.D]	[A.B.C.D]	Specify the primary time server IP address.
Gateway(config)# ntp server option		Get the access to NTP server using domain name.
Gateway(config)# ntp server option [1-5]	[1-5]	Specify a NTP server for the Residential Gateway to update its internal clock from an NTP server. If there is no particular NTP server which you prefer, you can select the given one of the default NTP servers. Or if you prefer a NTP server which is not available in, specify the IP address of the NTP server. Here is the list of default domain name: **1=time.Windows.com** **2=time.nist.gov** **3=time-nw.nist.gov** **4=time-a.nist.gov** **5=time-b.nist.gov**
Gateway(config)# ntp syn-interval [1-8]	[1-8]	Specify the interval time to synchronize from NTP time server. **1=1hour, 2=2hours, 3=3hours, 4=4hours** **5=6hours, 6=8hours, 7=12hours, 8=24hours**
Gateway(config)# ntp time-zone [0-135]	[0-135]	Specify the time zone to which the Gateway belongs. Use space and a question mark to view the complete code list of 147 time zones. For example, “Gateway(config)# ntp time-zone ?”
No command		
Gateway(config)# no ntp		Disable the Gateway to synchronize the clock with a time server.
Gateway(config)# no ntp daylight-saving		Disable the daylight saving function.
Gateway(config)# no ntp offset		Set the offset value back to the default setting.

Gateway(config)# no ntp server	Delete the time server IP address.
Gateway(config)# no ntp syn-interval	Set the synchronization interval back to the default setting.
Gateway(config)# no ntp time-zone	Set the time-zone setting back to the default.
Show command	
Gateway(config)# show ntp	Show or verify current time server settings.
NTP command example	
Gateway(config)# ntp	Enable the Gateway to synchronize the clock with a time server.
Gateway(config)# ntp daylight-saving date	Enable the daylight saving function at ddate mode
Gateway(config)# ntp offset [100,12:00-101,12:00]	Daylight saving time date start from the 100th day of the year to the 101th day of the year.
Gateway(config)# ntp server ip 192.180.0.12	Set the time server IP address to 192.180.0.12.
Gateway(config)# ntp syn-interval 4	Set the synchronization interval to 4 hours.
Gateway(config)# ntp time-zone 3	Set the time zone to GMT-8:00 Vancouver.

2.5.9 QoS

1. Set up Qos

QoS command	Parameter	Description
Gateway(config)# qos [802.1p | dscp | port-based]	[802.1p | dscp | port-based]	Specify QoS mode
Gateway(config)# qos 802.1p-map [0-7] [0-3]	[0-7]	Specify a 802.1p value.
	[0-3]	Specify a queue value.
Gateway(config)# qos dscp-map [0-63] [0-3]	[0-63]	Specify a DSCP value.
	[0-3]	Specify a queue value.
Gateway(config)# qos queuing-mode [weight]	[weight]	Specify QoS queuing mode as weight mode
Gateway(config)# qos queue-weighted [1:2:4:8]	[1:2:4:8]	Specify the queue weighted
No command		
Gateway(config)# no qos		Disable QoS function
Gateway(config)# no qos 802.1p-map		Undo 802.1p mapping
Gateway(config)# no qos dscp-map [0-63]	[0-63]	Undo specify a DSCP value
Gateway(config)# no queuing-mode		Specify QoS queuing mode as strict mode
Gateway(config)# no qos queue-weighted		Undo specify the queue weighted
Show command		

Gateway(config)# show qos		Show QoS configuration
Gateway(config)# show qos interface		Show QoS interface overall information

2. Use “interface” command to configure a group of ports’ QoS settings.

QoS & Interface command	Parameter	Description
Gateway(config)# interface [port_list]	[port_list]	Enter several discontinuous port numbers separated by commas or a range of ports with a hyphen. For example:1,3 or 2-4
Gateway(config-if-PORT-PORT)# qos default-class [0-3]	[0-3]	Assign the port a default queue.
Gateway(config-if-PORT-PORT)# qos rate-limit ingress [0 | 16-1048576] kbps	[0 | 16-1048576] kbps	Specify ingress rate limit value.
Gateway(config-if-PORT-PORT)# qos rate-limit egress [port | queue]	[port | queue]	Configure egress rate mode
Gateway(config-if-PORT-PORT)# qos user-priority [0-7]	[0-7]	Specify the default priority bit to the selected interfaces.
No command		
Gateway(config-if-PORT-PORT)# no qos default-class		Undo default queue on the port
Gateway(config-if-PORT-PORT)# no qos rate-limit ingress		Delete QoS ingress rate limit setting.
Gateway(config-if-PORT-PORT)# no qos rate-limit egress		Delete QoS egress rate limit setting.
Gateway(config-if-PORT-PORT)# no qos user-priority		Set the user priority value setting back to the factory default.

2.5.10 Security Command

1. General Settings

Command	Parameter	Description
Gateway(config)# security firewall		Enable Firewall function.
No Command		
Gateway(config)# no security firewall		Disable Firewall function.
Show Command		
Gateway(config)# show security firewall		Shows the current status of firewall.

2. Set up Packet Filter

Command	Parameter	Description
Gateway(config)# security packet-filter		Enable the packet filter function. When it is enabled, the Residential Gateway will

		drop packets which meet predetermined conditions of the rules in the following commands.
Gateway(config)# security packet-filter apply		Apply all the configured packet filter settings made.
Gateway(config)# security packet-filter application [1-10]	[1-10]	Specify the entry number of application packet filter. This allows you to edit the table of application filter rules. The Residential Gateway will drop packets when it receives packets which match the entries in the rule table.
Gateway(config-application-No.)# active		Enable the specified application filter rule.
Gateway(config-application-No.)# applications [1-11]	[1-11]	Specify an application whose packets will be denied by this filter rule. Where: **1:FTP 2:SSH 3:Telnet 4:SMTP** **5:DNS 6:HTTP 7:POP 8:NNTP** **9:IMAP 10:SNMP 11:HTTPS**
Gateway(config-application-No.)# source-ip-range [A.B.C.D] [1-254]	[A.B.C.D] [1-254]	Specify the source IP address range of the packets which will be denied by this rule.
Gateway(config)# security packet-filter lan [1-10]	[1-10]	Specify the entry number of lan packet filter. This allows you to edit the rule table for the LAN filter. The LAN filter will block packets which are received by the Residential Gateway from the private network and match the pre-determined condition of any entry in the rule table.
Gateway(config-lan-No.)# active		Enable this LAN rule.
Gateway(config-lan-No.)# destination ip [A.B.C.D]	[A.B.C.D]	Specify an IP address range for the LAN filter to block packets whose destination IP addresses are in this range.
Gateway(config-lan-No.)# destination port-number [1-65535]	[1-65535]	Specify the destination port number of the packets which the LAN Filter will block.
Gateway(config-lan-No.)# protocol [tcp | udp]	[tcp | udp]	Select *TCP* or *UDP* as the communication protocol of the packets which the LAN filter will block.
Gateway(config-lan-No.)# source-ip-range [A.B.C.D] [1-254]	[A.B.C.D] [1-254]	Specify an IP address range for the LAN filter to block packets whose source IP addresses are in this range.
Gateway(config)# security packet-filter mac [1-10]	[1-10]	Specify the entry number of MAC filter. This is allows you to edit the MAC filter rules. The Residential Gateway will drop packets which match the pre-determined condition of any entry in this table.
Gateway(config-mac-No.)# active		Enable this MAC rule.
Gateway(config-mac-No.)# destination ip [A.B.C.D]	[A.B.C.D]	Specify the destination IP address of the packets which will be denied by this rule.

Gateway(config-mac-No.)# destination port-number [1-65535]	[1-65535]	Specify the destination port number of the packet which will be denied by this rule.
Gateway(config-mac-No.)# mac-address [aa:bb:cc:dd:ee:ff]	[aa:bb:cc:dd:ee:ff]	Specify the MAC address of the packet which will be denied by this rule.
Gateway(config-mac-No.)# protocol [tcp | udp]	[tcp | udp]	Select *TCP* or *UDP* as the communication protocol of the packets which the MAC filter will block.
Gateway(config)# security packet-filter wan [1-10]	[1-10]	This allows you to edit the WAN filter rules. The WAN filter rule will block packets which are received by the Residential Gateway from the public network and match the pre-determined condition of the rule.
Gateway(config-wan-No.)# active		Enable this WAN rule.
Gateway(config-wan-No.)# destination ip [A.B.C.D]	[A.B.C.D]	Specify the destination IP address of the packets which will be denied by this rule.
Gateway(config-wan-No.)# destination port-number [1-65535]	[1-65535]	Specify the destination port number of the packet which will be denied by this rule.
Gateway(config-wan-No.)# protocol [tcp | udp]	[tcp | udp]	Select *TCP* or *UDP* as the communication protocol of the packets which the WAN filter will block.
Gateway(config-wan-No.)# source-ip-range [A.B.C.D] [1-254]	[A.B.C.D] [1-254]	Specify an IP address range for the WAN filter to block packets whose source IP addresses are in this range.
No Command		
Gateway(config)# no security packet-filter		Disable packet filter rule.
Gateway(config)# no security packet-filter application [1-10]	[1-10]	Delete the configured application rule.
Gateway(config)# no security packet-filter lan [1-10]	[1-10]	Delete the configured LAN rule.
Gateway(config)# no security packet-filter mac [1-10]	[1-10]	Delete the configured MAC rule.
Gateway(config)# no security packet-filter wan [1-10]	[1-10]	Delete the configured WAN rule.
Gateway(config-application-No.)# no active		Disable the configured application rule.
Gateway(config-application-No.)# no applications		Return application to FTP.
Gateway(config-application-No.)# no source-ip-range		Return IP address to default value 0.0.0.0

Gateway(config-lan-No.)# no active		Disable the configured LAN rule.
Gateway(config-lan-No.)# no destination ip		Return IP address to default value 0.0.0.0
Gateway(config-lan-No.)# no destination port-number		Return port number to default value 1
Gateway(config-lan-No.)# no protocol		Return protocol to default value TCP.
Gateway(config-lan-No.)# no source-ip-range		Return IP address to default value 0.0.0.0
Gateway(config-mac-No.)# no active		Disable the configured MAC rule.
Gateway(config-mac-No.)# no destination ip		Return IP address to default value 0.0.0.0
Gateway(config-mac-No.)# no destination port-number		Return port number to default value 1
Gateway(config-mac-No.)# no mac-address		Return MAC address to default value 00:00:00:00:00
Gateway(config-mac-No.)# no protocol		Return protocol to default value TCP.
Gateway(config-wan-No.)# no active		Disable the configured WAN rule.
Gateway(config-wan-No.)# no destination ip		Return IP address to default value 0.0.0.0
Gateway(config-wan-No.)# no destination port-number		Return port number to default value 1
Gateway(config-wan-No.)# no protocol		Return protocol to default value TCP.
Gateway(config-wan-No.)# no source-ip-range		Return IP address to default value 0.0.0.0
Show Command		
Gateway(config)# show security packet-filter		Shows all the security packet rule table, including Application, LAN, MAC and WAN table.
Gateway(config-application-No.)# show		Shows the specified application packet rule.
Gateway(config-lan-No.)# show		Shows the specified LAN packet rule.
Gateway(config-mac-No.)# show		Shows the specified MAC packet rule.
Gateway(config-wan-No.)# show		Shows the specified WAN packet rule.

3. Set up URL Filter

Command	Parameter	Description
Gateway(config)# security url-filter		Enable the URL filter function. URL Filter enables the network administrator to deny computers to access the specific websites on the Internet from the private network of

		the Residential Gateway.
Gateway(config)# security url-filter apply		Apply all the configured url filter settings made.
Gateway(config)# security url-filter [1-10]	[1-10]	Specify the entry number of URL filter.
Gateway(config-url-No.)# active		Enable the URL rule.
Gateway(config-url-No.)# url [URL/IP]	[URL/IP]	Specify the URL address which this rule will deny.
No Command		
Gateway(config)# no security url-filter		Disable URL function.
Gateway(config)# no security url-filter [1-10]	[1-10]	Delete the URL rule.
Gateway(config-url-No.)# no active		Disable the rule.
Gateway(config-url-No.)# no url		Clear the URL address.
Show Command		
Gateway(config)# show url-filter		Shows the current configuration of URL filter.

4. Set up VPN Passthrough

This feature enables the VPN traffic to be transmitted from the private network of the Residential Gateway to the public network. So the VPN client on the private network can establish a VPN tunnel to the remote VPN server.

Command	Parameter	Description
Gateway(config)# security vpn-passthrough ipsec		Enable IPSec passthrough on the Residential Gateway. IPSec stands for “Internet Protocol Security”. It is a suite of protocols for secure exchange of packets at the IP layer.
Gateway(config)# security vpn-passthrough l2tp		Enable the L2TP passthrough on the Residential Gateway. L2TP stands for “Layer 2 Tunneling Protocol”. It is used to enable Point-to-Point sessions via the Internet on the Layer 2 level.
Gateway(config)# security vpn-passthrough pptp		Enable PPTP passthrough on the Residential Gateway. PPTP stands for “Point-to-Point Tunneling Protocol”. And PPTP passthrough is a feature which allows the Point-to-Point Protocol to be tunneled through an IP network.
No Command		
Gateway(config)# no security vpn-passthrough ipsec		Disable IPSec passthrough function.

Gateway(config)# no security vpn-passthrough l2tp		Disable L2TP passthrough function.
Gateway(config)# no security vpn-passthrough pptp		Disable PPTP passthrough function.
Show Command		
Gateway(config)# security vpn-passthrough		Show the current status of VPN Passthrough.

5. Set up UPnP function

Command	Parameter	Description
Gateway(config)# security upnp		Enable UPnP function. Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically.
No Command		
Gateway(config)# no security upnp		Disable UPnP function.

6. Set up DDoS function

Command	Parameter	Description
Gateway(config)# security ddos		Activate DDoS prevention manually. And select the kinds of DDoS attacks to enable the Residential Gateway to detect them.
Gateway(config)# security ddos icmp-smurf		Enable ICMP smurf function to prevent the hacker to forge the IP address of the Residential Gateway and send repeated ping requests to it flooding the network.
Gateway(config)# security ddos ip-land		Enable IP land function to prevent an attack which involves a synchronized request being sent as part of the three way handshake of TCP to an open port specifying the port as both the source and destination effectively locking the port.
Gateway(config)# security ddos ip-spoof		Enable IP spoof function to prevent a hacker to create an alias IP address of the Residential Gateway to which all traffic is redirected.
Gateway(config)# security ddos ip-teardrop		Enable to prevent a Teardrop attack. A Teardrop attack sends mangled IP fragments with overlapping, over-sized, payloads to the Residential Gateway. The fragmented packets are processed by the

		Residential Gateway and will cause it to crash.
Gateway(config)# security ddos ping-of-death		Enable to prevent the Residential Gateway to receive oversized ping packets which it cannot handle. The Ping of Death attack will send packets which exceed the maximum IP packet size of 65,535 bytes.
Gateway(config)# security ddos per-source-ip fin		Enable to prevent a FIN attack on the LAN port IP address.
Gateway(config)# security ddos per-source-ip fin [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos per-source-ip icmp		Enable to prevent an ICMP attack on the LAN port IP address.
Gateway(config)# security ddos per-source-ip icmp [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos per-source-ip syn		Enable to prevent a SYN attack on a specified IP address.
Gateway(config)# security ddos per-source-ip syn [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos per-source-ip udp		Enable to prevent a UDP attack on the LAN port IP address.
Gateway(config)# security ddos per-source-ip udp [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos source-ip-blocking		Enable to block the IP.
Gateway(config)# security ddos source-ip-blocking [1-999]	[1-999]	Specify the time in second to block the IP.
Gateway(config)# security ddos tcp-scan		Enable to prevent the Residential Gateway to be probed by a hacker for open TCP ports to then block.
Gateway(config)# security ddos tcp-syn-with-data		Enable to prevent the hacker to send a volume of requests for connections that cannot be completed.
Gateway(config)# security ddos tcp-udp-portscan		Enable to prevent a series of systematic queries to the Residential Gateway for open ports through which to route traffic.
Gateway(config)# security ddos udp-bomb		Enable to prevent the hacker congesting the network by a flood of UDP packets between him and the Residential Gateway using the UDP chargen service.
Gateway(config)# security ddos udp-echo-chargen		Enable to prevent the hacker from sending a UDP packet to the echo server with a source port set to the chargen port.
Gateway(config)# security ddos whole-system-flood fin		Enable to prevent a FIN flood. This attack will flood the network with connection resets from an invalid IP address.

Gateway(config)# security ddos whole-system-flood fin [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos whole-system-flood icmp		Enable to prevent a flood of ICMP messages from an invalid IP address. This attack can cause all TCP requests to be halted.
Gateway(config)# security ddos whole-system-flood icmp [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos whole-system-flood syn		Enable to prevent a SYN attack. A SYN attack will interrupt the process of the three way handshake of TCP and redirect the acknowledge response to a malicious IP address. Or it will cause the targeted system to be flooded with false SYN requests.
Gateway(config)# security ddos whole-system-flood syn [1-999]	[1-999]	Specify the packets per second.
Gateway(config)# security ddos whole-system-flood udp		Enable to prevent a flood of large numbers of raw UDP packets targeted at the Residential Gateway.
Gateway(config)# security ddos whole-system-flood udp [1-999]	[1-999]	Specify the packets per second.
No Command		
Gateway(config)# no security ddos		Disable DDoS prevention
Gateway(config)# no security ddos icmp-smurf		Disable ICMP smurf
Gateway(config)# no security ddos ip-land		Disable IP land
Gateway(config)# no security ddos ip-spoof		Disable IP spoof
Gateway(config)# no security ddos ip-teardrop		Disable IP teardrop
Gateway(config)# no security ddos ping-of-death		Disable ping-of-death
Gateway(config)# no security ddos per-source-ip fin		Disable FIN attack prevention on the LAN port IP address
Gateway(config)# no security ddos per-source-ip icmp		Disable ICMP attack prevention on the LAN port IP address
Gateway(config)# no security ddos per-source-ip syn		Disable SYN attack prevention on the LAN port IP address
Gateway(config)# no security ddos per-source-ip udp		Disable UDP attack prevention on the LAN port IP address

Gateway(config)# no security ddos source-ip-blocking		Disable source IP blocking
Gateway(config)# no security ddos tcp-scan		Disable TCP scan
Gateway(config)# no security ddos tcp-syn-with-data		Disable TCP SYN with data
Gateway(config)# no security ddos tcp-udp-portscan		Disable TCP UDP port scan
Gateway(config)# no security ddos udp-bomb		Disable UDP bomb
Gateway(config)# no security ddos udp-echo-chargen		Disable UDP echo chargen
Gateway(config)# no security ddos whole-system-flood fin		Disable FIN flood attack prevention
Gateway(config)# no security ddos whole-system-flood icmp		Disable ICMP flood attack prevention
Gateway(config)# no security ddos whole-system-flood syn		Disable SYN flood attack prevention
Gateway(config)# no security ddos whole-system-flood udp		Disable UDP flood attack prevention
Show Command		
Gateway(config)# show security ddos		Shows the current status of DDoS

2.5.11 SNMP Command

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

Command	Parameter	Description
Gateway(config)# snmp-server community [community]	[community]	Specify a SNMP community name of up to 20 alphanumeric characters.
Gateway (config-community-NAME)# active		Enable this SNMP community account.
Gateway(config-community-NAME)# description [Description]	[Description]	Enter the description for this SNMP community of up to 35 alphanumerical characters.
Gateway(config-community-NAME)# level [admin | rw | ro]	[admin | rw | ro]	Specify the access privilege for this SNMP account. **admin:** Full access right, including maintaining user account, system information, loading factory settings, etc..

		rw: Read & Write access privilege. Partial access right, unable to modify user account, system information and load factory settings. **ro:** Read Only access privilege.
No command		
Gateway(config)# no snmp-server community [community]	[community]	Delete the specified community.
Gateway(config-community-NAME)# no active		Disable this SNMP community account. In this example "mycomm" community is disabled.
Gateway(config-community-NAME)# no description		Remove the SNMP community descriptions for "mycomm".
Gateway(config-community-NAME)# no level		Remove the configured access privilege. This will set this community's level to "access denied".
Show command		
Gateway(config)# show snmp-server		Show or verify whether SNMP is enabled or disabled.
Gateway(config)# show snmp-server community		Show or verify each SNMP server account's information.
Gateway(config)# show snmp-server community [community]		Show the specified SNMP server account's settings.
Gateway(config-community-NAME)# show		Show the selected community's settings.
Exit command		
Gateway(config-community-NAME)# exit		Return to Global Configuration mode.
Snmp-server example		
Gateway(config)# snmp-server community mycomm		Create a new community "mycomm" and edit the details of this community account.
Gateway(config-community-mycomm)# active		Activate the SNMP community "mycomm".
Gateway(config-community-mycomm)# description rddeptcomm		Add a description for "mycomm" community.
Gateway(config-community-mycomm)# level admin		Set "mycomm" community level to admin (full access privilege).

2. Set up a SNMP trap destination.

Command	Parameter	Description
Gateway(config)# snmp-server trap-destination [1-2]	[1-2]	Create a trap destination account.
Gateway(config-trap-ACCOUNT)# active		Enable this SNMP trap destination account.
Gateway(config-trap-ACCOUNT)# community [community]	[community]	Enter the community name of network management system.

Gateway(config-trap-ACCOUNT)# destination [A.B.C.D]	[A.B.C.D]	Enter the trap destination IP address for this trap destination account.
No command		
Gateway(config)# no snmp-server trap-destination [1-2]	[1-2]	Delete the specified trap destination account.
Gateway(config-trap-ACCOUNT)# no active		Disable this SNMP trap destination account.
Gateway(config-trap-ACCOUNT)# no community		Delete the configured community name.
Gateway(config-trap-ACCOUNT)# no description		Delete the configured trap destination description.
Show command		
Gateway(config)# show snmp-server trap-destination		Show SNMP trap destination account information.
Gateway(config)# show snmp-server trap-destination [1-2]	[1-2]	Show the specified SNMP trap destination account information.
Gateway(config-trap-ACCOUNT)# show		Show and verify the selected trap destination account's information.
Exit command		
Gateway(config-trap-ACCOUNT)# exit		Return to Global Configuration mode.
Trap-destination example		
Gateway(config)# snmp-server trap-destination 1		Create a trap destination account.
Gateway(config-trap-1)# active		Activate this trap destination account.
Gateway(config-trap-1)# community mycomm		Refer this trap destination account to the community "mycomm".
Gateway(config-trap-1)# description redepttrapdest		Add a description for this trap destination account.
Gateway(config-trap-1)# destination 192.168.1.254		Set trap destination IP address to 192.168.1.254.

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

Trap-type command	Parameter	Description
Gateway(config)# snmp-server trap-type [all | auth-fail | cold-start | port-link | power-down | warm-start]	[all | auth-fail | cold-start | port-link | power-down | warm-start]	Specify a trap type that will be sent when a certain situation occurs. **all:** A trap will be sent when authentication fails, broadcast packets exceed the threshold value, the device cold /warm starts, port link is up or down and power is down. **auth-fail:** A trap will be sent when any unauthorized user attempts to login. **cold-start:** A trap will be sent when the device boots up.

		port-link: A trap will be sent when the link is up or down. **power-down:** A trap will be sent when the power is off. **warm-start:** A trap will be sent when the device restarts.
No command		
Gateway(config)# no snmp-server trap-type [all | auth-fail | cold-start | port-link | power-down | warm-start]	[all | auth-fail | case-fan | cold-start | port-link | power-down | warm-start]	Specify a trap type that will not be sent when a certain situation occurs.
Show command		
Gateway(config)# show snmp-server community		Show community configuration.
Gateway(config)# show snmp-server trap-destination		Show trap destination configuration.
Gateway(config)# show snmp-server trap-type		Show the current enable/disable status of each type of trap.
Trap-type example		
Gateway(config)# snmp-server trap-type all		All types of SNMP traps will be sent.

2.5.12 Syslog Command

Syslog command	Parameter	Description
Gateway(config)# syslog		Enable system log function.
Gateway(config)# syslog level [emergency | alert | critical |error | warning | notice | info | debug]	[emergency | alert | critical | error | warning | notice | info | debug]	Select one of the syslog levels. The Residential Gateway will record log events at the chosen level and above. For example, if you choose *Error*, “error”, “critical”, “alert” and “emergency” events will be recorded. **Emergency: System is unusable.** **Alert: Emergent actions that must be taken immediately.** **Critical: Critical conditions.** **Error: Error conditions.** **Warning: Warning conditions.** **Notice: Normal but significant conditions.** **Info: Keep informational events message.** **Debug: Debug-level messages are logged.**

Gateway(config)# syslog server [A.B.C.D]	[A.B.C.D]	Specify the primary system log server IP address.
No command		
Gateway(config)# no syslog		Disable System log function.
Gateway(config)# no syslog level		Return Syslog level to default level.
Gateway(config)# no syslog server		Delete the primary system log server IP address.
Show command		
Gateway(config)# show syslog		Show current system log settings.
Gateway(config)# show log		Show event logs currently stored in the Gateway. These event logs will be saved to the system log server that you specify.
Syslog command example		
Gateway(config)# syslog		Enable System log function.
Gateway(config)# syslog server 192.180.2.1		Set the primary system log server IP address to 192.168.2.1.

2.5.13 System-Info Command

Command	Parameter	Description
Gateway(config)# system-info dhcp-vendor-id [dhcp_vendor_id]	[dhcp_vendor_id]	Enter a DHCP vendor ID, up to 55 alphanumeric characters, for this Gateway.
Gateway(config)# system-info host-name [host_name]	[host_name]	Enter a new hostname, up to 30 alphanumeric characters, for this Gateway. By default, the hostname prompt shows the model name of this Gateway. You can change the factory-assigned hostname prompt to the one that is easy for you to identify during network configuration and maintenance.
Gateway(config)# system-info system-contact [sys_contact]	[sys_contact]	Enter contact information for this Gateway, up to 55 alphanumeric characters.
Gateway(config)# system-info system-location [sys_location]	[sys_location]	Enter a brief description, up to 55 alphanumeric characters, of the Gateway location. Like the name, the location is for reference only, for example, “13th Floor”.
Gateway(config)# system-info system-name [sys_name]	[sys_name]	Enter a unique name, up to 55 alphanumeric characters, for this Gateway. Use a descriptive name to identify the Gateway in relation to your network, for example, “Backbone 1”. This name is mainly used for reference only.
No command		
Gateway(config)# no system-info dhcp-vendor-id		Delete the entered DHCP vendor ID information.

Gateway(config)# no system-info system-contact	Delete the entered system contact information.
Gateway(config)# no system-info system-location	Delete the entered system location information.
Gateway(config)# no system-info system-name	Delete the entered system name information.
Gateway(config)# no system-info host-name	Set the hostname to the factory default.
Show command	
Gateway(config)# show system-info	Show or verify Gateway information including system contact, system location, system name, model name, firmware version and fiber type.
Gateway(config)# show sfp information	Show the fiber information.
Gateway(config)# show sfp state	Show the SFP status.
System-info example	
Gateway(config)# system-info system-contact info@company.com	Set the system contact field to “info@compnay.com”.
Gateway(config)# system-info system-location 13thfloor	Set the system location field to “13thfloor”.
Gateway(config)# system-info system-name backbone1	Set the system name field to “backbone1”.
Gateway(config)# system-info host-name edgeswitch10	Change the Gateway’s hostname to “edgeswitch10”.

2.5.14 User Command

User command	Parameter	Description
Gateway(config)# user name [user_name]	[user_name]	Enter the new account’s username. The authorized user login name is up to 20 alphanumeric characters. Only 10 login accounts can be registered in this device.
Gateway(config-user-NAME)# active		Activate this user account.
Gateway(config-user-NAME)# description [description]	[description]	Enter the brief description for this user account.
Gateway(config-user-NAME)# level [superuser | editor | homeuser | guest]	[superuser | editor | homeuser | guest]	Specify this user’s access level. **Superuser:** Full access right, including maintaining user account & system information, loading factory settings, etc.. **Editor:** Partial access right, unable to modify user account & system information and load factory settings. **Homeuser:** Partial access right, less than superuser and editor, able to configure Setup (System information, DDNS, Network Setup), WiFi, Security, Applications, Administration

		(Diagnostics, User privilege, Save&Logout), etc. **Guest:** Read-Only access privilege
Gateway(config-user-NAME)# password [password]	[password]	Enter the password, up to 20 alphanumeric characters, for this user account.
No command		
Gateway(config)#no user name [username]	[username]	Delete the specified account.
Gateway(config-user-NAME)# no active		Deactivate the selected user account.
Gateway(config-user-NAME)# no description		Remove the configured description.
Gateway(config-user-NAME)# no password		Remove the configured password value.
Gateway(config-user-NAME)# no level		Reset access level privilege back to the factory default (access denied).
Show command		
Gateway(config)# show user name		List all user accounts.
Gateway(config)# show user name [user_name]	[user_name]	Show the specific account's information.
Gateway(config-user-NAME)# show		Show or verify the newly-created user account's information.
User command example		
Gateway(config)#user name miseric		Create a new login account "miseric".
Gateway(config-user-miseric)# description misengineer		Add a description to this new account "miseric".
Gateway(config-user-miseric)# password mis2256i		Set up a password for this new account "miseric"
Gateway(config-user-miseric)# level rw		Set this user account's privilege level to "read and write".

2.5.15 VLAN Command

Command	Parameter	Description
Gateway(config)# vlan apply		Apply all WAN interface configuration and all VLAN configuration.
Gateway(config)# vlan inside-nat-vlan [1-4094]	[1-4094]	Specify the PVID of LAN port on the private network. The default value is 9.

3. WEB MANAGEMENT

This chapter describes how to manage the Residential Gateway through a Web browser. The IP address concepts and gaining access to the Residential Gateway will be introduced first, and then followed by web-based management instructions.

3.1 The Concept of IP address

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

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

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

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

3.2 Start Configuring

The Residential Gateway can be managed via a Web browser. However, before doing so, you must assign a unique IP address to the Residential Gateway. Use a RJ-45 LAN cable and any of the four 10/100/1000Base-T RJ-45 ports of Residential Gateway as the temporary RJ-45 Management console port to login to the Residential Gateway and set up the IP address for the first time. (The default IP is **“192.168.0.1”**. You can change the Residential Gateway’s IP to the needed one in the **WAN Settings** under **Network Configuration** menu.)

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

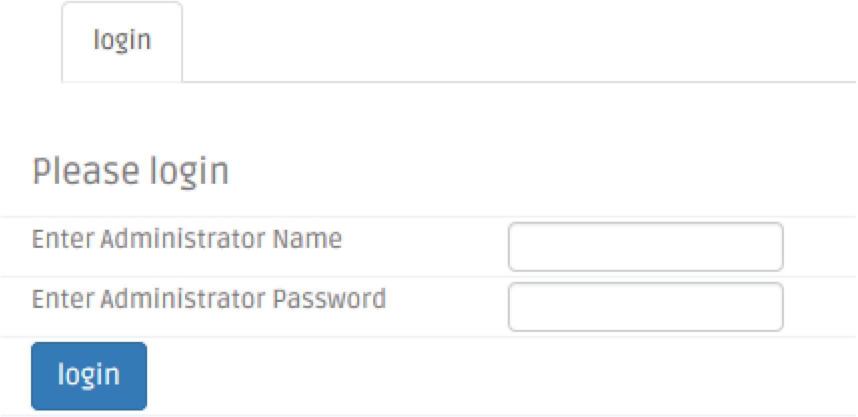
- Use one of the four 10/100/1000Base-T RJ-45 ports as the temporary RJ-45 Management console port to set up the assigned IP parameters of the Residential Gateway.

    1. IP address
    2. Subnet Mask
    3. Default gateway IP address, if required

- Run a Web browser and specify the Residential Gateway's IP address to reach it. (The default IP of Residential Gateway is **"192.168.0.1"** before any changes.)

- Login to the Residential Gateway to reach the Main Menu.

Once you gain the access, a Login window appears like the following:



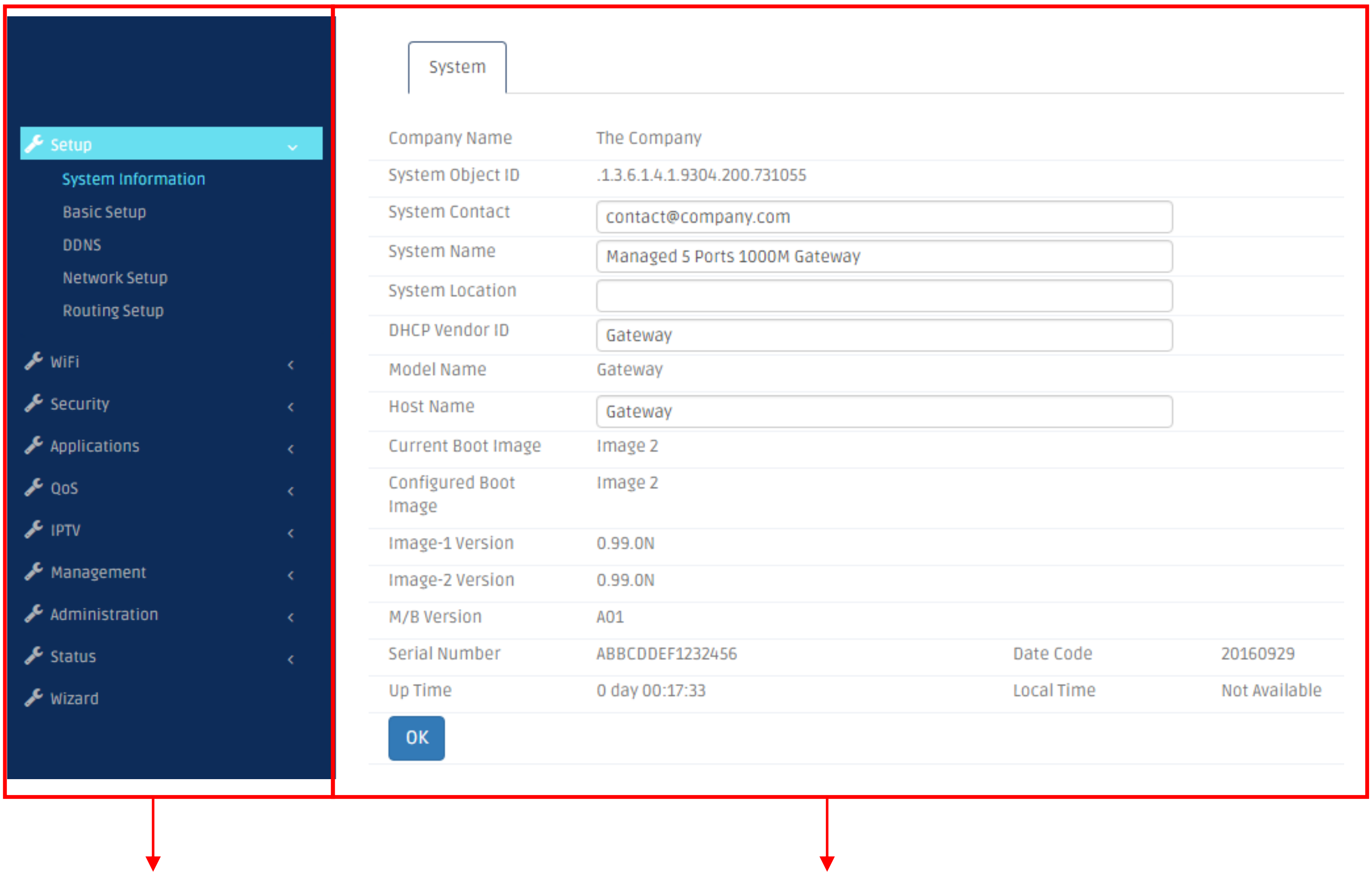
Enter the authorized user name and password then click **"Login"**. The default user name is **admin** and **without a password** (leaves this field blank).

After a successful login, the following Residential Gateway Main Menu screen appears.

NOTE: *By default, the remote access to the Residential Gateway is disabled. If you would like to login the Residential Gateway from WAN port or ports assigned in Bridge Mode, you must create a management interface in* ***Basic Setup*** *under the* ***Setup*** *Menu Bar and enable it. Then, specify the IP address (if necessary) of the management computer and specify Http port number for remote login in* ***Device Access*** *under the* ***Administration*** *Menu Bar. Once completed, you can type in the IP address of the WAN management interface and Http port number in URL field of your web browser like this* ***"192.168.1.198:8888"*** *to access to web management.*

3.3 Introduction to Sub-Menus

If you successfully login to the web management, the first page you will see is as follows:



Company Name	The Company		
System Object ID	.1.3.6.1.4.1.9304.200.731055		
System Contact	contact@company.com		
System Name	Managed 5 Ports 1000M Gateway		
System Location			
DHCP Vendor ID	Gateway		
Model Name	Gateway		
Host Name	Gateway		
Current Boot Image	Image 2		
Configured Boot Image	Image 2		
Image-1 Version	0.99.0N		
Image-2 Version	0.99.0N		
M/B Version	A01		
Serial Number	ABBCDDEF1232456	Date Code	20160929
Up Time	0 day 00:17:33	Local Time	Not Available

Main Menu Bar

Configuration Area

Main Menu Bar At the left of the screen page is the Main Menu bar. It contains the following main tabs:

Setup — To check or configure basic settings of the Residential Gateway, such as WAN and LAN Settings, DHCP, NAT, VLAN, DDNS, Static Routing etc.

IPTV — To set up IGMP functions.

Management — To enable or disable Auto-provision, TR069 and SNMP for management.

Administration – To configure Device Access, Interface Management, system Date/Time setting, Syslog, Ping test, User Privilege, Bakc/Restore, Factory Default and Firmware Update.

Status – To show the current status of each interface and the basic information of the Residential Gateway.

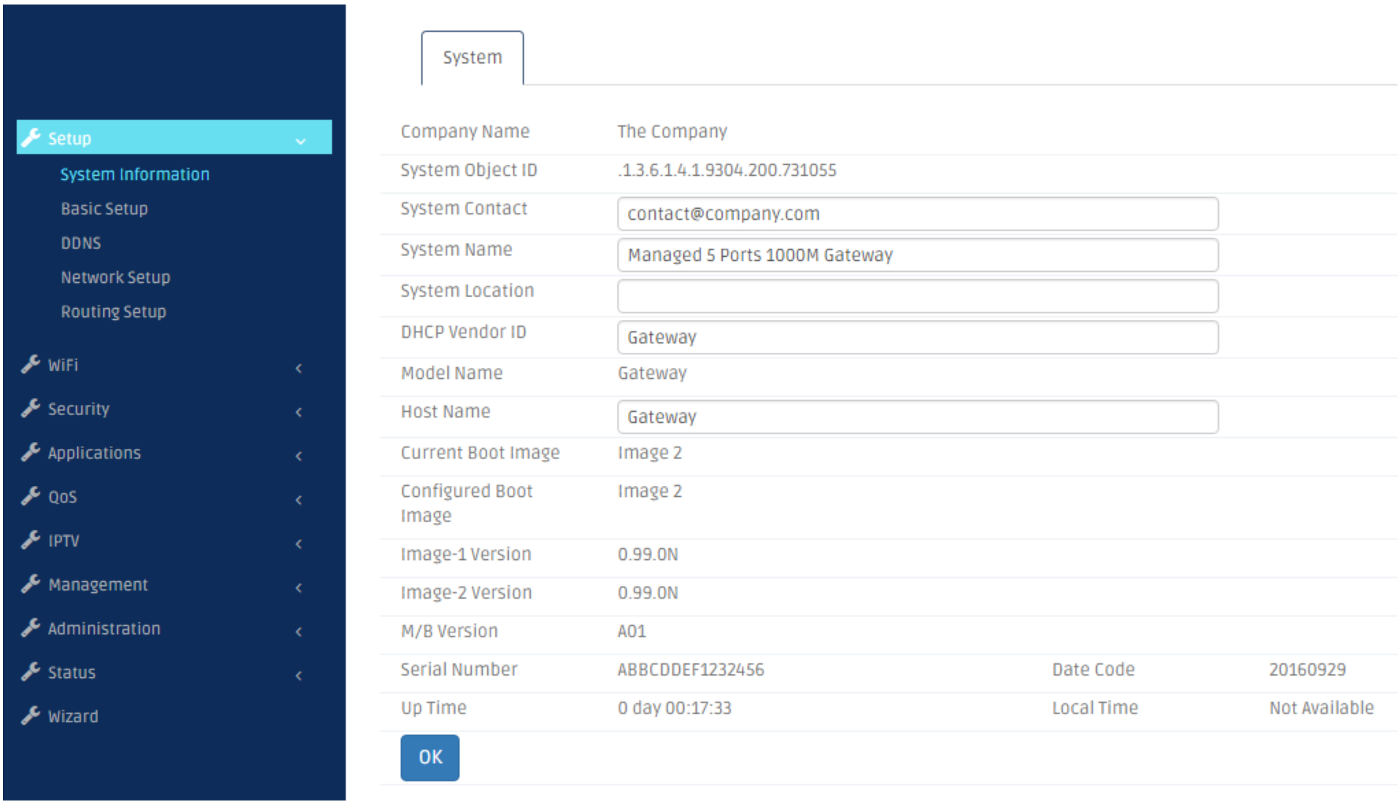
And note that when a main tab appears in the dark blue background, it is currently selected.

Configuration Area The part in the right side of the screen page is the configuration area. Select a tab in the Sub Menu Bar for a feature. Then, you can find the parameters which you can configure for this feature in the configuration area.

Below is the brief description for each sub-menu. For detailed function explanations, please refer to the individual section.

3.4 Setup

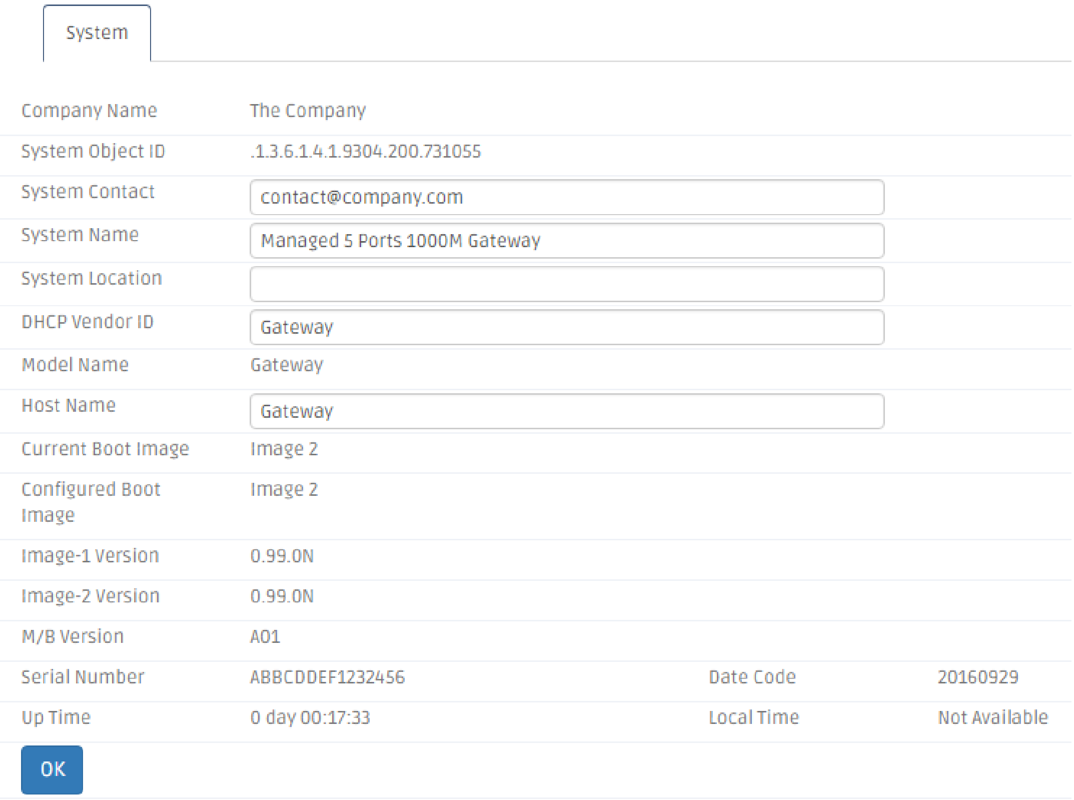
Select **Setup** from the Main Menu bar. Then you can see the sub-items – **System Information**, **Basic Setup**, **Network Setup** and **Routing Setup** – on the sub menu bar.



Company Name	The Company		
System Object ID	.1.3.6.1.4.1.9304.200.731055		
System Contact	contact@company.com		
System Name	Managed 5 Ports 1000M Gateway		
System Location			
DHCP Vendor ID	Gateway		
Model Name	Gateway		
Host Name	Gateway		
Current Boot Image	Image 2		
Configured Boot Image	Image 2		
Image-1 Version	0.99.0N		
Image-2 Version	0.99.0N		
M/B Version	A01		
Serial Number	ABBCDDEF1232456	Date Code	20160929
Up Time	0 day 00:17:33	Local Time	Not Available

3.4.1 System Information

Select **System Information** from the **Setup** sub menu bar. Then, **System Information** screen page appears as follows:



Company Name	The Company		
System Object ID	.1.3.6.1.4.1.9304.200.731055		
System Contact	contact@company.com		
System Name	Managed 5 Ports 1000M Gateway		
System Location			
DHCP Vendor ID	Gateway		
Model Name	Gateway		
Host Name	Gateway		
Current Boot Image	Image 2		
Configured Boot Image	Image 2		
Image-1 Version	0.99.0N		
Image-2 Version	0.99.0N		
M/B Version	A01		
Serial Number	ABBCDDEF1232456	Date Code	20160929
Up Time	0 day 00:17:33	Local Time	Not Available

This page displays basic information of the Residential Gateway and information about the SFP transceiver plugged in the WAN port. And for more details, please refer to the description of the individual section below.

System This is a view-only section which displays basic system information of the Residential Gateway. Below is a description of each item in this section.

Company Name — This is the name of the manufacturer.

System Object ID — This is the predefined system OID of the Residential Gateway.

System Contact — Display contact information for this Residential Gateway.

System Name — This is the model name of the Residential Gateway.

System Location — Display a brief location description for this Residential Gateway.

DHCP Vendor ID — Enter the Vendor ID used for DHCP relay agent function.

Model Name — Display the product’s model name.

Host Name — This is the host name of the Residential Gateway.

Current Boot Image — The image that is currently using.

Configured Boot Image — The image you want to use after reboot.

Image-1 Version — Display the firmware version 1 (image-1) used in this device.

Image-2 Version — Display the firmware version 2 (image-2) used in this device.

Firmware Version — This is the current firmware version of the Residential Gateway.

M/B Version — Display the main board version.

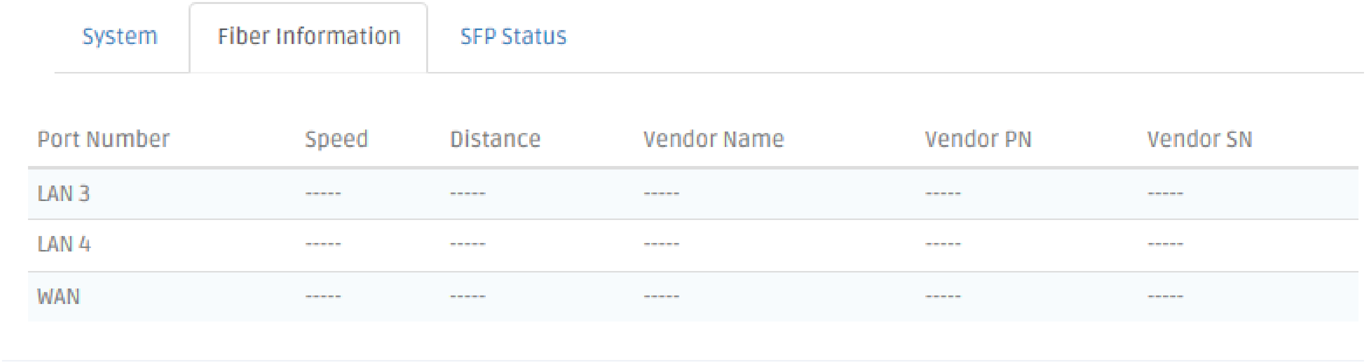
Serial Number — This is the serial number of the Residential Gateway.

Local Time — This is the time of the internal clock of the Residential Gateway.

Up Time — This is the time period since the Residential Gateway has been powered on

Date Code: Display the Residential Gateway Firmware date code.

Fiber Information This is a view-only section which displays information about the fiber transceiver in the fiber WAN port. Below is a description for each item in this section.



Port Number	Speed	Distance	Vendor Name	Vendor PN	Vendor SN
LAN 3	-----	-----	-----	-----	-----
LAN 4	-----	-----	-----	-----	-----
WAN	-----	-----	-----	-----	-----

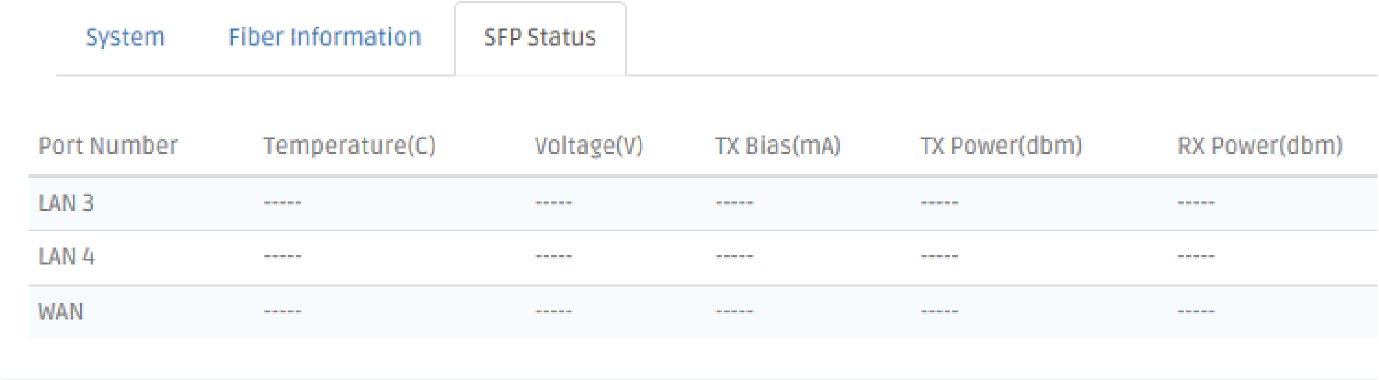
Speed — This is the maximal link speed which the fiber transceiver supports.

