FWRIII-3105-N

4 ports 10/100/1000Mbps RJ-45; built-in IEEE802.11n WiFi and 1 port 1000Mbps fiber optics uplink Residential Gateway

FWRIII-3105-N-DR

4 ports 10/100/1000Mbps RJ-45; built-in IEEE802.11n WiFi and 1 port 100/1000Mbps fiber optics uplink Residential Gateway

FWRIII-3105SFP-CW-N-DR

4 ports 10/100/1000Mbps RJ-45; built-in IEEE802.11n WiFi and 1 uplink port combo (10/100/1000Mbps RJ-45 and 100/1000Mbps SFP slot) Residential Gateway

FWRIII-3105TP-N

4 ports 10/100/1000Mbps RJ-45; built-in IEEE802.11n WiFi and 1 port 10/100/1000Mbps RJ-45 uplink Residential Gateway

Network Management

User's Manual

Version 0.93

Trademarks

Contents 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	Date	Description
0.93	20150226	Revise WLAN link speed of channel width in section 2.5.1

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 Front, Rear and Top-Front Panel

Figure 1-1~1-9 show the front, back and top views of the 802.11n device:

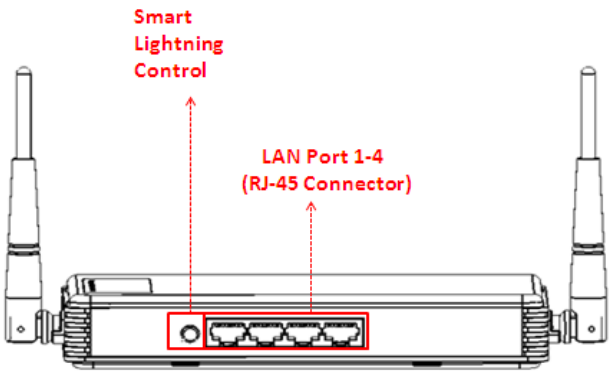


Figure 1-1. Front Panel of FWRIII-3105-N-DR

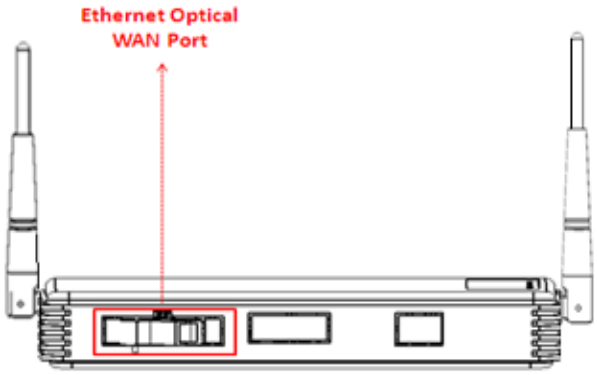


Figure 1-2. Back Panel of FWRIII-3105-N-DR

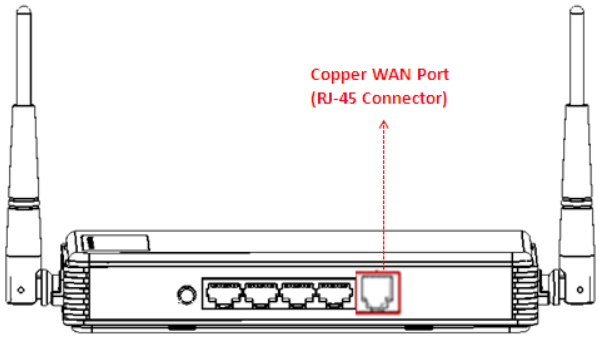


Figure 1-3. Front Panel of FWRIII-3105SFP-CW-N-DR

Figure 1-4. Back Panel of FWRIII-3105-SFP-CW-N-DR

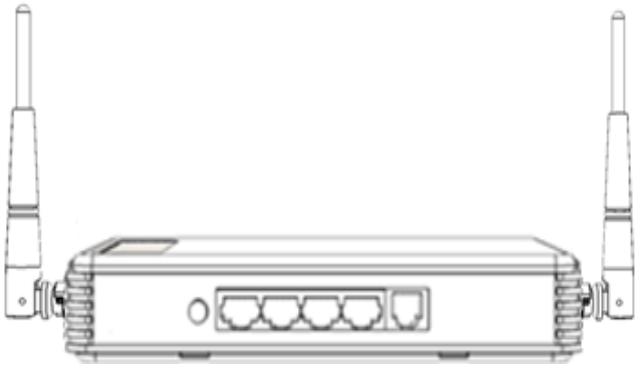


Figure 1-5. Front Panel of FWRIII-3105TP-N

Figure 1-6. Back Panel of FWRIII-3105TP-N

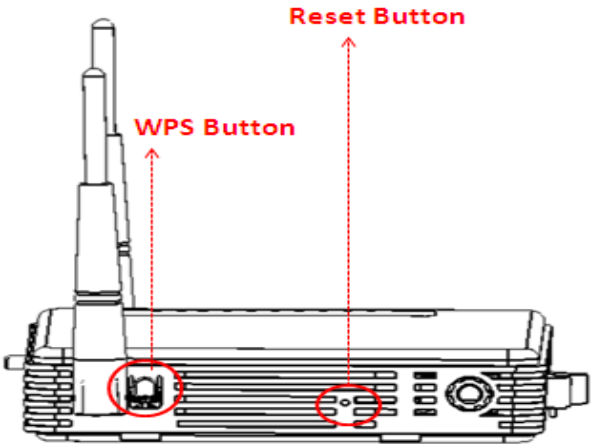


Figure 1-7. Left Panel

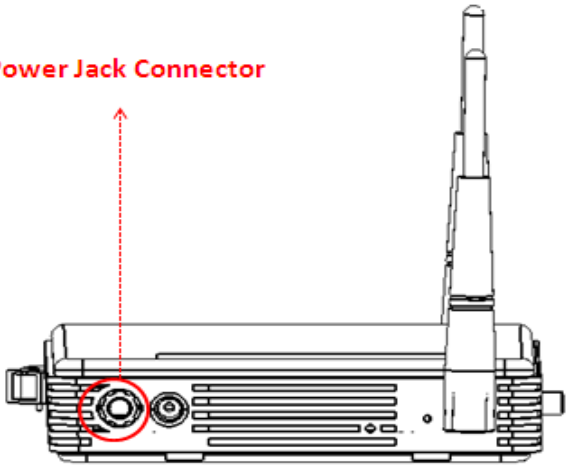


Figure 1-8. Right Panel

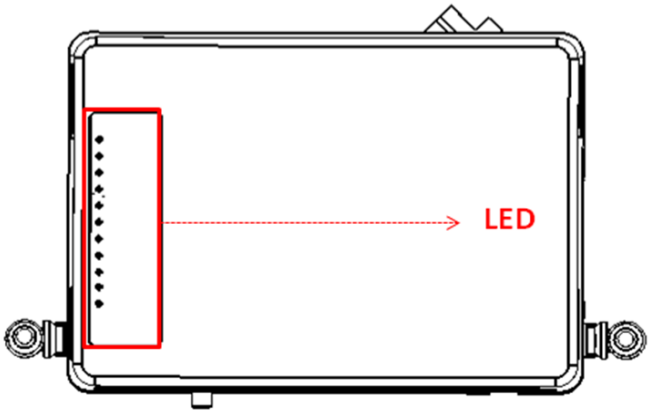


Figure 1-9. Top Panel

1.2 Management Options

Management options available in this Residential Gateway are listed below:

- **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 3. SNMP NETWORK MANAGEMENT for detailed descriptions.)

1.3 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 or 1000Base-X Fiber Port (With FWRIII-3105-N and FWRIII-3105-N-DR)**