Distance — This is the maximal transmission distance which the fiber transceiver supports.

Vendor Name — This is the name of the manufacturer.

Vendor PN — This is the model name of the fiber transceiver.

Vendor SN — This is serial number of the SFP transceiver.



Port Number	Temperature(C)	Voltage(V)	TX Bias(mA)	TX Power(dbm)	RX Power(dbm)
LAN 3	-----	-----	-----	-----	-----
LAN 4	-----	-----	-----	-----	-----
WAN	-----	-----	-----	-----	-----

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

Voltage (V) — The slide-in SFP module operation voltage.

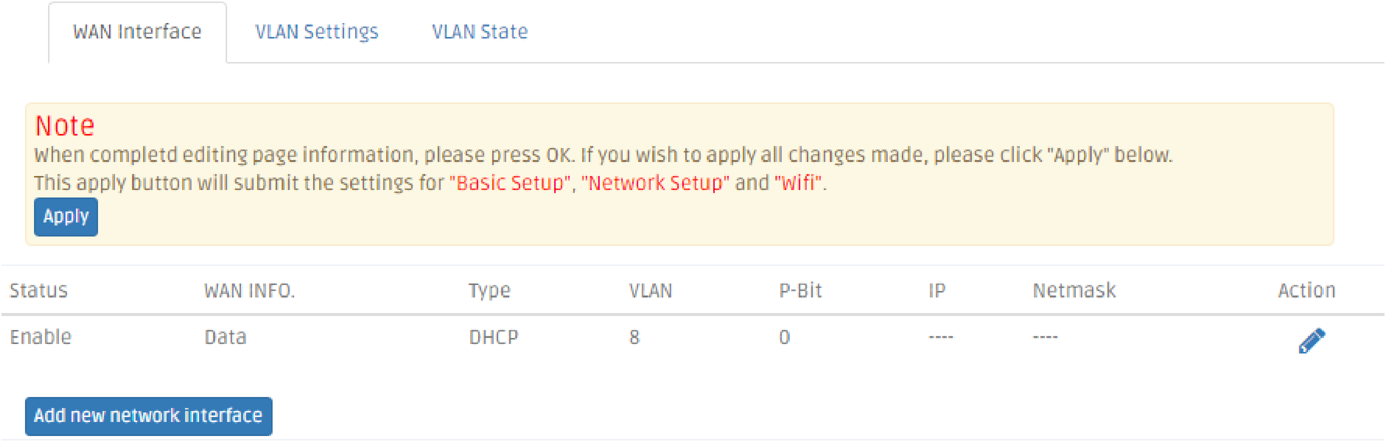
TX Bias (mA) — The slide-in SFP module operation current.

TX Power (dbm) — The slide-in SFP module optical Transmission power.

RX Power (dbm) — The slide-in SFP module optical Receiver power.

3.4.2 Basic Setup

This page enables the network administrator to configure the general settings of the Residential Gateway. Select **Setup** > **Basic Setup** to access this page. And it will appear as follows:



Note

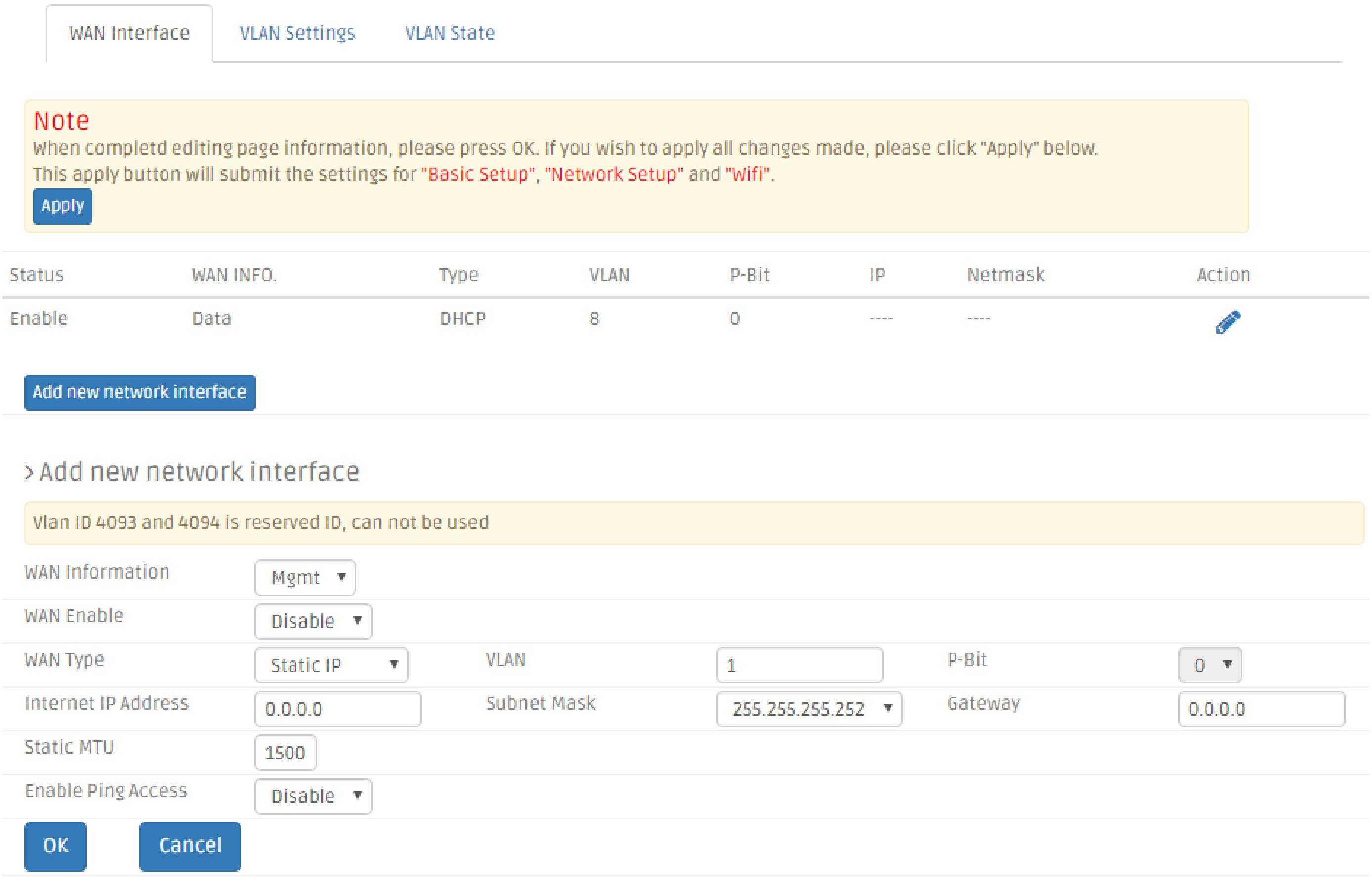
When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

This apply button will submit the settings for "Basic Setup", "Network Setup" and "Wifi".

Status	WAN INFO.	Type	VLAN	P-Bit	IP	Netmask	Action
Enable	Data	DHCP	8	0	----	----	✎

And for details on the settings of this page, please refer to the description of the individual section below.

3.4.2.1 WAN Interface



Note

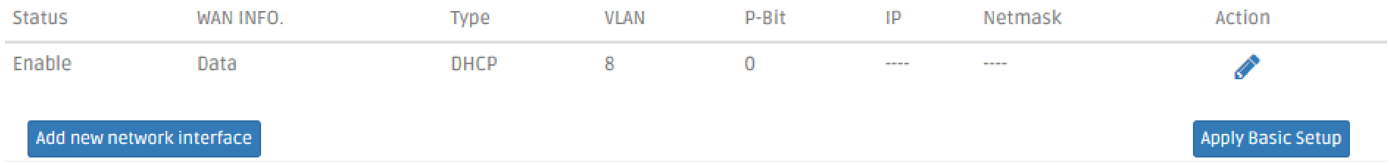
When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "Wifi".

Status	WAN INFO.	Type	VLAN	P-Bit	IP	Netmask	Action
Enable	Data	DHCP	8	0	----	----	✎

> Add new network interface

Vlan ID 4093 and 4094 is reserved ID, can not be used

WAN Information	Mgmt ▾				
WAN Enable	Disable ▾				
WAN Type	Static IP ▾	VLAN	1	P-Bit	0 ▾
Internet IP Address	0.0.0.0	Subnet Mask	255.255.255.252 ▾	Gateway	0.0.0.0
Static MTU	1500				
Enable Ping Access	Disable ▾				



Status	WAN INFO.	Type	VLAN	P-Bit	IP	Netmask	Action
Enable	Data	DHCP	8	0	----	----	✎

This section shows the basic information of the WAN interfaces of the Residential Gateway. Below is a description of each column in the list.

Status — It is *Enabled* if the WAN interface is activated. And it is *Disabled* if the WAN interface is deactivated.

WAN INFO. — This is the WAN information type of this interface. And the available the WAN information types include *Data*, *Management*, *Routing*, and *Alias Interface*.

Type — This is the Internet connection type of this WAN interface.

VLAN — This is the VLAN ID which this WAN interface will add to the egress untagged packets.

P-Bit —This is the 802.1p priority value which this WAN interface will add to the egress untagged packet together with its VLAN ID.

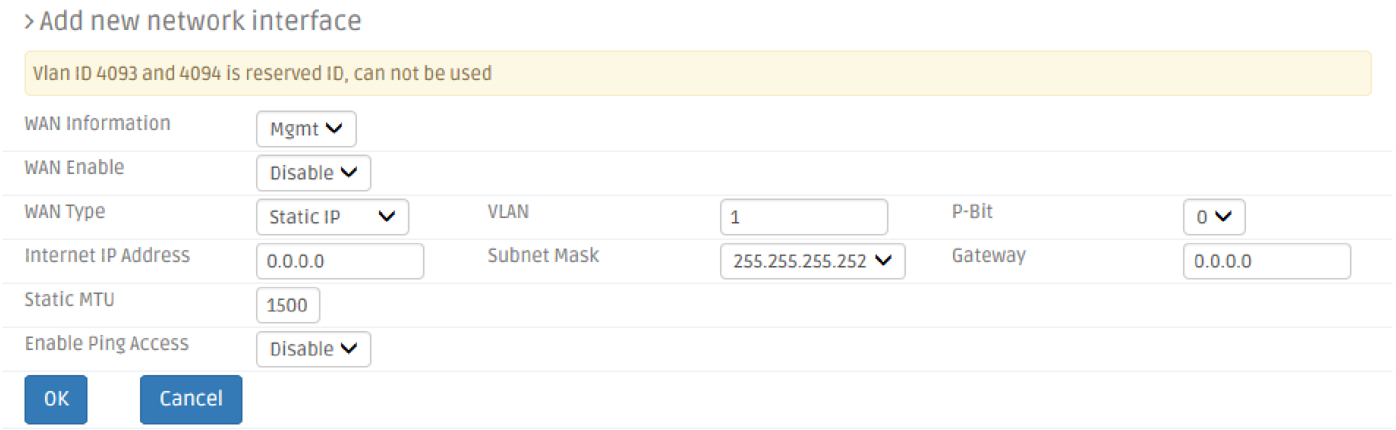
IP — This is the IP address of this WAN interface.

Netmask — This is the subnet mask of this WAN interface.

Action — Click *edit* to change the settings of an interface in the following section. Or click *delete* if you want to remove this entry from the interface list.

To create a new interface, click *Add new network interface* below the list and edit the settings of the new interface in the following section.

This section enables you to edit the settings of a new WAN interface or a WAN interface in the interface list above. And below is the description of configuration parameters in this section.



> Add new network interface

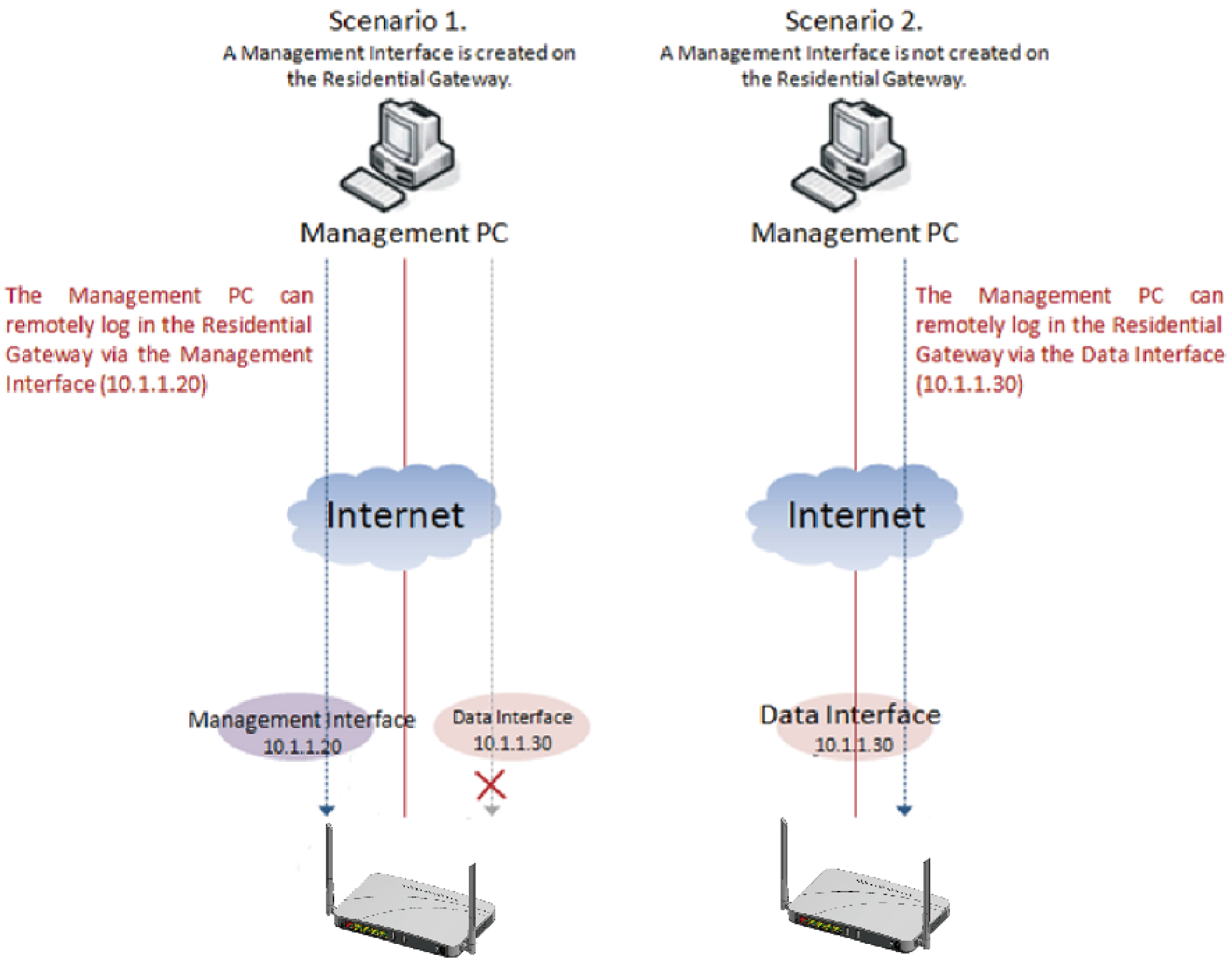
Vlan ID 4093 and 4094 is reserved ID, can not be used

WAN Information	Mgmt				
WAN Enable	Disable				
WAN Type	Static IP	VLAN	1	P-Bit	0
Internet IP Address	0.0.0.0	Subnet Mask	255.255.255.252	Gateway	0.0.0.0
Static MTU	1500				
Enable Ping Access	Disable				

WAN Enable — Enable or disable this WAN interface.

WAN Information — Select a WAN information type from the pull-down menu. You can refer to the following table for a description for the types of the WAN interfaces.

Management — The Management Interface enables the network administrator to remotely log in the Residential Gateway via the Management Interface's IP address if the source IP address is allowed in the “Device Access” page of the UI. And if the Management Interface is not created on the Residential Gateway, the network administrator can remotely log in the Residential Gateway via the data Interface’s IP address. The difference between the two scenarios is illustrated in the following diagram.


Scenario 1.
A Management Interface is created on the Residential Gateway.
Management PC
The Management PC can remotely log in the Residential Gateway via the Management Interface (10.1.1.20)
Internet
Management Interface
10.1.1.20
Data Interface
10.1.1.30
Scenario 2.
A Management Interface is not created on the Residential Gateway.
Management PC
The Management PC can remotely log in the Residential Gateway via the Data Interface (10.1.1.30)
Internet
Data Interface
10.1.1.30

Data — The data interface is the default WAN Interface of the Residential Gateway. It is open to remote management from the IP specified in the Device Access web page when the management interface is not created on the Residential Gateway.

WAN Type — Select an Internet connection type for the WAN interface.

VLAN － Specify a VLAN ID for the WAN interface in the text box. And the WAN interface will add this VLAN ID to the egress untagged packets. (This parameter is only available when the WAN information is Data, Management)

P-Bit － Select a P-Bit value which will be added to the egress untagged packets along with the VLAN ID by this WAN interface. (This parameter is only available when the WAN information is Data, Management)

Static IP

If you select *Static IP* as the WAN type of this interface, please specify the values for the following parameters.

Internet IP Address － Specify an IP address in the text box to assign the interface an IP address.

Subnet Mask － Select a subnet mask for this interface from the pull-down menu.

Gateway － Specify the IP address of a gateway or a router which can deliver the packets which leave the Residential Gateway from this interface to the other network.

Static MTU － Specify the maximal size of Ethernet packets which the Residential Gateway will transmit. MTU stands for “Maximum Transmission Unit.”

DNS1 － Specify the IP address of the primary DNS server of the WAN interface. (This parameter is only available for the data interface.)

DNS2 － Specify the IP address of the secondary DNS server of the WAN interface. (This field is only available for the data interface.)

DNS3 － Specify the IP address of the tertiary DNS server of the WAN interface. (This field is only available for the data interface.)

Enable Ping Access — Click _Enable_ to allow the WAN interface to reply the ICMP echo requests which it receives from the public network.

Note: If you want to assign manual DNS to LAN side, please go to “Network Setup” to disable DNS proxy.

DHCP Client

If you select _DHCP Client_ as the WAN type of this interface, please specify the values for the following parameters.

DHCP MTU — Specify the DHCP MTU for optimal performance.

Attain DNS Automatically & ***Set DNS Manually*** — Choose one of the two options **-** Manually or Automatically. (This parameter is only available for the data interface.)

DNS1 — If you choose to set the DNS manually, please specify the IP address of the primary DNS server of this interface. (This parameter is only available for the data interface.)

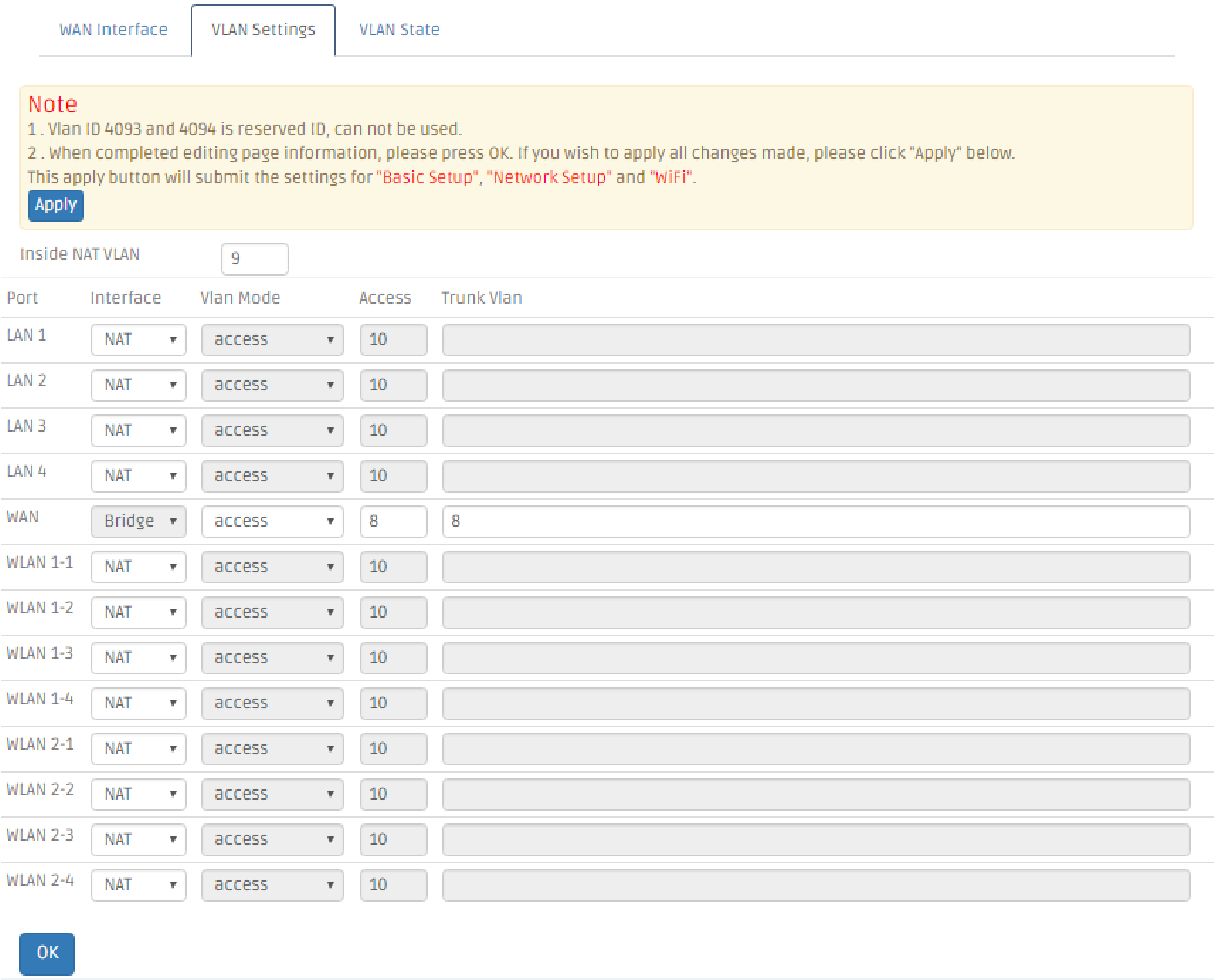
DNS2 — If you choose to set the DNS manually, please specify the IP address of the secondary DNS server of this interface. (This parameter is only available for the data interface.)

DNS3 — If you choose to set the DNS manually, please specify the IP address of the tertiary DNS server of the WAN interface. (This parameter is only available for the data interface.)

Click _Submit_ to apply this change after you finish configuring this WAN interface.

3.4.2.2 VLAN Settings

Select one of the following two system operation modes for the Residential Gateway in the pull-down menu:



Note
1 . Vlan ID 4093 and 4094 is reserved ID, can not be used.
2 . When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "WiFi".

Inside NAT VLAN 9

Port	Interface	Vlan Mode	Access	Trunk Vlan
LAN 1	NAT	access	10	
LAN 2	NAT	access	10	
LAN 3	NAT	access	10	
LAN 4	NAT	access	10	
WAN	Bridge	access	8	8
WLAN 1-1	NAT	access	10	
WLAN 1-2	NAT	access	10	
WLAN 1-3	NAT	access	10	
WLAN 1-4	NAT	access	10	
WLAN 2-1	NAT	access	10	
WLAN 2-2	NAT	access	10	
WLAN 2-3	NAT	access	10	
WLAN 2-4	NAT	access	10	

Inside NAT VLAN — This is the PVID of the LAN port on the private network.

Interface — Specify NAT or Bridge mode for each port. This section shows which LAN ports are on the private network (inside NAT) and which LAN ports are on the public network (outside NAT). When a LAN port is allocated to the private network, it is selected in its drop-down box. And a device which is connected to this port will be a host on the private network. When a LAN port is allocated to the public network, it is selected “Bridge” in the drop-down box. A device which is connected to this port will be a host on the public network.

Bridge Mode — When the Residential Gateway is in this mode, all devices connected to the Residential Gateway from its LAN ports or WLAN are in the public network.

NAT Mode — When the Residential Gateway is in this mode, all devices connected to the Residential Gateway from its LAN ports and WLAN are in the private network.

VLAN Mode (For Bridge mode only) —Select the appropriate mode for each port.

Access — Set the selected port to access mode (untagged).

Trunk — Set the selected port to trunk mode (tagged).

Trunk-Native — Enable native VLAN for untagged traffic on the selected port.

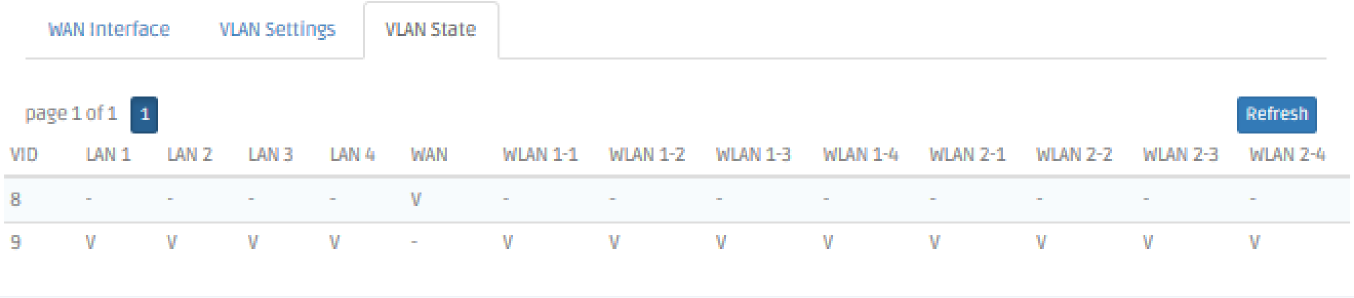
<table>
<tr><th>Mode</th><th colspan="2">Port Behavior</th></tr>
<tr><td rowspan="2"><b>Access</b></td><td colspan="2">Receive untagged packets only. Drop tagged packets.</td></tr>
<tr><td colspan="2">Send untagged packets only.</td></tr>
<tr><td rowspan="2"><b>Trunk</b></td><td colspan="2">Receive tagged packets only. Drop untagged packets.</td></tr>
<tr><td colspan="2">Send tagged packets only.</td></tr>
<tr><td rowspan="3"><b>Trunk Native</b></td><td rowspan="2">Receive both untagged and tagged packets</td><td>Untagged packets: PVID is added</td></tr>
<tr><td>Tagged packets: Stay intact</td></tr>
<tr><td colspan="2">When sending packets, PVID and VID will be compared.
If PVID and VID are the same, PVID will be removed.
If PVID and VID are different, the packets with the original tag (VID) will be sent.</td></tr>
</table>

Access VLAN — Specify the selected ports' Access-VLAN ID (PVID).

Trunk-VLAN — Specify the selected ports' Trunk-VLAN ID (VID).

3.4.2.3 VLAN State

This is to show which VID the ports belongs to. Click *VLAN State* to view the VLAN table or check members of the VLAN groups of the Residential Gateway.



VID	LAN 1	LAN 2	LAN 3	LAN 4	WAN	WLAN 1-1	WLAN 1-2	WLAN 1-3	WLAN 1-4	WLAN 2-1	WLAN 2-2	WLAN 2-3	WLAN 2-4
8	-	-	-	-	V	-	-	-	-	-	-	-	-
9	V	V	V	V	-	V	V	V	V	V	V	V	V

VID — View-only filed that shows the VID

- When untagged packets enter the Residential Gateway from a LAN port on the public network and leave from the WAN port of the Residential Gateway, they will be added the PVID and P-Bit value of the incoming LAN port.

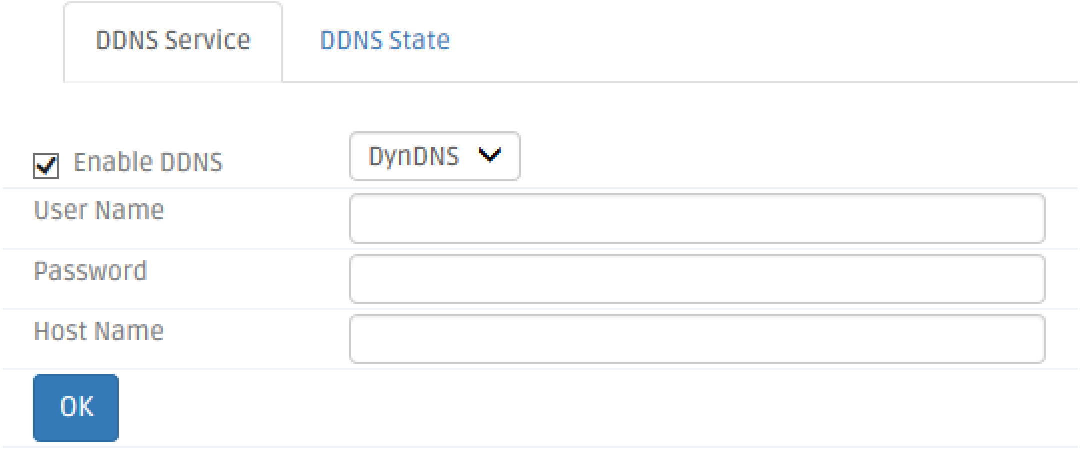
- When tagged packets enter the Residential Gateway from a LAN port on the public network and leave from the WAN port, the Residential Gateway will process them according to their original VLAN tags. If the original VLAN tags of the tagged packets are the same as the WAN port's PVID, the packets will be untagged by the Residential Gateway. Otherwise, they will keep their original VLAN tag when they leave the Residential Gateway.

- When untagged packets enter the Residential Gateway from a LAN port on the private network and leave from the WAN port, they will be added the PVID and P-Bit value of the WAN interface from which they leave the Residential Gateway.

- When a LAN port is allocated to the public network, you can specify its VLAN ID in the text box and select its P-Bit value in the pull-down menu. But when a LAN port is allocated to the private network, its VLAN ID and P-Bit value cannot be changed.

3.4.3 DDNS

DDNS stands for "Dynamic Domain Name Service". It allows a host to bind with a permanent domain name so the host can be found on the internet with this domain name. With DDNS, the network administrator can access the Residential Gateway with a permanent domain name even if it is often assigned different IP addresses by DHCP. And users on the Internet can access the server (such as the web service) on the private network by the domain name of the Residential Gateway. They do not have to access the server by an IP address which is usually not as easy to remember as a domain name. Select **DDNS** from the **Setup** sub menu bar. Then, **DDNS** screen page appears as follows.



☑ Enable DDNS	DynDNS
User Name	
Password	
Host Name	

For details on the settings of DDNS, please refer to the description of the individual section.

DDNS Service To utilize the DDNS service, you need to first register an exclusive domain name for the Residential Gateway in the website of the DynDNS or NoIP.org. And after you register in the website successfully, you need to make a proper setting on the Residential Gateway.

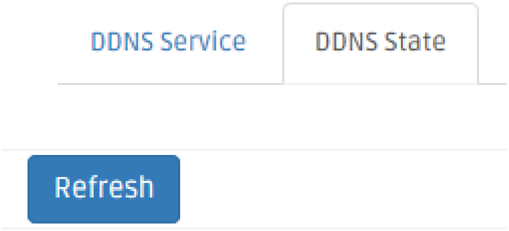
Enable DDNS — Click the checkbox to enable the DDNS service. And select a registration server to which you already registered a domain name.

Username — Specify the username provided by the DDNS server.

Password — Enter the password provided by the DDNS server.

Host Name — Enter the DDNS URL assigned by the DDNS server..

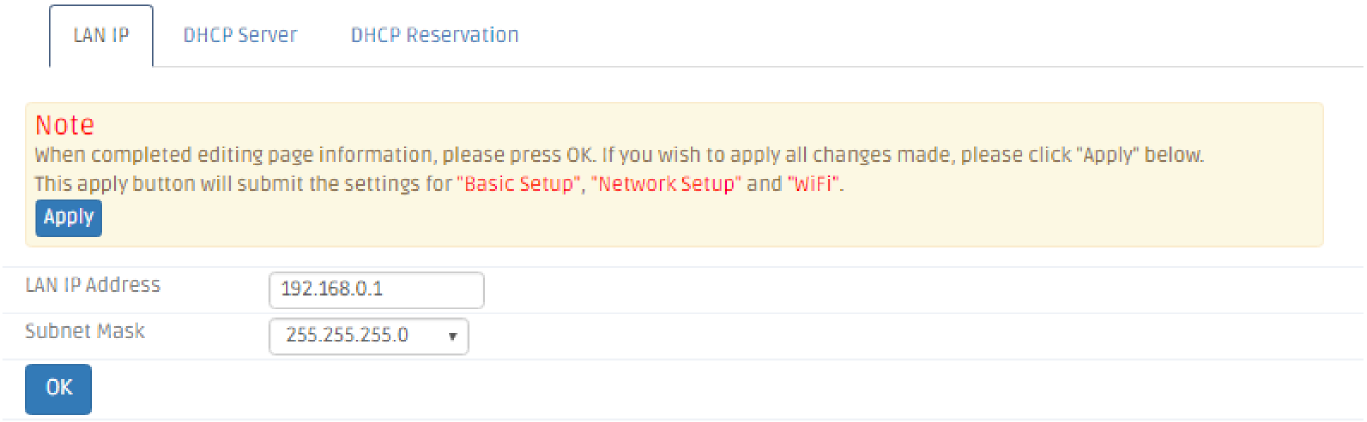
Click *Apply* to submit your settings after you finish configuring this page.



DDNS State This is a view-only section. It displays information about the current status of the DDNS service such as “Initiating DDNS service”, “good (The update was successful, and the hostname is now updated.)” and “Badauth (The username and password pair do not match a real user.)”. You can click *Refresh* to update the information to the last status.

3.4.4 Network Setup

This page allows the network administrator to configure the private network settings of the Residential Gateway. Select **Network Setup** from the **Setup** sub menu bar. Then, **Network Setup** screen page appears as follows:



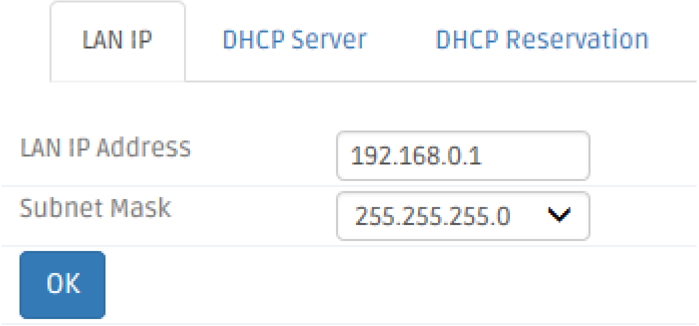
Note
When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "WiFi".

LAN IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

3.4.4.1 LAN IP

This section allows you to assign a private IP address to the Residential Gateway. This is an IP address which the Residential Gateway has on the private network. Below is the description of the configuration parameters for the private network setup.



LAN IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

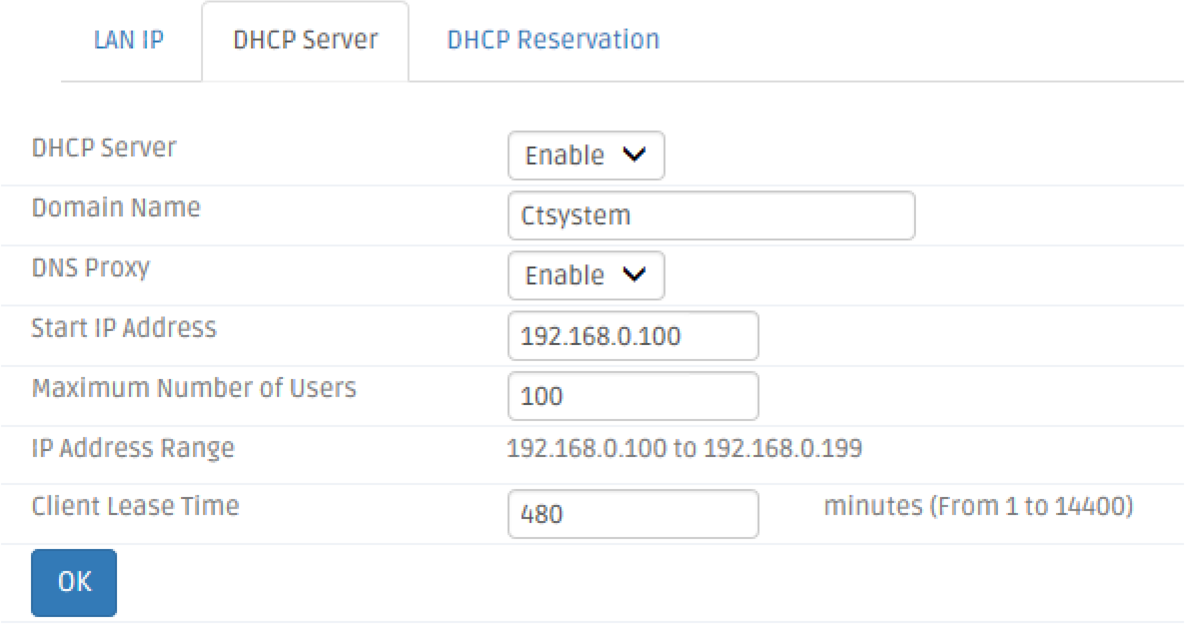
IP Address — Specify the private IP address of the Residential Gateway in the text boxes.

Subnet Mask — Select a subnet mask from the pull-down menu. The subnet mask and the private IP address will determine the private network of the Residential Gateway.

Note that the private network and the public network of the Residential Gateway should not be overlapped. Otherwise, the Residential Gateway cannot forward the packets to the correct destination.

3.4.4.2 DHCP Server

This section allows you to configure the DHCP server function of the Residential Gateway. This function enables the Residential Gateway to assign IP addresses to the hosts on the private network. Below is the description of the configuration parameters for this function.



DHCP Server: Enable
Domain Name: Ctsystem
DNS Proxy: Enable
Start IP Address: 192.168.0.100
Maximum Number of Users: 100
IP Address Range: 192.168.0.100 to 192.168.0.199
Client Lease Time: 480 minutes (From 1 to 14400)

DHCP Server — Enable or disable the DHCP server function of the Residential Gateway.

Domain Name — Specify the domain name of the Residential Gateway in the text boxes.

Start IP Address — Specify an IP address from which the Residential Gateway will start to assign the IP addresses to the DHCP clients on the private network.

Maximum Number of Users — Specify the maximum number of IP addresses which the Residential Gateway can assign to the DHCP clients.

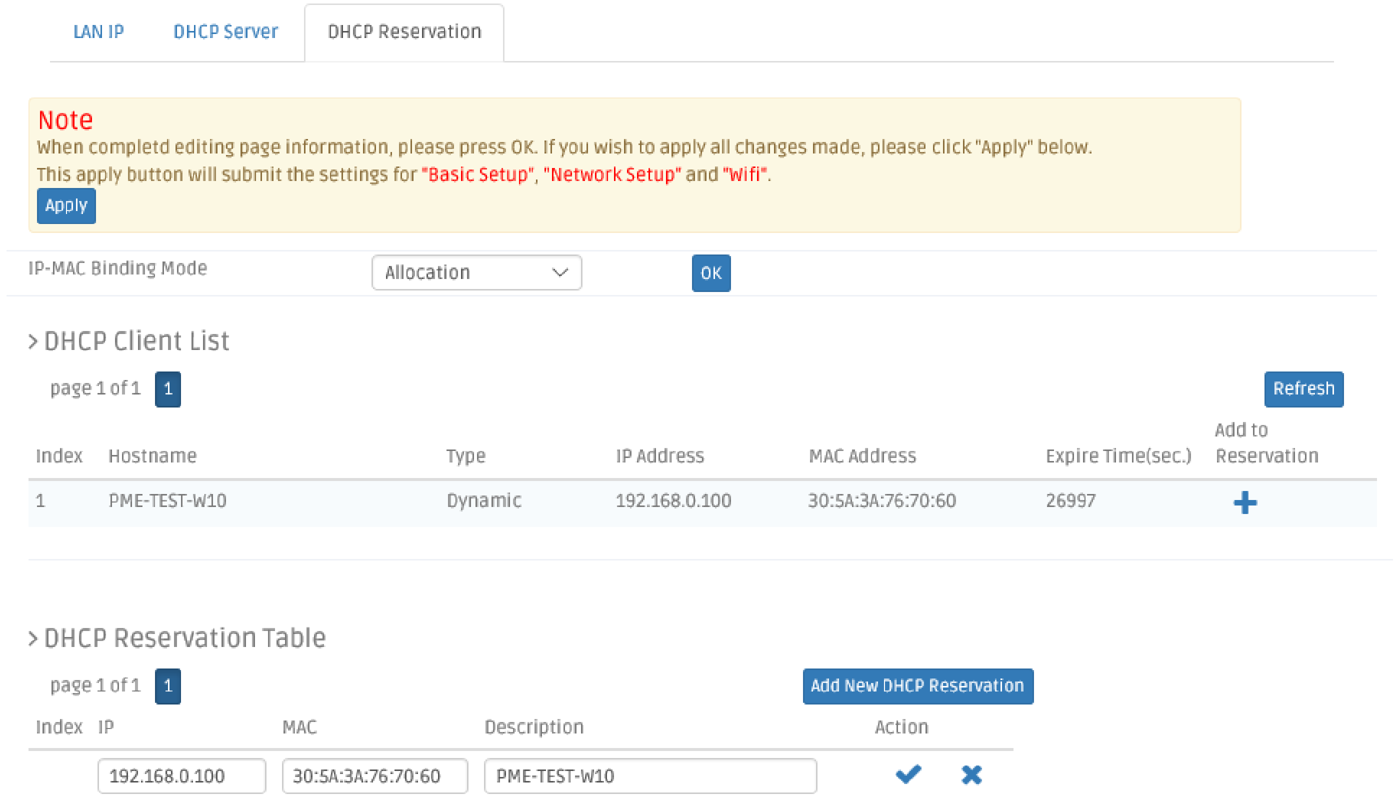
IP Address Range — A view-only field. It displays a range of contiguous IP addresses which are determined by the ***Start IP Address*** field and the ***Maximum Number of Users*** field. The IP addresses in this IP address range can be assigned by the Residential Gateway to the DHCP clients on the private network.

Client Lease Time — This is a time period in which the DHCP clients can keep their IP addresses since the last time in which they receive the DHCP acknowledgement packet from the Residential Gateway.

Click ***OK*** to submit your settings after you finish configuring this page.

3.4.4.3 DHCP Reservation

This section contains the ***DHCP Reservation Table***. The ***DHCP Reservation Table*** includes the IP addresses reserved for the designated DHCP clients. You can create a new entry or modify an entry of this table in the text boxes. Below is the description for each column of the ***DHCP Reservation Table***.



Note
When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "Wifi".

IP-MAC Binding Mode: Allocation

> DHCP Client List

page 1 of 1

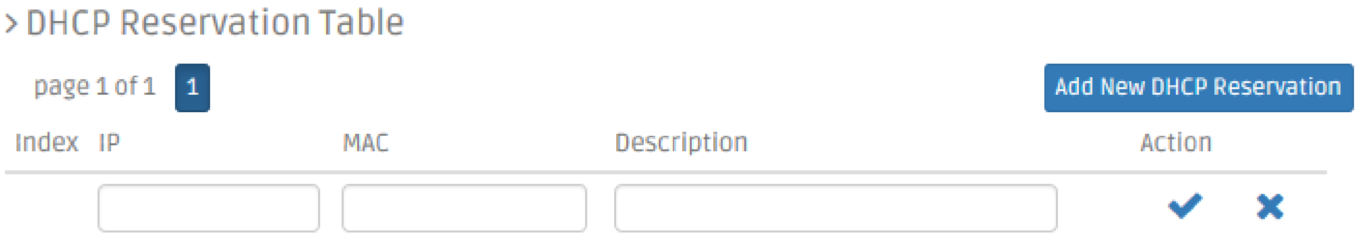
Index	Hostname	Type	IP Address	MAC Address	Expire Time(sec.)	Add to Reservation
1	PME-TEST-W10	Dynamic	192.168.0.100	30:5A:3A:76:70:60	26997	+

> DHCP Reservation Table

page 1 of 1

Index	IP	MAC	Description	Action
	192.168.0.100	30:5A:3A:76:70:60	PME-TEST-W10	✓ ✗

IP-MAC Binding Mode — Select the desired mode to use, either *Allocation* or *Access Restriction.*



> DHCP Reservation Table

page 1 of 1 1

Add New DHCP Reservation

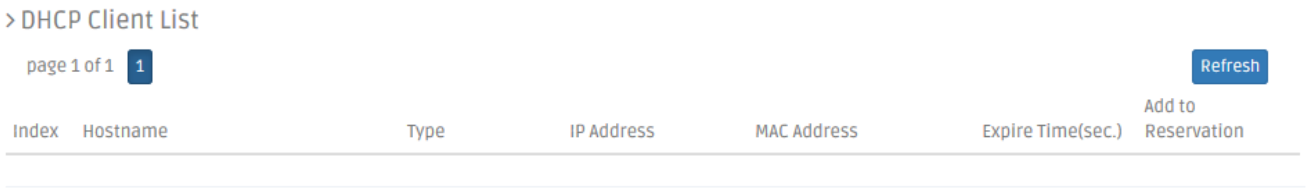
Index	IP	MAC	Description	Action
				✓ ✗

Description — This is a brief description for this entry.

IP — This is an IP address which you want to reserve for a specific DHCP client.

MAC — This is the MAC address of the DHCP client which you want to bundle with the IP address in ***IP*** field.

Action — Click *Check Icon* to add a new entry after you configure it in the textboxes of the table. Click *Pencil Icon* to modify this entry in the text boxes. Or click *Cross Icon* to remove an entry in this table.



> DHCP Client List

page 1 of 1 1

Refresh

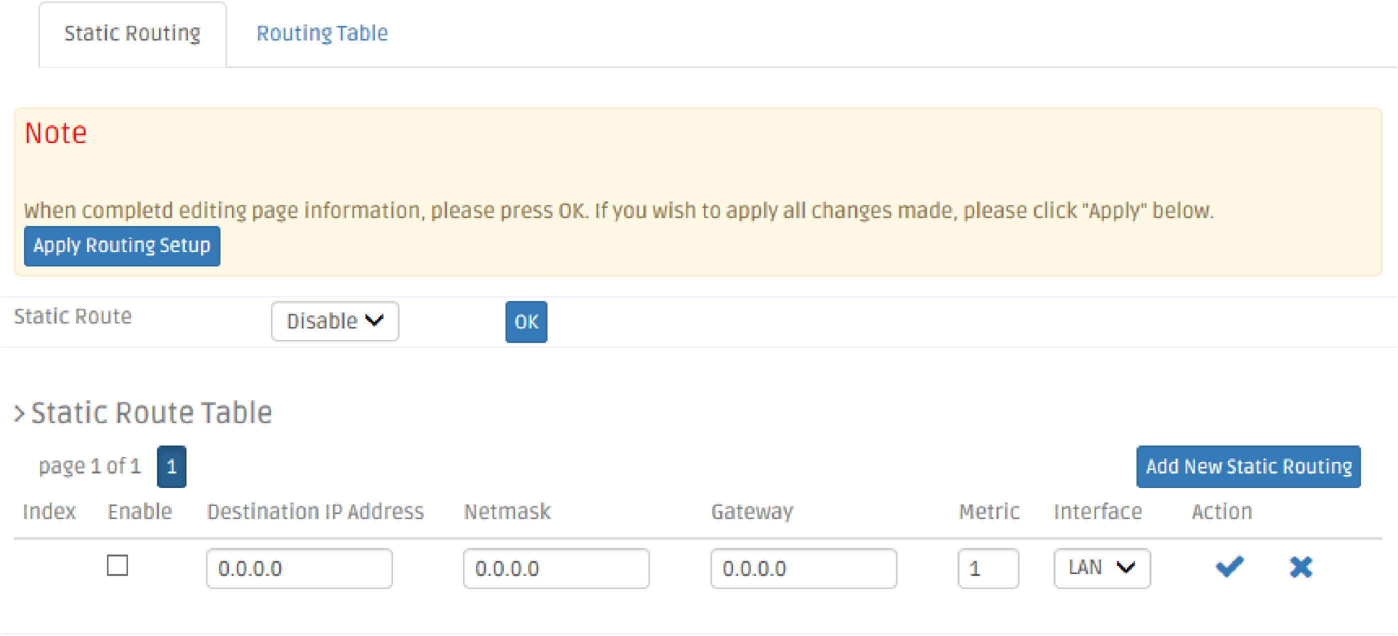
Index	Hostname	Type	IP Address	MAC Address	Expire Time(sec.)	Add to Reservation

DHCP Client List displays information such as the hostname, the IP address, the type of the IP address, the MAC address and the expire time of the leased IP address.

Click *Refresh* to update the DHCP client list.
Click *Apply* to submit your settings after you finish configuring this table.

3.4.5 Routing Setup

This page allows the network administrator to decide how the Residential Gateway will process the received packets. Select **Routing Setup** from the **Setup** sub menu bar. Then, **Routing Setup** screen page appears as follows:



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Static Route: Disable

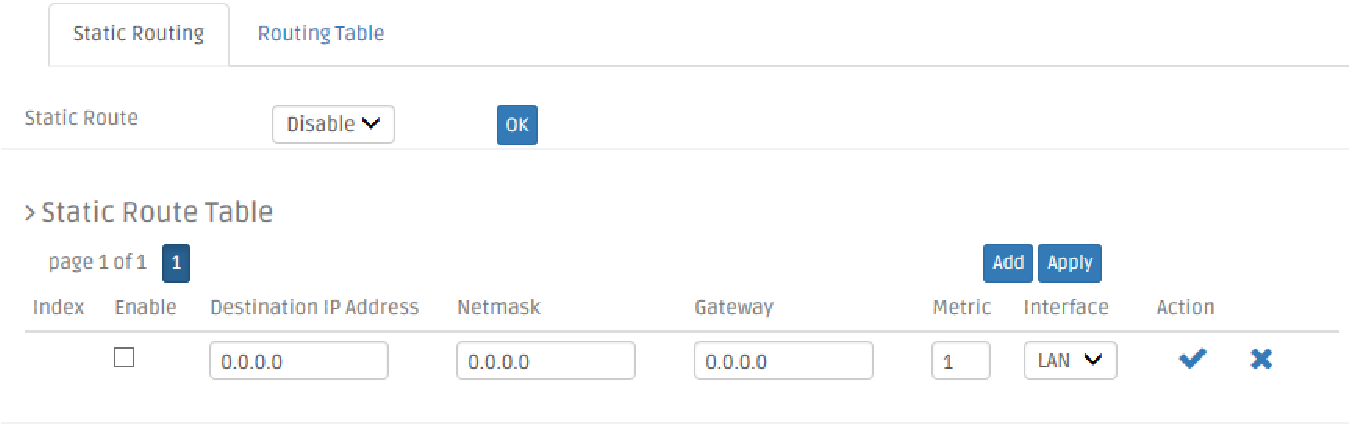
> Static Route Table

page 1 of 1

Index	Enable	Destination IP Address	Netmask	Gateway	Metric	Interface	Action
	□	0.0.0.0	0.0.0.0	0.0.0.0	1	LAN	✓ ✖

3.4.5.1 Static Routing

This section allows you to edit or modify an entry in the ***Static Route Table*** of the Residential Gateway. A static route is a pre-determined pathway that packets can travel to reach a specific destination network. Enter the information below to set up a static route in the ***Static Route Table***.



Static Route: Disable

> Static Route Table

page 1 of 1

Index	Enable	Destination IP Address	Netmask	Gateway	Metric	Interface	Action
	□	0.0.0.0	0.0.0.0	0.0.0.0	1	LAN	✓ ✖

Static Route — Enable or disable static route function. Click ***OK*** to apply.

Static Route Table

Enable — Click to enable the configured static route.

Destination IP Address — Specify the destination IP address of the static route.

Netmask — Specify the subnet mask of the destination network of the static route.

Gateway — Specify the IP address of a gateway through which this static route will send the packets to the destination network.

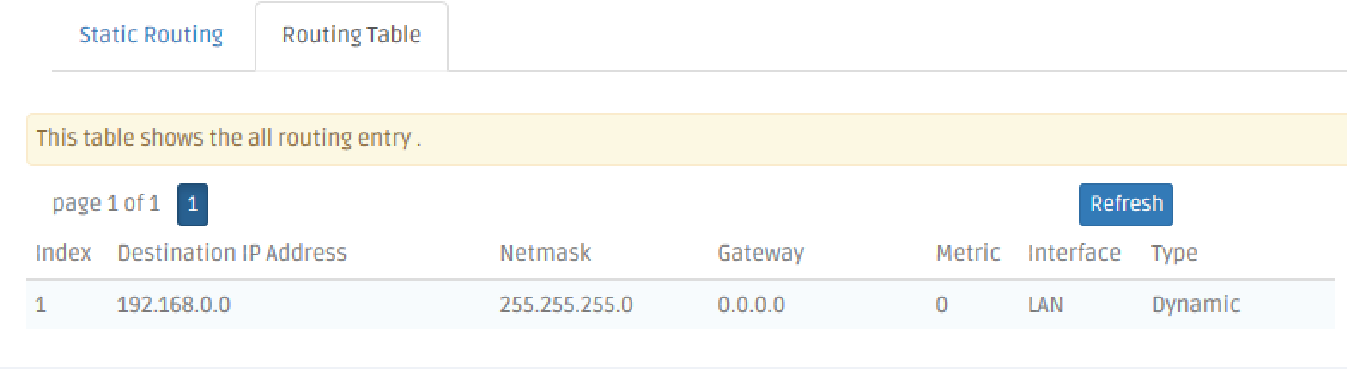
Metric — Metric is the cost of a route to a destination network.

Interface — Specify an interface of the Residential Gateway from which the static route will forward the packets to the destination network.

Click *Apply* to submit your settings or click *Add to create a new static routing rule.*

3.4.5.2 Routing Table

This table displays all the static routes created on the Residential Gateway. Click ***Refresh*** to renew the current status of routing table.

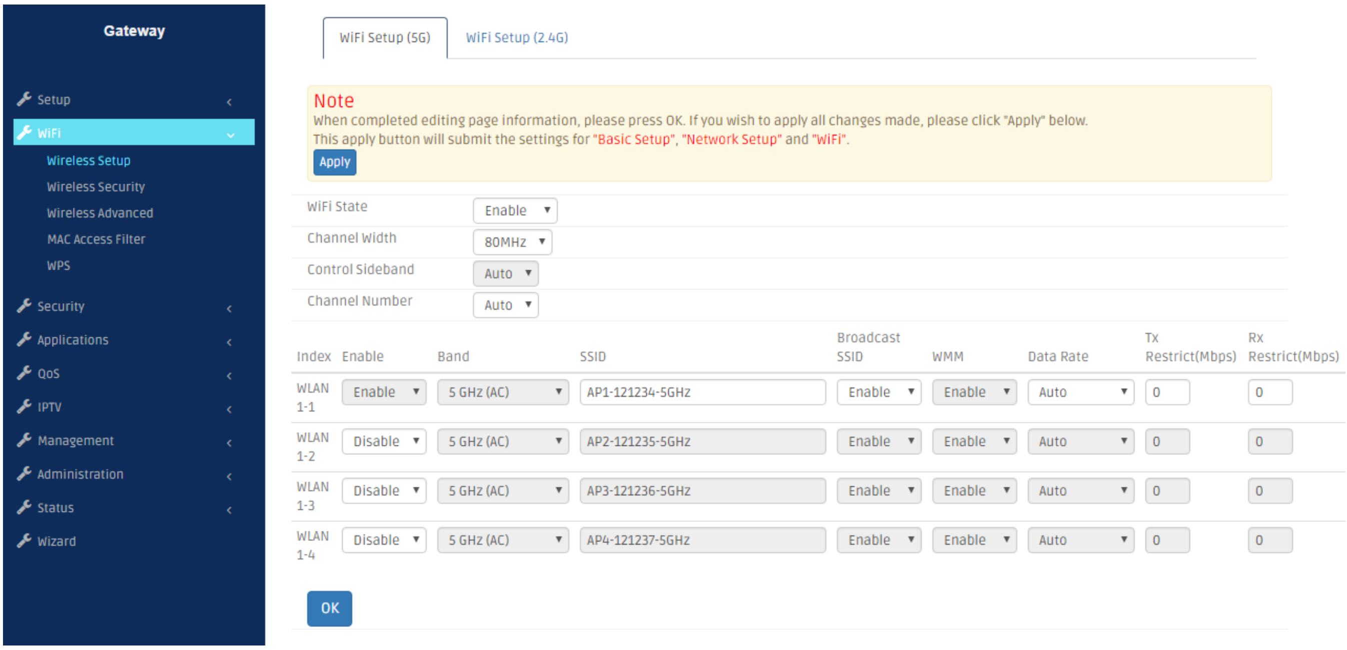


This table shows the all routing entry .

Index	Destination IP Address	Netmask	Gateway	Metric	Interface	Type
1	192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	Dynamic

3.5 WiFi (For WiFi Model Only)

Select **WiFi** in the Main Menu bar. Then you can see the sub-items – **Wireless Setup**, **Wireless Security** and **Wireless Advanced** – on the sub menu bar.



Note

When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "WiFi".

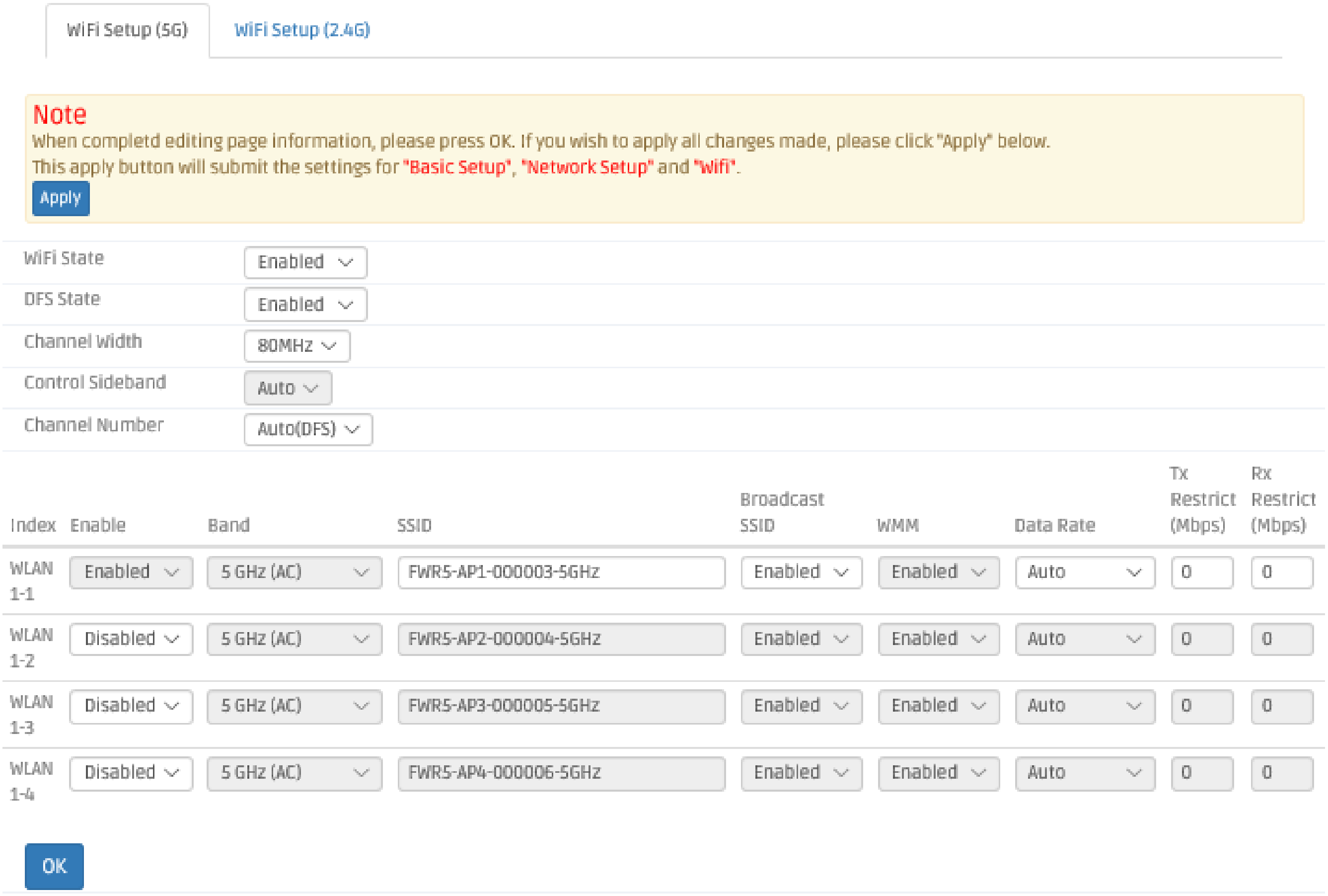
WiFi State	Enable
Channel Width	80MHz
Control Sideband	Auto
Channel Number	Auto

Index	Enable	Band	SSID	Broadcast SSID	WMM	Data Rate	Tx Restrict(Mbps)	Rx Restrict(Mbps)
WLAN 1-1	Enable	5 GHz (AC)	AP1-121234-5GHz	Enable	Enable	Auto	0	0
WLAN 1-2	Disable	5 GHz (AC)	AP2-121235-5GHz	Enable	Enable	Auto	0	0
WLAN 1-3	Disable	5 GHz (AC)	AP3-121236-5GHz	Enable	Enable	Auto	0	0
WLAN 1-4	Disable	5 GHz (AC)	AP4-121237-5GHz	Enable	Enable	Auto	0	0

3.5.1 Wireless Setup

This page allows the network administrator to set up a wireless network of the Residential Gateway. Select **Wireless Setup** from **WiFi** sub menu bar. Then, **Wireless Setup** screen page appears as follows:

For Bandwidth 5G:



Note
When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "Wifi".

WiFi State	Enabled
DFS State	Enabled
Channel Width	80MHz
Control Sideband	Auto
Channel Number	Auto(DFS)

Index	Enable	Band	SSID	Broadcast SSID	WMM	Data Rate	Tx Restrict (Mbps)	Rx Restrict (Mbps)
WLAN 1-1	Enabled	5 GHz (AC)	FWR5-AP1-000003-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-2	Disabled	5 GHz (AC)	FWR5-AP2-000004-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-3	Disabled	5 GHz (AC)	FWR5-AP3-000005-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-4	Disabled	5 GHz (AC)	FWR5-AP4-000006-5GHz	Enabled	Enabled	Auto	0	0

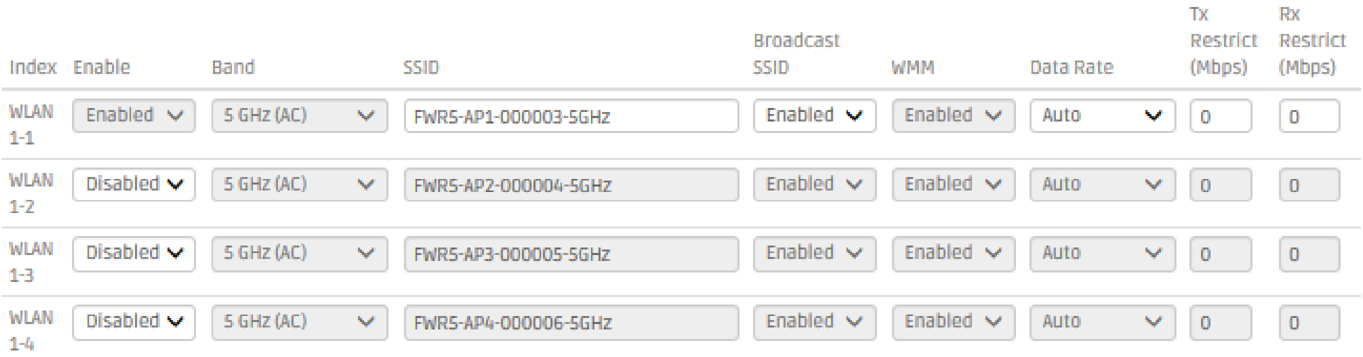
WiFi State — Enable WiFi function for 5G bandwidth.

DFS State — Enable DFS function for 5G bandwidth. Dynamic Frequency Selection helps automatically skip the crucial channel for applications such as milirary or weather use.

Channel Width — Select *20MHz*, *40MHz* or *80MHz* for Channel Width.

Control Sideband — The extra bandwidth will be available when the channel bandwidth is 40MHz. If you select *Upper*, the extra bandwidth will be extended in the upper sideband. (*This field is only available when the network mode is 2.4 GHz (N), 2.4 GHz (G+N), or 2.4 GHz (B+G+N).*)

Channel Number —Select one of the channels in the pull-down menu. The wireless channels are stipulated to prevent too many APs from using the same frequency. Select the channel which is used by fewer APs in your application environment. Or you can select *Auto(DFS)* for the Residential Gateway to choose a WiFi channel automatically.



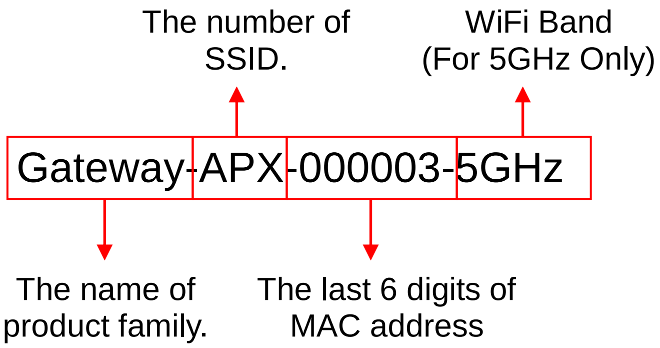
Index	Enable	Band	SSID	Broadcast SSID	WMM	Data Rate	Tx Restrict (Mbps)	Rx Restrict (Mbps)
WLAN 1-1	Enabled	5 GHz (AC)	FWR5-AP1-000003-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-2	Disabled	5 GHz (AC)	FWR5-AP2-000004-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-3	Disabled	5 GHz (AC)	FWR5-AP3-000005-5GHz	Enabled	Enabled	Auto	0	0
WLAN 1-4	Disabled	5 GHz (AC)	FWR5-AP4-000006-5GHz	Enabled	Enabled	Auto	0	0

Index —Shows the number of 5G WLAN number.

Enable —Enable or disable the service set. WLAN 1-1 is always fixed at “Enabled”.

Band — Fixed field that shows the Bandwidth.

SSID — Shows Service Set Identifier for each index. The default SSID should be shown as below format:


The number of SSID.
WiFi Band (For 5GHz Only)
Gateway-APX-000003-5GHz
The name of product family.
The last 6 digits of MAC address

Broadcast SSID — Enable to have the SSID disclose in public, or disable to have the SSID hidden in public.

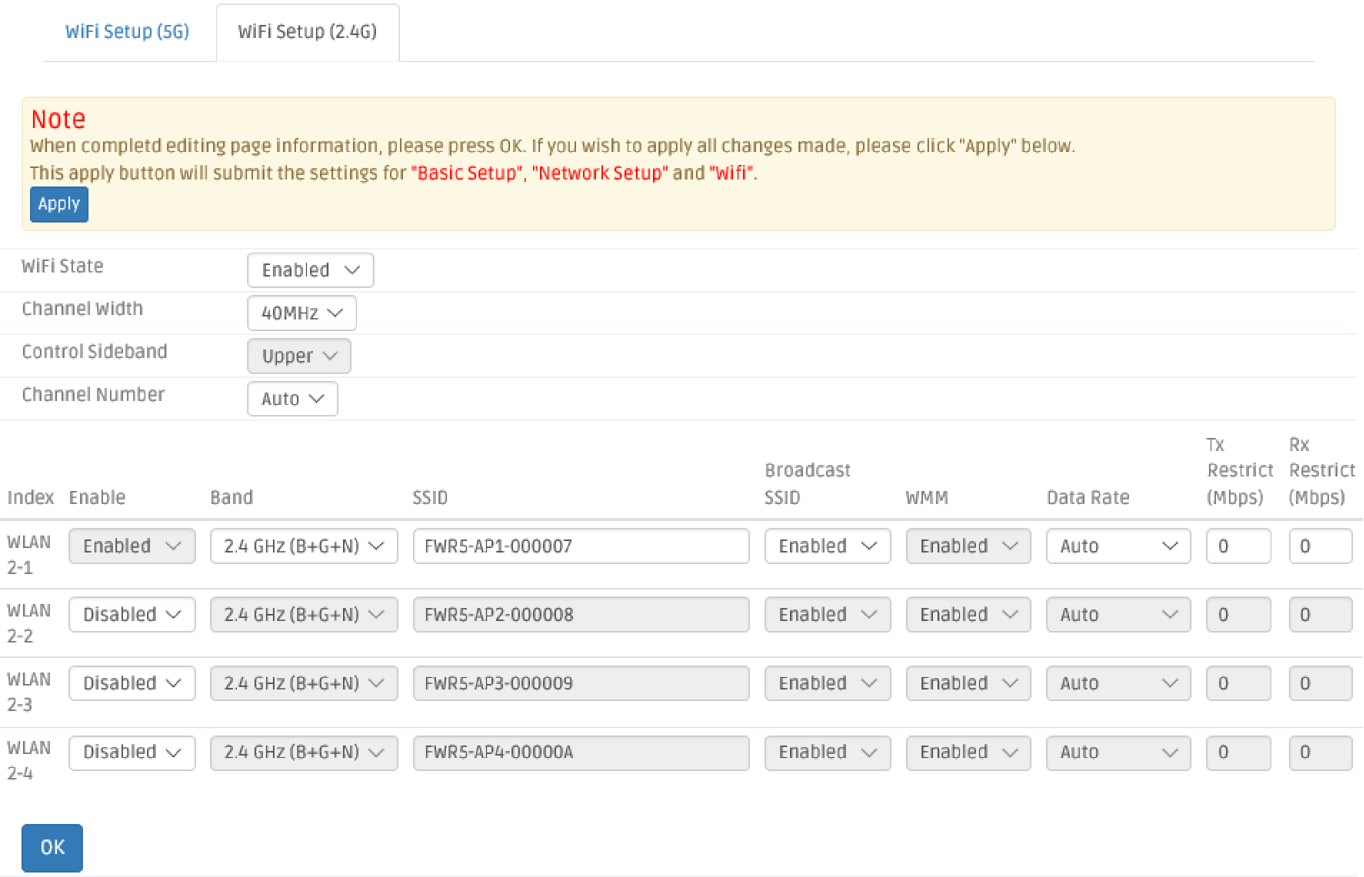
WMM — Click to enable or disable Wireless Multimedia function. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.

Data Rate — Select a data rate in the pull-down menu to decide the speed of the wireless network.

Tx Restrict (Mbps) — Set a limit for data transmission.

Rx Restrict (Mbps) — Set a limit for data receipt.

For Bandwidth 2.4G:



WiFi Setup (5G) | WiFi Setup (2.4G)

Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "Wifi".

Apply

WiFi State	Enabled
Channel Width	40MHz
Control Sideband	Upper
Channel Number	Auto

Index	Enable	Band	SSID	Broadcast SSID	WMM	Data Rate	Tx Restrict (Mbps)	Rx Restrict (Mbps)
WLAN 2-1	Enabled	2.4 GHz (B+G+N)	FWR5-AP1-000007	Enabled	Enabled	Auto	0	0
WLAN 2-2	Disabled	2.4 GHz (B+G+N)	FWR5-AP2-000008	Enabled	Enabled	Auto	0	0
WLAN 2-3	Disabled	2.4 GHz (B+G+N)	FWR5-AP3-000009	Enabled	Enabled	Auto	0	0
WLAN 2-4	Disabled	2.4 GHz (B+G+N)	FWR5-AP4-00000A	Enabled	Enabled	Auto	0	0

OK

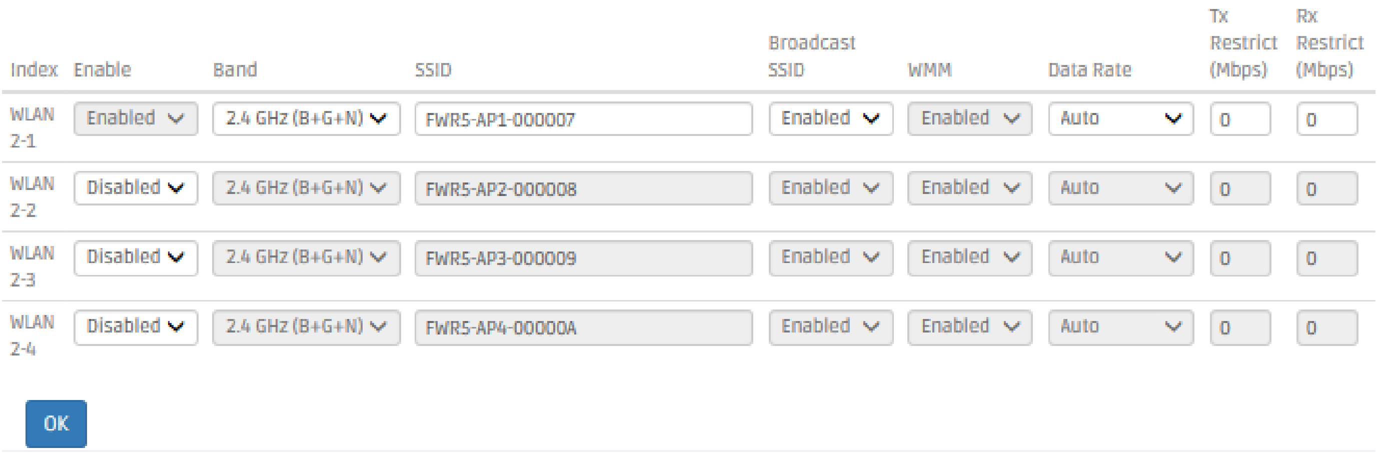
WiFi State — Enable WiFi function for 2.4G bandwidth.

DFS State — Enable DFS function for 2.4G bandwidth. Dynamic Frequency Selection helps automatically skip the crucial channel for applications such as milirary or weather use.

Channel Width — Select *20MHz*, *40MHz* or *80MHz* for Channel Width.

Control Sideband — The extra bandwidth will be available when the channel bandwidth is 40MHz. If you select *Upper*, the extra bandwidth will be extended in the upper sideband. (*This field is only available when the network mode is 2.4 GHz (N), 2.4 GHz (G+N), or 2.4 GHz (B+G+N).*)

Channel Number —Select one of the channels in the pull-down menu. The wireless channels are stipulated to prevent too many APs from using the same frequency. Select the channel which is used by fewer APs in your application environment. Or you can select *Auto(DFS)* for the Residential Gateway to choose a WiFi channel automatically.



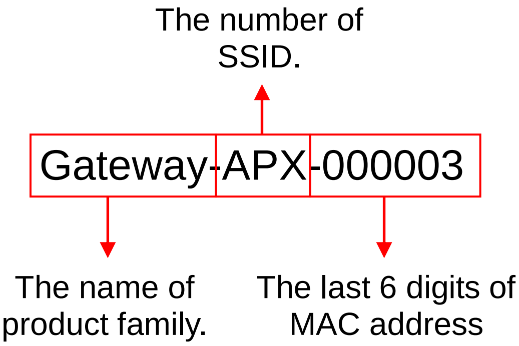
Index	Enable	Band	SSID	Broadcast SSID	WMM	Data Rate	Tx Restrict (Mbps)	Rx Restrict (Mbps)
WLAN 2-1	Enabled	2.4 GHz (B+G+N)	FWR5-AP1-000007	Enabled	Enabled	Auto	0	0
WLAN 2-2	Disabled	2.4 GHz (B+G+N)	FWR5-AP2-000008	Enabled	Enabled	Auto	0	0
WLAN 2-3	Disabled	2.4 GHz (B+G+N)	FWR5-AP3-000009	Enabled	Enabled	Auto	0	0
WLAN 2-4	Disabled	2.4 GHz (B+G+N)	FWR5-AP4-00000A	Enabled	Enabled	Auto	0	0

Index —Shows the number of 2.4G WLAN number.

Enable —Enable or disable the service set. WLAN 2-1 is always fixed at “Enabled”.

Band — Fixed field that shows the Bandwidth.

SSID — Shows Service Set Identifier for each index. The default SSID should be shown as below format:



Broadcast SSID — Enable to have the SSID disclose in public, or disable to have the SSID hidden in public.

WMM — Click to enable or disable Wireless Multimedia function. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.

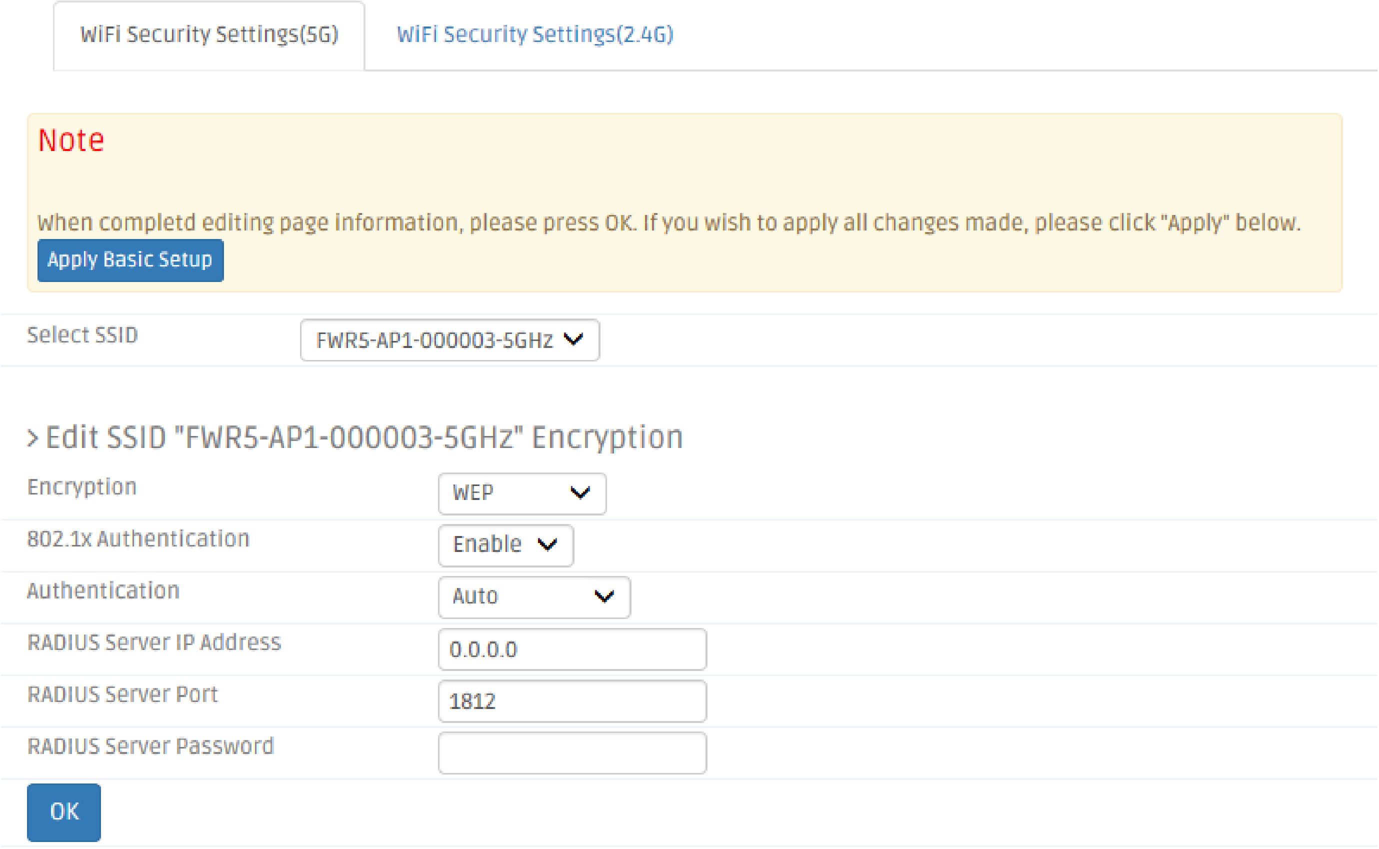
Data Rate — Select a data rate in the pull-down menu to decide the speed of the wireless network.

Tx Restrict (Mbps) — Set a limit for data transmission.

Rx Restrict (Mbps) — Set a limit for data receipt.

3.5.2 Wireless Security

This page allows the network administrator to set the authentication method for the wireless network of the Residential Gateway when the WiFi connection is set up manually. Select **Wireless Security** from **WiFi** sub menu bar. Then, **Wireless Security** screen page appears as follows:



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

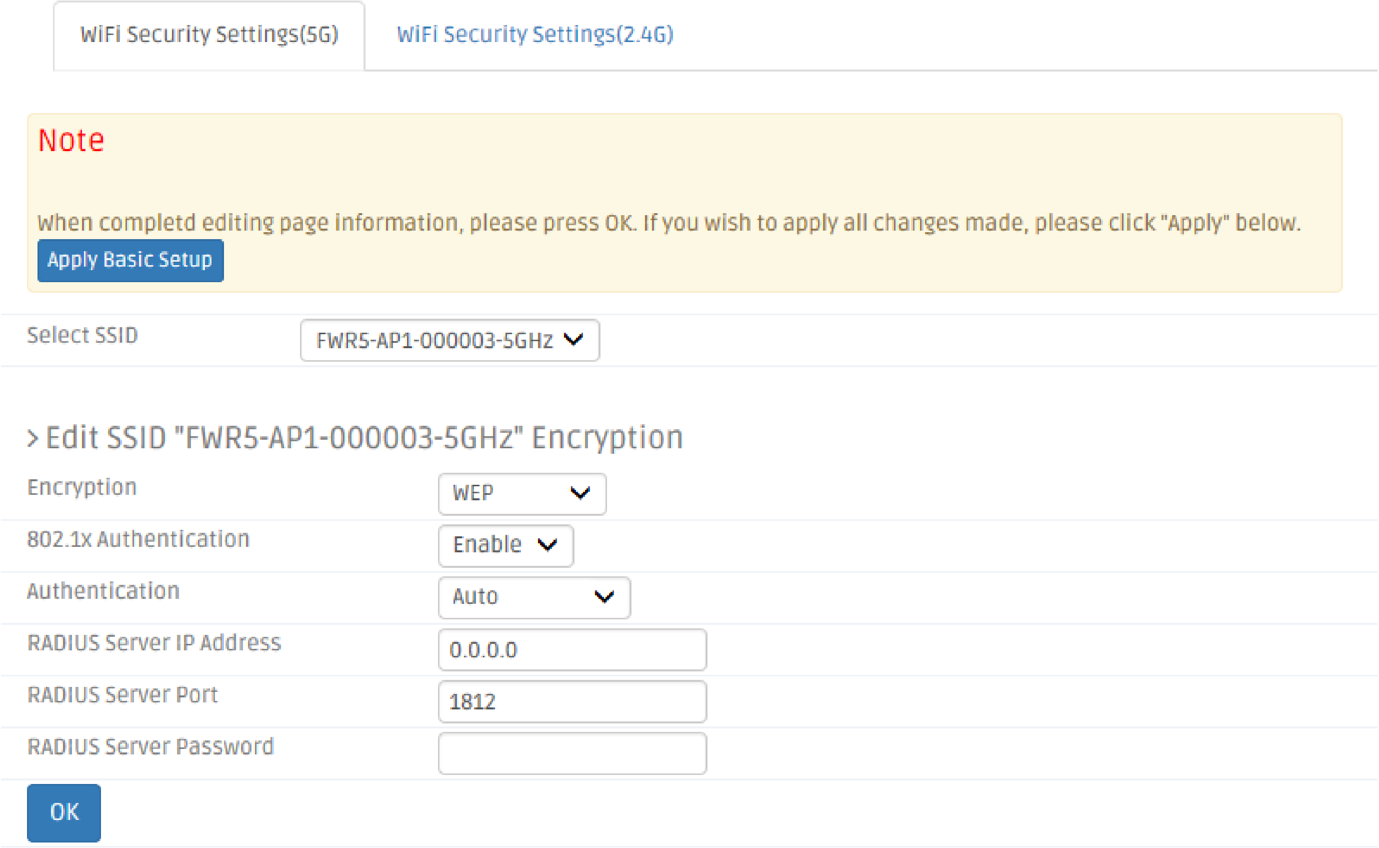
Select SSID	FWR5-AP1-000003-5GHz

> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WEP
802.1x Authentication	Enable
Authentication	Auto
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

This section enables you to set the authentication type for the WLAN whose SSID is selected in the section above. And below is the description of the configuration parameters in this section.

For Bandwidth 5G



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Select SSID: FWR5-AP1-000003-5GHz

> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WEP
802.1x Authentication	Enable
Authentication	Auto
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

Select SSID — Select the SSID you want to configure.

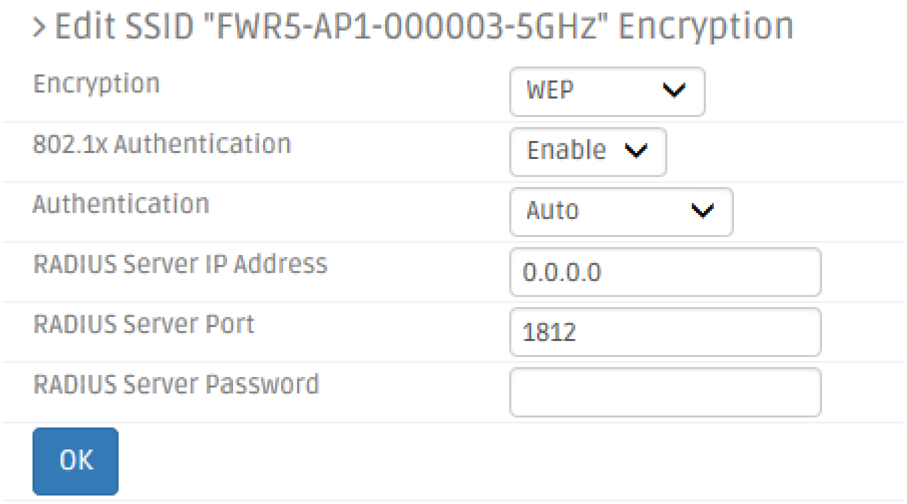
Encryption — The Residential Gateway supports four types of encryptions – *WEP*, *WPA*, *WPA2* and *WPA-Mixed*. Select one of them in the drop-down menu as the encryption of this WLAN. Or select *Disabled* if you don't want any data encryption for this WLAN.

WEP

WEP stands for "Wired Equivalent Privacy". It is a basic encryption method based on IEEE 802.11 standard.

802.1x Authentication – Enable or disable the 802.1x authentication for the WLAN with a RADIUS server.

If you enable ***802.1x Authentication***, please specify the values of the following parameters:



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WEP
802.1x Authentication	Enable
Authentication	Auto
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

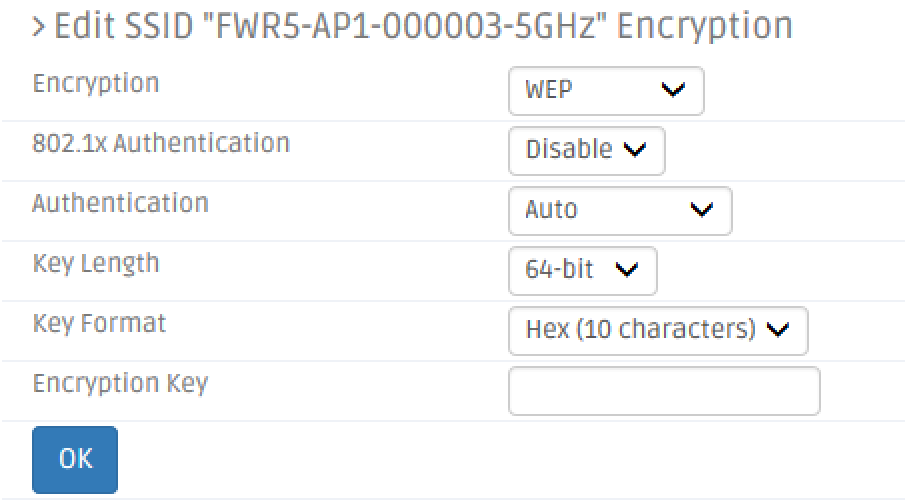
Authentication — Select _Auto_, _Open System_ or _Shared Key_ for authentication.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number for the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the password which the RADIUS server will verify.

If you disable ***802.1x Authentication***, please specify the values of the following parameters:



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WEP
802.1x Authentication	Disable
Authentication	Auto
Key Length	64-bit
Key Format	Hex (10 characters)
Encryption Key	

Authentication — Select *Auto*, *Open System* or *Shared Key* for authentication.

Key Length — Select **64 bits** or **128 bits** from the pull-down menu. The wireless client devices must have the same WEP encryption length as the Residential Gateway.

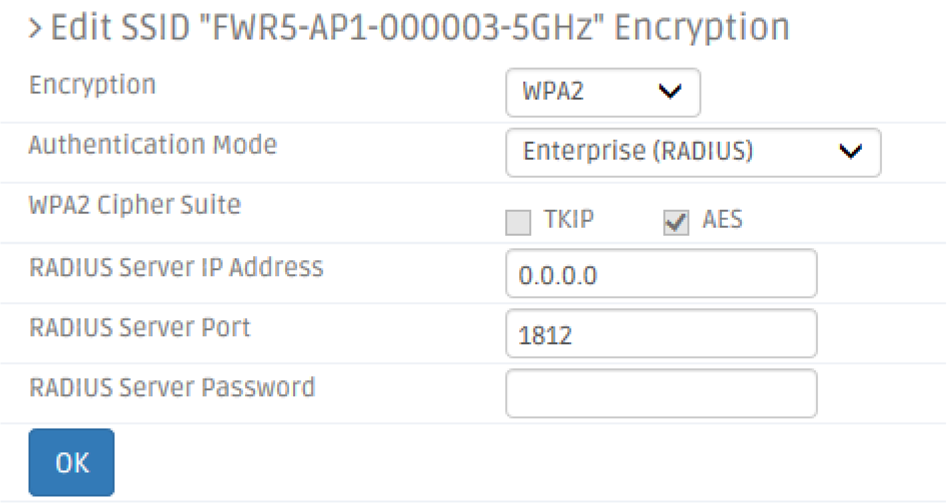
Key Format — Select **ASCII (5 characters)** or **HEX (10 characters)** from the pull-down menu as the format of the key.

Encryption Key — Specify the alphanumeric password for the WLAN.

WPA & *WPA2*

WPA stands for "Wi-Fi Protected Access". It is a kind of encryption which improves the security of WEP. It adopts two security-enhanced types to encrypt data — *TKIP* (Temporal Key Integrity Protocol) and *AES* (Advanced Encryption Standard). *AES* is a stronger encryption method than *TKIP*. *WPA2* is based on 802.11i. And it provides a stronger wireless security than *WPA*.

Authentication Mode — Select *Enterprise (RADIUS)* to ask the wireless client devices to pass the authentication of a RADIUS server. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WPA2
Authentication Mode	Enterprise (RADIUS)
WPA2 Cipher Suite	□ TKIP ☑ AES
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

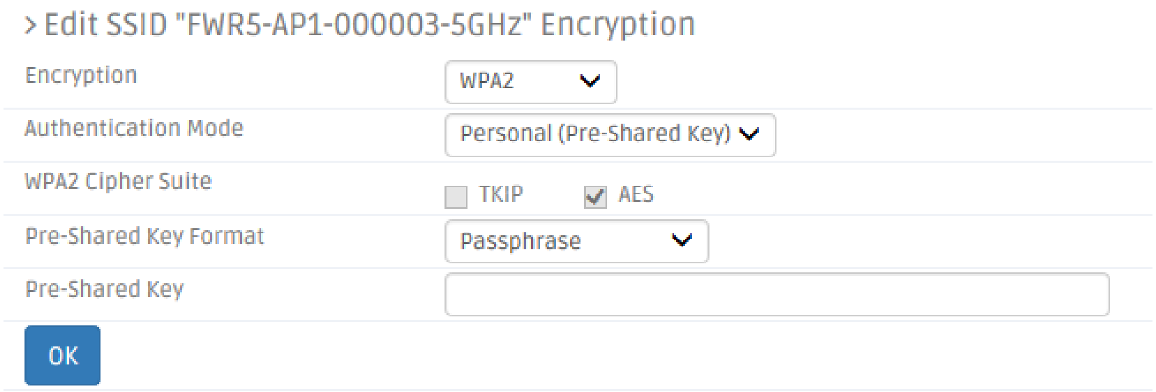
WPA2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number of the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the shared password which will be verified by the RADIUS server.

If you select *Personal (Pre-Shared Key)*, please specify the values of the following parameters for the wireless authentication.



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WPA2
Authentication Mode	Personal (Pre-Shared Key)
WPA2 Cipher Suite	□ TKIP ☑ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

WPA2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

Pre-Shared Key Format — Select *Passphrase* (alphanumeric format) or

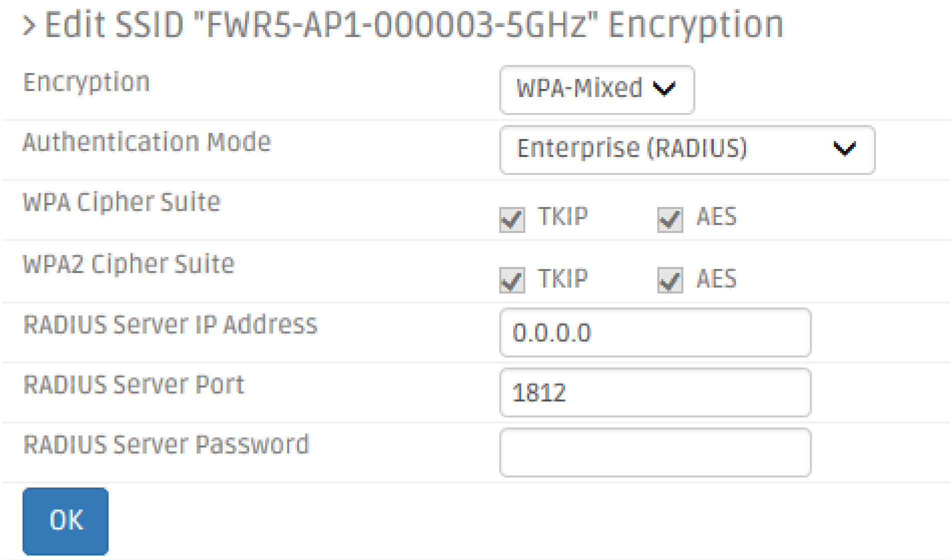
Hex(64characters) (“A-F”, “a-f” and “0-9”) in the pull-down menu.

WPA 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 used.

WPA Mixed

WPA Mixed is the security mode which permits the coexistence of WPA and WPA2 clients on a WLAN. When the wireless security is set in this mode, the wireless client device can connect to the Residential Gateway with WPA/TKIP or WPA2/AES. Some older wireless client devices only support WPA/TKIP. So you have to select the mixed mode to open the WiFi service to this device.

Authentication Mode — Select *Enterprise (RADIUS)* to ask the wireless client devices to pass the authentication of a RADIUS server. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WPA-Mixed
Authentication Mode	Enterprise (RADIUS)
WPA Cipher Suite	☑ TKIP ☑ AES
WPA2 Cipher Suite	☑ TKIP ☑ AES
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

WPA Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

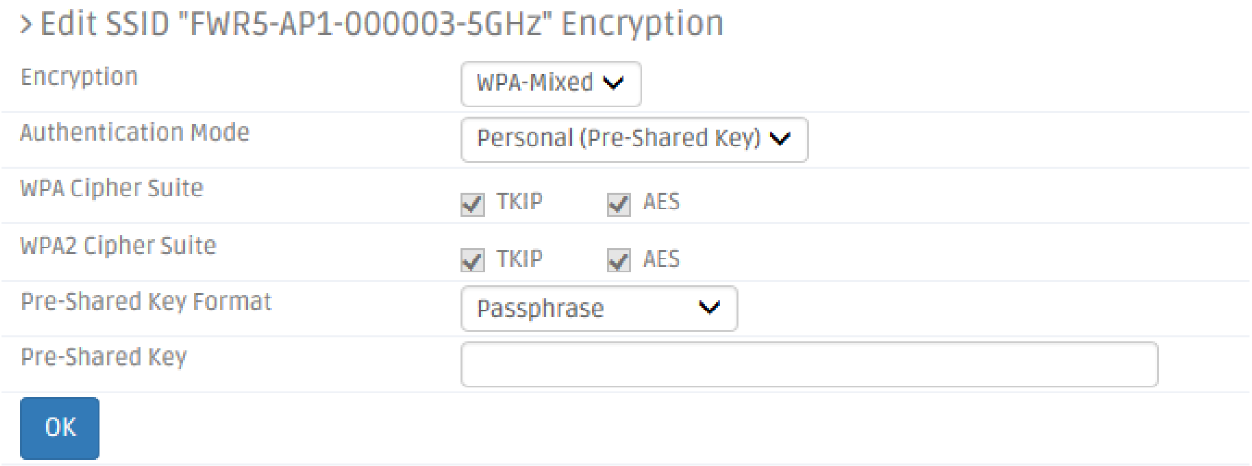
WPA 2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number of the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the shared password which will be verified by the RADIUS server.

Select _Personal (Pre-Shared Key)_ as the authentication mode. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000003-5GHz" Encryption

Encryption	WPA-Mixed
Authentication Mode	Personal (Pre-Shared Key)
WPA Cipher Suite	☑ TKIP ☑ AES
WPA2 Cipher Suite	☑ TKIP ☑ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

WPA Cipher Suite —View-only field that shows _TKIP_ or _AES_ is currently used.

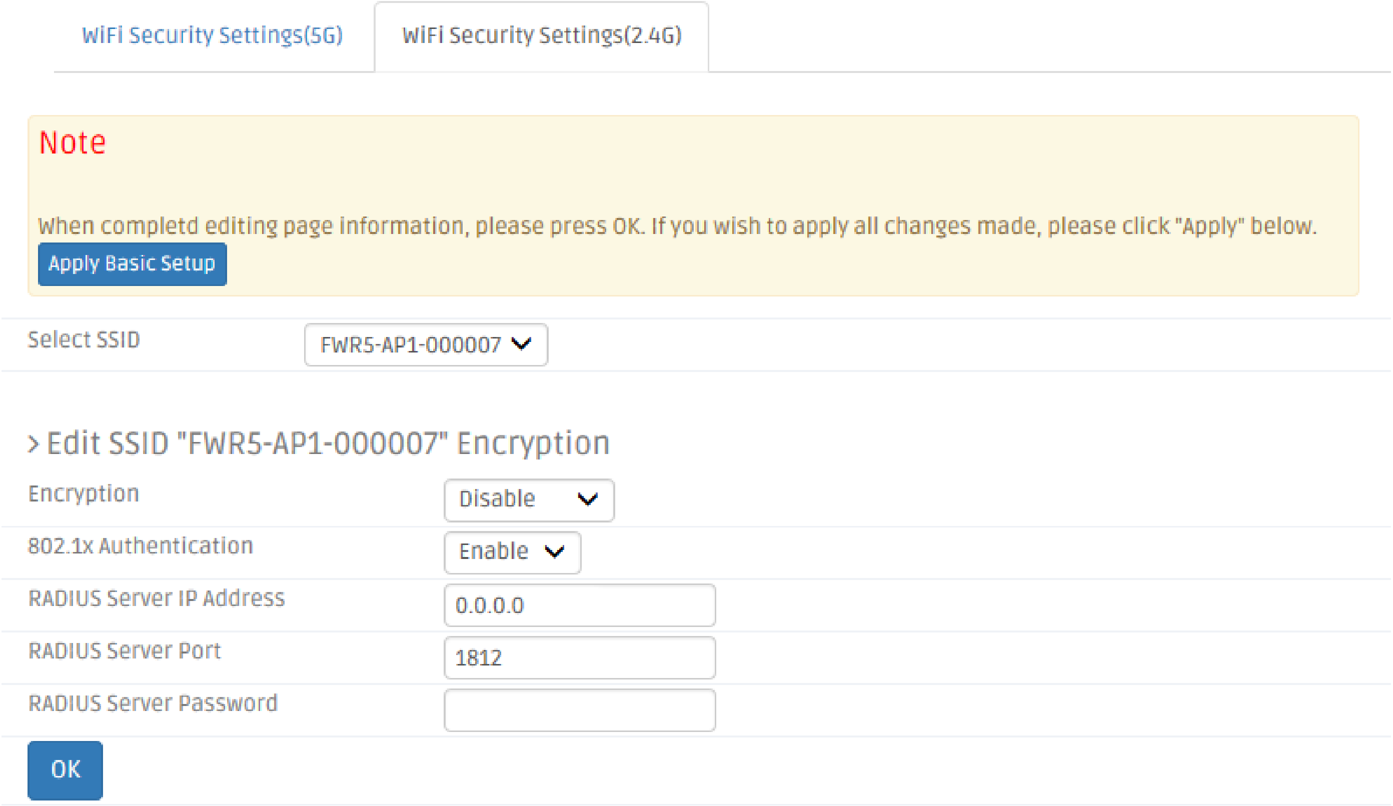
WPA 2 Cipher Suite — View-only field that shows _TKIP_ or _AES_ is currently used.