  1x100/1000Base-X or 1000Base-X Fiber port is located within the back panel of the Residential Gateway. This port is primarily used for up-link connection and will operate at 100M or 1000M Full Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with other Fast Ethernet Fiber port.

- **WAN 100/1000Base-X or 1000Base-X SFP Port (With FWRIII-3105-CW-N-DR)**

  1x1000Base-X or 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.

1.4 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.

1.5 LED Descriptions

LED	Color	Operation
Power	Off	Power is off.
	Green	Power is functioning normally.
STATUS	Green	System is ready.
	Orange	System is not ready.
	Orange blinking	Insert a pin or paper clip to press the Reset button for 3 seconds to restart the device. The STATUS LED will blink in orange once.
		Insert a pin or paper clip to press the Reset button for 10 seconds to reset the device to factory defaults. The STATUS LED will blink in orange three times.
WAN	Off	The port link is off or it is up in 10Mbps.
	Green	The link is up and works at 100Mbps.
	Orange	The link is up and works at 1000Mbps.
	Blinking	The traffic is present.
LAN 1	Off	The port link is off or it is up in 10Mbps.
	Green	The link is up and works at 100Mbps.
	Orange	The link is up and works at 1000Mbps.
	Blinking	The traffic is present.
LAN 2	Off	The port link is off or it is up in 10Mbps.
	Green	The link is up and works at 100Mbps.
	Orange	The link is up and works at 1000Mbps.
	Blinking	The traffic is present.
LAN 3	Off	The port link is off or it is up in 10Mbps.
	Green	The link is up and works at 100Mbps.
	Orange	The link is up and works at 1000Mbps.
	Blinking	The traffic is present.
LAN 4	Off	The port link is off or it is up in 10Mbps.
	Green	The link is up and works at 100Mbps.
	Orange	The link is up and works at 1000Mbps.
	Blinking	The traffic is present.
Wi-Fi	Off	WLAN link is off.
	Green	WLAN link is up
	Green blinking	The traffic is present.
WPS	Off	WLAN link is off.
	Green	WPS is searching for the WPS client.

2. 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.

2.1 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.

2.2 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:

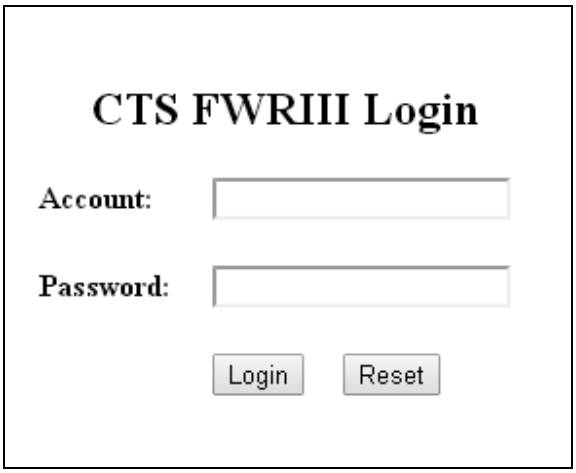
- Use one of the four 10/100/1000Base-T RJ-45 ports as the temporary RJ-45 Management console port to set up the assigned IP parameters of the Residential Gateway.

    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:



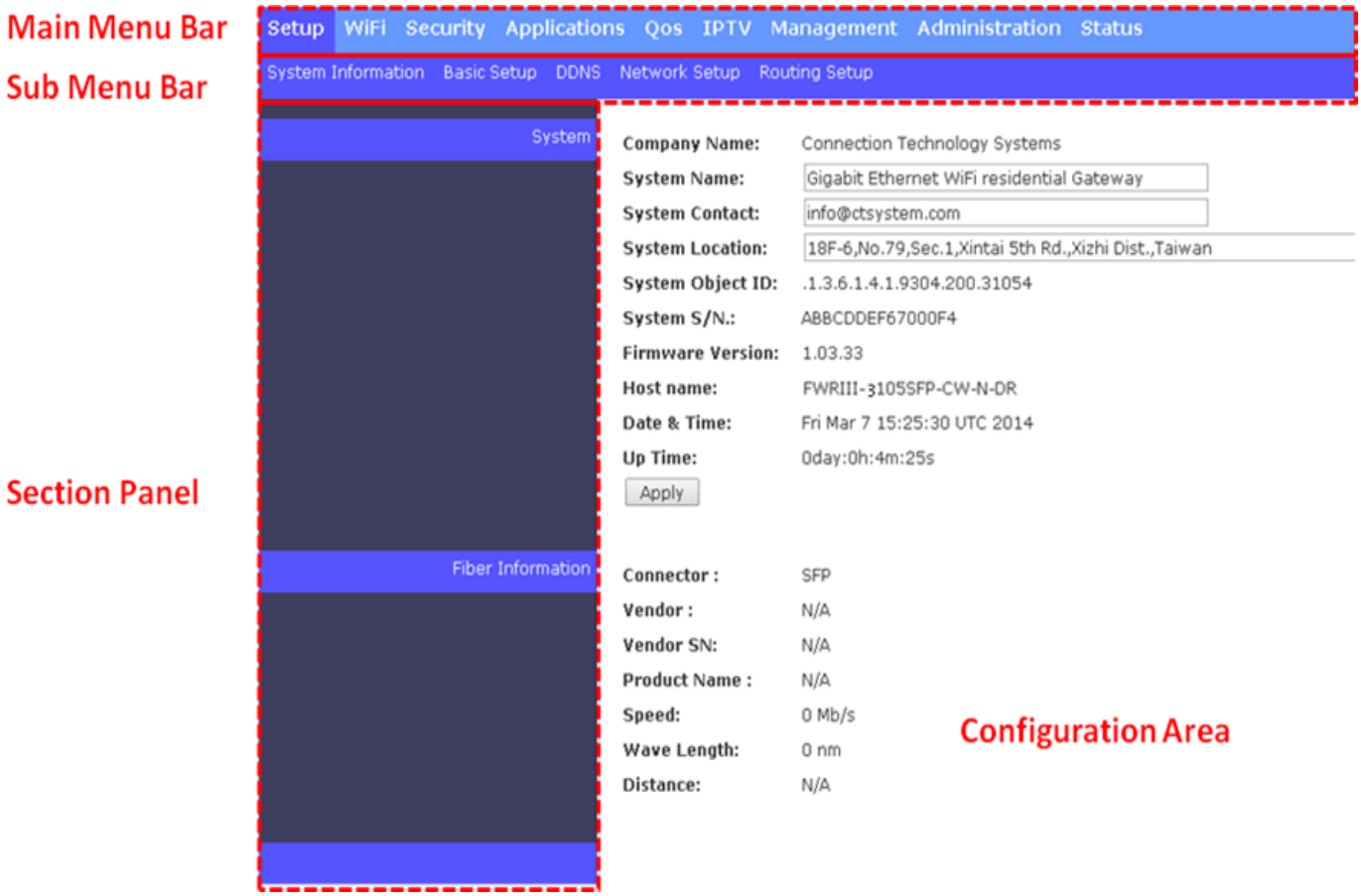
Enter the authorized user name and password then click **"Login"**. The default user name is **admin** and **without a password** (leaves this field blank).