Pre-Shared Key Format — Select either _Passphrase_ (alphanumeric format) or _Hex(64characters)_ ("A-F", "a-f" and "0-9") in 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 used.

Click _Apply Basic Setup_ to submit the settings after you finish configuring this page

For Bandwidth 2.4G



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Select SSID	FWR5-AP1-000007

> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	Disable
802.1x Authentication	Enable
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

Select SSID — Select the SSID you want to configure.

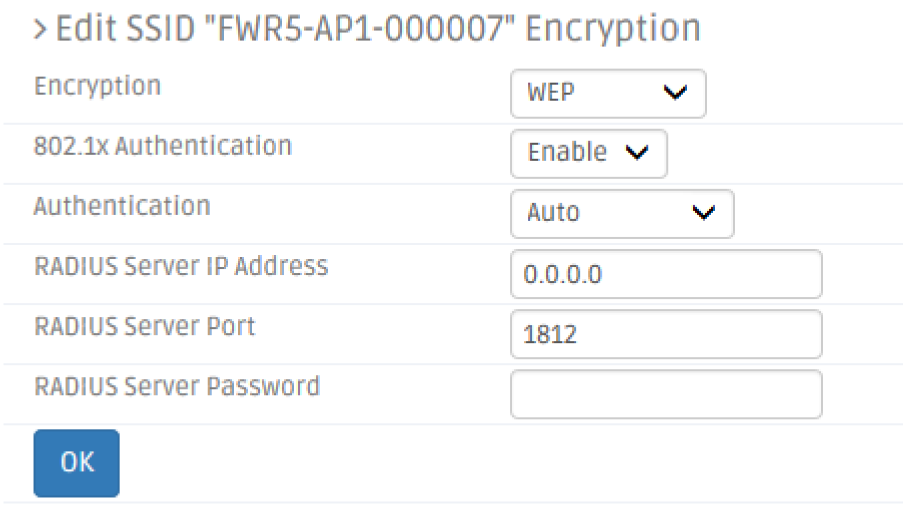
Encryption — The Residential Gateway supports four types of encryptions — *WEP*, *WPA*, *WPA2* and *WPA-Mixed*. Select one of them in the drop-down menu as the encryption of this WLAN. Or select *Disabled* if you don’t want any data encryption for this WLAN.

WEP

WEP stands for “Wired Equivalent Privacy”. It is a basic encryption method based on IEEE 802.11 standard.

802.1x Authentication — Enable or disable the 802.1x authentication for the WLAN with a RADIUS server.

If you enable ***802.1x Authentication***, please specify the values of the following parameters:



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WEP
802.1x Authentication	Enable
Authentication	Auto
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

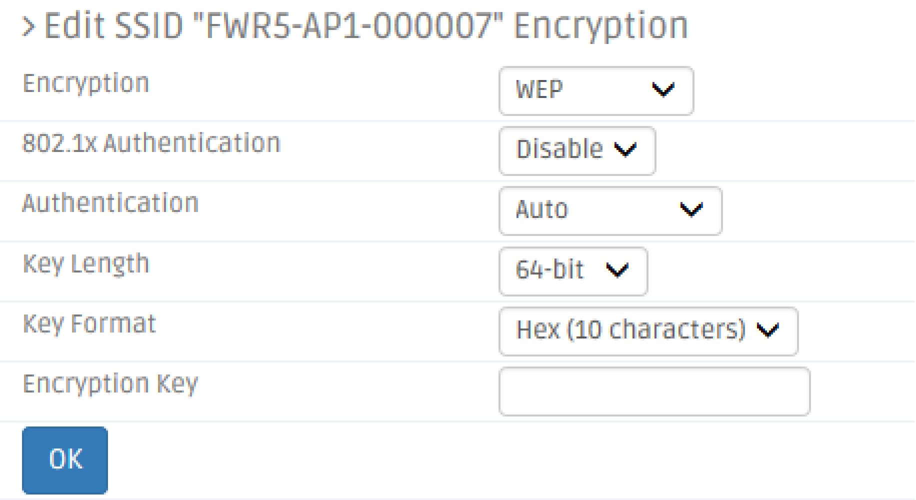
Authentication — Select *Auto*, *Open System* or *Shared Key* for authentication.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number for the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the alphanumeric password which the RADIUS server will verify.

If you disable ***802.1x Authentication***, please specify the values of the following parameters:



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WEP
802.1x Authentication	Disable
Authentication	Auto
Key Length	64-bit
Key Format	Hex (10 characters)
Encryption Key	

Authentication — Select *Auto*, *Open System* or *Shared Key* for authentication.

Key Length — Select **64 bits** or **128 bits** from the pull-down menu. The wireless client devices must have the same WEP encryption length as the Residential Gateway.

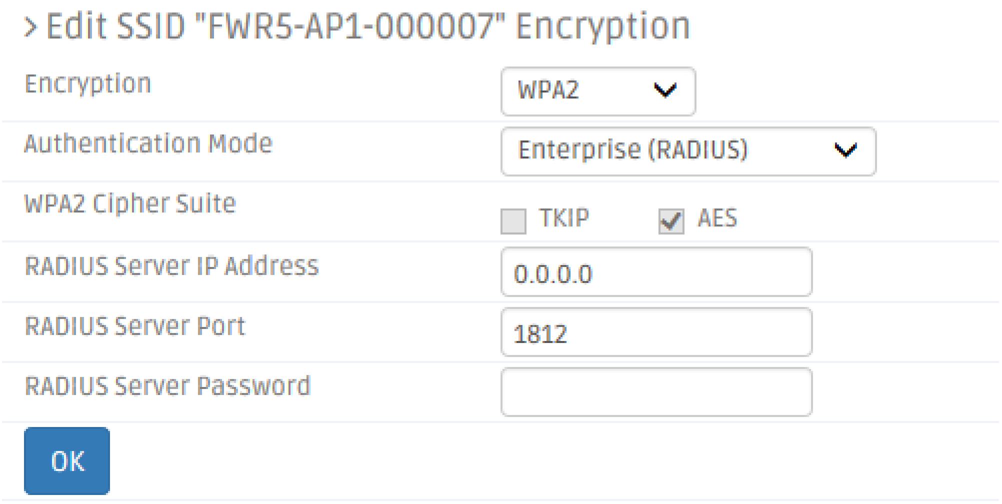
Key Format — Select **ASCII (5 characters)** or **HEX (10 characters)** from the pull-down menu as the format of the key.

Encryption Key — Specify the alphanumeric password for the WLAN.

WPA & *WPA2*

WPA stands for "Wi-Fi Protected Access". It is a kind of encryption which improves the security of WEP. It adopts two security-enhanced types to encrypt data — *TKIP* (Temporal Key Integrity Protocol) and *AES* (Advanced Encryption Standard). *AES* is a stronger encryption method than *TKIP*. *WPA2* is based on 802.11i. And it provides a stronger wireless security than *WPA*.

Authentication Mode — Select *Enterprise (RADIUS)* to ask the wireless client devices to pass the authentication of a RADIUS server. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WPA2
Authentication Mode	Enterprise (RADIUS)
WPA2 Cipher Suite	□ TKIP ☑ AES
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

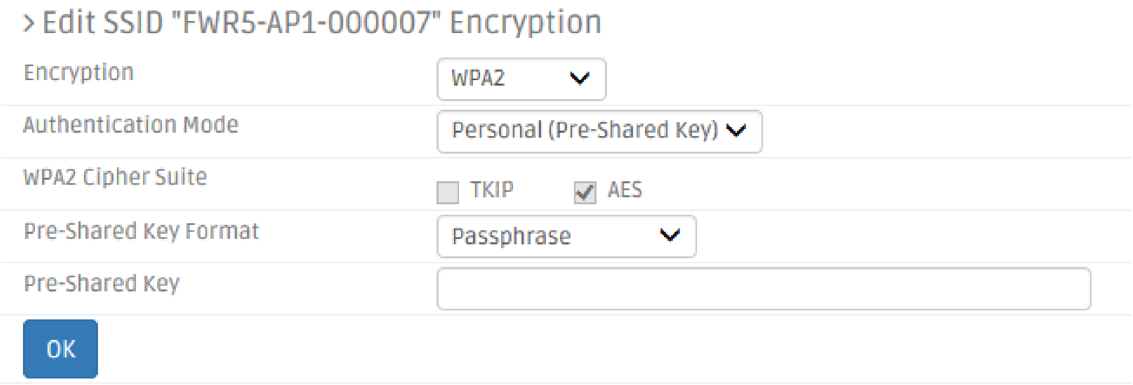
WPA2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number of the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the shared alphanumeric password which will be verified by the RADIUS server.

If you select *Personal (Pre-Shared Key)*, please specify the values of the following parameters for the wireless authentication.



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WPA2
Authentication Mode	Personal (Pre-Shared Key)
WPA2 Cipher Suite	□ TKIP ☑ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

WPA2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

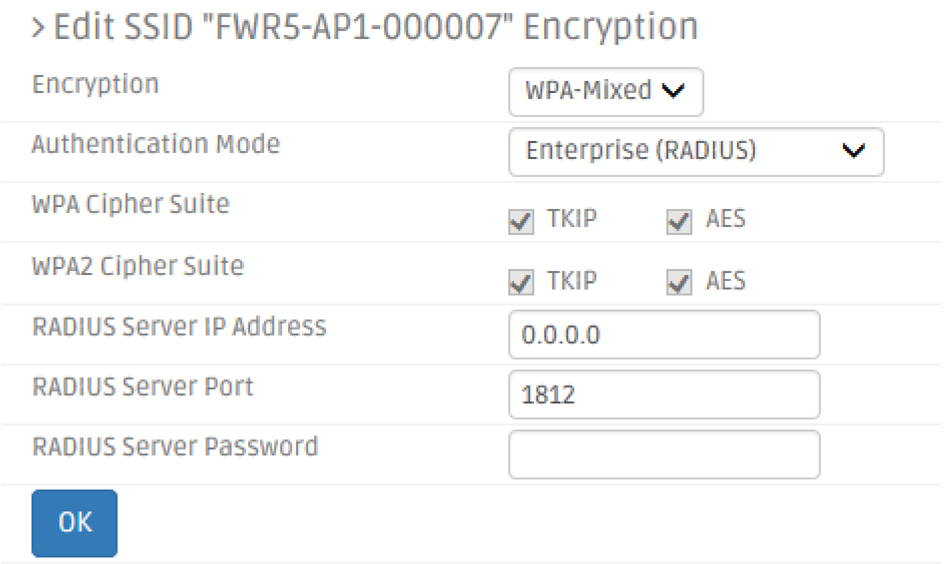
Pre-Shared Key Format — Select *Passphrase* (alphanumeric format) or *Hex(64characters)* ("A-F", "a-f" and "0-9") in the pull-down menu.

WPA 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 used.

WPA Mixed

WPA Mixed is the security mode which permits the coexistence of WPA and WPA2 clients on a WLAN. When the wireless security is set in this mode, the wireless client device can connect to the Residential Gateway with WPA/TKIP or WPA2/AES. Some older wireless client devices only support WPA/TKIP. So you have to select the mixed mode to open the WiFi service to this device.

Authentication Mode — Select *Enterprise (RADIUS)* to ask the wireless client devices to pass the authentication of a RADIUS server. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WPA-Mixed
Authentication Mode	Enterprise (RADIUS)
WPA Cipher Suite	☑ TKIP ☑ AES
WPA2 Cipher Suite	☑ TKIP ☑ AES
RADIUS Server IP Address	0.0.0.0
RADIUS Server Port	1812
RADIUS Server Password	

WPA Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

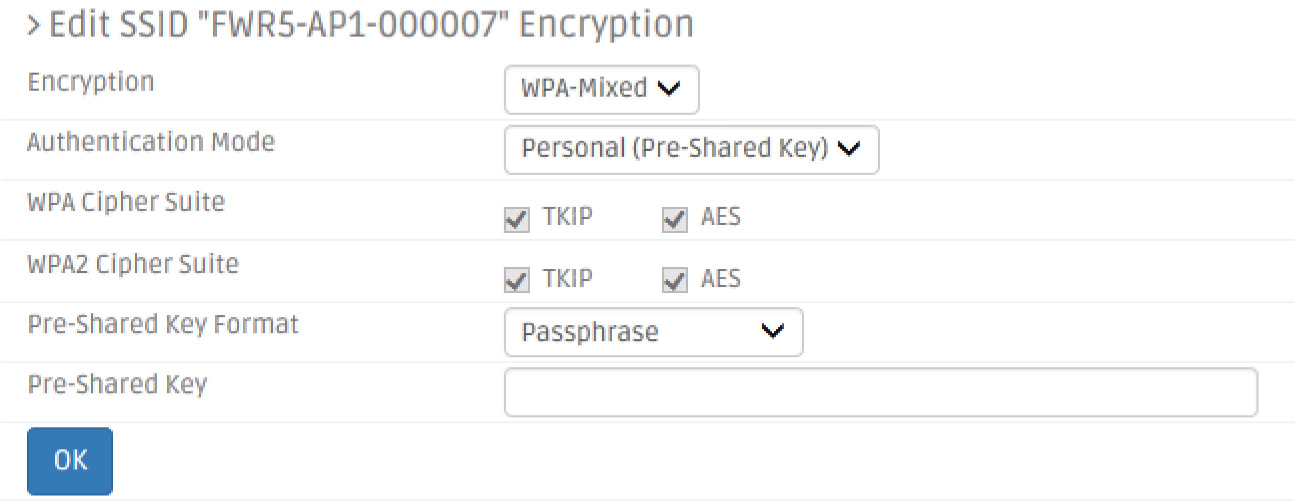
WPA 2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

RADIUS Sever IP Address — Specify the IP address of the RADIUS server in the text box.

RADIUS Server Port — Specify the port number of the RADIUS server in the text box. The default value is 1812.

RADIUS Server Password — Specify the shared alphanumeric password which will be verified by the RADIUS server.

Select *Personal (Pre-Shared Key)* as the authentication mode. And specify the values of the following parameters.



> Edit SSID "FWR5-AP1-000007" Encryption

Encryption	WPA-Mixed
Authentication Mode	Personal (Pre-Shared Key)
WPA Cipher Suite	☑ TKIP ☑ AES
WPA2 Cipher Suite	☑ TKIP ☑ AES
Pre-Shared Key Format	Passphrase
Pre-Shared Key	

WPA Cipher Suite —View-only field that shows *TKIP* or *AES* is currently used.

WPA 2 Cipher Suite — View-only field that shows *TKIP* or *AES* is currently used.

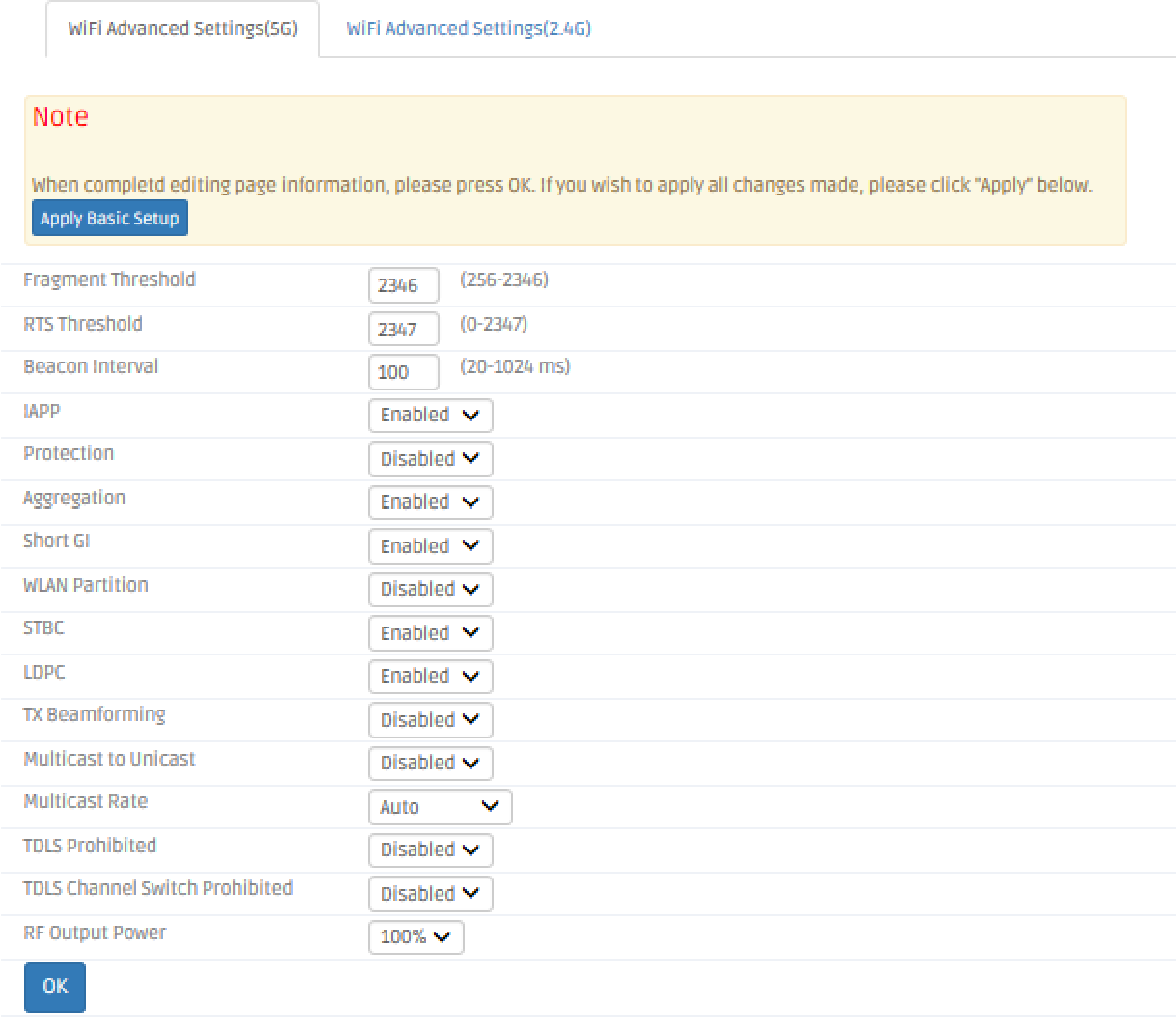
Pre-Shared Key Format — Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* (“A-F”, “a-f” and “0-9”) in the pull-down menu.

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 used.

Click *Apply* to submit the settings after you finish configuring this page

3.5.3 Wireless Advanced

For Bandwidth 5G:



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(0-2347)
Beacon Interval	100	(20-1024 ms)
IAPP	Enabled	
Protection	Disabled	
Aggregation	Enabled	
Short GI	Enabled	
WLAN Partition	Disabled	
STBC	Enabled	
LDPC	Enabled	
TX Beamforming	Disabled	
Multicast to Unicast	Disabled	
Multicast Rate	Auto	
TDLS Prohibited	Disabled	
TDLS Channel Switch Prohibited	Disabled	
RF Output Power	100%	

Fragment Threshold — Specify the fragment threshold ranging between 256-2346. The default value is 2346.

RTS Threshold — Specify the RTS threshold ranging between 0-2347. The default value is 2347.

Beacon Interval — Specify the Beacon Interval threshold ranging between 20-1024. The default value is 100.

IAPP — Click to enable or disable IAPP function.

Protection — Click to enable or disable Protection function.

Aggregation — Click to enable or disable Aggregation function.

Short GI — Click to enable or disable Short GI function.

WLAN Partition — Click to enable or disable WLAN Partition function.

STBC — Click to enable or disable STBC function.

LDPC — Click to enable or disable LDPC function.

Tx Beamforming — Click to enable or disable Tx Breamforming function.

Multicast to Unicast — Click to enable or disable Multicast to Unicast function.

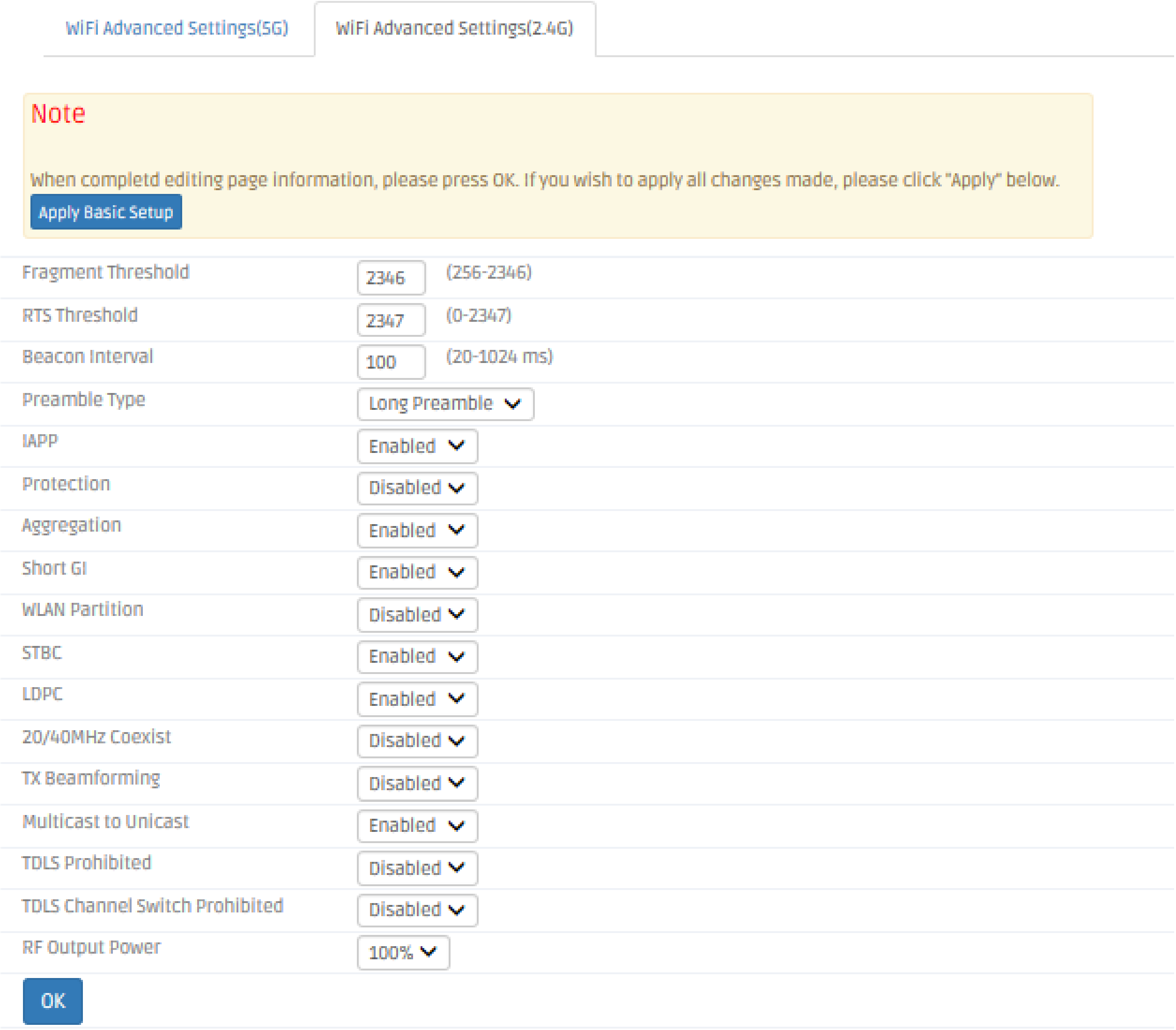
Multicast Rate — Click to specify the multicast rate.

TDLS Prohibited — Click to enable or disable TDLS Prohibited function.

TDLS Channel Switch Prohibited — Click to enable or disable TDLS Channel Switch Prohibited function.

RF Output Power — Click to select the percentage of RF Output Power level, 100%, 70%, 50%, 35% and 15% are available.

For Bandwidth 2.4G



Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(0-2347)
Beacon Interval	100	(20-1024 ms)
Preamble Type	Long Preamble	
IAPP	Enabled	
Protection	Disabled	
Aggregation	Enabled	
Short GI	Enabled	
WLAN Partition	Disabled	
STBC	Enabled	
LDPC	Enabled	
20/40MHz Coexist	Disabled	
TX Beamforming	Disabled	
Multicast to Unicast	Enabled	
TDLS Prohibited	Disabled	
TDLS Channel Switch Prohibited	Disabled	
RF Output Power	100%	

Fragment Threshold — Specify the fragment threshold ranging between 256-2346. The default value is 2346.

RTS Threshold — Specify the RTS threshold ranging between 0-2347. The default value is 2347.

Beacon Interval — Specify the Beacon Interval threshold ranging between 20-1024. The default value is 100.

Preamble Type — Click to choose Preamble Type, either Long Preamble or Short Preamble.

IAPP ─ Click to enable or disable IAPP function.

Protection ─ Click to enable or disable Protection function.

Aggregation ─ Click to enable or disable Aggregation function.

Short GI ─ Click to enable or disable Short GI function.

WLAN Partition ─ Click to enable or disable WLAN Partition function.

STBC ─ Click to enable or disable STBC function.

LDPC ─ Click to enable or disable LDPC function.

20/40MHz Coexist ─ Click to enable or disable 20/40MHz Coexist function.

Tx Beamforming ─ Click to enable or disable Tx Breamforming function.

Multicast to Unicast ─ Click to enable or disable Multicast to Unicast function.

Multicast Rate ─ Click to specify the multicast rate.

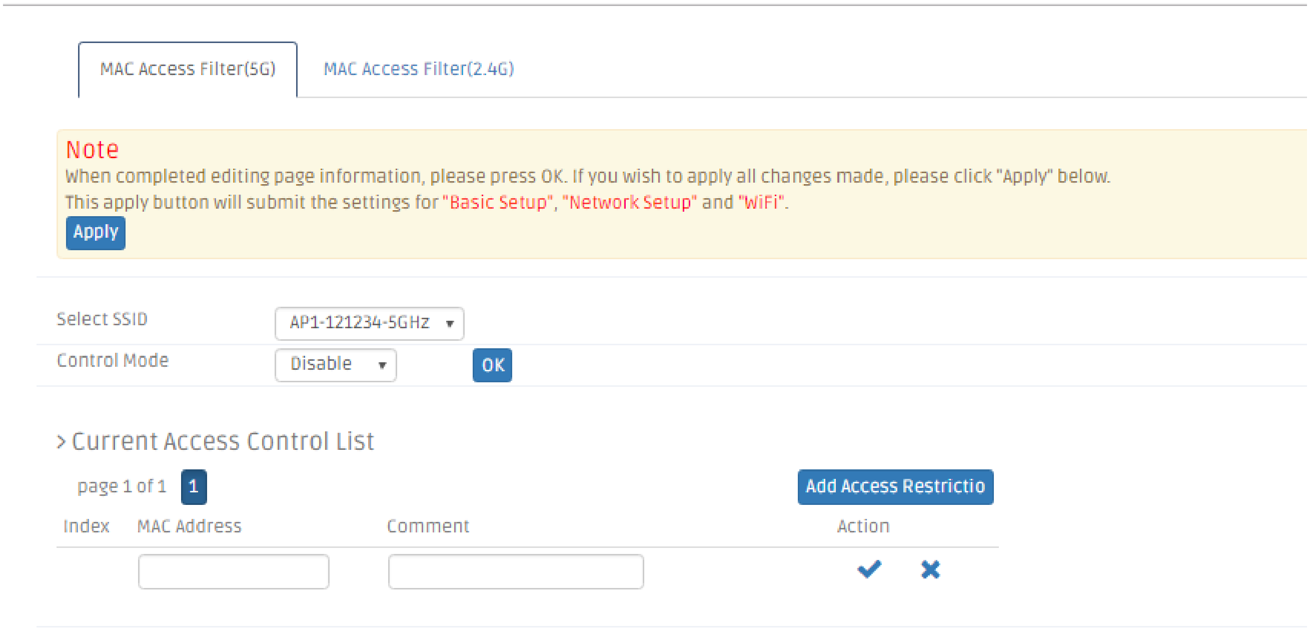
TDLS Prohibited ─ Click to enable or disable TDLS Prohibited function.

TDLS Channel Switch Prohibited ─ Click to enable or disable TDLS Channel Switch Prohibited function.

RF Output Power ─ Click to select the percentage of RF Output Power level, 100%, 70%, 50%, 35% and 15% are available.

3.5.4 MAC Access Filter

This page allows the network administrator to make its wireless access policy for the Residential Gateway. Afterwards, the Residential Gateway can deny or allow access of specific wireless client devices to its wireless network. Select **MAC Access Filter** from **WiFi** menu. Then, **MAC Access Filter** screen page appears as follows:



Note
When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "WiFi".

Select SSID: AP1-121234-5GHz
Control Mode: Disable

For details on the settings, please refer to the description of the individual section below.

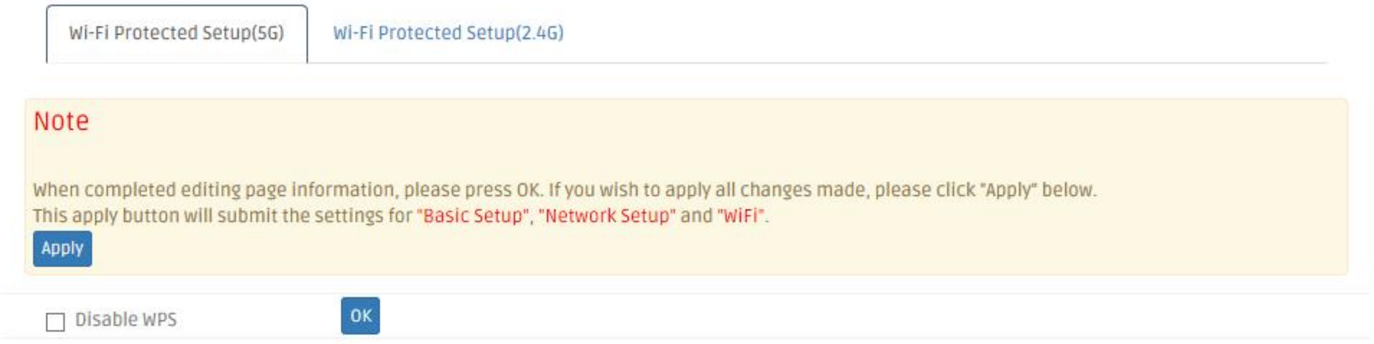
Select SSID — Choose a SSID you want to configure.

Control Mode

- Select *Disabled* to deactivate the MAC access filter feature.
- Select *Allow List* to open the WiFi service of the Residential Gateway only to the wireless clients in the list.
- Select *Deny List* to open the WiFi service of the Residential Gateway to any wireless clients except those in the list.

Current Access Control List This section enables you to create or modify an entry in the ***Current Access Control List***. Please Click ***Add Access Restriction*** and specify the MAC address (with the AAAAAAAAAAAA format) of a wireless client in the ***MAC Address*** text box to add it to the list. Specify a description in the ***Comment*** text box if you need to. And click *Check Icon* to apply the changes in the text boxes to the list. Or click *Reset* to clear all the values in the text boxes.

3.5.5 WPS



Wi-Fi Protected Setup(5G) | Wi-Fi Protected Setup(2.4G)

Note

When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.
This apply button will submit the settings for "Basic Setup", "Network Setup" and "WiFi".

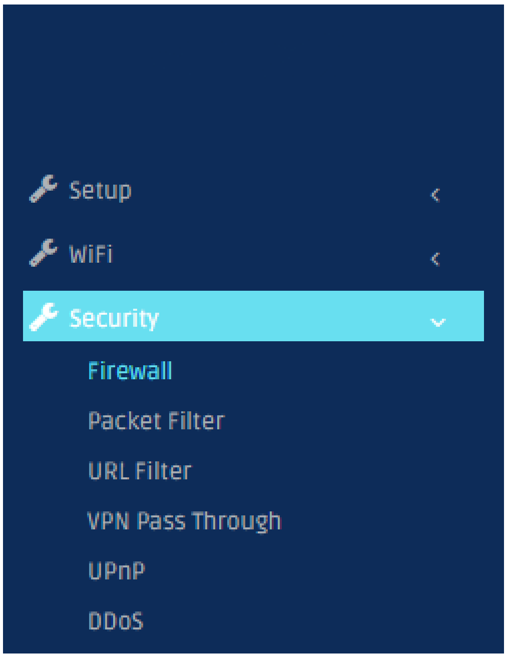
Apply

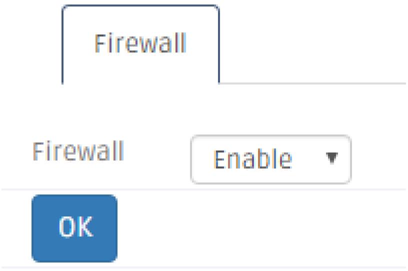
□ Disable WPS OK

Disable WPS – Check the box to disable WPS function. WPS stands for "Wi-Fi Protected Setup". It is a standard which makes the WiFi security simpler and easier.

3.6 Security

Select **Security** in the Main Menu bar. And the sub-items – **Firewall**, **Packet Filter, URL Filter and VPN Pass Through** – will show up on the sub menu bar.





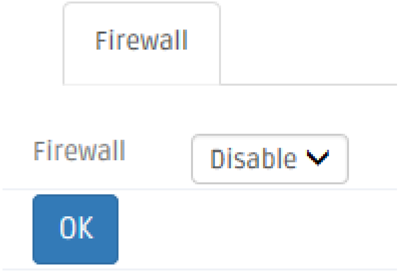
Firewall

Firewall Enable

OK

3.6.1 Firewall

Select **Firewall** in the sub menu bar for **Security**. Then, the following screen page will appear



Firewall: Disable

This section allows you to enable or disable the firewall protection of the Residential Gateway. When the firewall protection is enabled, the Residential Gateway will inspect the packets which are transmitted from the public network to its private network.

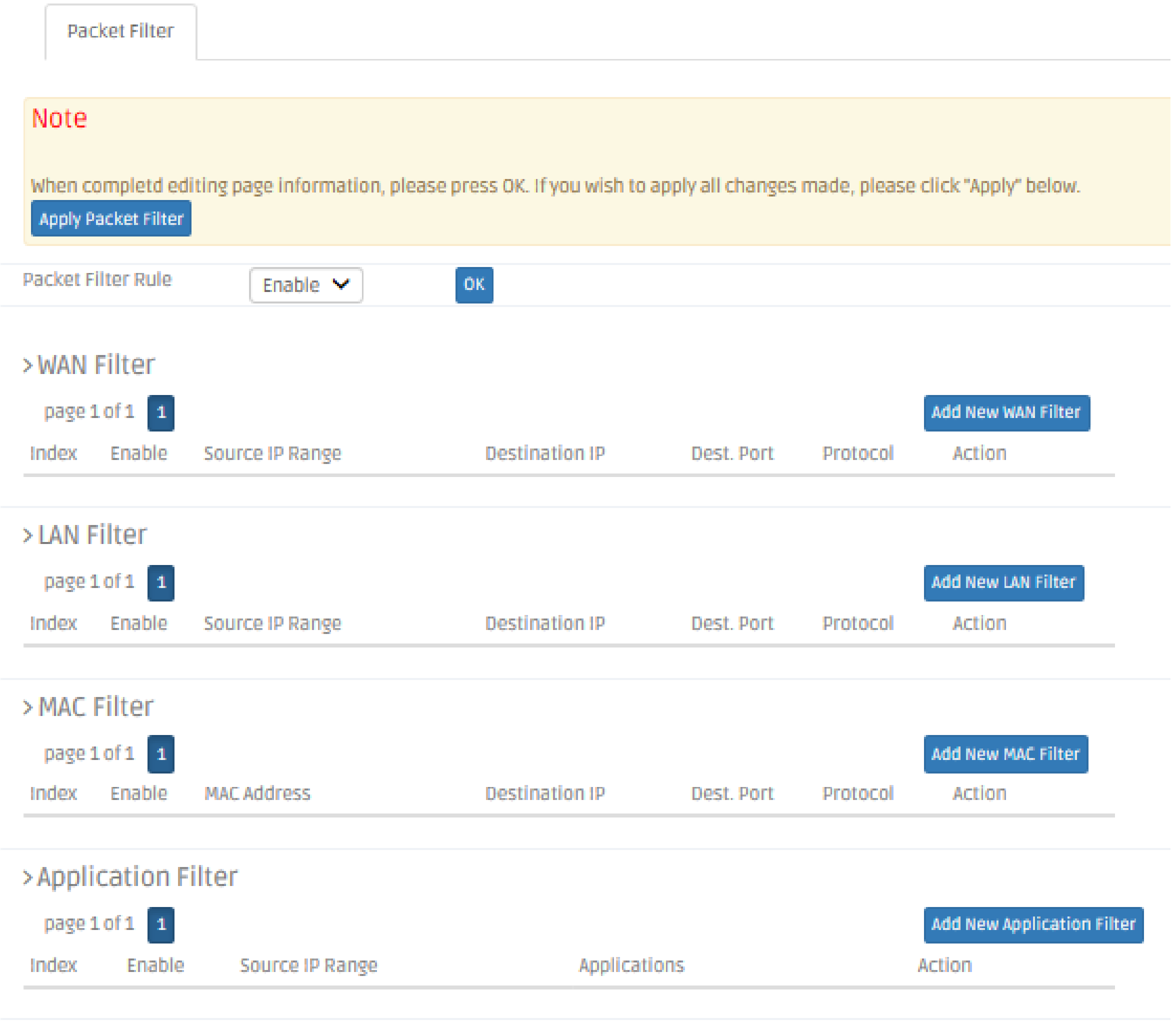
Note: *When you disable the firewall protection, the security features such as "Packet Filter" and "URL Filter" will stop working.*

Click *OK* to submit your settings after you finish configuring this page.

3.6.2 Packet Filter

This function enables the Residential Gateway to filter out the unwanted packets according to the IP address, the source MAC address or the application protocol. So the network administrator can set up the access policies on the Residential Gateway.

Select **Packet Filter** in the sub menu bar of **Security**. Then, **Packet Filter** screen page appears as follows:



Packet Filter

Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Apply Packet Filter

Packet Filter Rule: Enable | OK

> WAN Filter

page 1 of 1 | 1 | Add New WAN Filter

Index	Enable	Source IP Range	Destination IP	Dest. Port	Protocol	Action

> LAN Filter

page 1 of 1 | 1 | Add New LAN Filter

Index	Enable	Source IP Range	Destination IP	Dest. Port	Protocol	Action

> MAC Filter

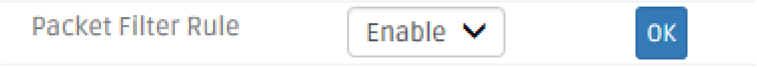
page 1 of 1 | 1 | Add New MAC Filter

Index	Enable	MAC Address	Destination IP	Dest. Port	Protocol	Action

> Application Filter

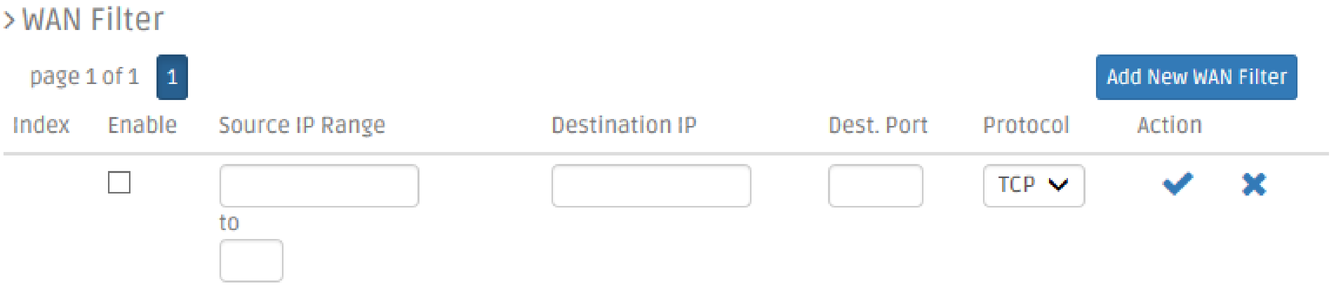
page 1 of 1 | 1 | Add New Application Filter

Index	Enable	Source IP Range	Applications	Action



Packet Filter Rule: Enable | OK

Packet Filter Rule Enable or disable the packet filter function. When it is enabled, the Residential Gateway will drop packets which meet predetermined conditions of the rules in the following sections.



> WAN Filter

page 1 of 1 | 1 | Add New WAN Filter

Index	Enable	Source IP Range	Destination IP	Dest. Port	Protocol	Action
	□	to			TCP	✓ ✖

WAN Filter This section allows you to edit the WAN filter rules. The WAN filter rule will block packets which are received by the Residential Gateway from the public network and match the pre-determined condition of the rule. Below is an explanation for each column of the rule table.

Enable — Enable or disable this WAN filter rule.

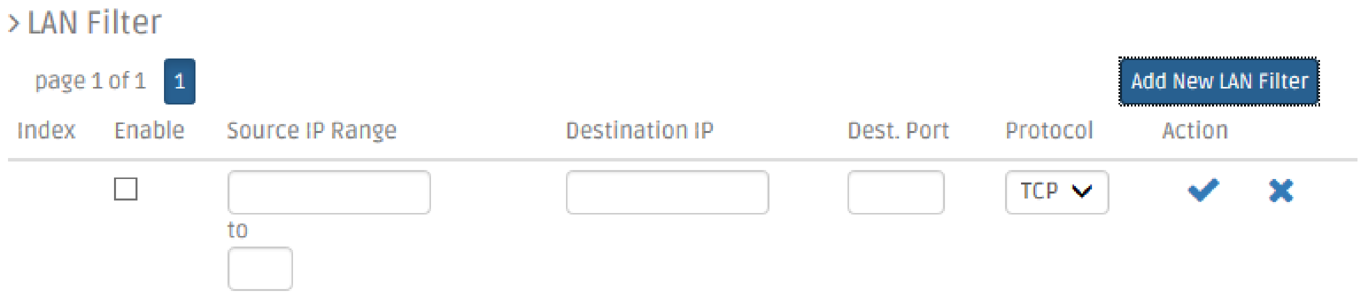
Source IP Range — Specify an IP address range for the WAN filter rule to block packets whose source IP addresses are in this range.

Destination IP — Specify an IP address range for the WAN filter rule to block packets whose destination IP addresses are in this range.

Dest. Port — Specify the destination port number of the packets which the WAN filter rule will block.

Protocol — Select *TCP* or *UDP* in the pull-down menu for the WAN filter rule to block packets of this communication protocol.

Actions — Click *Add New WAN Filter* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.



> LAN Filter

page 1 of 1 1

Index	Enable	Source IP Range	Destination IP	Dest. Port	Protocol	Action
	☐	to			TCP	✓ ✗

LAN Filter This section allows you to edit the rule table for the LAN filter. The LAN filter will block packets which are received by the Residential Gateway from the private network and match the pre-determined condition of any entry in the rule table. Below is a description for each column of this table.

Enable — Select the checkbox to enable this rule.

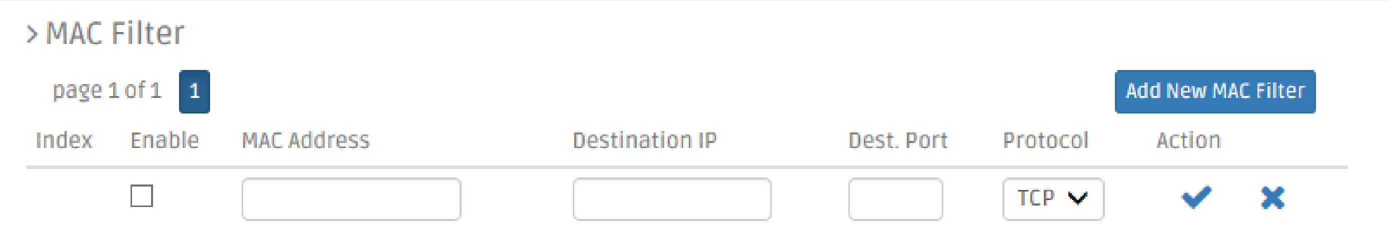
Source IP Range — Specify an IP address range for the LAN filter to block packets whose source IP addresses are in this range.

Destination IP — Specify an IP address range for the LAN filter to block packets whose destination IP addresses are in this range.

Dest. Port — Specify the destination port number of the packets which the LAN Filter will block.

Protocol — Select *TCP* or *UDP* in the pull-down menu as the communication protocol of the packets which the LAN filter will block.

Actions — Click *Add New LAN Filter* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.



> MAC Filter

page 1 of 1 1

Add New MAC Filter

Index	Enable	MAC Address	Destination IP	Dest. Port	Protocol	Action
	□				TCP	✓ ✗

MAC Filter This section allows you to edit the rule table for the LAN filter. The LAN filter will block packets which are received by the Residential Gateway from the private network and match the pre-determined condition of any entry in the rule table. Below is a description for each column of this table.

This section allows you to edit the MAC filter rules in the table. The Residential Gateway will drop packets which match the pre-determined condition of any entry in this table. Below is a description of each column in this table.

Enable — Select the checkbox if you want to enable this rule.

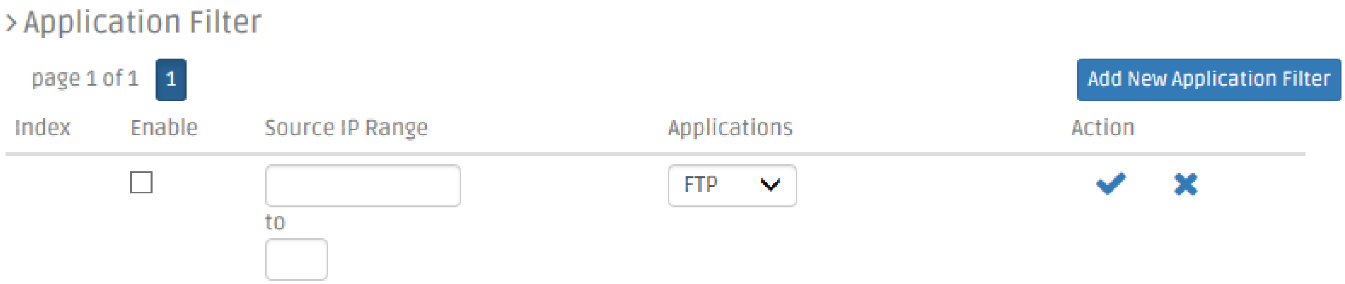
MAC Address — Specify the MAC address of the packet which will be denied by this rule.

Destination IP — Specify the destination IP address of the packets which will be denied by this rule.

Dest. Port — Specify the destination port number of the packet which will be denied by this rule.

Protocol — Select *TCP* or *UDP* in the pull-down menu as the communication protocol inside the packet which will be denied by this rule.

Actions — Click *Add New MAC Filter* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.



> Application Filter

page 1 of 1 1

Add New Application Filter

Index	Enable	Source IP Range	Applications	Action
	□	to	FTP	✓ ✗

Application Filter This section allows you to edit the table of application filter rules. The Residential Gateway will drop packets when it receives packets which match the entries in the rule table. Below is a description of configuration parameters in this table.

Enable — Select the checkbox if you want to enable this rule.

Source IP Range — Specify the source IP address range of the packets which will be denied by this rule.