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.*

2.3 Introduction to Sub-Menus

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



Main Menu Bar At the top 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.

WiFi — To configure the WiFi settings of the Residential Gateway.

Security — To configure the security policies of the Residential Gateway, such as Firewall, Packet Filter, URL Filter, VPN Passthrough, UPnP, and DDoS.

Applications — To configure the port forwarding function, port triggering function and DMZ.

Qos — To configure the QoS settings and the rate limit of the Residential Gateway

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.

Sub Menu Bar Below the Main Menu Bar is the Sub Menu Bar. The Sub Menu Bar includes the items which are associated to the selected main tab.

The area below the Sub Menu Bar includes two sub parts.

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.

Section Panel This is a panel in the left side of the configuration area which displays the sections available in the configuration area. The sections are the outline for the parameters of this screen page.

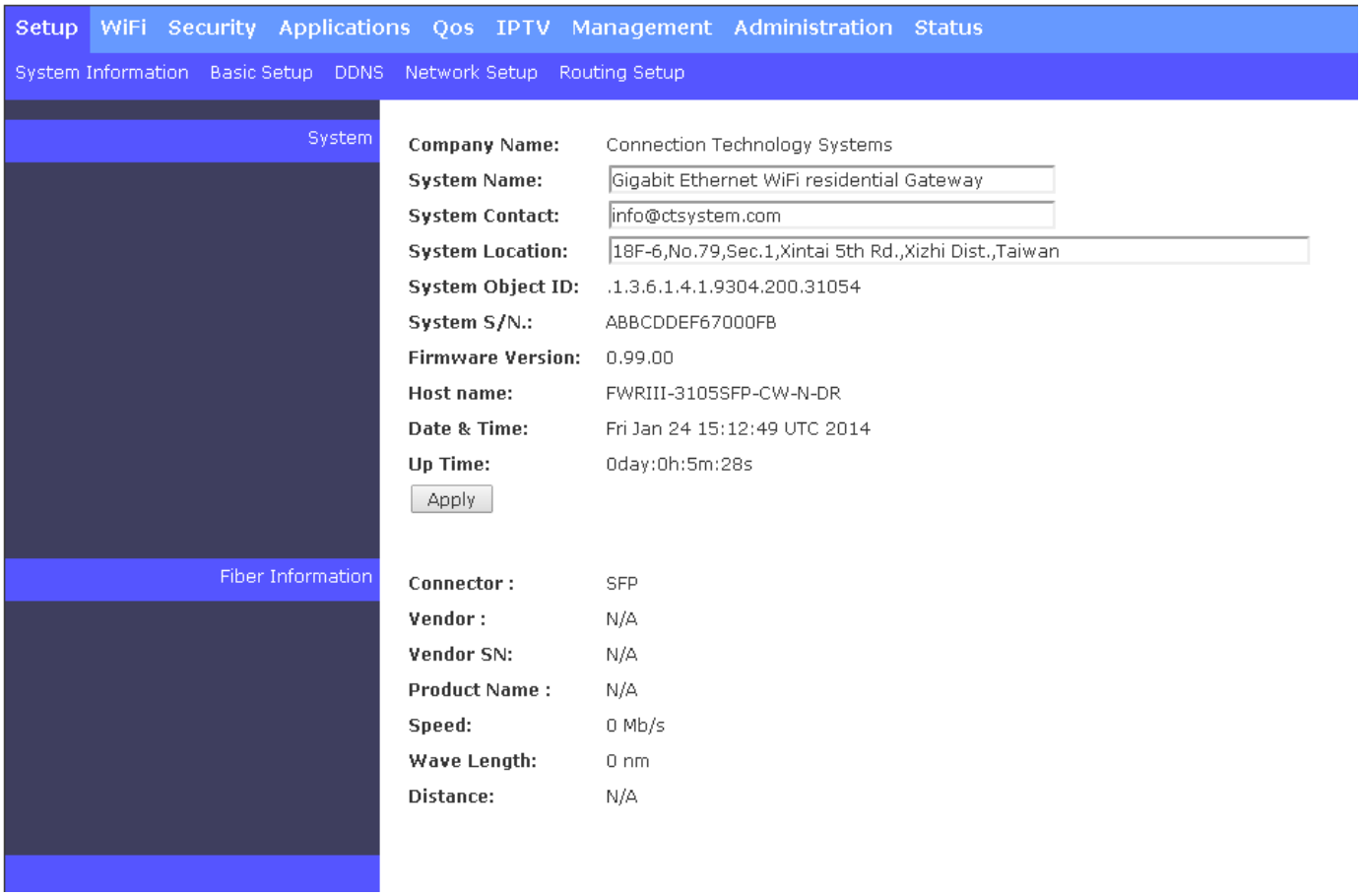
Below is the brief description for each sub-menu. For detailed function explanations, please refer to the individual section.