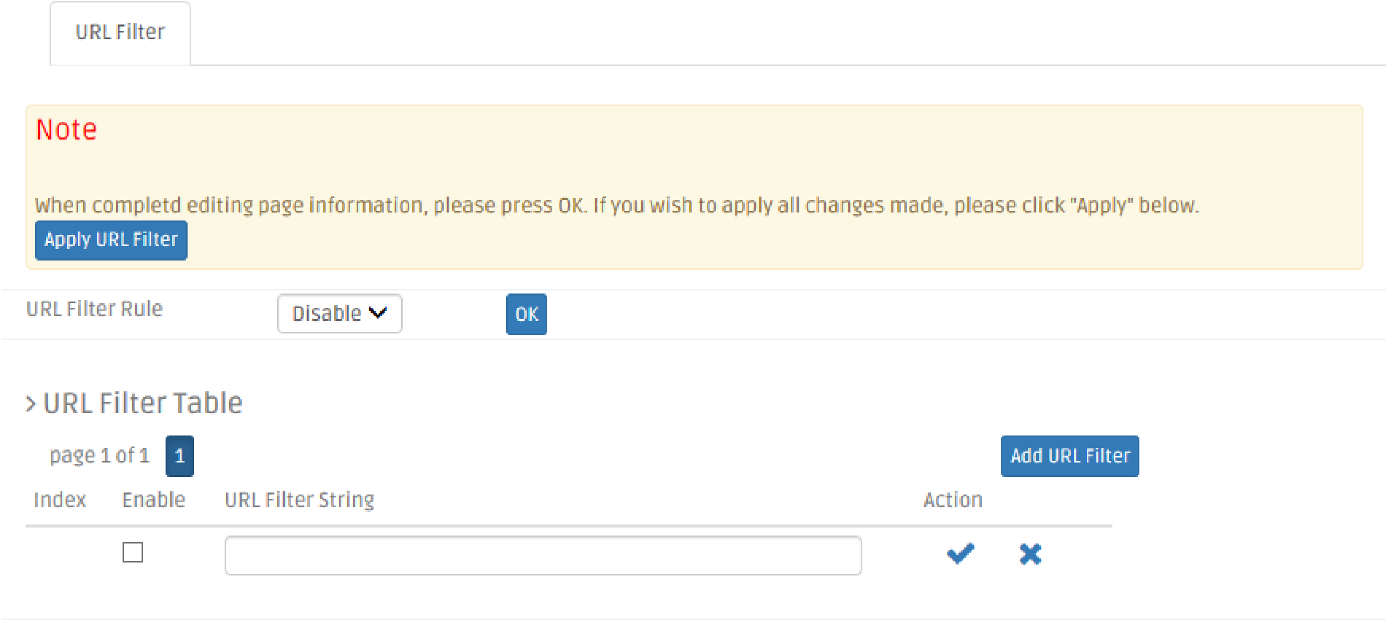
Application — The drop-down menu offers the most widely used Internet applications, including *FTP*, *SSH*, *Telnet*, *SMTP*, *DNS*, *HTTP*, *POP*, *NNTP*, *IMAP*, *SNMP*, and *HTTPS*. Select an application whose packets will be denied by this filter rule.

Actions — Click *Add New Application Filter* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.

Click *Apply Packet Filter* to submit your settings after you finish configuring this page.

3.6.3 URL Filter

URL Filter enables the network administrator to deny computers to access the specific websites on the Internet from the private network of the Residential Gateway. Select **URL Filter** from the **Security** sub menu bar. Then, **URL Filter** screen page appears as follows:


URL Filter

Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Apply URL Filter

URL Filter Rule: Disable

OK

> URL Filter Table

page 1 of 1 | 1

Add URL Filter

Index	Enable	URL Filter String	Action
	□		✓ ✖

For details on the settings, please refer to the description of the individual section below.

URL Filter Rule Enable or disable the URL filter function. When it is enabled, the Residential Gateway will drop packets whose destination URL addresses are specified in the URL filter rules.

URL Filter Table This section contains a table for the URL filter rules. The URL filter rules will prevent the hosts on the private network to visit the specified URL addresses on the Internet. You can create or modify a URL filter rule in the text boxes of the rule table. Below is a description of configuration parameters in this table.

Enable — Select the checkbox if you want to enable this rule.

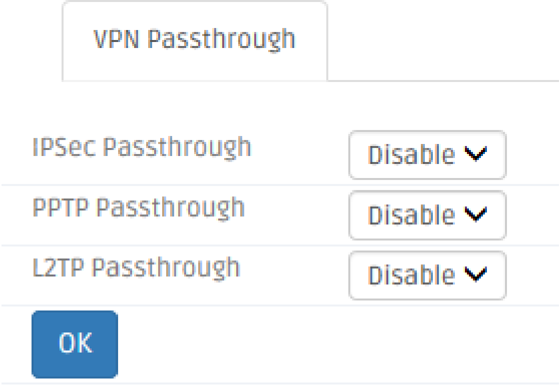
URL Filter String — Specify the URL address which this rule will allow or deny.

Action — Click *Add URL Filter* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.

Click *Apply URL Filter* to submit your settings after you finish configuring this page.

3.6.4 VPN Pass Through

This feature enables the VPN traffic to be transmitted from the private network of the Residential Gateway to the public network. So the VPN client on the private network can establish a VPN tunnel to the remote VPN server. Select **VPN pass through** from the **Security** sub menu bar. Then, **VPN pass through** screen page appears as follows:



VPN Passthrough

IPSec Passthrough: Disable

PPTP Passthrough: Disable

L2TP Passthrough: Disable

For details on the settings, please refer to the description of the individual section below.

VPN Pass Through The Residential Gateway supports VPN pass through of the most popular VPN tools - IPSec (IP Security), PPTP and L2TP. This section allows you to enable the VPN pass through feature for any of these tools which the VPN client on the private network uses. Below is a description of configuration parameters in this section.

IPSec Pass Through — Enable or disable IPSec pass through on the Residential Gateway. IPSec stands for “Internet Protocol Security”. It is a suite of protocols for secure exchange of packets at the IP layer.

PPTP Pass Through — Enable or disable PPTP pass through on the Residential Gateway. PPTP stands for “Point-to-Point Tunneling Protocol”. And PPTP pass through is a feature which allows the Point-to-Point Protocol to be tunneled through an IP network.

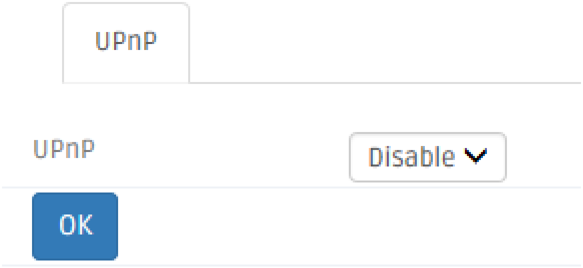
L2TP Pass Through — Enable or disable the L2TP pass through on the Residential Gateway. L2TP stands for “Layer 2 Tunneling Protocol”. It is used to enable Point-to-Point sessions via the Internet on the Layer 2 level.

Click *OK* to submit your settings after you finish configuring this page.

3.6.5 UPnP

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. An UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically.

Select **UPnP** from the **Security** sub menu bar. Then, this screen page appears as follows:



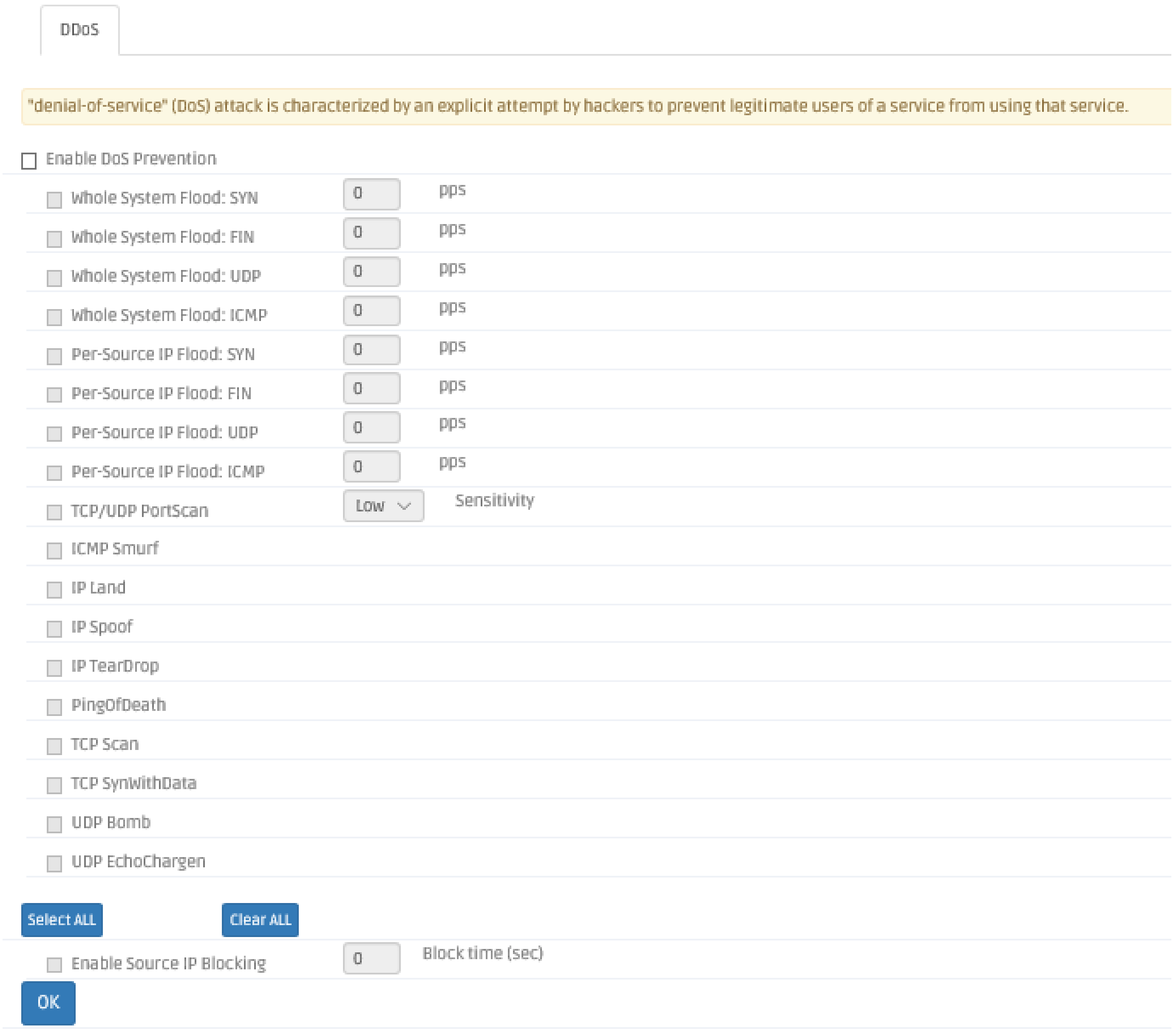
UPnP

UPnP Disable

Click this drop-down box then click OK button to enable UPnP feature. UPNP provides compatibility with networking equipment, software and peripherals.

3.6.6 DDoS

The Residential Gateway supports DDoS Prevention. DDoS stands for “Distributed Denial of Service”. It is a Hacker’s attack from a multitude of compromised systems to a target. It will cause the target to deny the service for normal users. Select **DDoS** from the **Security** sub menu bar. Then, **DDoS** screen page appears as follows:



DDoS

"denial-of-service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.

☐ Enable DoS Prevention

☐ Whole System Flood: SYN	0	pps
☐ Whole System Flood: FIN	0	pps
☐ Whole System Flood: UDP	0	pps
☐ Whole System Flood: ICMP	0	pps
☐ Per-Source IP Flood: SYN	0	pps
☐ Per-Source IP Flood: FIN	0	pps
☐ Per-Source IP Flood: UDP	0	pps
☐ Per-Source IP Flood: ICMP	0	pps
☐ TCP/UDP PortScan	Low	Sensitivity
☐ ICMP Smurf		
☐ IP Land		
☐ IP Spoof		
☐ IP TearDrop		
☐ PingOfDeath		
☐ TCP Scan		
☐ TCP SynWithData		
☐ UDP Bomb		
☐ UDP EchoChargen		

☐ Enable Source IP Blocking — 0 — Block time (sec)

This section allows you to configure the DDoS prevention feature to prevent the Residential Gateway from malicious attacks. Below is a description of configuration parameters in this section.

Enable DoS Prevention — Tick the checkbox to activate DDoS prevention manually. And select the kinds of DDoS attacks to enable the Residential Gateway to detect them. Or untick the checkbox to disable this feature. But note that when the feature is disabled, the Residential Gateway will be vulnerable to DDoS attacks.

Whole System Flood: SYN — Tick the checkbox to prevent a SYN attack. A SYN attack will interrupt the process of the three way handshake of TCP and redirect the acknowledge response to a malicious IP address. Or it will cause the targeted system to be flooded with false SYN requests.

Whole System Flood: FIN — Tick the checkbox to prevent a FIN flood. This attack will flood the network with connection resets from an invalid IP address.

Whole System Flood: UDP — Tick the checkbox to prevent a flood of large numbers of raw UDP packets targeted at the Residential Gateway.

Whole System Flood: ICMP — Tick the checkbox to prevents a flood of ICMP messages from an invalid IP address. This attack can cause all TCP requests to be halted.

Per Source IP Flood: SYN — Tick the checkbox to prevent a SYN attack on a specified IP address.

Per Source IP Flood: FIN — Tick the checkbox to prevent a FIN attack on the LAN port IP address.

Per Source IP Flood: UDP — Tick the checkbox to prevent a UDP attack on the LAN port IP address.

Per Source IP Flood: ICMP — Tick the checkbox to prevent an ICMP attack on the LAN port IP address.

TCP/UDP Port Scan — Tick the checkbox to prevent a series of systematic queries to the Residential Gateway for open ports through which to route traffic.

ICMP Smurf — Tick the checkbox to prevent the hacker to forge the IP address of the Residential Gateway and send repeated ping requests to it flooding the network.

IP Land — Tick the checkbox to prevent an attack which involves a synchronized request being sent as part of the three way handshake of TCP to an open port specifying the port as both the source and destination effectively locking the port.

IP Spoof — Tick the checkbox to prevent a hacker to create an alias IP address of the Residential Gateway to which all traffic is redirected.

IP Teardrop — Tick the checkbox to prevent a Teardrop attack. A Teardrop attack sends mangled IP fragments with overlapping, over-sized, payloads to the Residential Gateway. The fragmented packets are processed by the Residential Gateway and will cause it to crash.

PingofDeath — Tick the checkbox to prevent the Residential Gateway to receive oversized ping packets which it cannot handle. The Ping of Death attack will send packets which exceed the maximum IP packet size of 65,535 bytes.

TCP Scan — Tick the checkbox to prevent the Residential Gateway to be probed by a hacker for open TCP ports to then block.

TCP SynWithData — Tick the checkbox to prevent the hacker to send a volume of requests for connections that cannot be completed.

UDP Bomb — Tick the checkbox to prevent the hacker congesting the network by a flood of UDP packets between him and the Residential Gateway using the UDP chargen service.

UDP EchoChargen — Tick the checkbox to prevent the hacker from sending a UDP packet to the echo server with a source port set to the chargen port.

packets/second — Specify the number of packets per second that you want to scan for malicious activity.

Sensitivity — Select *High* or *Low* from the pull-down menu for the sensitivity of the TCP/UDP port scan prevention.

Click *Select All* to select all of kinds of DDoS attacks in the checkboxes. Or click *Clear all* to unselect all of the checkboxes.

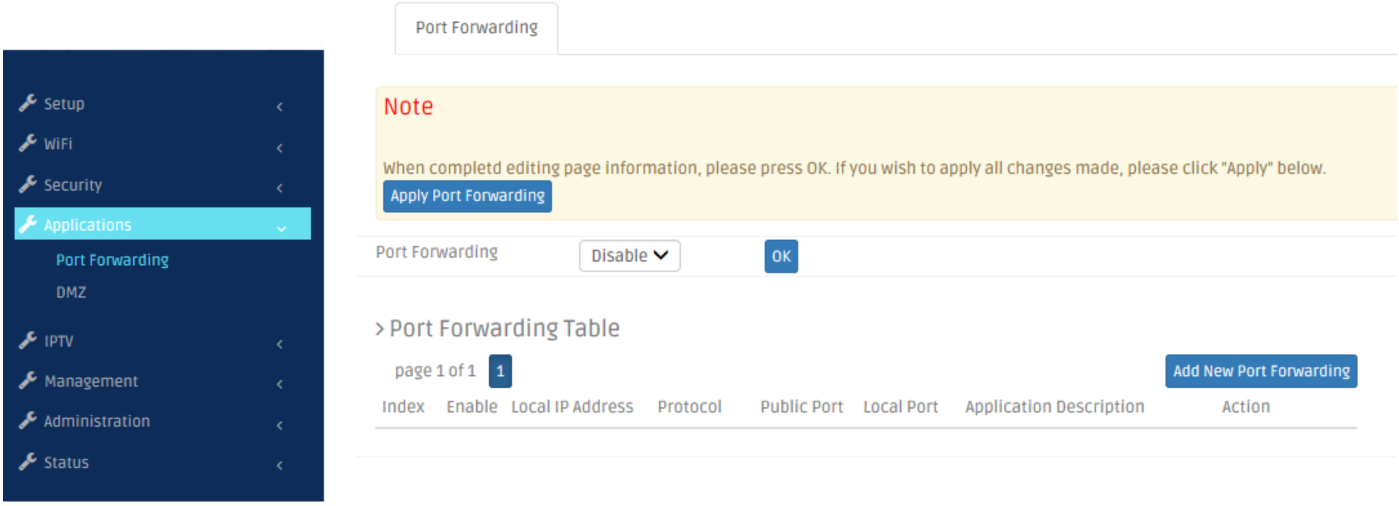
Enable Source IP Blocking — Tick the checkbox to block the IP.

Blocking Time — Specify the time to block the IP.

Click *OK* to submit your settings after you finish configuring this page.

3.7 Application

Select **Application** in the Main Menu bar. And the sub-items – **Port Forwarding** and **DMZ** – will show up on the sub menu bar.



When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Port Forwarding: Disable

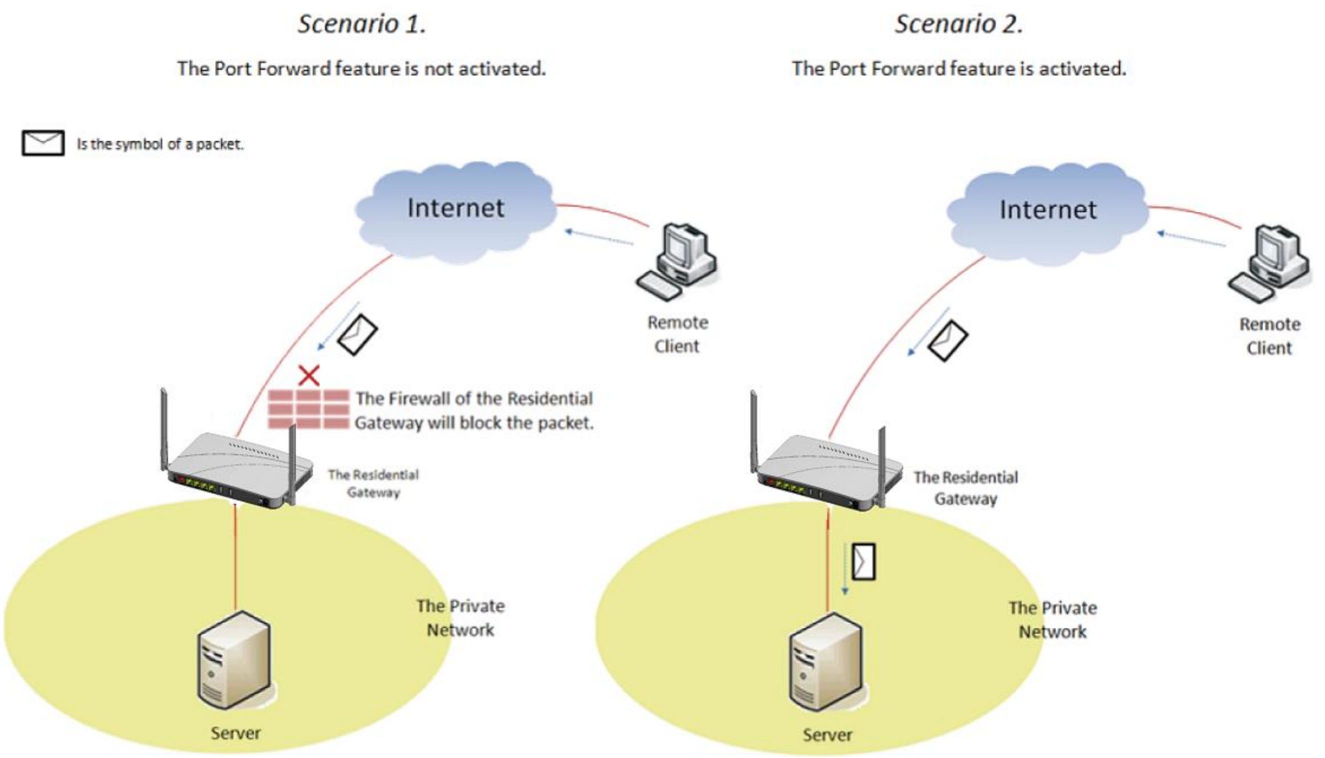
> Port Forwarding Table

page 1 of 1

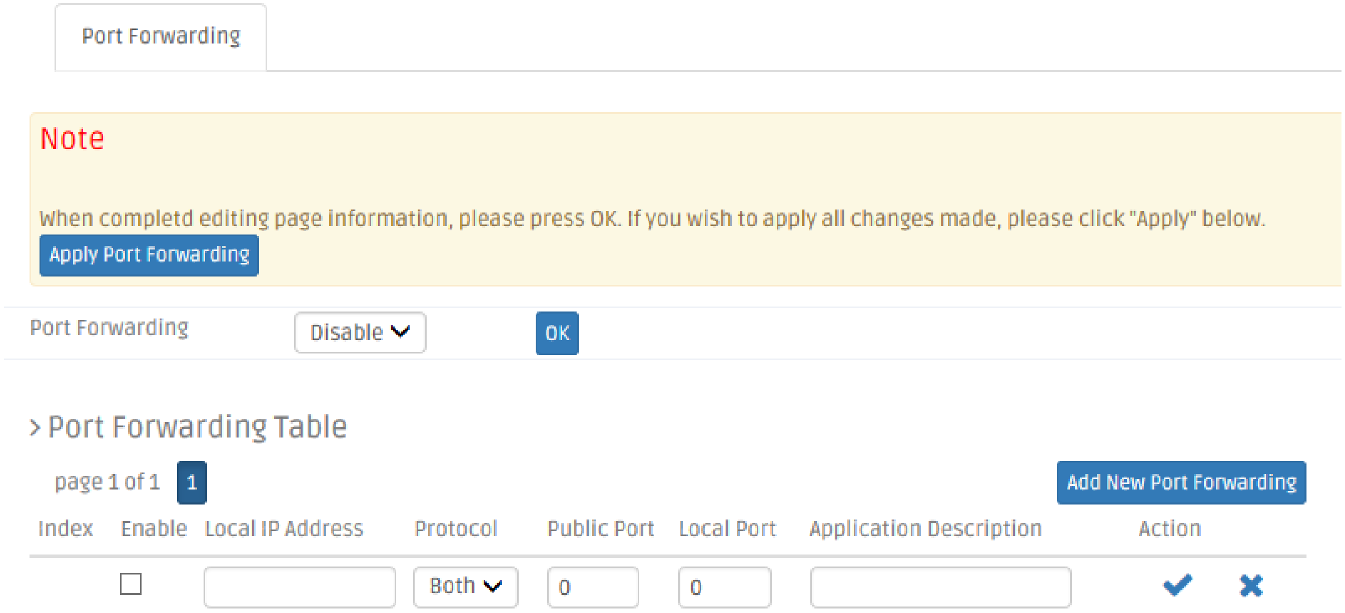
Index	Enable	Local IP Address	Protocol	Public Port	Local Port	Application Description	Action

3.7.1 Port Forwarding

A host on the private network of the Residential Gateway is invisible from the Internet for it is protected by the firewall. Therefore, when a server is on the private network, its service will be inaccessible from the Internet. To open the service to hosts on the Internet, the network administrator may adopt Port Forwarding feature. Port Forwarding allows an IP address on the private network to be accessed from an IP address on the public network. It will redirect packets from the public network to a specified private IP address if the packets meet the pre-condition of a port forwarding rule. The diagram below compares the two scenarios when the Port Forwarding feature is enable and when it is not.


Scenario 1.
The Port Forward feature is not activated.
Scenario 2.
The Port Forward feature is activated.
Is the symbol of a packet.
Internet
Remote Client
The Firewall of the Residential Gateway will block the packet.
The Residential Gateway
The Private Network
Server
Internet
Remote Client
The Residential Gateway
The Private Network
Server

Select **Port Forwarding** from the **Application** sub menu bar. Then, the screen page appears as follows:



Port Forwarding

Note

When completd editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Apply Port Forwarding

Port Forwarding: Disable OK

› Port Forwarding Table

page 1 of 1 1 Add New Port Forwarding

Index	Enable	Local IP Address	Protocol	Public Port	Local Port	Application Description	Action
	☐		Both	0	0		✓ ✖

Port Forwarding Table This section allows you to create or modify a port forwarding rule which will be executed by the Residential Gateway. Below is a description of configuration parameters in this section.

Enable — Select the checkbox if you want to enable this rule.

Protocol — Choose *TCP*, *UDP* or *Both* in the pull-down menu as your desired protocol.

Public Port — Specify the port number which the packets from the Internet are destined to (1~65535).

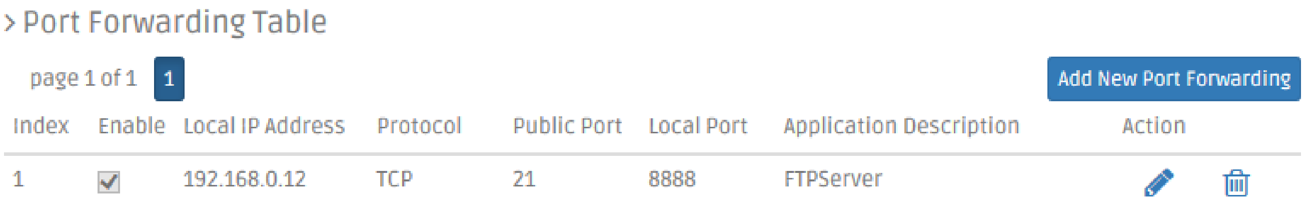
Local Port — Specify the port number which the packets are destined to (1~65535).

Application Description — Enter a brief description for this entry if you want to.

Action — Click *Add New Port Forwarding* to add a new rule to the table after you configure it in the text boxes. Then, click *Check Icon* to submit the new settings. If you need to remove any entry from this table, click *Cross Icon*.

Click *Add New Port Forwarding* to submit your settings after you finish configuring a rule in the text boxes.

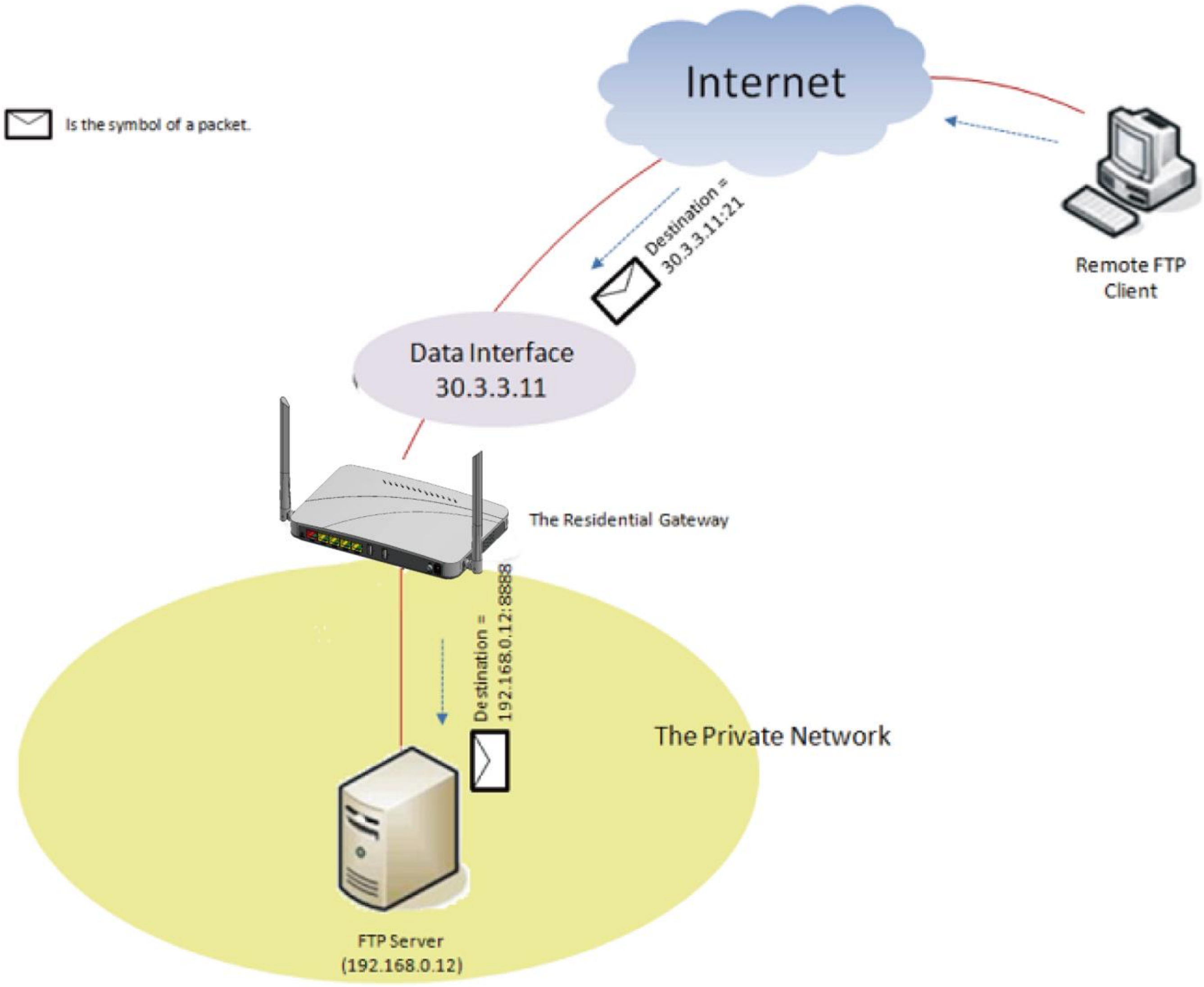
The example below illustrates how the Residential Gateway will execute a port forwarding rule in the table.



> Port Forwarding Table

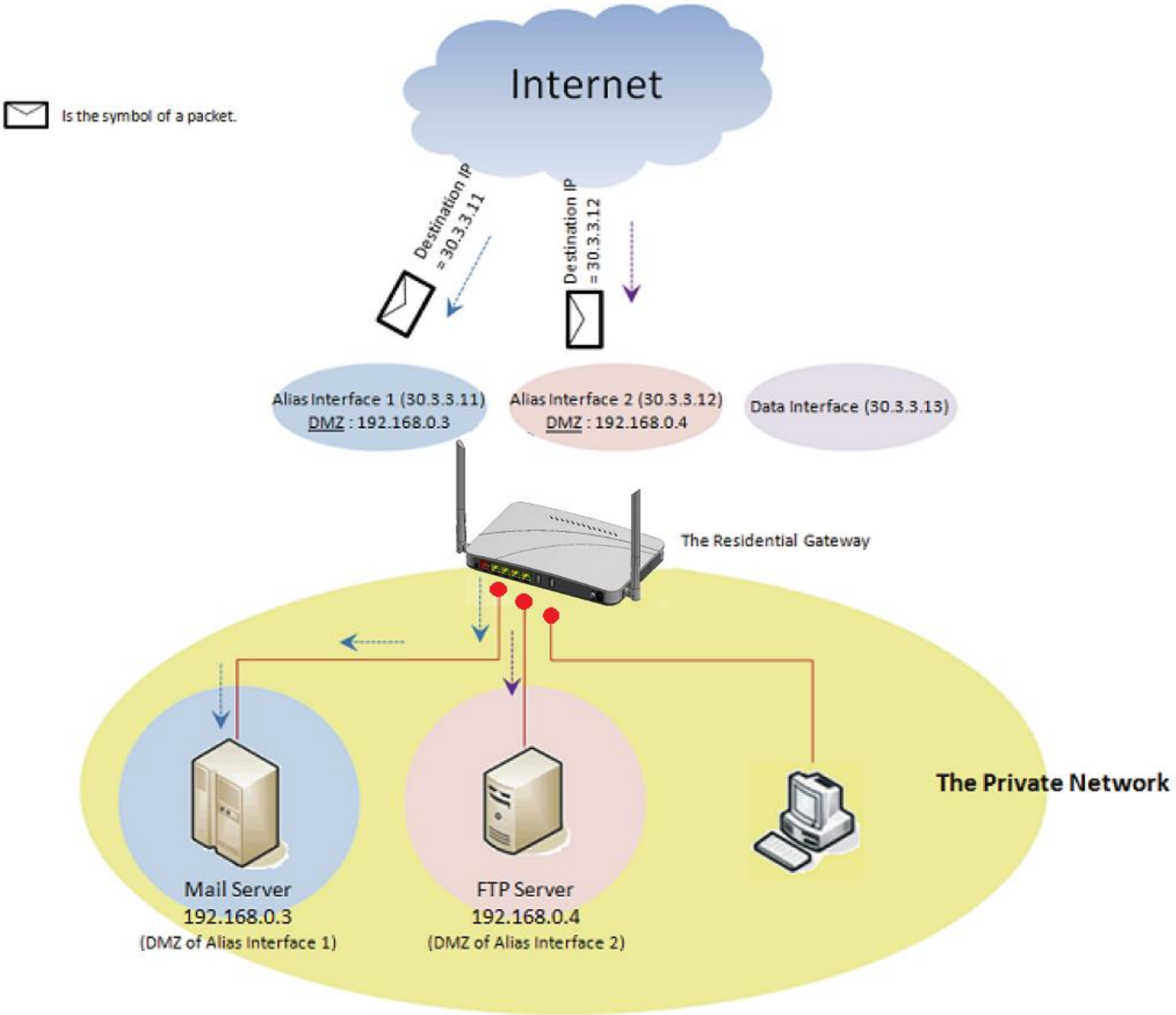
page 1 of 1 | 1 | Add New Port Forwarding

Index	Enable	Local IP Address	Protocol	Public Port	Local Port	Application Description	Action
1	☑	192.168.0.12	TCP	21	8888	FTPServer	✎ 🗑

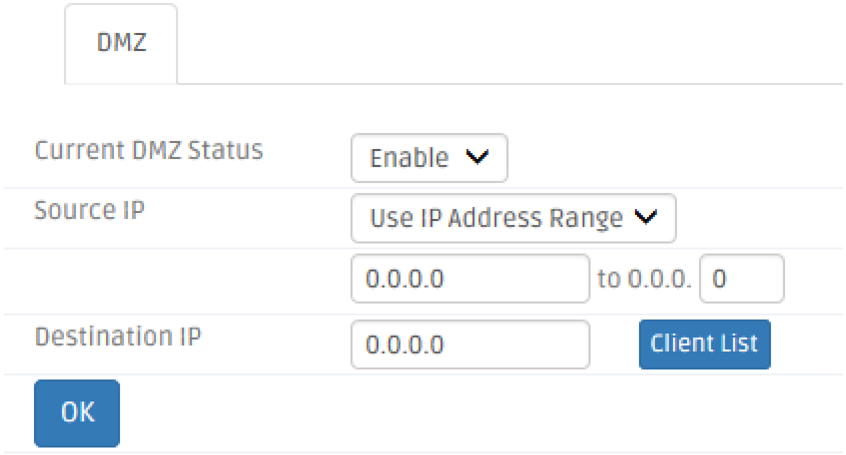

Is the symbol of a packet.
Internet
Remote FTP Client
Destination = 30.3.3.11:21
Data Interface 30.3.3.11
The Residential Gateway
Destination = 192.168.0.12:8888
The Private Network
FTP Server (192.168.0.12)

3.7.2 DMZ

DMZ stands for "Demilitarized Zone". It is an IP address on the private network of the Residential Gateway. But it is exposed to the Internet for special-purpose services. So a host on the private network can be assigned the IP address of the DMZ to provide services to the hosts on the Internet. The network administrator should be cautious of adopting DMZ. If a host is on DMZ, it is not protected by the firewall. And the Residential Gateway will open all ports to expose DMZ to the Internet. This may expose the local network to a variety of security risk.


Is the symbol of a packet.
Internet
Destination IP = 30.3.3.11
Destination IP = 30.3.3.12
Alias Interface 1 (30.3.3.11)
DMZ : 192.168.0.3
Alias Interface 2 (30.3.3.12)
DMZ : 192.168.0.4
Data Interface (30.3.3.13)
The Residential Gateway
The Private Network
Mail Server
192.168.0.3
(DMZ of Alias Interface 1)
FTP Server
192.168.0.4
(DMZ of Alias Interface 2)

Select **DMZ** from the **Application** sub menu bar. Then, **DMZ** screen page appears as follows:



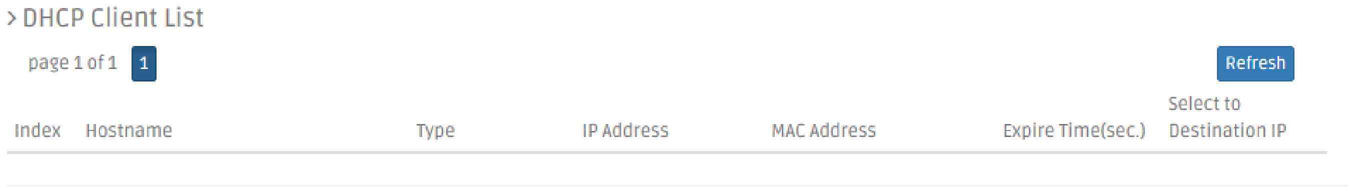
Current DMZ Status	Enable
Source IP	Use IP Address Range
	0.0.0.0 to 0.0.0. 0
Destination IP	0.0.0.0

DMZ Settings This section allows you to create or edit the DMZ of a selected interface in the Interface List. Below is a description of configuration parameters in this section.

Current DMZ Status — Enable or disable the DMZ of the selected WAN interface.

Source IP — Select *Any IP Address* to expose the DMZ to any IP address on the Internet. Or you can select the other radio button and specify an IP address range in the text boxes so the DMZ will be exposed to the IP address in the specified IP address range only.

Destination IP — Specify the IP address of the host on the DMZ. You can click *Client List* to view the DHCP client list in the pop-out window as blow. You can click Destination IP under “Select to Destination IP” column to easily gain the Destination IP.



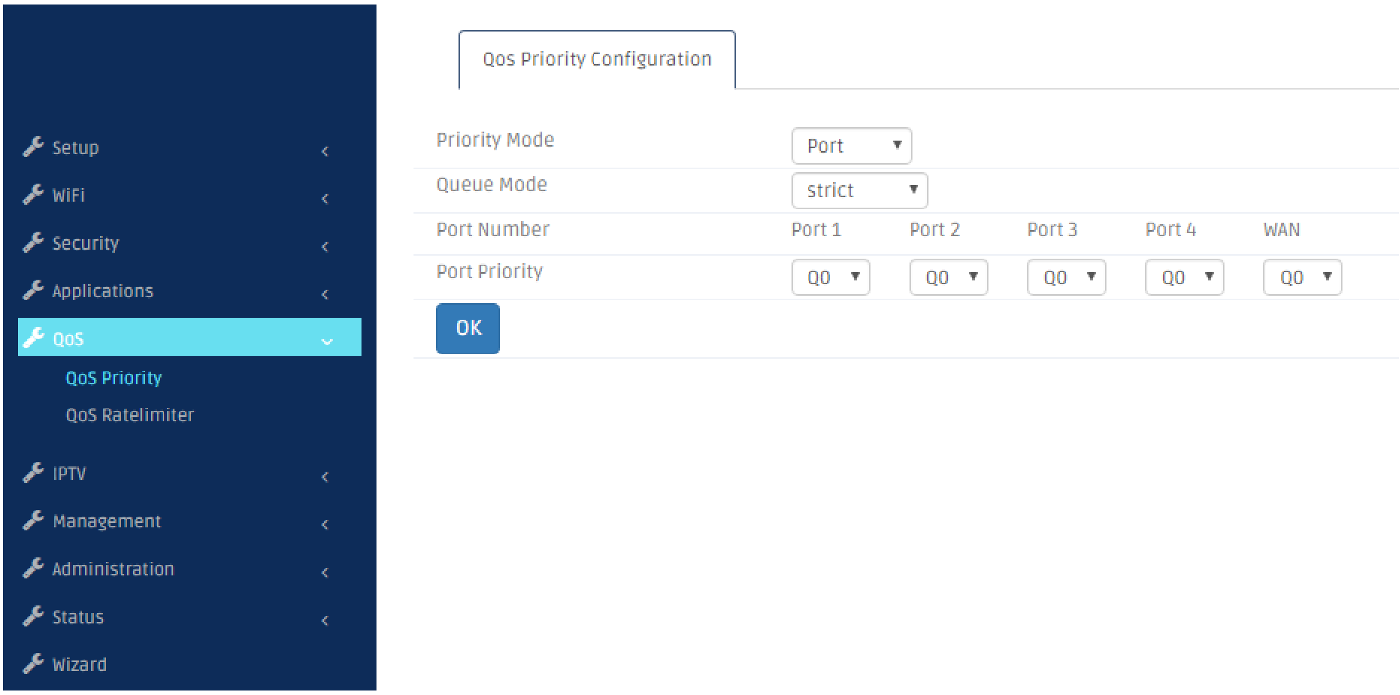
› DHCP Client List

page 1 of 1 1

Index	Hostname	Type	IP Address	MAC Address	Expire Time(sec.)	Select to Destination IP

3.8 QoS

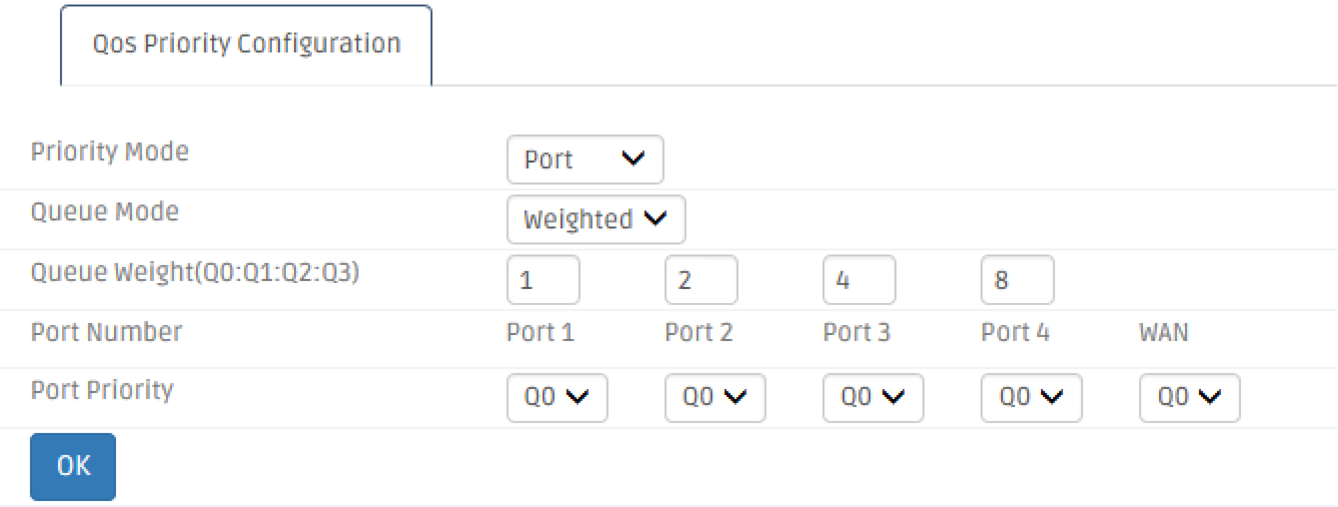
Select **QoS** in the Main Menu bar. And the sub-items – **QoS Priority** and **QoS Ratelimiter** will show up on the sub menu bar.



Priority Mode	Port				
Queue Mode	strict				
Port Number	Port 1	Port 2	Port 3	Port 4	WAN
Port Priority	Q0	Q0	Q0	Q0	Q0

3.8.1 QoS Priority

QoS stands for the “Quality of Service”. It allows the network administrator to give traffic of a service a higher priority for bandwidth to ensure its quality. Some services on the Internet, like the multimedia service, require larger bandwidth than the other services do. So the network administrator needs QoS to guarantee that their traffics will not be assigned too few bandwidth when there are many other traffics in the same link. Select **QoS Priority** from the **QoS** sub menu bar. Then, the **QoS Priority** screen page appears as follows:



Priority Mode	Port				
Queue Mode	Weighted				
Queue Weight(Q0:Q1:Q2:Q3)	1	2	4	8	
Port Number	Port 1	Port 2	Port 3	Port 4	WAN
Port Priority	Q0	Q0	Q0	Q0	Q0

For details on the settings, please refer to the description of the individual section below.

QoS Priority Configuration: The Residential Gateway supports QoS of the egress traffic. QoS of the Residential Gateway provides four queues for packet transmission – Queue 0, Queue 1, Queue 2 and Queue 3. Queues are used to store packets before the packets are transmitted. You can designate a queue to store packets if they meet a pre-determined condition of the QoS rule. Then, the queues will follow the priority order or the ratio of transmission rates to transmit the packets. Below is a description of configuration parameters in this section.

Priority Modes — The Residential Gateway provides three QoS priority modes — *Port*, *DSCP*, and *802.1p*. Select one of them in the pull-down menu to decide how you want to map the packets to the queues. Or select *Disable* to deactivate the QoS feature.

Port — Select this mode to bind every port of the Residential Gateway with a queue. And packets will be assigned to different queues according to the ports from which they leave the Residential Gateway. The Residential Gateway will follow the priority orders or the ratio of the transmission rates of the queues which store the packets to transmit packets.

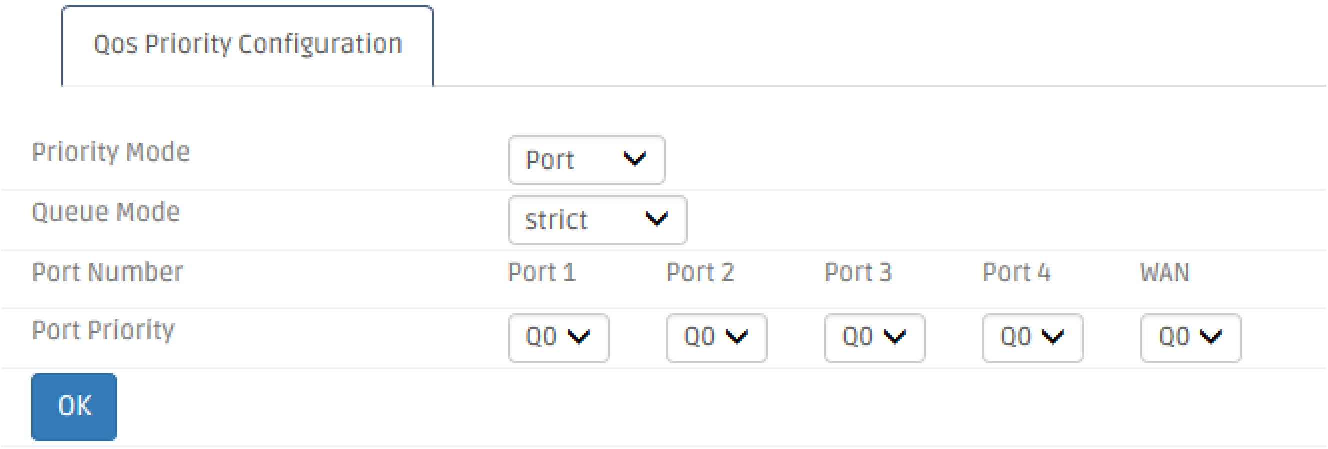
802.1p — Select this mode to bind the 802.1p values of the packets with the designated queues. And packets will be assigned to different queues according to their 802.1p values. The Residential Gateway will follow the priority orders or the ratio of the transmission rates of the queues which store the packets to transmit packets.

DSCP — Select this mode to bind the DSCP values of the packets with the designated queues. And packets will be assigned to different queues according to their DSCP values. The Residential Gateway will follow the priority orders or the ratio of the transmission rates of the queues which store the packets to transmit packets.

Queue Mode — If you select *strict*, the Residential Gateway will follow the priority orders of the queues to transmit packets. It will not start to transmit packets in a queue until all packets in the queues which have higher priorities are transmitted. And the priorities of the four queues from high to low are Queue 3, Queue 2, Queue 1 and Queue 0. If you select *weight*, the Residential Gateway will follow the pre-determined ratio of the transmission rates to transmit the packets.

Port Priority Mode > **Strict Queue Mode**

If you select *Port* for the ***Priority Mode*** and *strict* for the ***Queue Mode***, you need to decide how the ports of the Residential Gateway will be mapped to the queues.



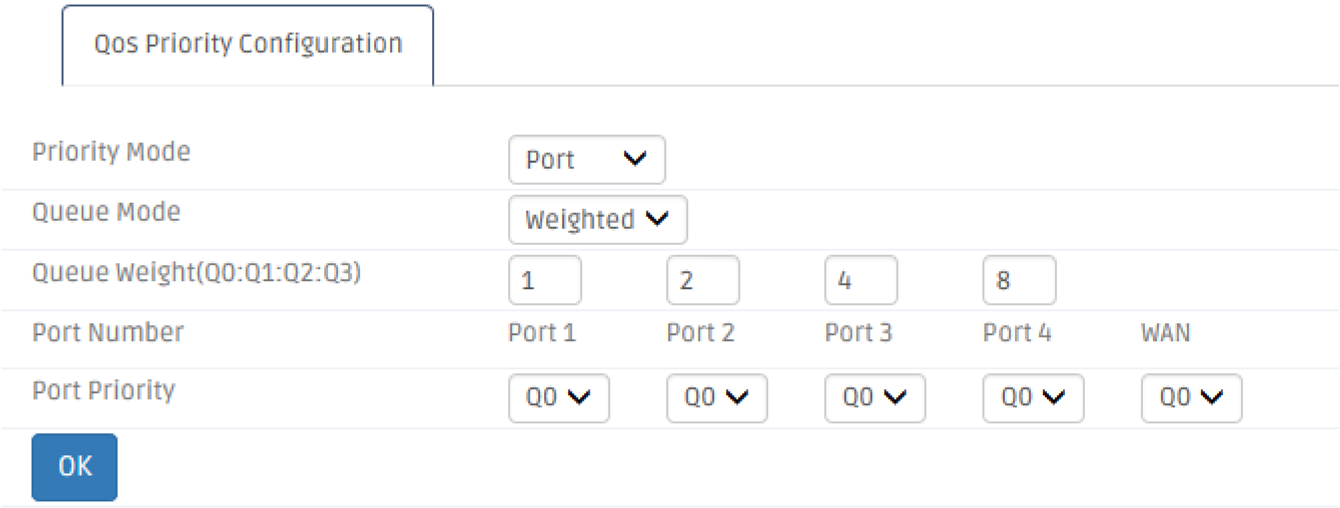
Qos Priority Configuration

Priority Mode	Port				
Queue Mode	strict				
Port Number	Port 1	Port 2	Port 3	Port 4	WAN
Port Priority	Q0	Q0	Q0	Q0	Q0

Port Priority — Select a queue from the pull-down menu to bind the selected queue with the port.