2.4 Setup

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

2.4.1 System Information

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



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

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

System S/N — This is the serial number of the Residential Gateway.

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

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

Date & 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

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.

Connector — This is the type of the fiber connector in the fiber WAN port.

Vendor — This is the name of the manufacturer.

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

Product Name — This is the model name of the fiber transceiver.

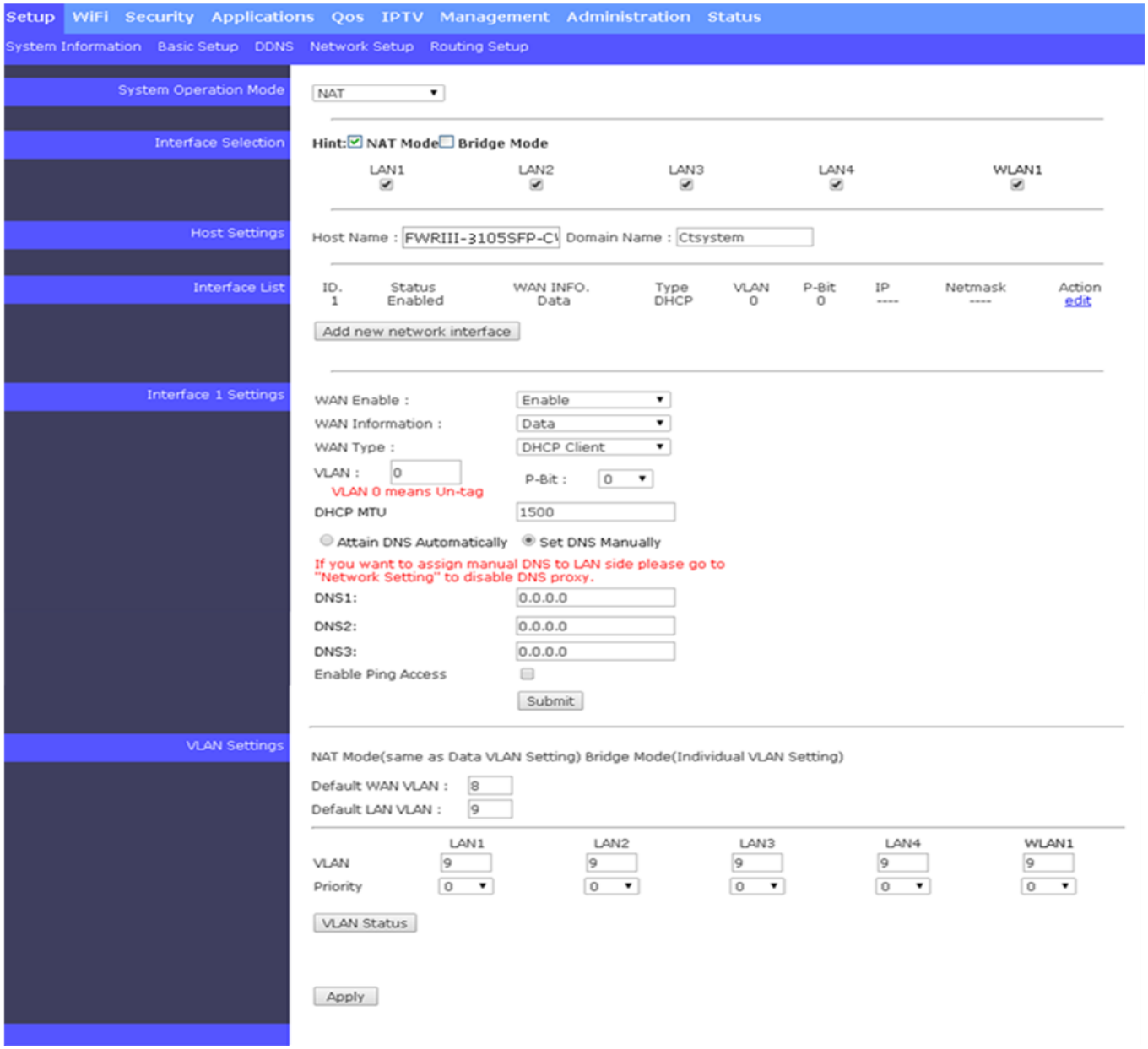
Speed — This is the maximal link speed which the fiber transceiver supports.

Wave Length — This is the receiving and transmitting wave length of this fiber..

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

2.4.2 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:



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

System Operation Mode Select one of the following three system operation modes for the Residential Gateway in the pull-down menu:

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.

Hybrid Mode –When the Residential Gateway is in this mode, some devices connected to the Residential Gateway from its LAN ports and WLAN are in the public network and the others are in the private network.

Interface Selection 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 checkbox. 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 unselected in the checkbox. A device which is connected to this port will be a host on the public network.

In the *Hybrid Mode*, you can change the allocation of LAN ports. Select a LAN port in the checkbox to allocate it to the private network. Or unselect it in the checkbox to allocate it to the public network.

In the *Bridge Mode*, all LAN ports of the Residential Gateway will be unselected. And you cannot change the allocation of any port manually.

In the *NAT Mode*, all LAN ports of the Residential Gateway will be selected. And you cannot change the allocation of any port manually.

Host Settings Specify the host name and the domain name of the Residential Gateway in the text boxes. They should be provided by your Internet service provider. However, they are usually optional and it should be fine to leave the text boxes blank.

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

ID — This is the index of this WAN interface in this 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.

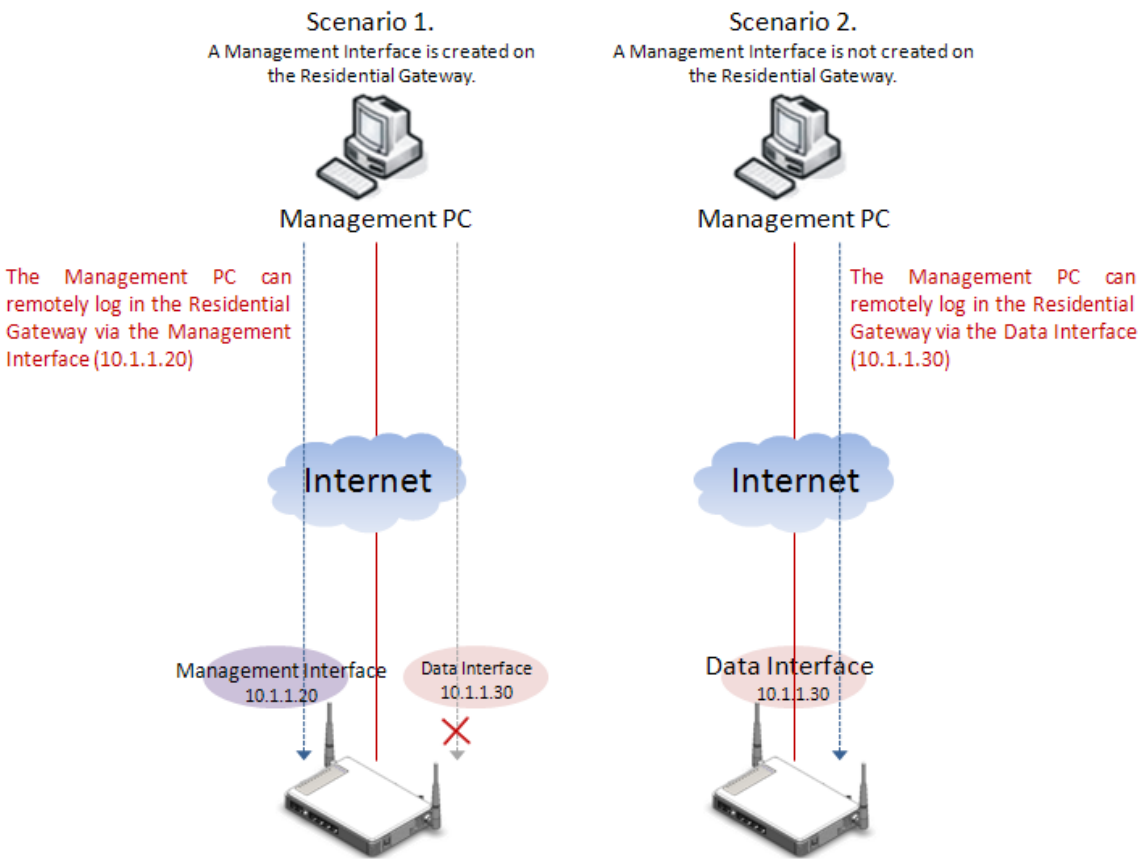
To create a new interface, click *Add new network interface* below the list and edit the settings of the new interface in the following section.