Port Priority Mode > **Weighted Queue Mode**

If you select *Port* for the ***Priority Mode*** and *weighted* for the ***Queue Mode***, you need to specify the ratio of the transmission rates of the queues to decide how the ports of the Residential Gateway will be mapped to the queues.



Qos Priority Configuration

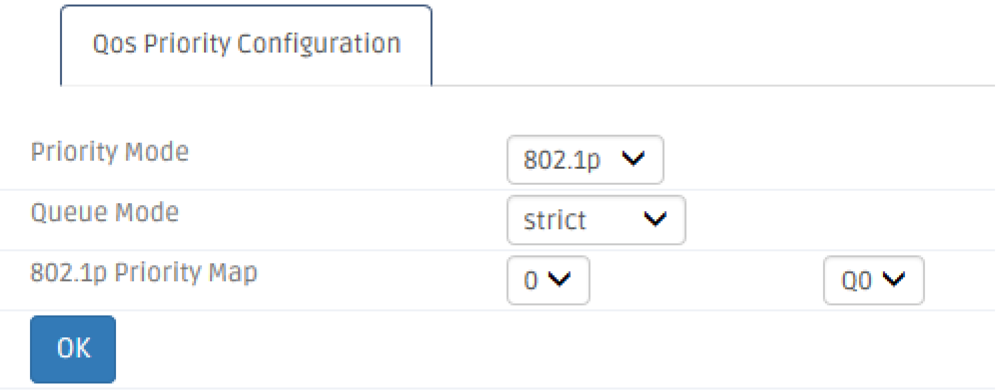
Priority Mode	Port				
Queue Mode	Weighted				
Queue Weight(Q0:Q1:Q2:Q3)	1	2	4	8	
Port Number	Port 1	Port 2	Port 3	Port 4	WAN
Port Priority	Q0	Q0	Q0	Q0	Q0

Queue Weight(Q0:Q1:Q2:Q3) — Specify the ratio of the transmission rates for queues in the text boxes.

Port Priority — Select a queue from the pull-down menu to map it to the port.

802.1p Priority Mode > **Strict Queue Mode**

If you select *802.1p* for the ***Priority Mode*** and *strict* for the ***Queue Mode***, you need to determine how the 802.1p value will be mapped to the queues.



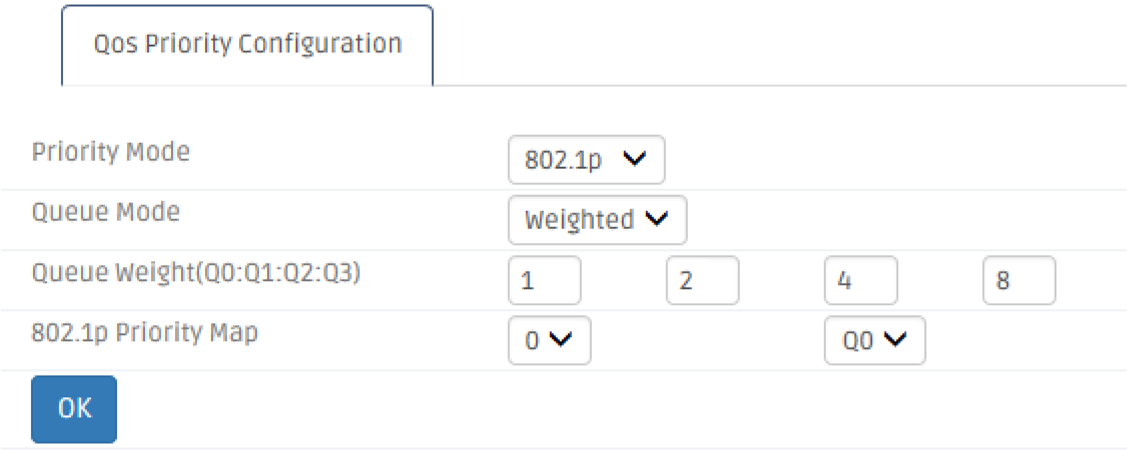
Qos Priority Configuration

Priority Mode	802.1p	
Queue Mode	strict	
802.1p Priority Map	0	Q0

802.1p Priority Map — Select a 802.1p value from the first pull-down menu. And select a queue from the second pull-down menu to map the 802.1p value to it.

802.1p Priority Mode > Weighted Queue Mode

If you select *802.1p* for the ***Priority Mode*** and *weighted* for the ***Queue Mode***, you need to specify the ratio of the transmission rates of the queues and decide how the 802.1p value should be mapped to the queues.



Qos Priority Configuration

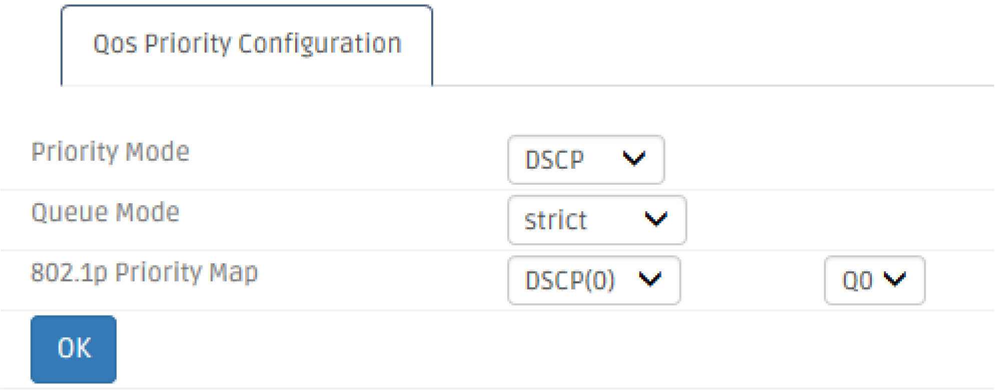
Priority Mode	802.1p			
Queue Mode	Weighted			
Queue Weight(Q0:Q1:Q2:Q3)	1	2	4	8
802.1p Priority Map	0		Q0	

Queue Weight(Q0:Q1:Q2:Q3) — Specify the ratio of the transmission rate for queues in the text boxes.

802.1p Priority Map — Select a 802.1p value from the first pull-down menu. And select a queue in the second pull-down menu to map the 802.1p value to it.

DSCP Priority Mode > Strict Queue Mode

If you select *DSCP* for the ***Priority Mode*** and *strict* for the ***Queue Mode***, you need to determine how the DSCP value should be mapped to the queues.



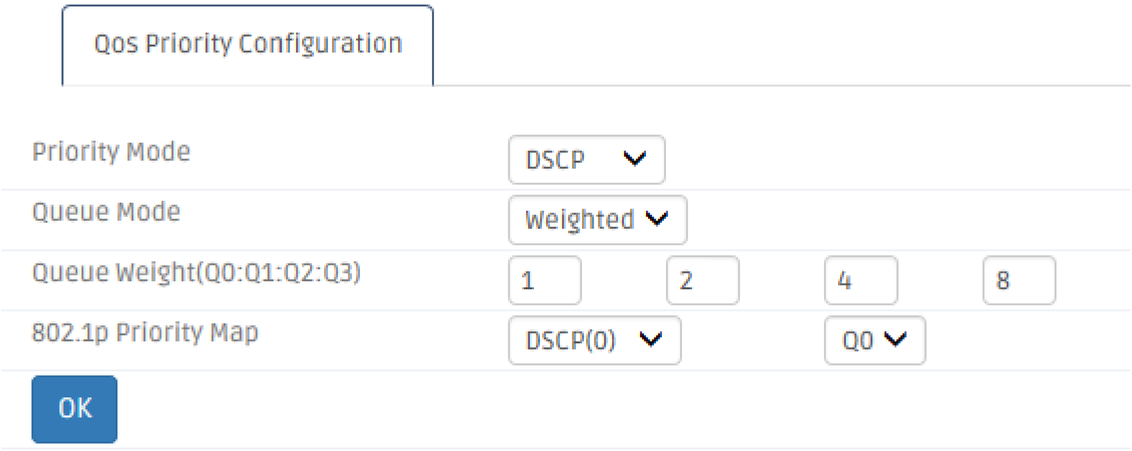
Qos Priority Configuration

Priority Mode	DSCP	
Queue Mode	strict	
802.1p Priority Map	DSCP(0)	Q0

DSCP Priority Map — Select a DSCP value from the first pull-down menu. And select a queue from the second pull-down menu to map the DSCP value to it.

DSCP Priority Mode > **Weighted Queue Mode**

If you select *DSCP* for the ***Priority Mode*** and weighted for the ***Queue Mode***, you need to specify the ratio of the transmission rates of the queues and determine how the DSCP value should be mapped to the queues.



Priority Mode	DSCP			
Queue Mode	Weighted			
Queue Weight(Q0:Q1:Q2:Q3)	1	2	4	8
802.1p Priority Map	DSCP(0)		Q0	

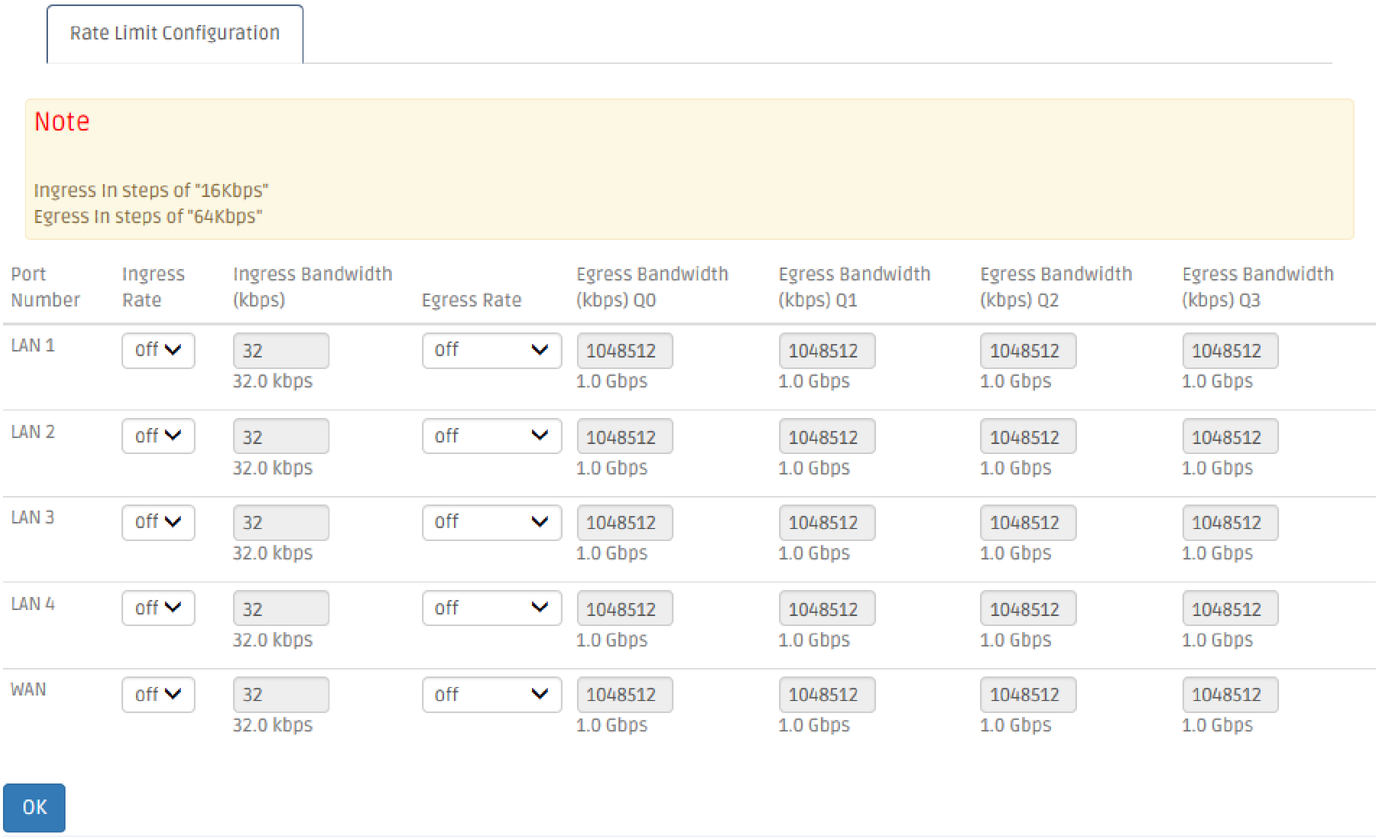
Queue Weight(Q0:Q1:Q2:Q3) — Specify the ratio of the transmission rate for queues in the text boxes.

DSCP Priority Map — Select a DSCP value from the first pull-down menu. And select a queue from the second pull-down menu to map the DSCP value to it.

Click *Apply* to submit the settings after you finish configuring this page.

3.8.2 QoS Ratelimiter

QoS Ratelimiter allows the network administrator to set the maximum transmission rate limit for the ingress or egress traffic. So the network administrator can give different rate limits to different Internet services or clients according to their privilege levels. Select **QoS Ratelimiter** from the **QoS** sub menu bar. Then, the **QoS Ratelimiter** screen page appears as follows:



Rate Limit Configuration

Note

Ingress In steps of "16Kbps"
Egress In steps of "64Kbps"

Port Number	Ingress Rate	Ingress Bandwidth (kbps)	Egress Rate	Egress Bandwidth (kbps) Q0	Egress Bandwidth (kbps) Q1	Egress Bandwidth (kbps) Q2	Egress Bandwidth (kbps) Q3
LAN 1	off	32 32.0 kbps	off	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps
LAN 2	off	32 32.0 kbps	off	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps
LAN 3	off	32 32.0 kbps	off	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps
LAN 4	off	32 32.0 kbps	off	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps
WAN	off	32 32.0 kbps	off	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps	1048512 1.0 Gbps

For details on the settings, please refer to the description of the individual section below.

Rate Limit Configuration This section contains a table which displays the current rate limit settings of the Residential Gateway. It allows you to set the maximum rate limit of the ingress and egress traffic on each port. Or you can set the maximum rate limit on the queues for each port. Below is a description of configuration parameters in this section.

Port Number — Select a port from the pull-down menu to edit its maximum rate limit. Or you can click *Edit* in the last row of the table to edit the rate limit settings of the port.

Ingress Rate — Select *on* to enable the ingress rate limit of this port. Or select *off* to disable it.

Ingress Bandwidth — If you select *on* for the ***Ingress Rate***, specify the rate limit for the ingress traffic of this port in the text box.

Egress Rate — Select *per port* to give an egress rate limit to the port. Select *per queue* to give an egress rate limit to each queue for this port. Or select *disable* to deactivate this feature.

Egress Bandwidth Q0 — If you select *Per Port* for the ***Egress Rate***, specify the rate limit for the egress traffic of the port in the text box. And if you select *Per Queue* for the ***Egress Rate***, specify for this port the maximum egress rate of the traffic stored in Queue 0 in the text box.

Egress Bandwidth Q1 — Specify for this port the maximum egress rate of the traffic stored in Queue 1 in the text box.

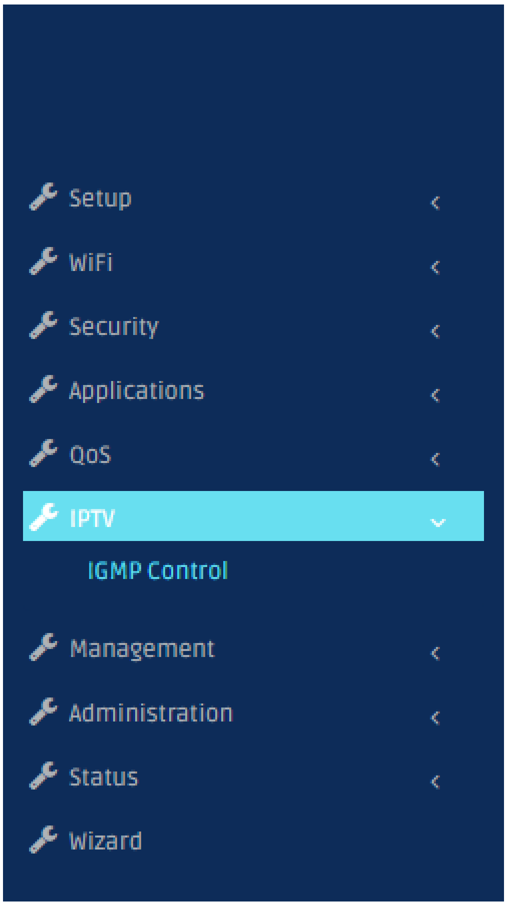
Egress Bandwidth Q2 — Specify for this port the maximum egress rate of the traffic stored in Queue 2 in the text box.

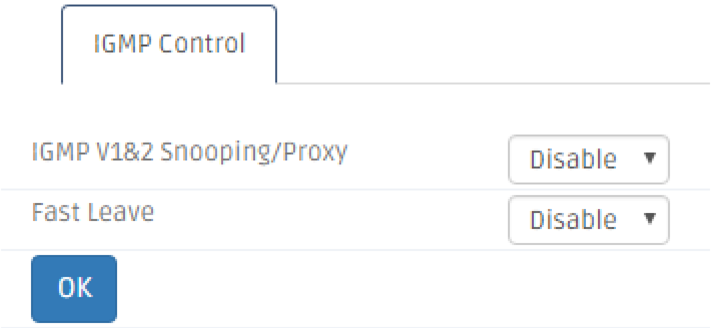
Egress Bandwidth Q3 — Specify for this port the maximum egress rate of the traffic stored in Queue 3 in the text box.

Click *OK* to submit your settings after you finish configuring this page.

3.9 IPTV

Select **IPTV** in the Main Menu bar. And the sub-items – **IGMP Control** – will show up on the sub menu bar.



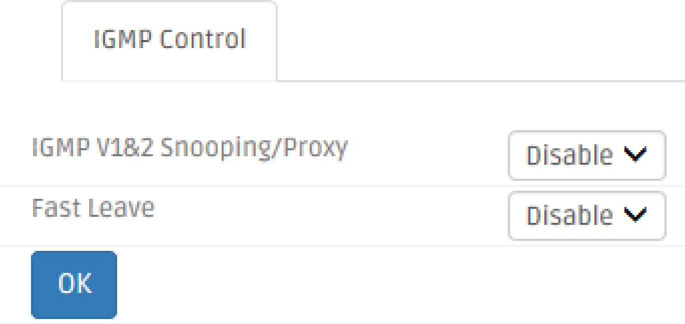


IGMP V1&2 Snooping/Proxy: Disable

Fast Leave: Disable

3.9.1 IGMP Control

The Residential Gateway supports the IGMP snooping and the IGMP proxy. IGMP stands for “Internet Group Management Protocol”. It is widely used by the multimedia services which rely on the multicast protocol to conduct multimedia streams to the hosts (such as IPTVs). When a host makes a request for the multimedia stream of a channel, it will send a request packet to join the multicast group of this channel to the multicast router. And if the device between the host and the multicast router supports the IGMP snooping or proxy, it will remember the port from which it receives the request. Then, it will forward the multimedia stream to the host when it receives the multimedia stream from the router. For details on the settings, please refer to the description of the individual section below. Select **IGMP Control** from the **IPTV** sub menu bar. Then, **IGMP Control** screen page appears as follows:



IGMP V1&2 Snooping/Proxy: Disable

Fast Leave: Disable

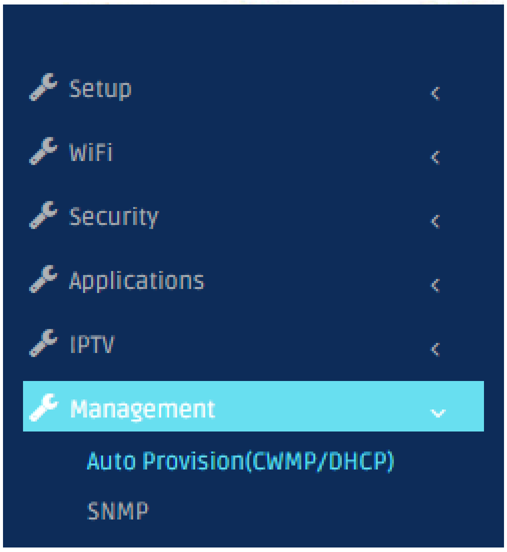
IGMP Snooping/Proxy Enable or disable the IGMP snooping and IGMP proxy function on the Residential Gateway. When the IGMP host is on the private network, the IGMP proxy must be activated for the Residential Gateway to learn the request of the host. And when the IGMP host is on the public network, the IGMP snooping must be enabled for the Residential Gateway to learn this request of the host.

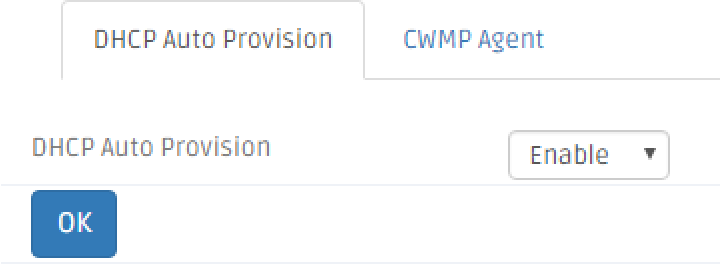
Fast Leave — If Enabled, it allows the host to change its multicast memberships faster. Thus, you can change the channels on the host faster.

Click *OK* to submit your settings after you finish configuring this page. Or click *Cancel* to clear all the unsaved values in this page.

3.10 Management

Select **Management** in the Main Menu bar. And the sub-items – **Auto-Provision (DHCP) & SNMP**– will show up on the sub menu bar.





DHCP Auto Provision: Enable

3.10.1 DHCP Auto Provision

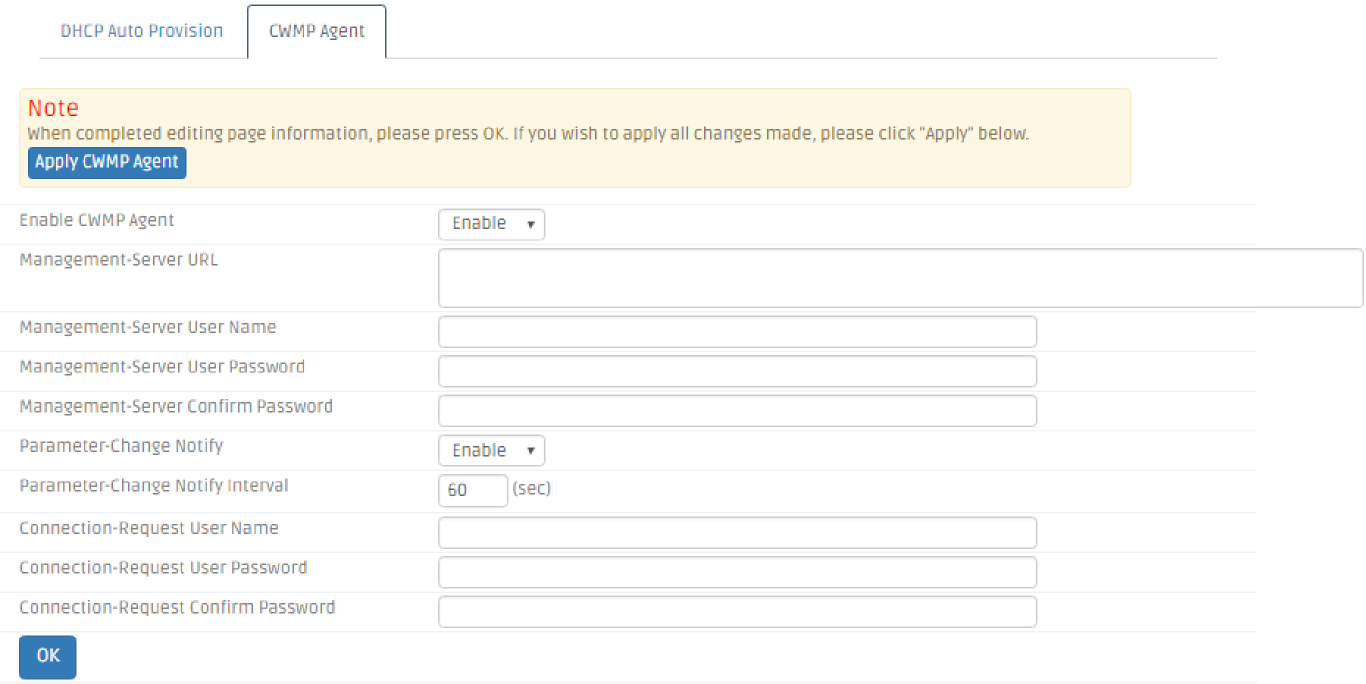
This section allows you to enable or disable the DHCP auto-provisioning function.

DHCP Auto Provision — Click to enable or disable DHCP Auto Provision

Click OK to submit your settings after you finish configuring this page.

3.10.1.1 CWMP Agent

TR-069 (Technical Report 069) is a technical specification that defines an application layer protocol for remote management of end-user devices. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.



Note
When completed editing page information, please press OK. If you wish to apply all changes made, please click "Apply" below.

Enable CWMP Agent	Enable ▾
Management-Server URL	
Management-Server User Name	
Management-Server User Password	
Management-Server Confirm Password	
Parameter-Change Notify	Enable ▾
Parameter-Change Notify Interval	60 (sec)
Connection-Request User Name	
Connection-Request User Password	
Connection-Request Confirm Password	

Enable CWMP Agent — Enable or disable TR-069 function.

Management Server URL — Specify HTTP address of the Auto Configuration Server.

Management Server User Name — Specify the password of the Auto Configuration Server.

Management Server Confirm Password — Specify the password of the Auto Configuration Server again.

Periodic Change Notify — Enable or disable Periodic Information function. It defines the time interval that a piece of information will be sent after a communication session is done.

Note: If a communication session has been incomplete for long time, the time interval will start counting at the beginning of communication session.

Periodic Change Notify Interval — Specify the time in second after which a piece of information will be sent again. The default value is 60.

Connect Request User Name — Specify the name of the Connection Request Server.

Connect Request User Password — Specify the name of the Connection Request Server.

Connect Request Confirm Password — Specify the name of the Connection Request Server again.

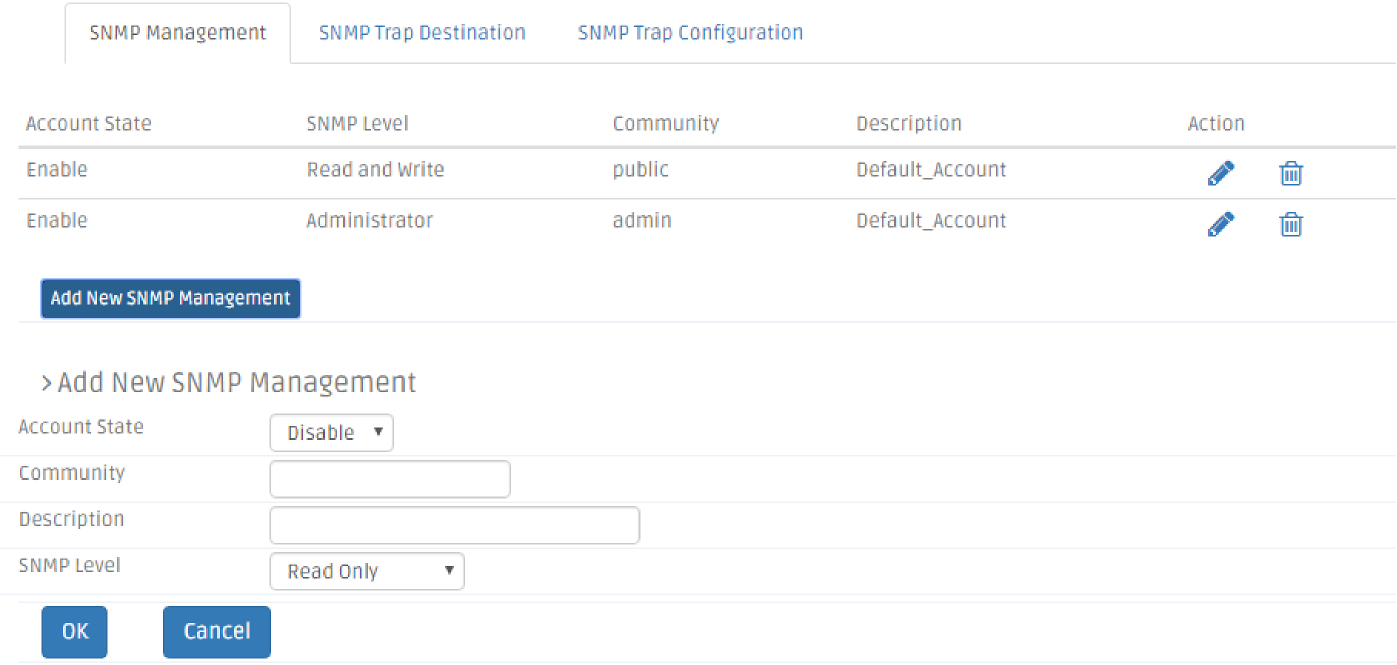
Click *Apply Basic Setup* to submit your settings after you finish configuring this page.

3.10.2 SNMP

The Residential Gateway supports SNMP management. SNMP stands for “Simple Network Management Protocol”. A brief introduction for SNMP will be found in Chapter 4 of this document.

3.10.2.1 SNMP Management

Select **SNMP** from the **Management** sub menu bar. And then the following screen page appears.



Account State	SNMP Level	Community	Description	Action
Enable	Read and Write	public	Default_Account	✎ 🗑
Enable	Administrator	admin	Default_Account	✎ 🗑

> Add New SNMP Management

Account State	Disable ▾
Community	
Description	
SNMP Level	Read Only ▾

This section allows you to make proper settings on the Residential Gateway so you can manage the Residential Gateway by SNMP. Below is a description of the configuration parameters of this section.

Account State — Shows the SNMP service is Enable or Disable.

SNMP Level — Shows user's authentication level.

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

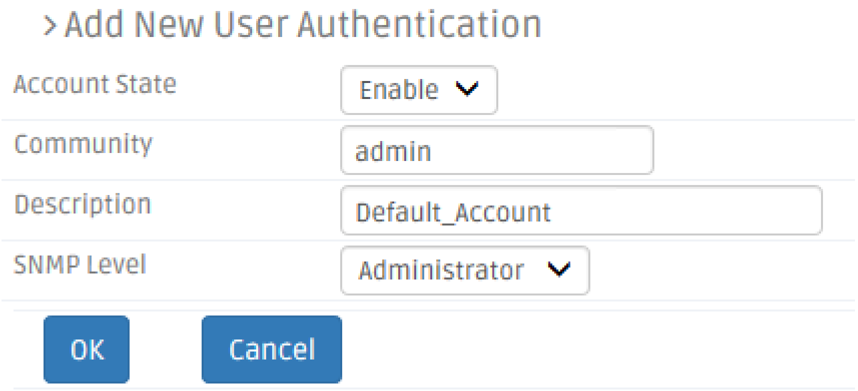
Read & Write: Full access right but cannot modify user account & system information, cannot load factory settings.

Read Only: Allow to view only.

Community — Shows the authorized alphanumeric SNMP community name

Description —Shows a unique description for this community name. This is mainly for reference only.

Action — Click *Add New SNMP Management* to add a new rule to the table after you configure it in the text boxes. And to modify an entry in the rule table, click *Pencil Icon.* Then, click *OK* to submit the new settings. If you need to remove any entry from this table, click *Bin Icon*.



> Add New User Authentication

Account State	Enable
Community	admin
Description	Default_Account
SNMP Level	Administrator

Account State — Enable or disable the SNMP service.

Community — Specify the authorized SNMP community name

Description —Enter a unique description for this community name. This is mainly for reference only.

SNMP Level — Specify user's authentication level.

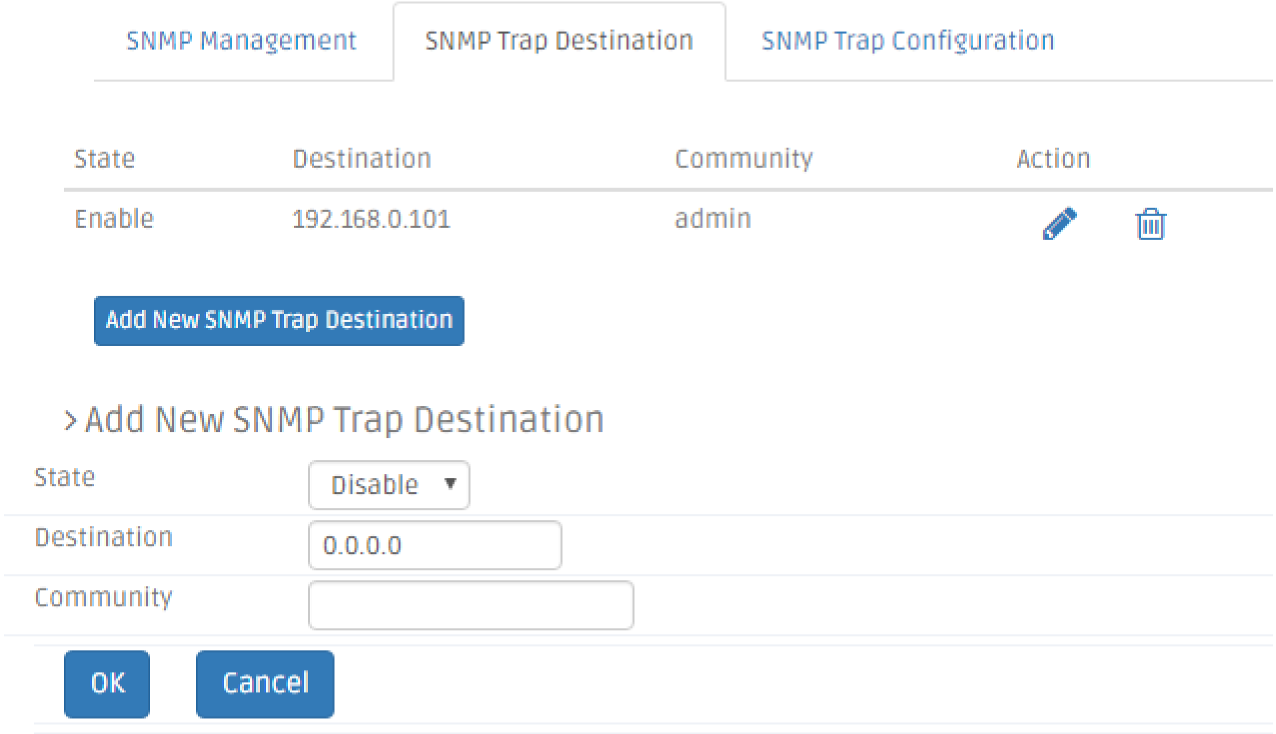
Administrator: Full access right including maintaining user account & system information, load factory settings …etc.

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

Read Only: Allow to view only.

3.10.2.2 SNMP Destination

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



SNMP Management | SNMP Trap Destination | SNMP Trap Configuration

State	Destination	Community	Action
Enable	192.168.0.101	admin	✎ 🗑

Add New SNMP Trap Destination

> Add New SNMP Trap Destination

State	Disable ▼
Destination	0.0.0.0
Community	

OK Cancel

State — Enable or disable the function of sending trap to the specified destination.

Destination — Enter the specific IP address of the network management system that will receive the trap.

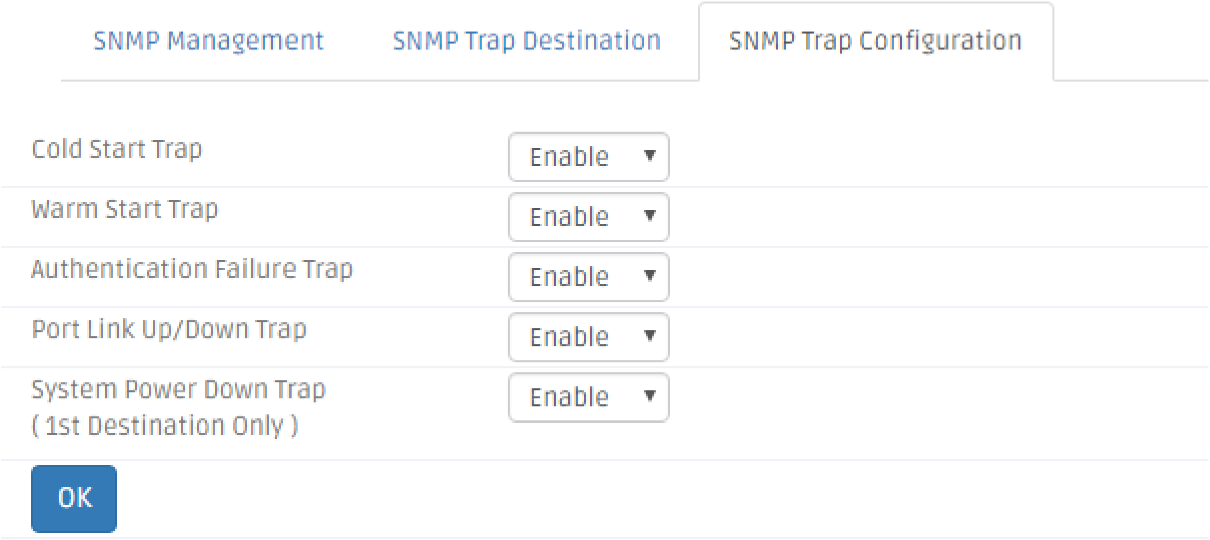
Community — Enter the community name of the network management system.

Action — Click *Add New Trap Destination* to add a new rule to the table after you configure it in the text boxes. And to modify an entry in the rule table, click *Pencil Icon*. Then, click *OK* to submit the new settings. If you need to remove any entry from this table, click *Bin Icon*.

Click *OK* to submit your settings or *Cancel* to remove your settings after you finish configuring this page.

3.10.2.3 SNMP Configuration

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



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

Cold Start Trap — Enable or disable the Gateway to send a trap when the Gateway is turned on.

Warm Start Trap — Enable or disable the Gateway to send a trap when the Gateway restarts.

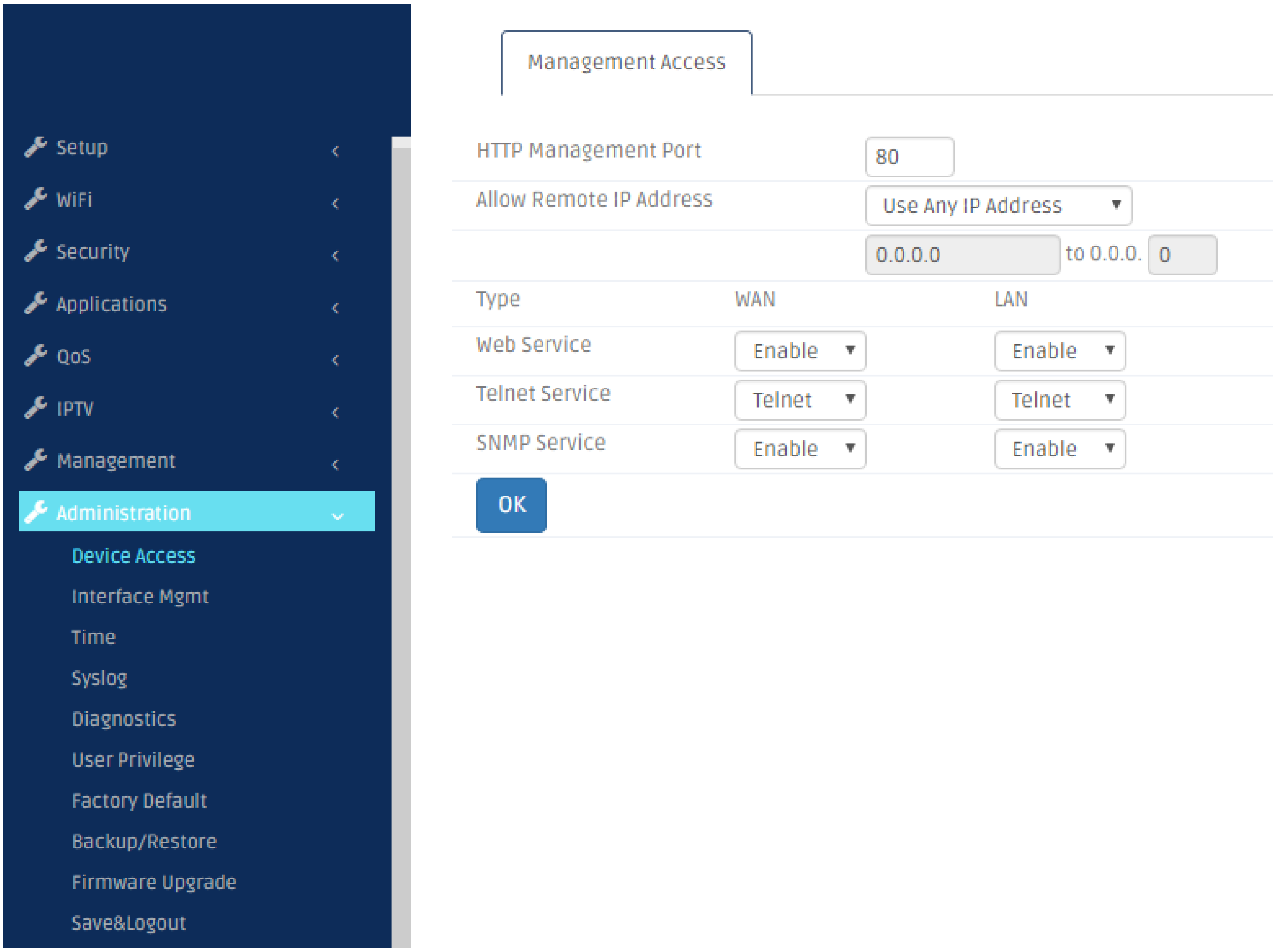
Authentication Failure Trap — Enable or disable the Gateway to send authentication failure trap after any unauthorized users attempt to login.

Port Link Up/Down Trap — Enable or disable the Gateway to send port link up/link down trap.

System Power Down Trap (1st Destination Only): Send a trap notice while the Gateway is power down.

3.11 Administration

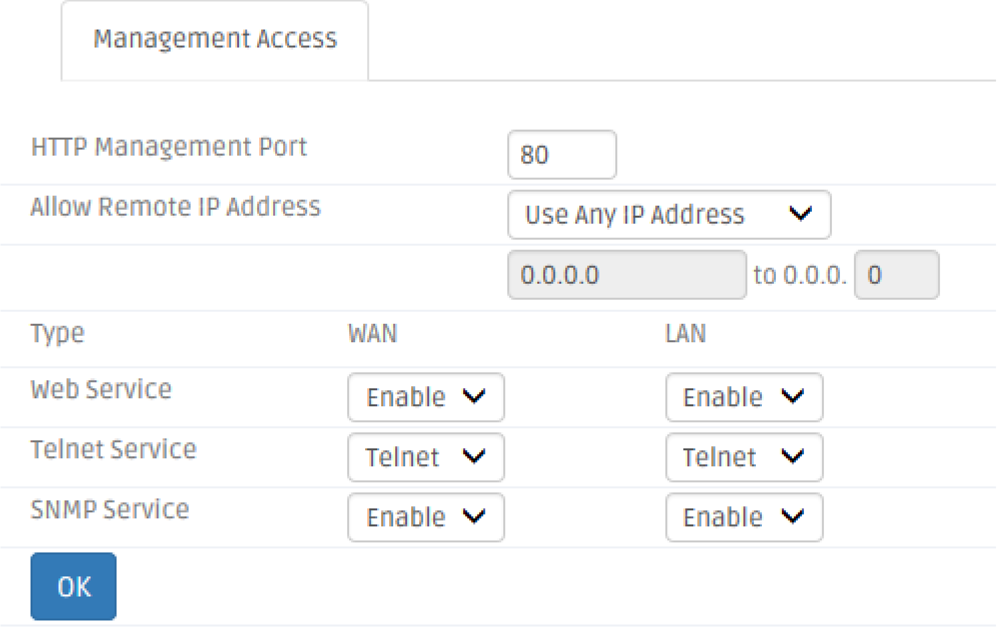
Select **Administration** in the Main Menu bar. And the sub-items – **Device Access, Interface Management**, **Time**, **Syslog**, **Diagnostics**, **User Privilege**, **Backup/Restore**, **Factory Default**, **Firmware Upgrade** and **Save & Logout**– will show up on the sub menu bar.



HTTP Management Port	80	
Allow Remote IP Address	Use Any IP Address	
	0.0.0.0 to 0.0.0. 0	
Type	WAN	LAN
Web Service	Enable	Enable
Telnet Service	Telnet	Telnet
SNMP Service	Enable	Enable

3.11.1 Device Access

The network administrator may need to restrict the management access from LAN ports so he can prevent end users to change the settings of the Residential Gateway. Or he may want to manage the Residential Gateway via SNMP and deactivate management access via HTTP for security concern. This page allows him to make the management access policies of the Residential Gateway. Select **Device Access** from the **Administration** sub menu bar. Then, **Device Access** screen page appears as follows:

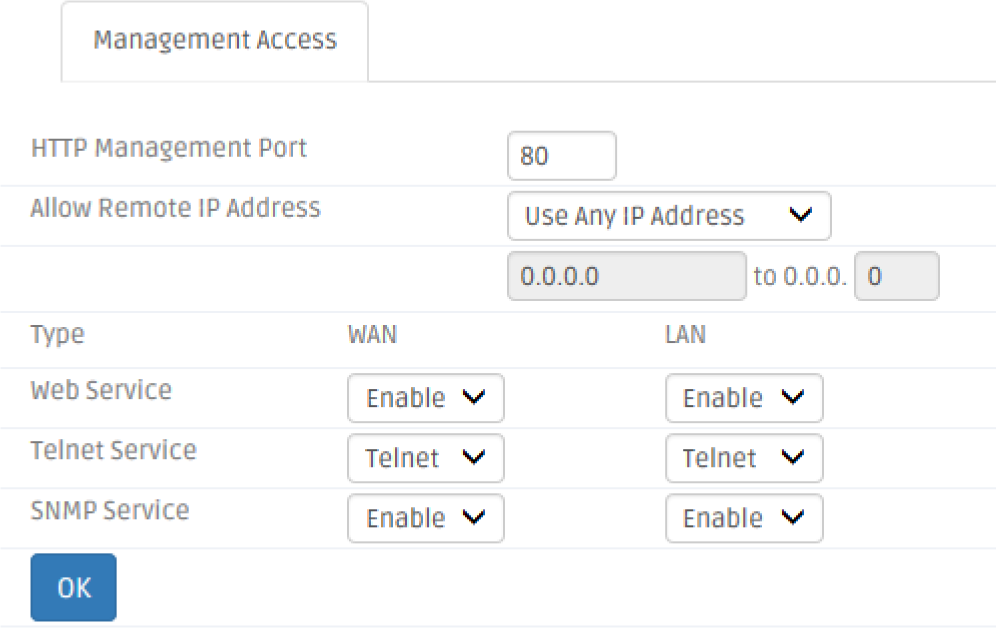


Management Access

HTTP Management Port	80	
Allow Remote IP Address	Use Any IP Address	
	0.0.0.0 to 0.0.0. 0	
Type	WAN	LAN
Web Service	Enable	Enable
Telnet Service	Telnet	Telnet
SNMP Service	Enable	Enable

3.11.1.1 Management Access

This section allows you to configure the management methods for the Residential Gateway. Below is a description of the configuration parameters of this section.



Management Access

HTTP Management Port	80	
Allow Remote IP Address	Use Any IP Address	
	0.0.0.0 to 0.0.0. 0	
Type	WAN	LAN
Web Service	Enable	Enable
Telnet Service	Telnet	Telnet
SNMP Service	Enable	Enable

HTTP Management Port — This is 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 default value is 80.

Allow Remote IP address — Select _Any IP Address_ for the Residential Gateway to be managed from its WAN port by any remote IP address. Or select the second radio button and specify a range of IP addresses in the text boxes to enable these IP addresses to manage the Residential Gateway from the WAN port.

Type — Shows which types of port you can access to manage the Gateway.

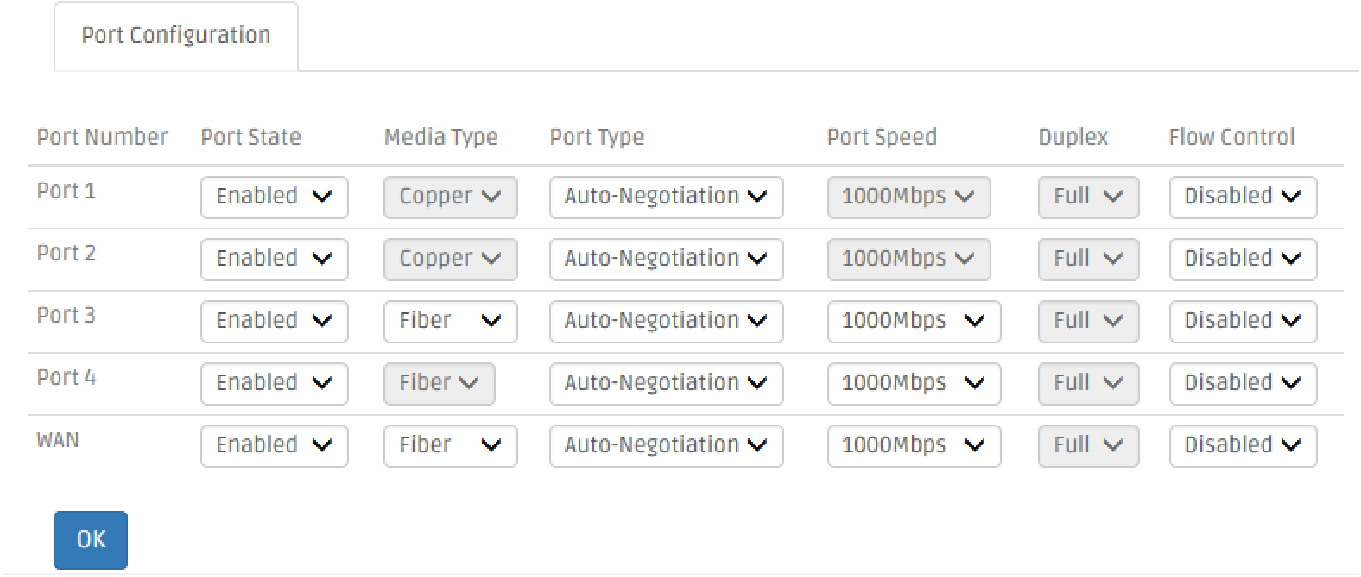
Web Service — Click _enable_ to gain the Web management access on WAN or LAN port.