Interface 1 Settings, **Edit Interface N** & **Add New Interface N** 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.

WAN Enable — Enable or disable this WAN interface.

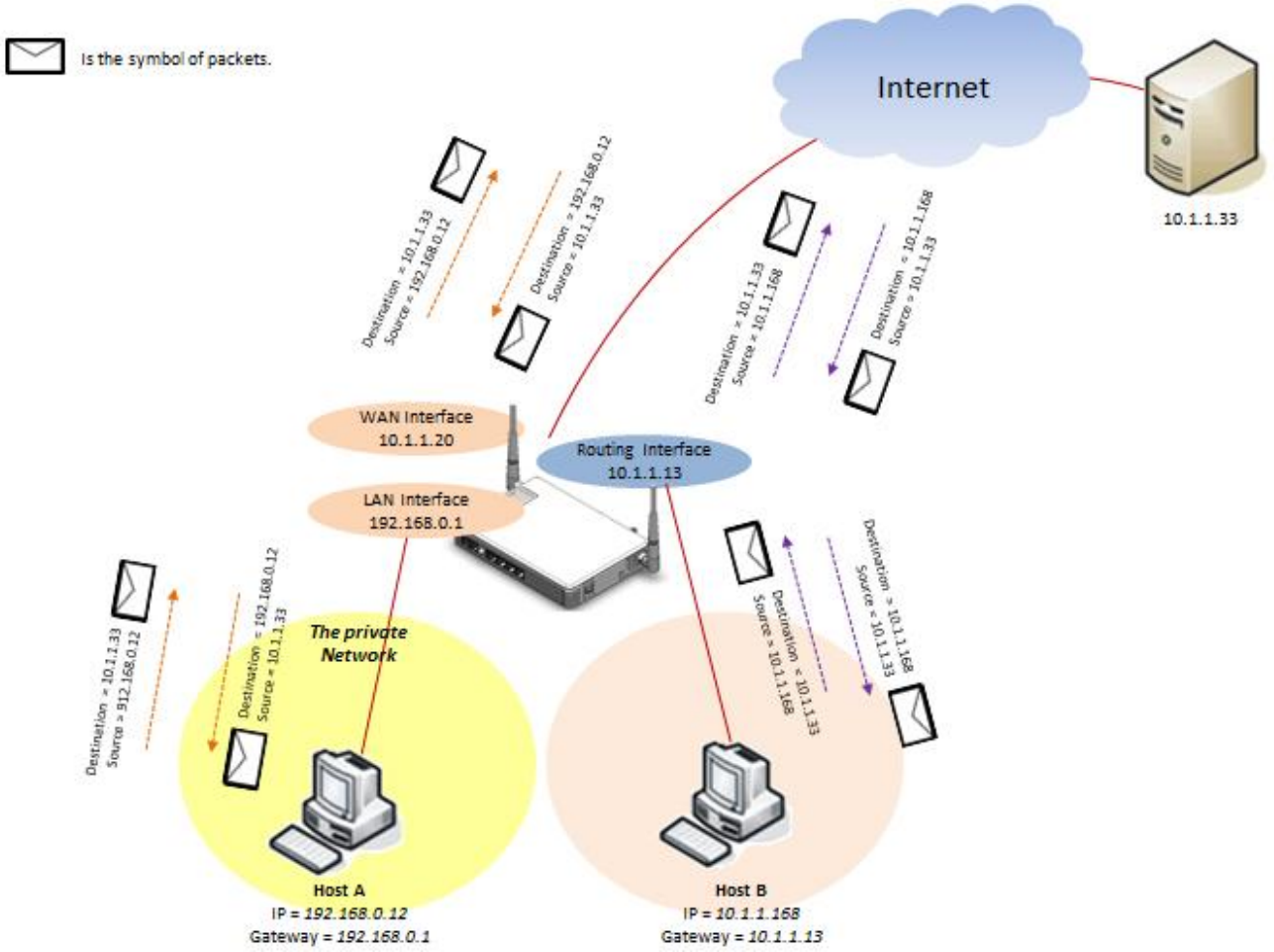
WAN Information — Select a WAN information type from the pull-down menu. You can refer to the following table for a description for the types of the WAN interfaces.