Telnet Service —Click _Telnet_ to gain the Telnet management access on WAN or LAN port.

SNMP Service —Click _SNMP_ to gain the SNMP management access on WAN or LAN port.

3.11.2 Interface Management

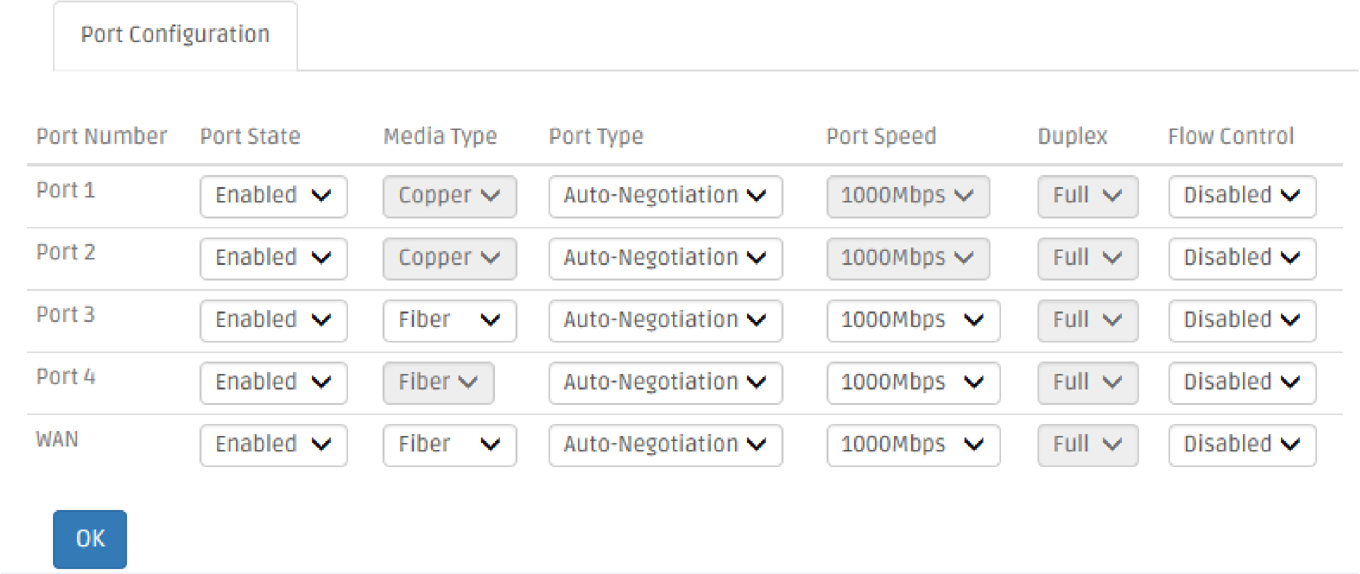
This page enables the network administrator to edit the port settings of the Residential Gateway. Select **Interface Mgmt** from the **Administration** sub menu bar. Then, the following screen page appears.



Port Number	Port State	Media Type	Port Type	Port Speed	Duplex	Flow Control
Port 1	Enabled	Copper	Auto-Negotiation	1000Mbps	Full	Disabled
Port 2	Enabled	Copper	Auto-Negotiation	1000Mbps	Full	Disabled
Port 3	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled
Port 4	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled
WAN	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled

3.11.2.1 Port Configuration

This section displays the port state of the Residential Gateway. You can click drop-down arrow in each column of the table to configure the settings of the selected port in the next section. Below is a description of the configuration parameters of this section.



Port Configuration

Port Number	Port State	Media Type	Port Type	Port Speed	Duplex	Flow Control
Port 1	Enabled	Copper	Auto-Negotiation	1000Mbps	Full	Disabled
Port 2	Enabled	Copper	Auto-Negotiation	1000Mbps	Full	Disabled
Port 3	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled
Port 4	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled
WAN	Enabled	Fiber	Auto-Negotiation	1000Mbps	Full	Disabled

Port Number — Click the pull-down menu to select the port number for configuration. Or it will display the port which you select in the section above.

Port State — Enable or disable the selected port.

Media Type — This field shows the media type (either Fiber or Copper) of the selected port. And it is open to select when this port is a combo port.

Port Type — This is a view-only field. It indicates that the selected port is in the auto-negotiation mode so this port will negotiate with the other device to link up in the maximum link speed. And the port of the device on the other side should support auto-negotiation as well.

Port Speed — This field shows the speed of the selected port. And it is open to select when the selected port is a combo port.

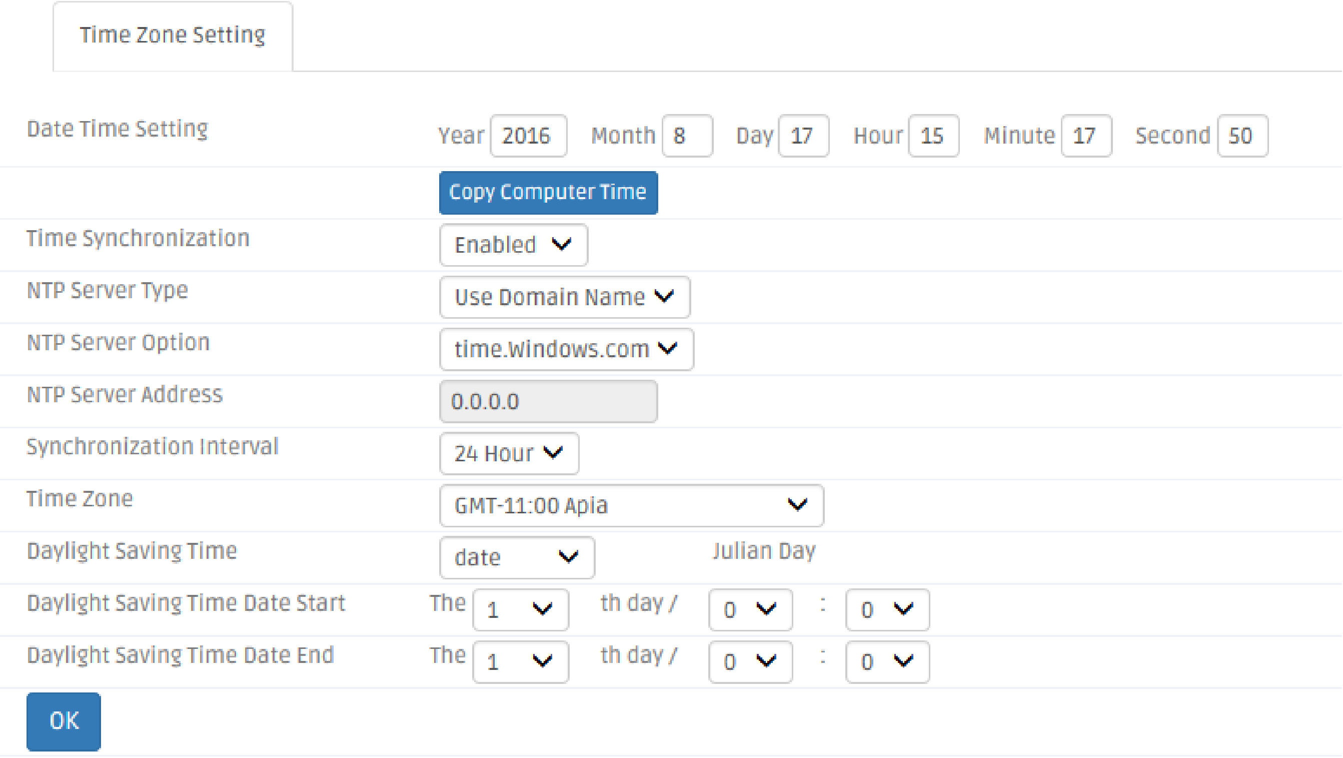
Duplex — This is a view only field. It indicates that the selected port is in the full duplex mode.

Flow Control — Enable or disable the flow control function.

Click _OK_ to submit your settings after you finish configuring this page.

3.11.3 Time

This page enables the network administrator to change the settings of the Residential Gateway's internal clock. Select **Time** from the **Administration** sub menu bar, and then **Time** screen page will appear as follows:



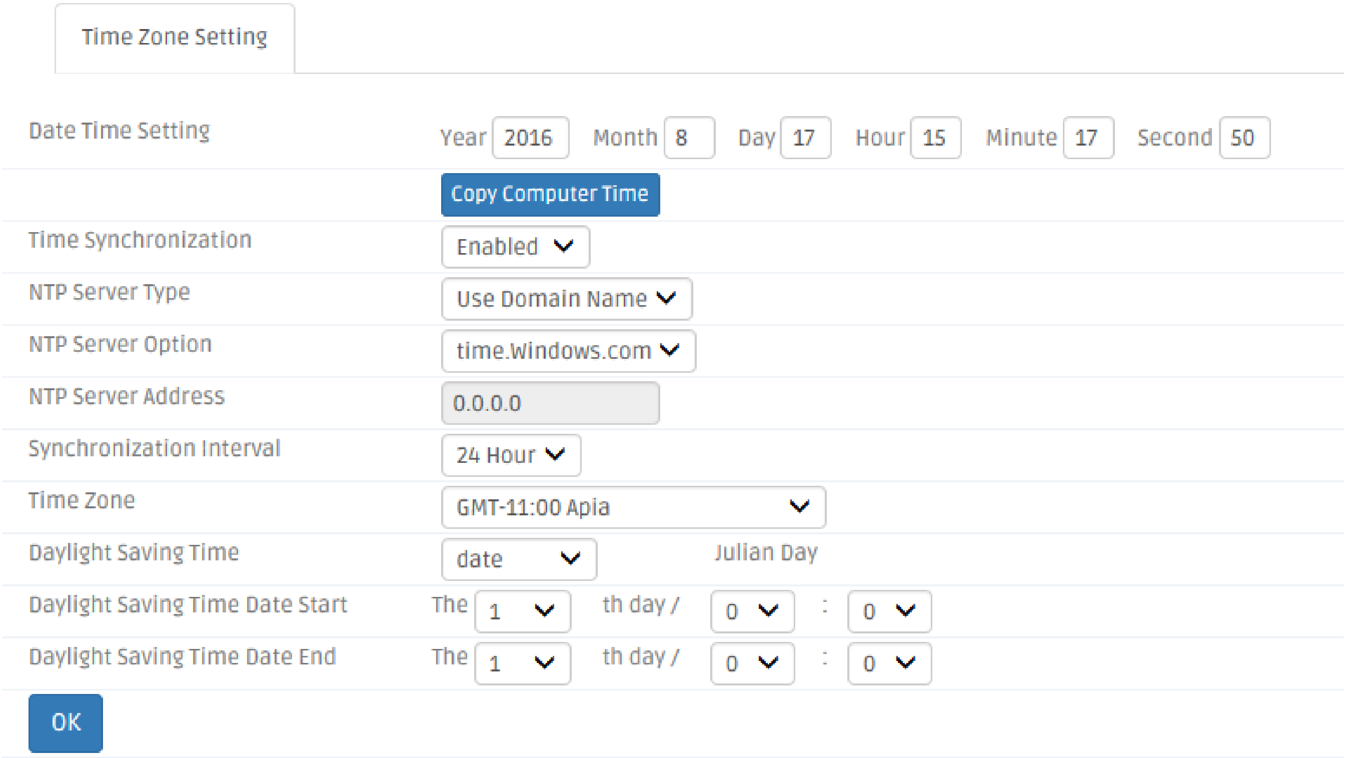
Time Zone Setting

Date Time Setting	Year 2016 Month 8 Day 17 Hour 15 Minute 17 Second 50
	Copy Computer Time
Time Synchronization	Enabled
NTP Server Type	Use Domain Name
NTP Server Option	time.windows.com
NTP Server Address	0.0.0.0
Synchronization Interval	24 Hour
Time Zone	GMT-11:00 Apia
Daylight Saving Time	date Julian Day
Daylight Saving Time Date Start	The 1 th day / 0 : 0
Daylight Saving Time Date End	The 1 th day / 0 : 0

OK

3.11.3.1 Time Zone Setting

This section enables you to make the date and time settings of the Residential Gateway. Below is a description of the configuration parameters of this section.



Time Zone Setting

Date Time Setting	Year 2016 Month 8 Day 17 Hour 15 Minute 17 Second 50
	Copy Computer Time
Time Synchronization	Enabled
NTP Server Type	Use Domain Name
NTP Server Option	time.windows.com
NTP Server Address	0.0.0.0
Synchronization Interval	24 Hour
Time Zone	GMT-11:00 Apia
Daylight Saving Time	date Julian Day
Daylight Saving Time Date Start	The 1 th day / 0 : 0
Daylight Saving Time Date End	The 1 th day / 0 : 0

OK

Date Time Setting — Specify the date and time in the text boxes to set the internal clock of the Residential Gateway manually. Or click *Copy Computer Time* to update the Residential Gateway's internal clock from the management computer.

Time Synchronization — Click to enable or disable time synchronization.

NTP Server Option — Two Options are available: Use Domain Name and Use IP Address.

Domain Name — Select the intended Domain Name.

Time Server Address — Specify NTP time server address that you want to get time information from.

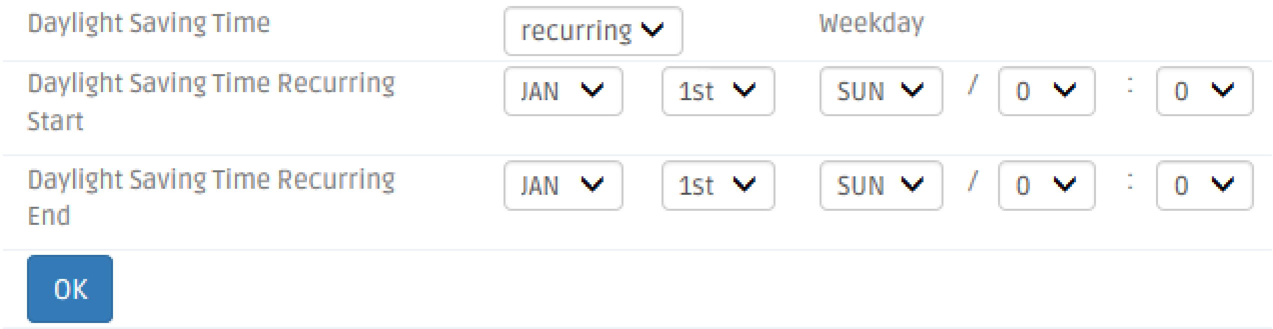
Synchronization Interval — Specify the time interval to synchronize from NTP time server.

Time Zone — Select your time zone from the pull-down menu.

Daylight Saving Time — To enable or disable the daylight saving time function. Daylight saving time is the practice of advancing clocks during summer months by one hour so that evening daylight lasts an hour longer, while sacrificing normal sunrise times.

Daylight Saving Time Date Start — Click the pull-down menu to select the annual start date of daylight saving time.

Daylight Saving Time Date End — Click the pull-down menu to select the annual end date of daylight saving time.



Daylight Saving Time	recurring		Weekday				
Daylight Saving Time Recurring Start	JAN	1st	SUN	/	0	:	0
Daylight Saving Time Recurring End	JAN	1st	SUN	/	0	:	0

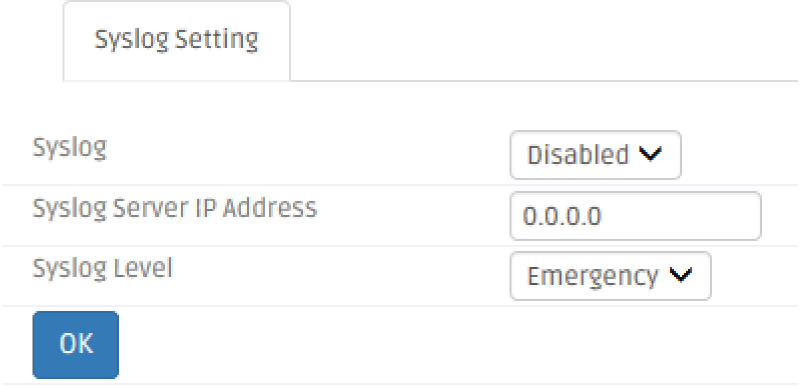
Daylight Saving Time Recurring Start — Click the pull-down menu to select the start date of daylight saving time using calendar algorithm.

Daylight Saving Time Recurring Start — Click the pull-down menu to select the start date of daylight saving time using calendar algorithm.

Click *OK* to apply the settings.

3.11.4 Syslog

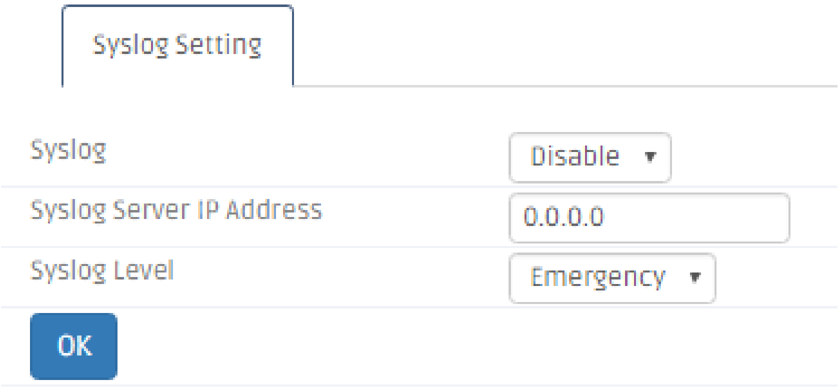
Syslog enables the Residential Gateway to send the debug log to the syslog server. Select **Syslog** from the **Administration** sub menu bar, and then **Syslog** screen page will appear as follows.



Syslog: Disabled
Syslog Server IP Address: 0.0.0.0
Syslog Level: Emergency

3.11.4.1 Syslog Setting

Below is a description of the configuration parameters of this section.



Syslog: Disable
Syslog Server IP Address: 0.0.0.0
Syslog Level: Emergency

Syslog — Tick the checkbox to enable this feature. Or untick the checkbox to deactivate it.

Syslog Server IP Address — Specify the IP address of the Syslog server in the text box.

Syslog Level — Select one of the syslog levels from the pull down menu. The Residential Gateway will record log events at the chosen level and above. For example, if you choose *Error*, "error", "critical", "alert" and "emergency" events will be recorded.

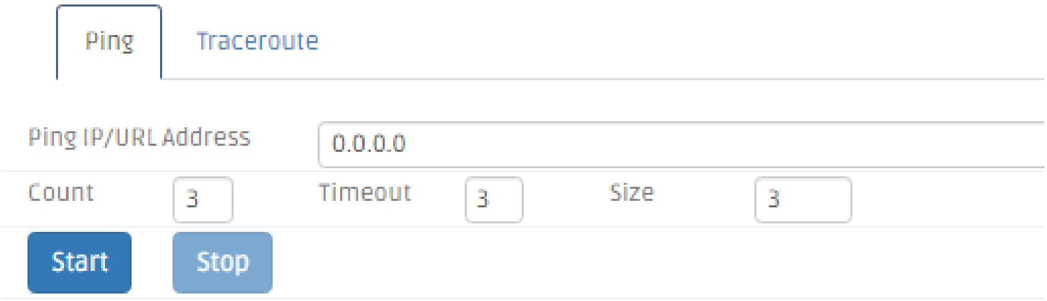
Level		Description
1	Emergency	System is unusable.

2	Alert	Emergent actions that must be taken immediately.
3	Critical	Critical conditions.
4	Error	Error conditions.
5	Warning	Warning conditions.
6	Notice	Normal but significant conditions.
7	informational	Keep informational events message.
8	Debug	Debug-level messages are logged.

Click _OK_ after you finish configuring the setting of this page.

3.11.5 Diagnostics

This page enables the network administrator to use ICMP to check the network connectivity. The Residential Gateway supports the diagnostic tools such as ICMP. It can emit ICMP Ping messages to a destination host on the Internet and see if it can receive the replies from the host. Select **Diagnostics** from **Administration** sub menu bar. Then, **Diagnostics** screen page will appear as follows:

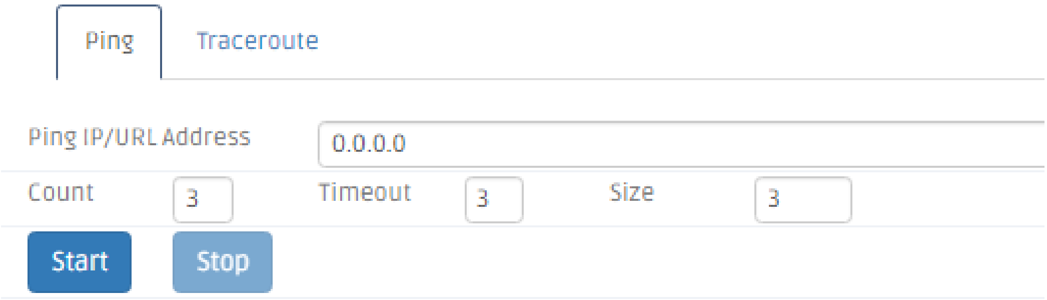


Ping IP/URL Address: 0.0.0.0

Count: 3 Timeout: 3 Size: 3

3.11.5.1 Ping

This section allows you to use ICMP to check the connectivity between the Residential Gateway and a host on the Internet. Below is a description of the configuration parameters of this section.



Ping IP/URL Address: 0.0.0.0

Count: 3 Timeout: 3 Size: 3

Ping IP Address — Specify an IP address as the destination of the ICMP Ping packets.

Count — Enter the repeat value that how many times should be pinged.

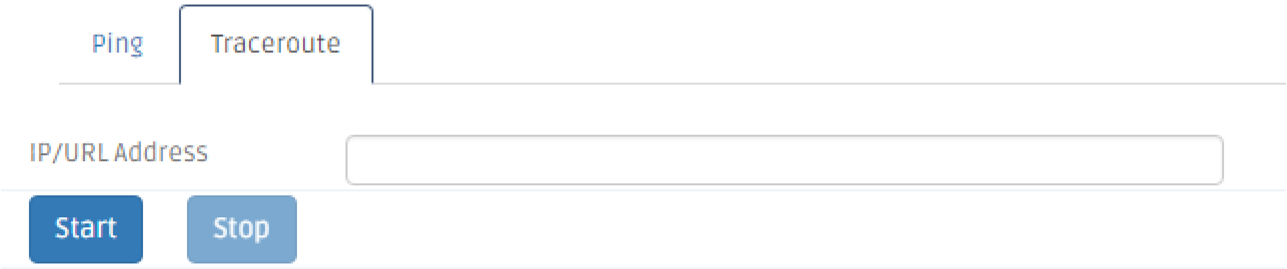
Timeout — Enter the timeout value when the specified IP address is not reachable. (optional)

Packet Size — Enter the packet size that would be sent. The allowable packet size is from 1 to 65500 bytes. (optional)

Click *Start* for the Residential Gateway to emit ICMP packets to the destination IP address. And the ICMP replies from the destination host or any other ICMP messages will be displayed in this section.

3.11.5.2 Traceroute

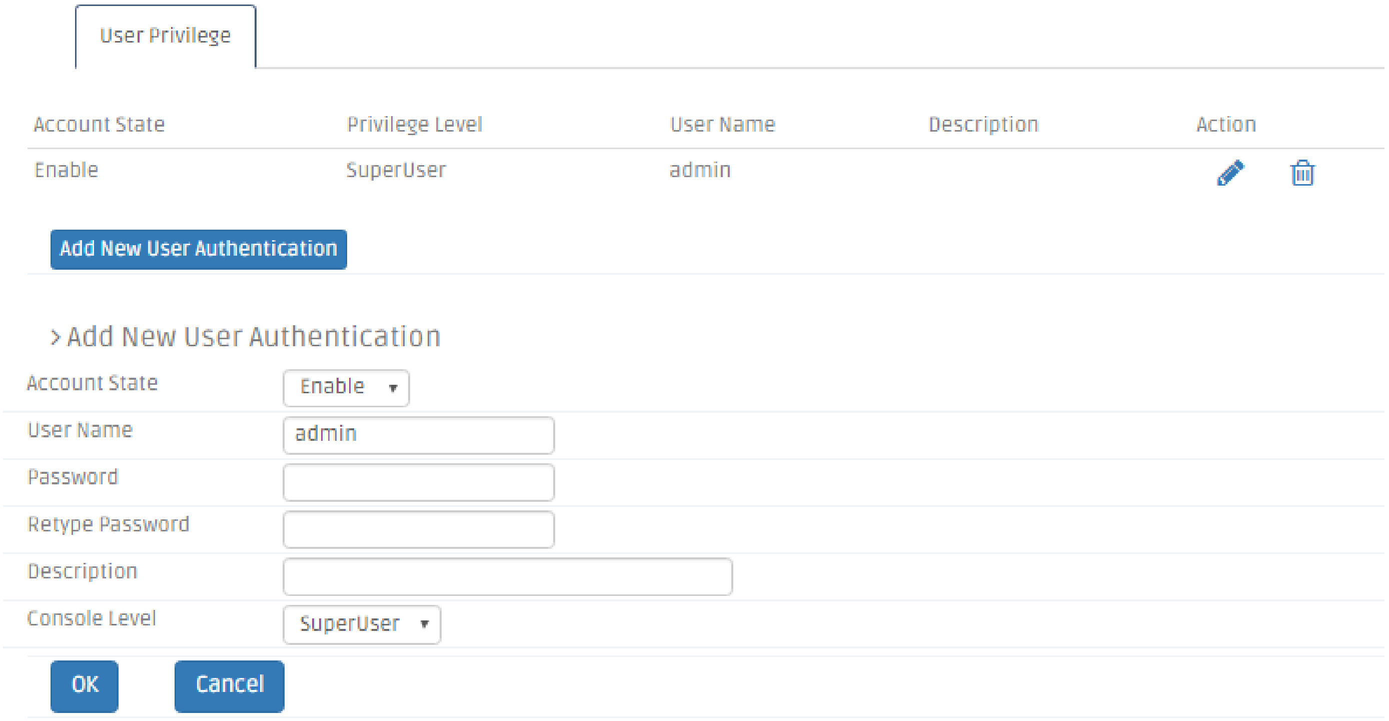
Traceroute is used to trach the path between the local host and the remote host. Enter the **traceroute** command in User mode. In this command, you can add an optional max hops value for the number of hops that packets are sent and received.



***IP/URL Address* —** Specify target IP address or URL.

3.11.6 User Privilege

This page enables the network administrator to modify the user account settings of the Residential Gateway. Select **User Privilege** from **Administration** sub menu bar. Then, **User Privilege** screen page will appear as follows:



Account State	Privilege Level	User Name	Description	Action
Enable	SuperUser	admin		✎ 🗑

› Add New User Authentication

Account State	Enable ▾
User Name	admin
Password	
Retype Password	
Description	
Console Level	SuperUser ▾

Account State — Shows the entry is enabled or disabled.

Privilege Level — Shows which authority the account is qualified for. Three privilege levels as follows.

Superuser — Full access right, including maintaining user account, system information, loading factory settings, etc..

Editor — Partial access right, unable to modify user account, system information and items under System Utility menu.

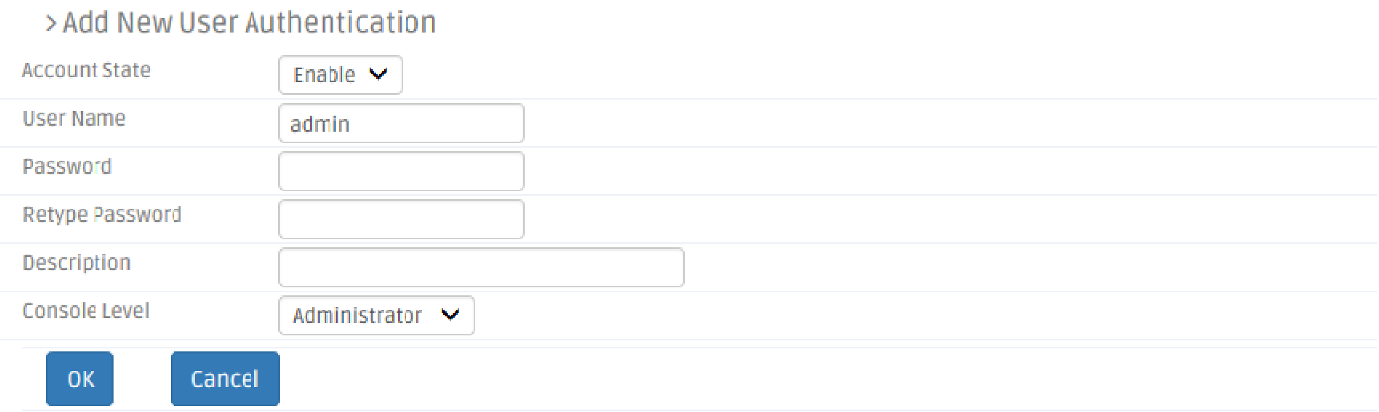
***Homeuser* —** Partial access right, less than superuser and editor, able to configure Setup (System information, DDNS, Network Setup), WiFi, Security, Applications, Administration (Diagnostics, User privilege, Save&Logout), etc.

Guest — Read-Only access privilege.

User Name —Shows a name for the user account.

Description — Shows the given remark for the account.

Action — If you want to edit an entry in this table, click _pencil icon_ under Action column.



> Add New User Authentication

Account State	Enable
User Name	admin
Password	
Retype Password	
Description	
Console Level	Administrator

Account State — Enable or disable this user account.

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

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

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

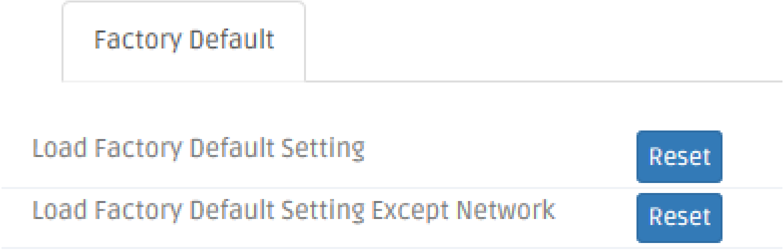
Description — Enter a unique description up to 35 alphanumeric characters for the user. This is mainly for reference only.

Console Level — Select the desired privilege for the console operation from the pull-down menu. Four operation privileges are available in the Gateway:

> ***Superuser*** — Full access right, including maintaining user account, system information, loading factory settings, etc..
>
> ***Editor*** — Partial access right, unable to modify user account, system information and items under System Utility menu.
>
> ***Homeuser* —** Partial access right, less than superuser and editor, able to configure Setup (System information, DDNS, Network Setup), WiFi, Security, Applications, Administration (Diagnostics, User privilege, Save&Logout), etc.
>
> ***Guest*** — Read-Only access privilege.

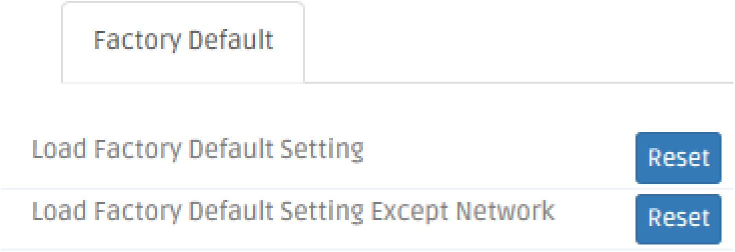
3.11.7 Backup/Restore

Select **Backup/Restore** from **Administration** sub menu bar. Then, **Backup/Restore** screen page will appear as follows:


Factory Default
Load Factory Default Setting
Reset
Load Factory Default Setting Except Network
Reset

3.11.8 Factory Default

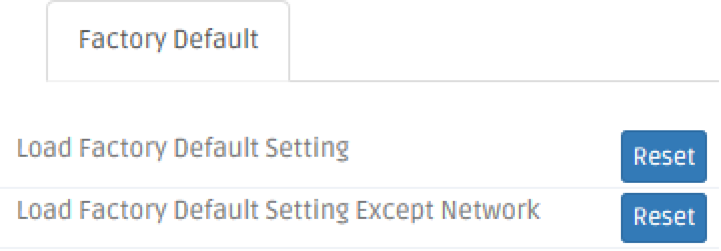
Select **Factory Default** from **Administration** sub menu bar. Then, **Factory Default** screen page will appear as follows:


Factory Default
Load Factory Default Setting
Reset
Load Factory Default Setting Except Network
Reset

3.11.8.1 Factory Default

Load Factory Setting will set all the configurations of the Gateway back to the factory default settings, including the IP and Gateway address. **Load Factory Setting** 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.

Load Factory Settings Except Network Configuration will set all the configurations of the Gateway back to the factory default settings. However, IP and Gateway addresses will not restore to the factory default. It 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 network connections.



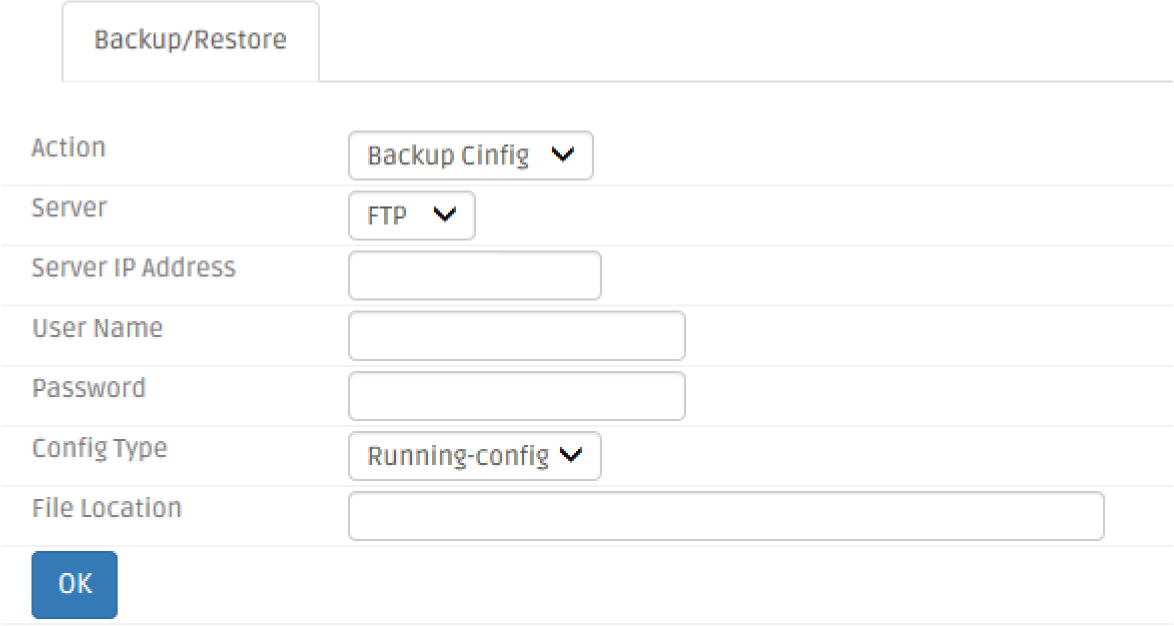
Factory Default

Load Factory Default Setting	Reset
Load Factory Default Setting Except Network	Reset

Click *Reset* to reset the Gateway to the default settings.

3.11.8.2 Backup/Restore

This section enables you to create a backup file for the current configuration of the Residential Gateway. And you can load a backup configuration file to restore the previous configuration. Below is a description of the configuration parameters of this section.



Backup/Restore

Action	Backup Cinfig
Server	FTP
Server IP Address	
User Name	
Password	
Config Type	Running-config
File Location	

OK

Backup — Click *Backup Config* to create a backup file for the current configuration of the Residential Gateway on the management computer.

Server — Click to choose the Server type HTTP or FTP.

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

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

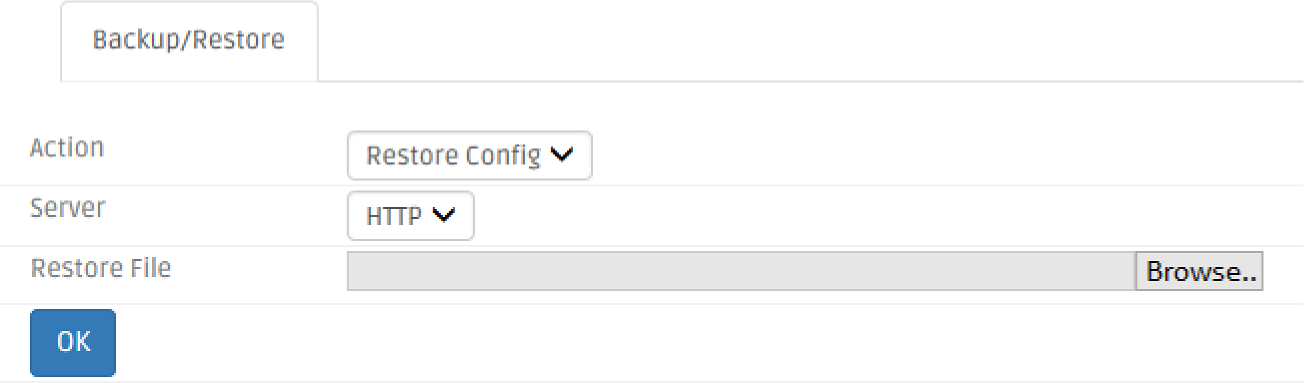
Config Type — There are three types of Config Type: Running-config, Default-config and Start-up-config.

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

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

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

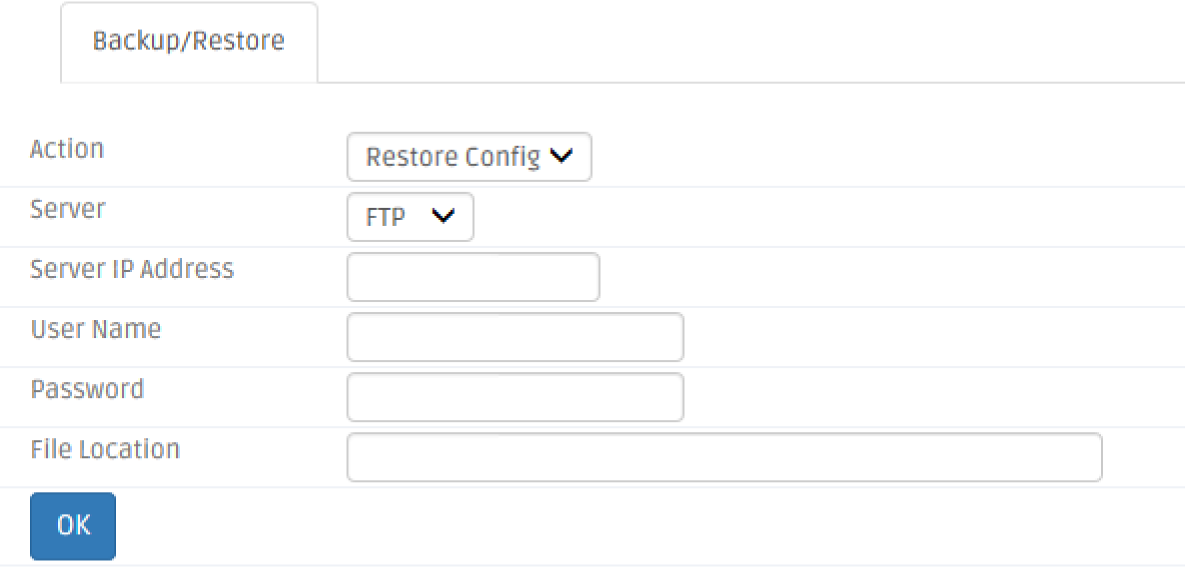
File Location — Specify the name of backup file.



Backup/Restore

Action	Restore Config
Server	HTTP
Restore File	Browse..

Restore using HTTP— If you want to load a backup file from the management computer, click *Browse* to find the path to the backup file in the pop-out window. Then, select the backup file after you find its path and click *Upload* to restore it to the Residential Gateway.



Backup/Restore

Action	Restore Config
Server	FTP
Server IP Address	
User Name	
Password	
File Location	

Restore using FTP— You may restore configuration using FTP server as long as following the procedure below.

Action — Click to choose Restore Config.

Server — Click to choose FTP.

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

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

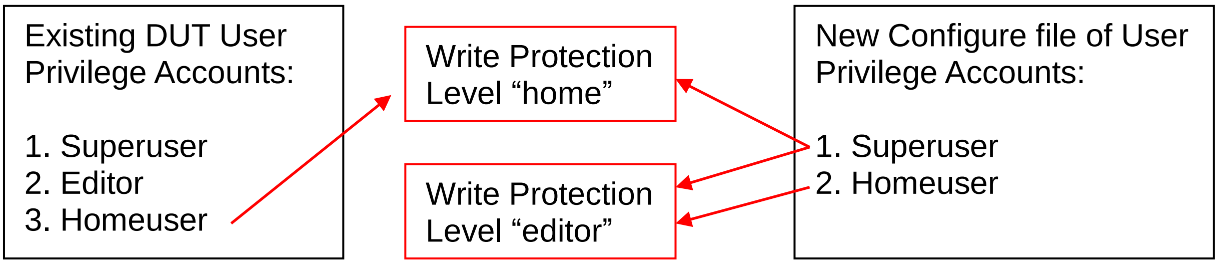
Password — Enter the specific password to access the File Server.

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

Note: For ISP, the default write protection level is set "home" in configuration file on the ground of safety, which means the following functions are unable to be overwritten when executing configure restoration.

1. DDNS
2. Network Setup (LAN-IP, DHCP Server, DHCP Reserved)
3. WiFi (Wireless Setup, Wireless Security)
4. Application (DMZ, Port Forwarding)
5. Security (Firewall, Packet Filter, URL Filter, VPN Pass-Through, UPnP, DDoS)
6. Administration (User Privilege) - Yet if the write protection level is "home", the user privilege level "superuser" and "editor" will be deleted except "homeuser". However, the "homeuser" is copied from either existing DUT or new configure file. It depends on the write protection level.

Assume that we have a setting of existing User Privilege in DUT and a configure file ready to be loaded.


Existing DUT User Privilege Accounts:
1. Superuser
2. Editor
3. Homeuser
Write Protection Level "home"
Write Protection Level "editor"
New Configure file of User Privilege Accounts:
1. Superuser
2. Homeuser

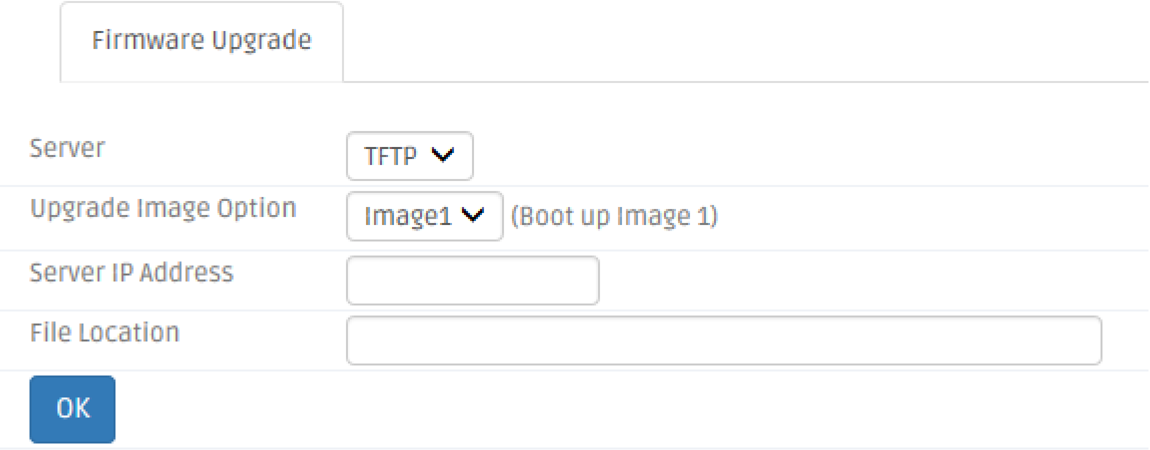
Here is the treatment of User Privilege of configure restoration:

A. Save the existing homeuser configuration in DUT
B. Reset the DUT back to default setting.
C. Check the write protection level. If the write protection level is "home", it loads DUT's homeuser configure back into DUT.

To overwrite all of configuration, please change the write protection level “home” into “editor”.In terms of User Privilege. If the write protection level is “editor”, it loads the homeuser of new homeuser configure file into DUT

3.11.9 Firmware Upgrade

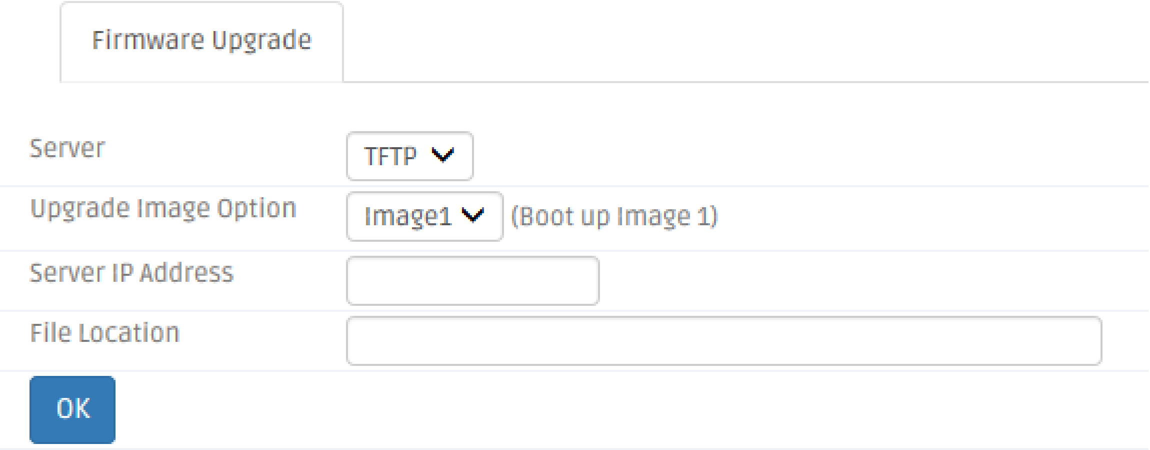
This page enables the network administrator to upgrade the firmware of the Residential Gateway. Select **Firmware Upgrade** from **Administration** sub menu bar. Then, **Firmware Upgrade** screen page will appear as follows:



Firmware Upgrade

Server	TFTP
Upgrade Image Option	Image1 (Boot up Image 1)
Server IP Address	
File Location	

3.11.9.1 TFTP Upgrade



Firmware Upgrade

Server	TFTP
Upgrade Image Option	Image1 (Boot up Image 1)
Server IP Address	
File Location	

Server — Select the TFTP protocol.

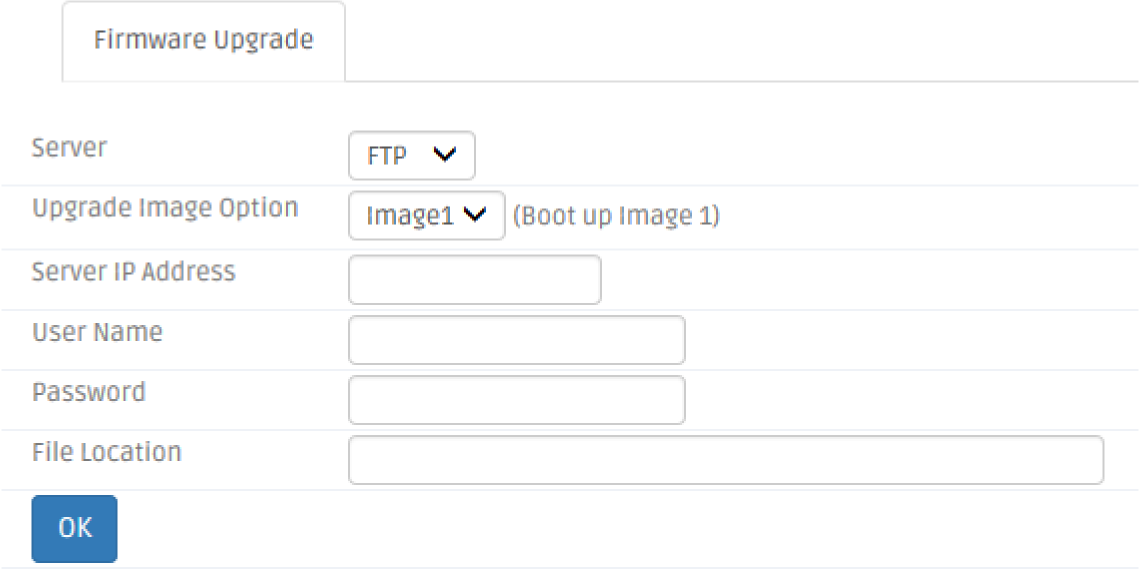
Upgrade Image Option — Select the Image you want to boot up.

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

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

Click **OK** to start the download process and receive files from the server.

3.11.9.2 FTP Upgrade



Server	FTP
Upgrade Image Option	Image1 (Boot up Image 1)
Server IP Address	
User Name	
Password	
File Location	

Server —Select the FTP protocol.

Upgrade Image Option — Select the Image you want to boot up.

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

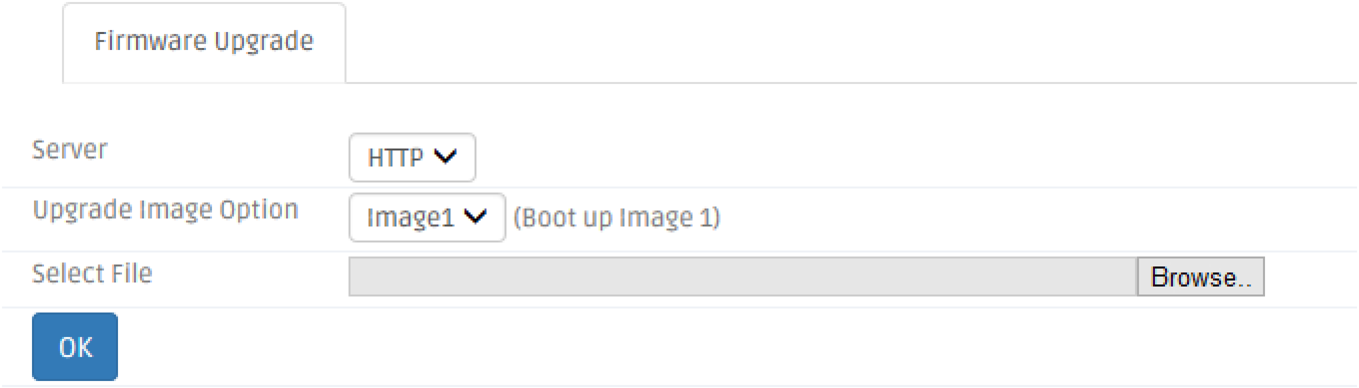
User Name — Enter the specific username to access the File Server.

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

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

Click **OK** to start the download process and receive files from the server.

3.11.9.3 HTTP Upgrade



Firmware Upgrade

Server	HTTP
Upgrade Image Option	Image1 (Boot up Image 1)
Select File	Browse..

OK

Server —Select the FTP protocol.

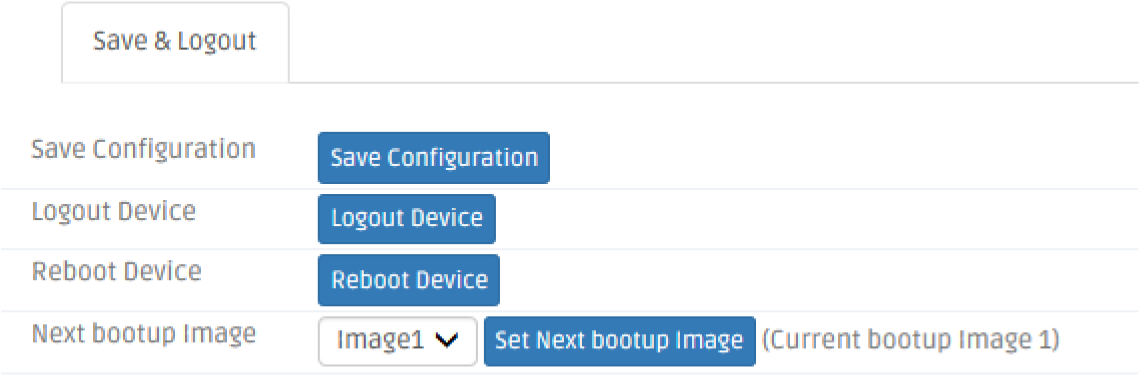
Upgrade Image Option — Select the Image you want to boot up.

Select File —Click browse, select the desired file**.**

Click **OK** to start the download process and receive files

3.11.10 Save&Logout

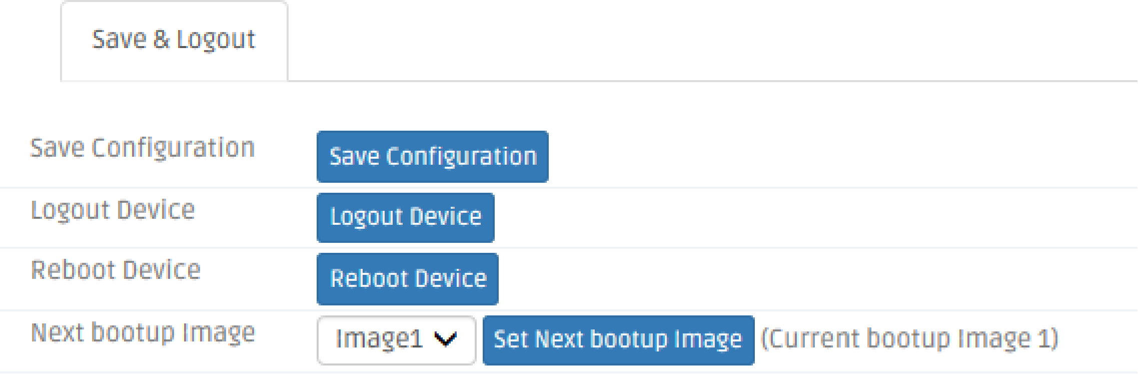
Select **Save and Logout** from **Administration** sub menu bar. Then, **Save and Logout** screen page will appear as follows:



Save & Logout

Save Configuration	Save Configuration
Logout Device	Logout Device
Reboot Device	Reboot Device
Next bootup Image	Image1 Set Next bootup Image (Current bootup Image 1)

3.11.10.1 Save&Logout



Save Configuration Click *Save Configuration* to save the current settings of the Residential Gateway.

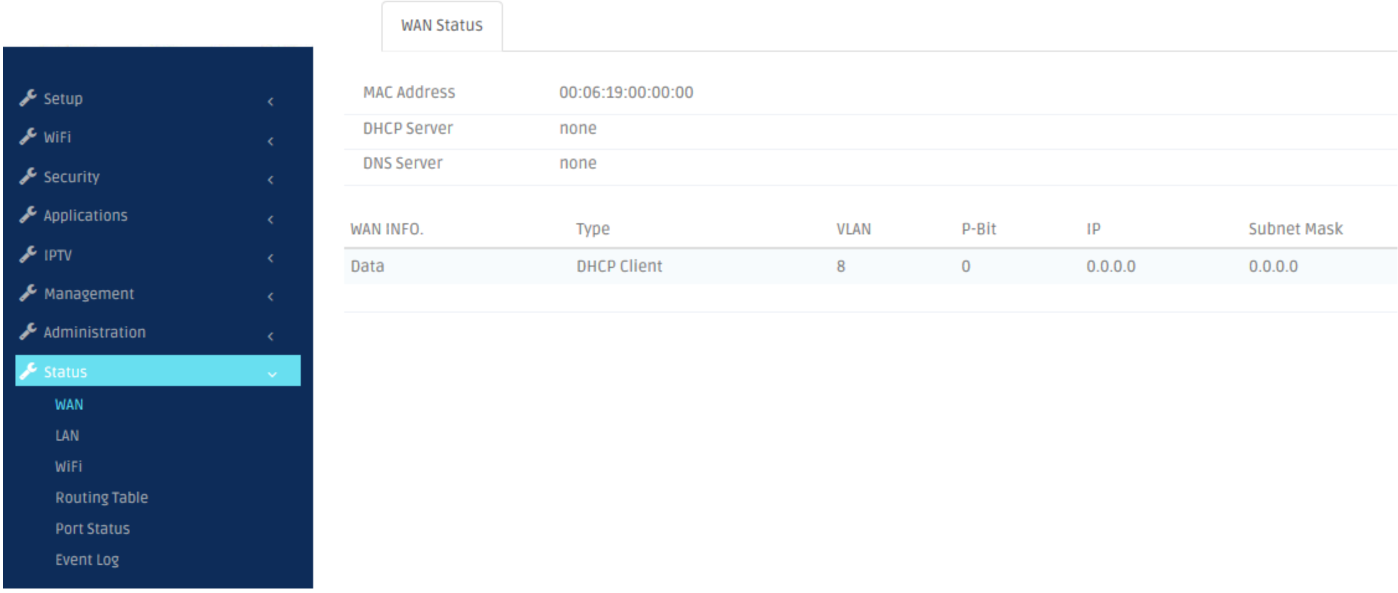
Logout Device Click *Logout Device* to log out your account,

Reboot Device Click *Reboot Device* to restart the Residential Gateway.

Next bootup Image Click drop-down box to select Image and click *Set Next bootup Image* to set the desired next bootup Image.

3.12 Status

Select **Status** in the Main Menu bar. And the sub-items – **WAN**, **LAN**, **WiFi**, **Routing Table**, **Port Status and Event Log**– will show up on the sub menu bar.

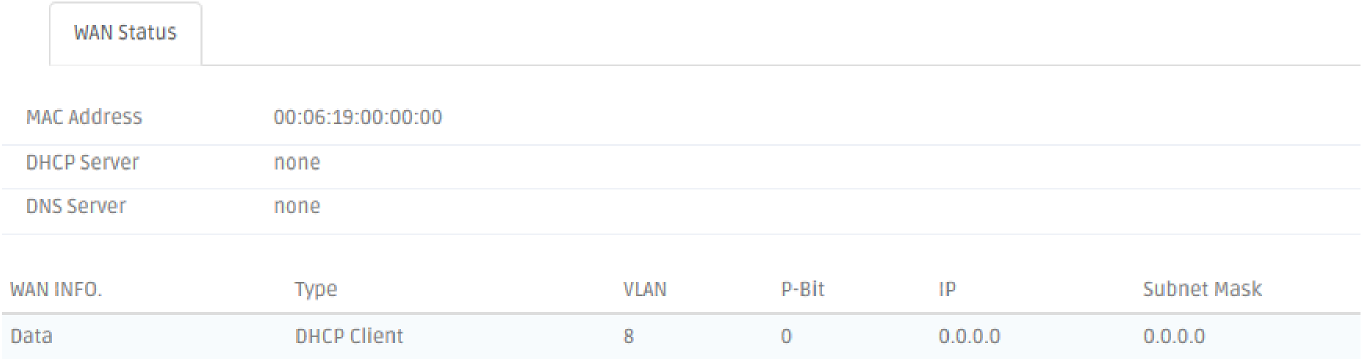


MAC Address	00:06:19:00:00:00
DHCP Server	none
DNS Server	none

WAN INFO.	Type	VLAN	P-Bit	IP	Subnet Mask
Data	DHCP Client	8	0	0.0.0.0	0.0.0.0

3.12.1 WAN

This page displays information about the WAN port and the WAN interfaces. Select **WAN** from the **Status** sub menu bar. Then, **WAN** screen page appears as follows:



MAC Address	00:06:19:00:00:00
DHCP Server	none
DNS Server	none

WAN INFO.	Type	VLAN	P-Bit	IP	Subnet Mask
Data	DHCP Client	8	0	0.0.0.0	0.0.0.0

This is a view-only section which displays information about the WAN port's status and the WAN interfaces of the Residential Gateway. Below is a description of each item in this section.

MAC Address — This is the MAC address of the Residential Gateway on the public network.

DHCP Server — This is the DHCP server which the Residential Gateway has on the public network.

DNS Server— This is the DNS server which the Residential Gateway has on the public network.

And the table in this section displays the current status of each WAN interface which is enabled or activated. Below is the description for each column of this table.

WAN INFO. — This is the type of the WAN interface.

Type — This is the Internet access type of this WAN interface.

VLAN — This is the VLAN ID of this WAN interface.

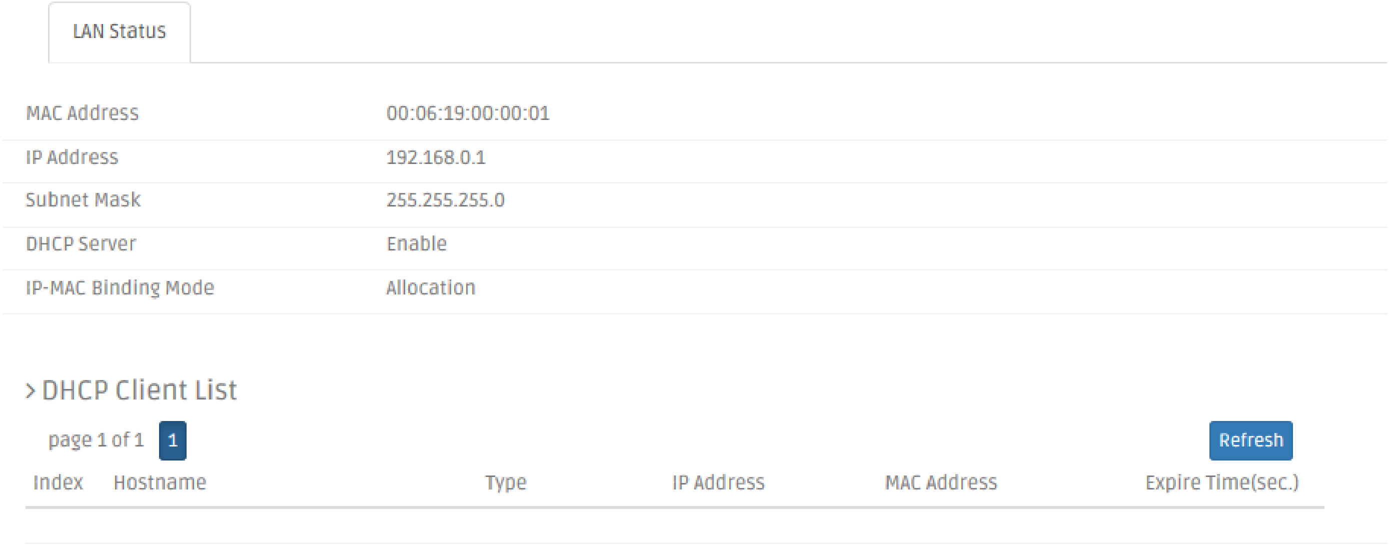
P-Bit — This is the P-bit value of this WAN interface.

IP — This is the IP address which this interface has.

Subnet Mask — This is the he subnet mask of this WAN interface.

3.12.2 LAN

This page displays information of the Residential Gateway on the private network. Select **LAN** from the **Status** sub menu bar. Then, **LAN** screen page appears as follows:



MAC Address	00:06:19:00:00:01
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
IP-MAC Binding Mode	Allocation

> DHCP Client List

Index	Hostname	Type	IP Address	MAC Address	Expire Time(sec.)

And for more details, please refer to the description of the individual section below.

LAN Status: This is a view-only section which displays information about the the Residential Gateway on the private network. Below is a description of each item in this section.

MAC Address — This is the MAC address which the Residential Gateway has on the private network

IP Address — This is the private IP address of the Residential Gateway.

Subnet Mask — This is the subnet mask which the Residential Gateway has for its private IP address.

DHCP Server — It is *Enabled* when the DHCP server function of the Residential Gateway is activated. And it is *Disabled* when the DHCP server function of the Residential Gateway is deactivated.

IP-MAC Binding Mode — Shows the mode that are currently using.

DHCP Client List This is a view-only section. It displays the list of the DHCP clients which are assigned IP addresses by the Residential Gateway.

Index — The number of each client assigned.

Host Name — The name of each host.

Type — Shows the type of each host.

IP Address — The IP Address of each host.

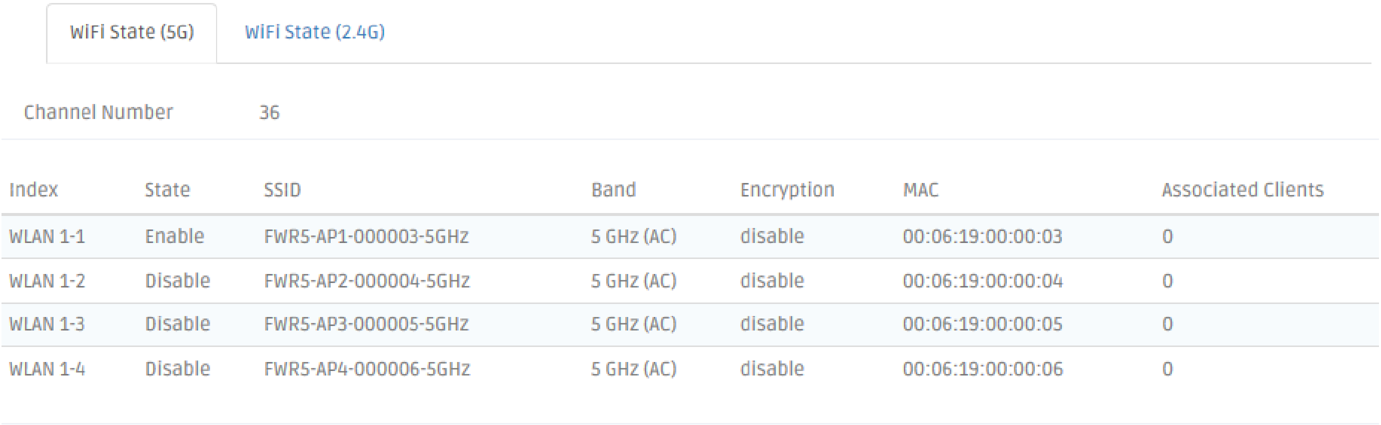
MAC Address — The MAC Address of each host.

Expire Time(sec) — The lease time in second that DHCP server assigns the host for.

3.12.3 WiFi

This section shows the current status of WiFi.

For Bandwidth 5G:



Channel Number 36

Index	State	SSID	Band	Encryption	MAC	Associated Clients
WLAN 1-1	Enable	FWR5-AP1-000003-5GHz	5 GHz (AC)	disable	00:06:19:00:00:03	0
WLAN 1-2	Disable	FWR5-AP2-000004-5GHz	5 GHz (AC)	disable	00:06:19:00:00:04	0
WLAN 1-3	Disable	FWR5-AP3-000005-5GHz	5 GHz (AC)	disable	00:06:19:00:00:05	0
WLAN 1-4	Disable	FWR5-AP4-000006-5GHz	5 GHz (AC)	disable	00:06:19:00:00:06	0

Index — The number of each WiFi service set assigned.

State — Shows the WiFi service set is enabled or disabled.

SSID — Shows identification number of service set.

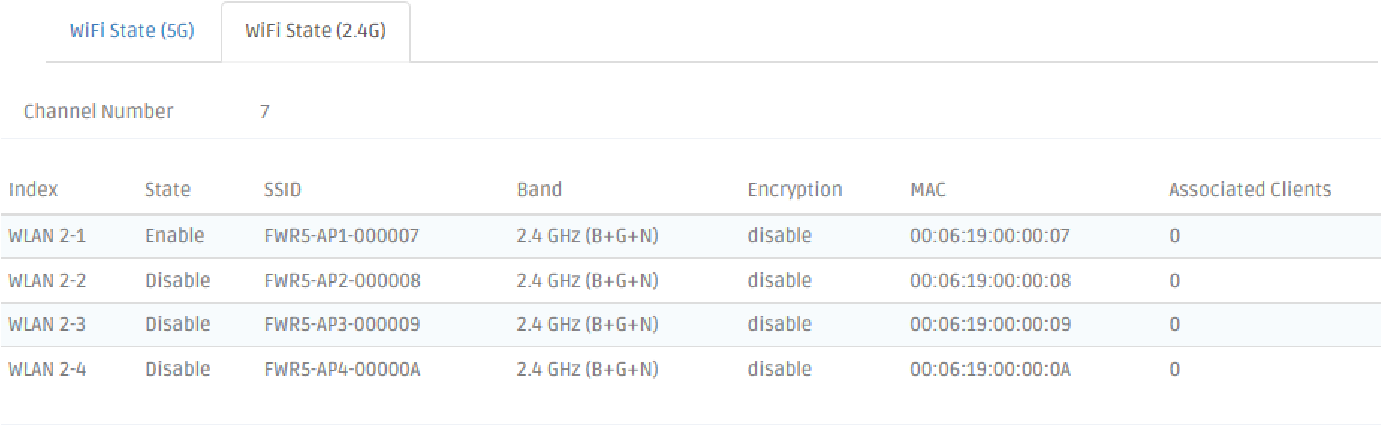
Band — Shows the bandwidth of the service set.

Encryption — Shows the encryption mechanism is enabled or disabled.

MAC — The MAC address of the service set.

Associated Clients — Shows the number of users who are connected with the WiFi service set.

For Bandwidth 2.4G:



Channel Number 7

Index	State	SSID	Band	Encryption	MAC	Associated Clients
WLAN 2-1	Enable	FWR5-AP1-000007	2.4 GHz (B+G+N)	disable	00:06:19:00:00:07	0
WLAN 2-2	Disable	FWR5-AP2-000008	2.4 GHz (B+G+N)	disable	00:06:19:00:00:08	0
WLAN 2-3	Disable	FWR5-AP3-000009	2.4 GHz (B+G+N)	disable	00:06:19:00:00:09	0
WLAN 2-4	Disable	FWR5-AP4-00000A	2.4 GHz (B+G+N)	disable	00:06:19:00:00:0A	0

Index — The number of each WiFi service set assigned.

State — Shows the WiFi service set is enabled or disabled.

SSID — Shows identification number of service set.

Band — Shows the bandwidth of the service set.

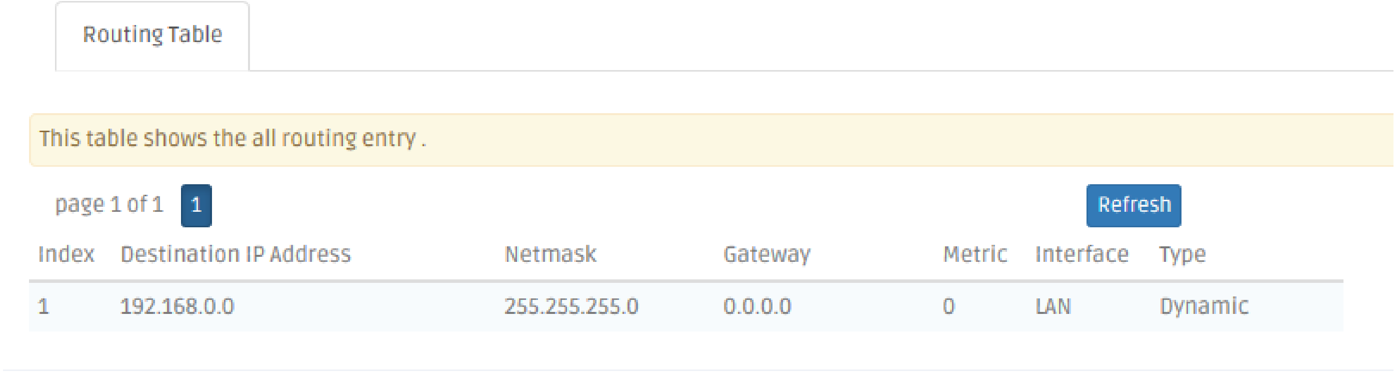
Encryption — Shows the encryption mechanism is enabled or disabled.

MAC — The MAC address of the service set.

Associated Clients — Shows the number of users who are connected with the WiFi service set.

3.12.4 Routing Table

Select **Routing Table** from the **Status** sub menu bar. Then, **Routing Table** screen page appears as follows:



This table shows the all routing entry .

Index	Destination IP Address	Netmask	Gateway	Metric	Interface	Type
1	192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	Dynamic

Routing Table This section displays the routing table of the Residential Gateway. The routing table will include a default route, a route to the WAN and all the routes to the LAN. And it consists of both the configured static routes and the dynamic routes learned by RIP (or RIPv2).

Index — The number of each route assigned.

Destination IP Address —The destination IP address of the route.

Netmask — The subnet mask of the destination network of the route.

Gateway — The IP address of a gateway through which this route will send the packets to the destination network.

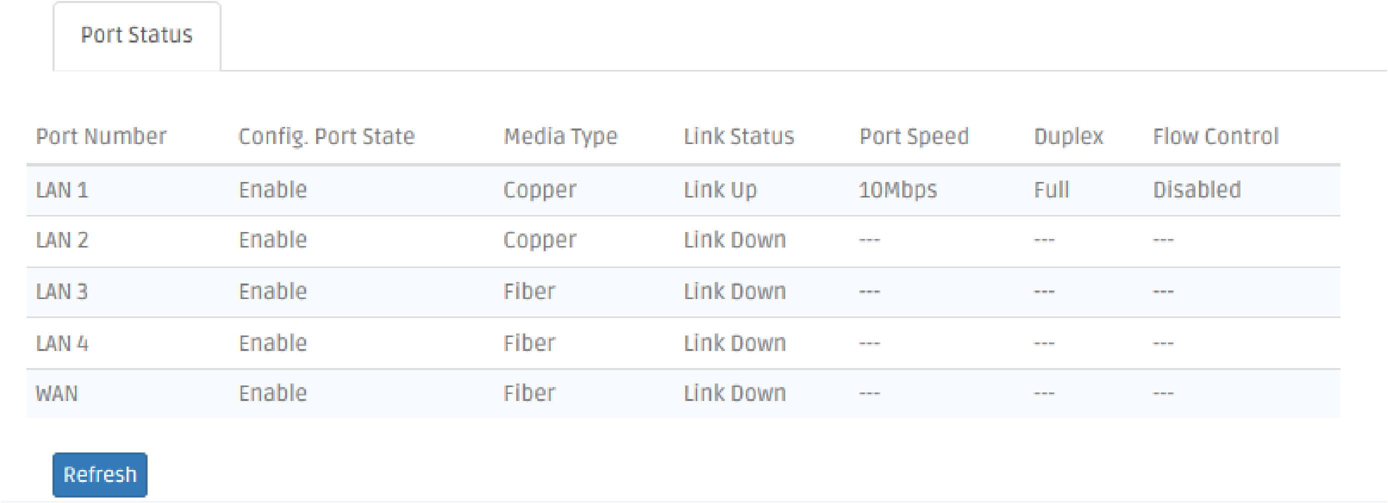
Metric — Metric is the cost of a route to a destination network.

Interface — An interface of the Residential Gateway from which the route will forward the packets to the destination network.

Type — Shows the type is Static or Dynamic.

3.12.5 Port Status

Select **Port Status** from the **Status** sub menu bar. Then, the following screen page appears.



Port Number	Config. Port State	Media Type	Link Status	Port Speed	Duplex	Flow Control
LAN 1	Enable	Copper	Link Up	10Mbps	Full	Disabled
LAN 2	Enable	Copper	Link Down	---	---	---
LAN 3	Enable	Fiber	Link Down	---	---	---
LAN 4	Enable	Fiber	Link Down	---	---	---
WAN	Enable	Fiber	Link Down	---	---	---

Port Status This is a view-only section which displays information about the port status of the Residential Gateway. Below is a description of each item in this section.

Port Number — This is the port number.

Config. Port State — This field shows if the port is enabled or disabled.

Media Type — It is the media type of this port, either *Copper* or *Fiber*.

Link Status — It is the current link status of the port, either *Link Up* or *Link Down*..

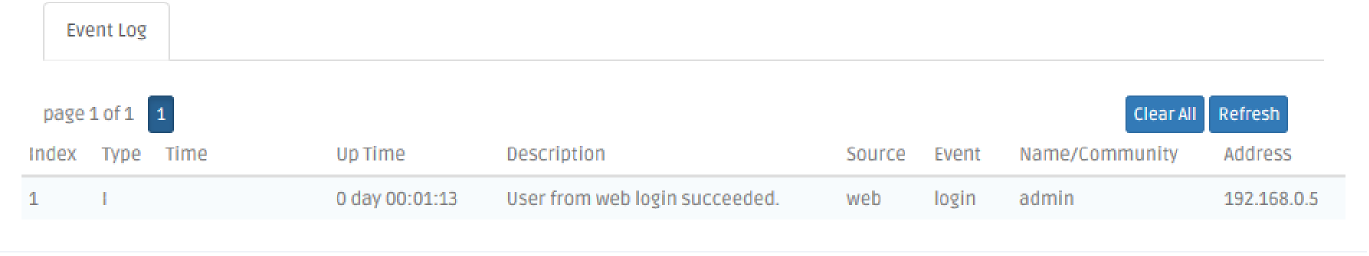
Port Speed — It is the channel of the wireless network of the Residential Gateway.

Duplex — This field shows that the port is in the full duplex mode when it links up.

Flow Control — It is the current status of the flow control function, either *Enabled* or *Disabled*.

3.12.6 Event Log

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



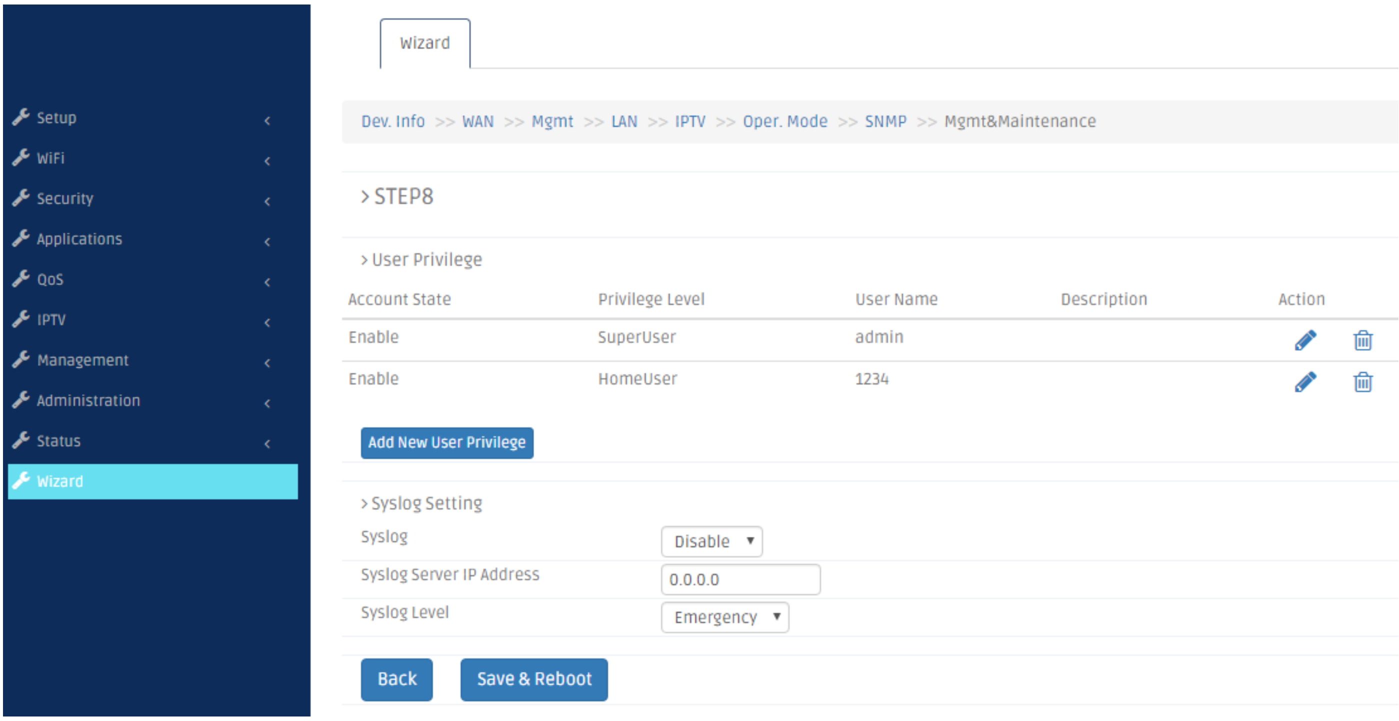
Index	Type	Time	Up Time	Description	Source	Event	Name/Community	Address
1	I		0 day 00:01:13	User from web login succeeded.	web	login	admin	192.168.0.5

Click **Refresh** to renew all Event Log records.

Click **Clear All** to delete all Event Log records.

3.13 Wizard

For beginners, this section is a quick guide for configuration step by step. Here is the procedure : Dev. Info.→ WAN → Mgmt → LAN → IPTV → Oper. Mode → SNMP → Mgmt&Maintenance



Setup
WiFi
Security
Applications
QoS
IPTV
Management
Administration
Status
Wizard
Wizard
Dev. Info >> WAN >> Mgmt >> LAN >> IPTV >> Oper. Mode >> SNMP >> Mgmt&Maintenance

> STEP8

> User Privilege

Account State	Privilege Level	User Name	Description	Action
Enable	SuperUser	admin		✎ 🗑
Enable	HomeUser	1234		✎ 🗑

> Syslog Setting

Syslog	Disable ▾
Syslog Server IP Address	0.0.0.0
Syslog Level	Emergency ▾

4. SNMP NETWORK MANAGEMENT

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP consists of the following key components:

Managed device is a network node that contains SNMP agent. Managed devices collect and store management information and make this information available to NMS using SNMP. Managed devices can be switches/Hub, etc.

MIB (Management Information Base) defines the complete manageable entries of the managed device. These MIB entries can be either read-only or read-write. For example, the System Version is read-only variables. The Port State Enable or Disable is a read-write variable and a network administrator can not only read but also set its value remotely.

SNMP Agent is a management module resides in the managed device that responds to the SNMP Manager request.

SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources required for the complete network management. SNMP Manager is often composed by desktop computer/work station and software program such as HP OpenView. Totally, 4 types of operations are used between SNMP Agent & Manager to change MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

GET: This command is used by an SNMP Manager to monitor managed devices. The SNMP Manager examines different variables that are maintained by managed devices.

GET Next: This command provides traversal operation and is used by the SNMP Manager to sequentially gather information in variable tables, such as a routing table.

SET: This command is used by an SNMP Manager to control managed devices. The NMS changes the values of variables stored within managed devices.

Trap: Trap is used by the managed device to report asynchronously a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager. The system built-in management module also supports SNMP management. Users must install the MIB file before using the SNMP based network management system. The MIB file is on a disc or diskette that accompanies the system. The file name extension is .mib, which SNMP based compiler can read.

Please refer to the appropriate documentation for the instructions of installing the system private MIB.

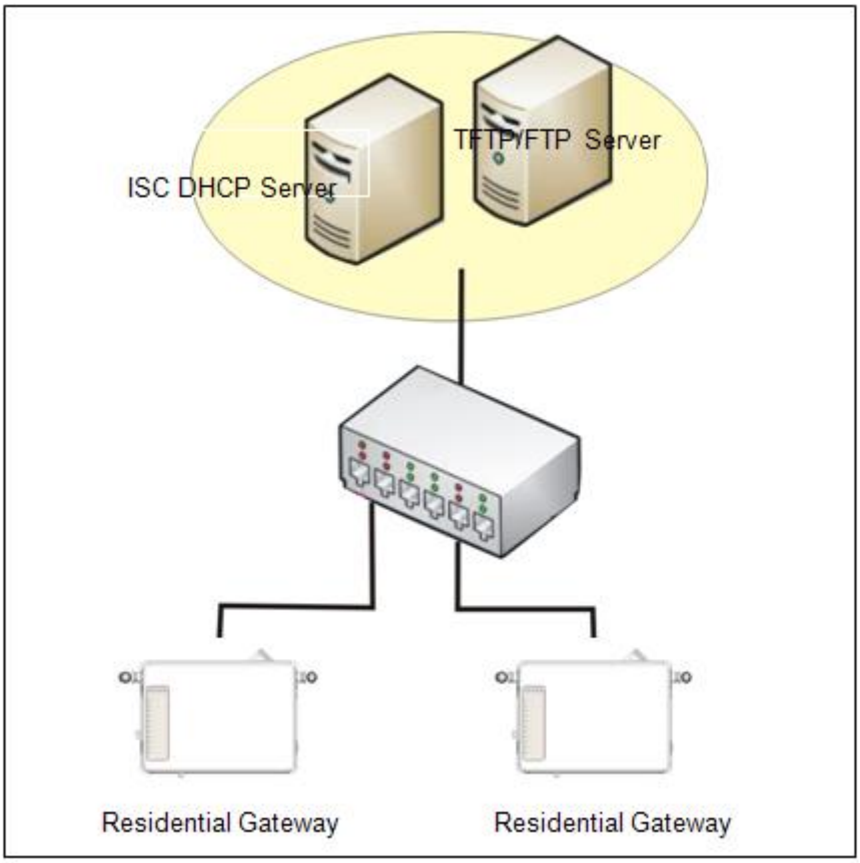
APPENDIX A: Set Up DHCP Auto-Provisioning

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

A. Setup Procedures

Step 1. Setup Environment

DHCP Auto-provisioning-enabled products that you purchased support the DHCP option 60 to work as a DHCP client. The system includes ISC DHCP server, File server (TFTP or FTP) and the Residential Gateway.



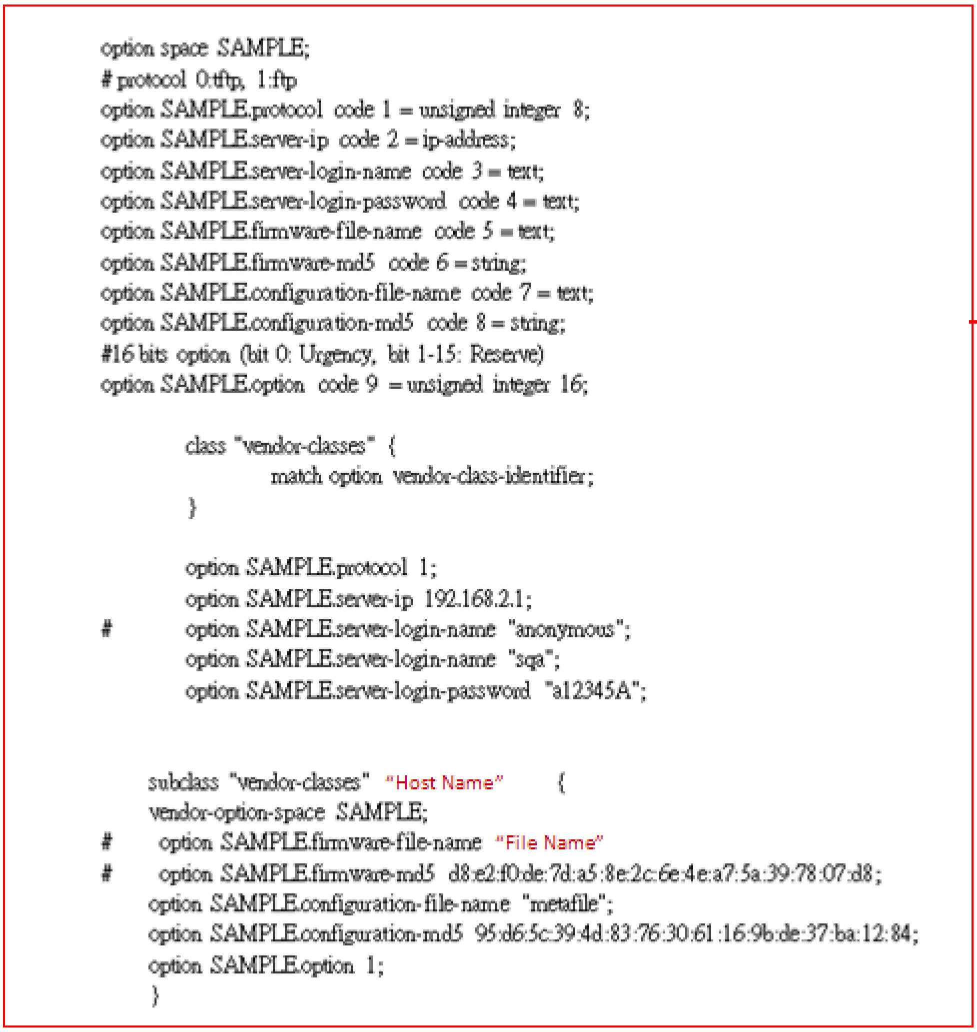
Typology Example

Step 2. Prepare “dhcpd.conf” file

You can find this file in Linux ISC DHCP server.
/usr/local/etc/dhcpd.conf

Step 3. Copy the marked text to “dhcpd.conf”

A sample of dhcp text is provided in Appendix B. Please copy the marked area to “dhcpd.conf” file.

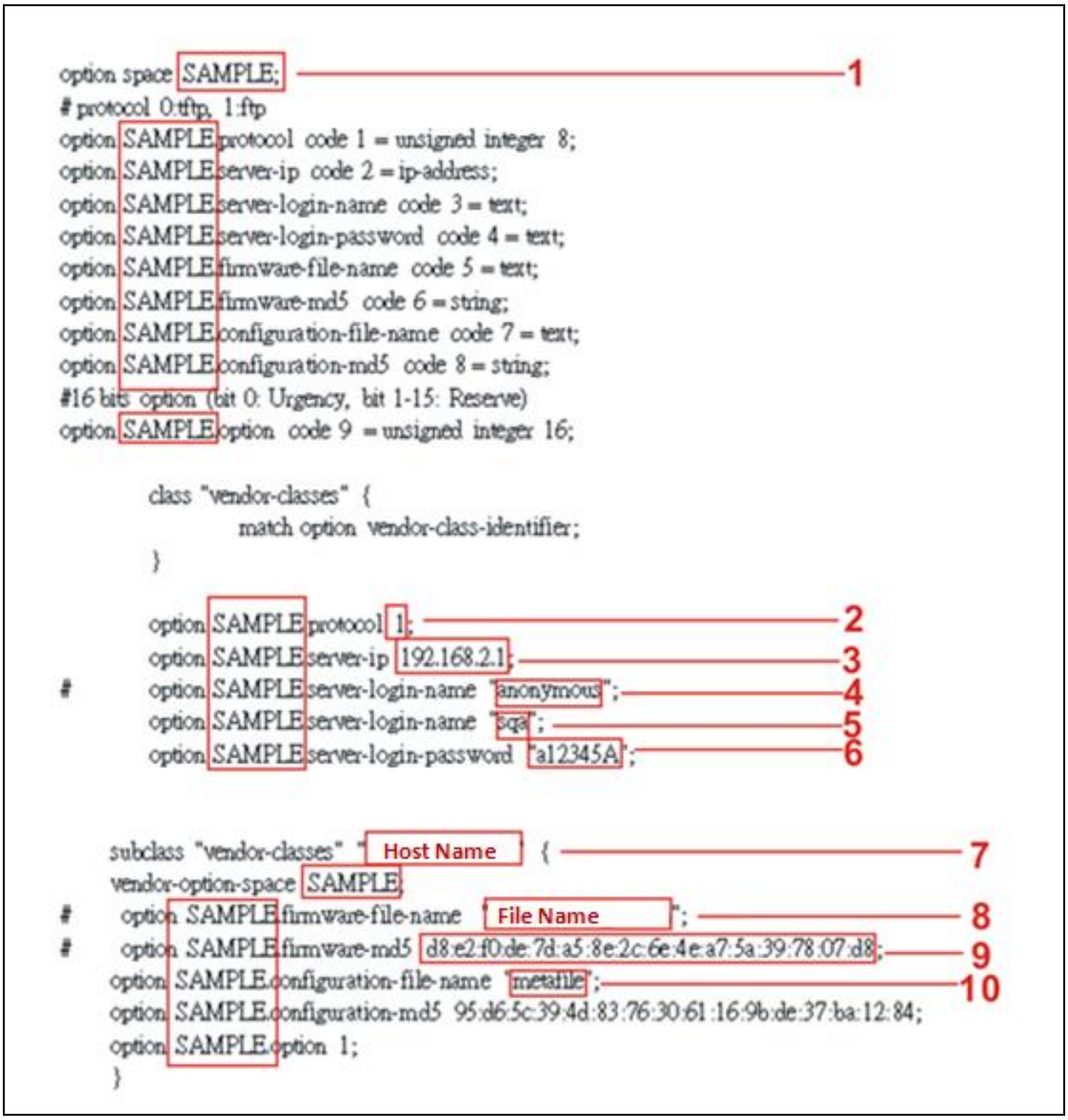


```
option space SAMPLE;
# protocol 0:tftp, 1:ftp
option SAMPLE.protocol code 1 = unsigned integer 8;
option SAMPLE.server-ip code 2 = ip-address;
option SAMPLE.server-login-name code 3 = text;
option SAMPLE.server-login-password code 4 = text;
option SAMPLE.firmware-file-name code 5 = text;
option SAMPLE.firmware-md5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

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

        option SAMPLE.protocol 1;
        option SAMPLE.server-ip 192.168.2.1;
#       option SAMPLE.server-login-name "anonymous";
        option SAMPLE.server-login-name "sqa";
        option SAMPLE.server-login-password "a12345A";


    subclass "vendor-classes" "Host Name"      {
    vendor-option-space SAMPLE;
#    option SAMPLE.firmware-file-name "File Name"
#    option SAMPLE.firmware-md5 d8:e2:f0:de:7d:a5:8e:2c:6e:4e:a7:5a:39:78:07:d8;
    option SAMPLE.configuration-file-name "metafile";
    option SAMPLE.configuration-md5 95:d6:5c:39:4d:83:76:30:61:16:9b:de:37:ba:12:84;
    option SAMPLE.option 1;
    }
```

Copy the text to
dhcpd.conf file

Sample dhcp text

Step 4. Modify “dhcpd.conf” file



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

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

        option SAMPLE.protocol 1;
        option SAMPLE.server-ip 192.168.2.1;
#       option SAMPLE.server-login-name "anonymous";
        option SAMPLE.server-login-name "sqa";
        option SAMPLE.server-login-password "a12345A";

    subclass "vendor-classes" "Host Name" {
    vendor-option-space SAMPLE;
#     option SAMPLE.firmware-file-name "File Name";
#     option SAMPLE.firmware-md5 d8:e2:f0:de:7d:a5:8e:2c:6e:4e:a7:5a:39:78:07:d8;
    option SAMPLE.configuration-file-name "metafile";
    option SAMPLE.configuration-md5 95:d6:5c:39:4d:83:76:30:61:16:9b:de:37:ba:12:84;
    option SAMPLE.option 1;
    }
```

Modify the marked area with your own settings.

1. This value is configurable and can be defined by users.
2. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
3. Specify the FTP or TFTP IP address.
4. Login FTP server anonymously.
5. Specify FTP Server login name.
6. Specify FTP Server login password.
7. Specify the product model name.
8. Specify the firmware filename.
9. Specify the MD5 for firmware image. The format of MD5 might be the same as the one in the sample text.
10. Specify the configuration image filename.

Step 5. Generate a Configuration File

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

In order for your Residential Gateway to retrieve the correct configuration image in TFTP/FTP Server, please use the following rule to define the configuration image’s filename. The filename should contain the configuration image filename specified in **dhcpd.conf** followed by the last three octets of your device’s MAC address. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile” and the MAC address of your device is “00:06:19:03:21:80”, the configuration image filename should be named to “metafile032180.dat”.

Step 6. Place a copy of Firmware and Configuration File in TFTP/FTP Server

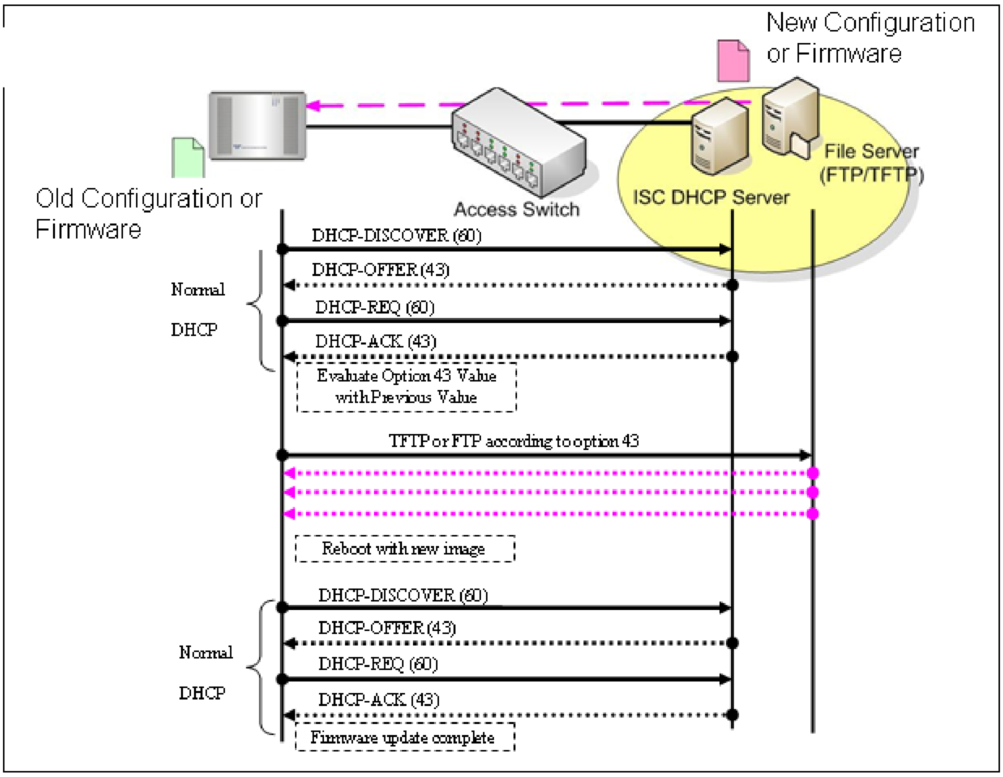
The TFTP/FTP File server should include the following items:

1. Firmware image
2. Configuration image
3. User account for your device (For FTP server only)

B. Auto-Provisioning Process

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

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



APPENDIX B: DHCP Text Sample

```
default-lease-time 90;
max-lease-time 7200;


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

subnet 192.168.2.0 netmask 255.255.255.0 {
        range 192.168.2.1 192.168.2.99;
    option subnet-mask   255.255.255.0;
        option broadcast-address 192.168.2.255;
        option routers 192.168.2.2;
    option domain-name-servers 168.95.1.1, 168.95.192.1, 192.168.2.2;

 host   CTS-FAE {
 hardware ethernet 00:14:85:06:5A:06;
 fixed-address 192.168.2.99;
 }

}
#Please copy the text below to your dhcpd.conf file#

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

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

        option SAMPLE.protocol 1;
        option SAMPLE.server-ip 192.168.2.1;
#       option SAMPLE.server-login-name "anonymous";
        option SAMPLE.server-login-name "sqa";
        option SAMPLE.server-login-password "a12345A";


    subclass "vendor-classes" "Host Name of the Residential Gateway" {
    vendor-option-space SAMPLE;
#     option SAMPLE.firmware-file-name "Name of the Firmware File";
#     option SAMPLE.firmware-md5 d8:e2:f0:de:7d:a5:8e:2c:6e:4e:a7:5a:39:78:07:d8;
    option SAMPLE.configuration-file-name "metafile";
    option SAMPLE.configuration-md5 95:d6:5c:39:4d:83:76:30:61:16:9b:de:37:ba:12:84;
    option SAMPLE.option 1;
    }
```

This page is intentionally left blank.