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.



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.

Routing — The routing interface is a WAN interface which does not belong to the NAT. When a host on the private network has the routing interface as the default gateway, it can send packets through the routing interface to the Internet directly. And the packets will keep the original IP address after they pass through the Residential Gateway. The diagram below illustrates the two different paths for the packet to pass through the Residential Gateway via the NAT and the routing interface.



Alias Interface — An Alias Interface is an interface which allows the network administrator to create a DMZ. For more details about the interoperability of the Alias Interface and the DMZ, please refer to the section 2.7.3 in this document.

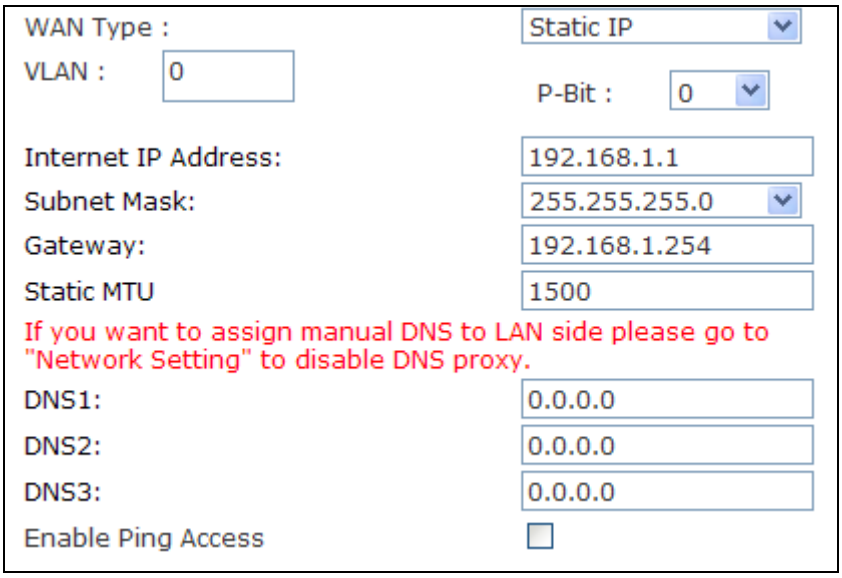
WAN Type — Select an Internet connection type for the WAN interface.

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.”

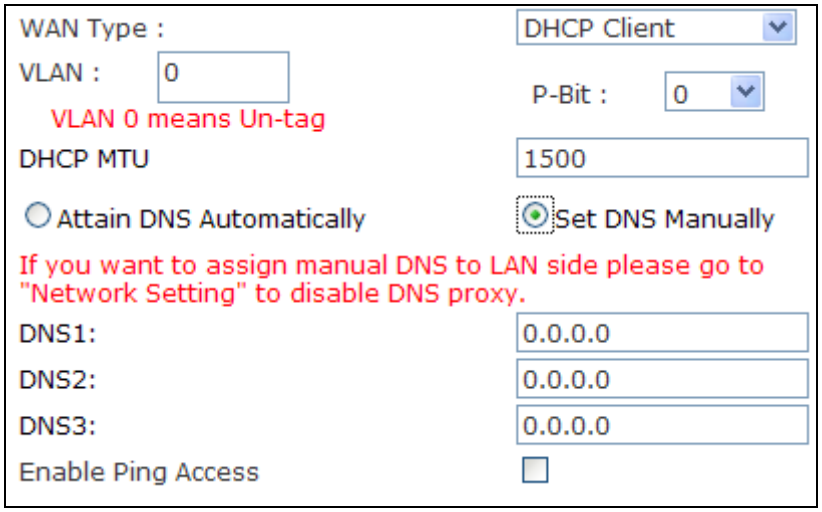
DNS1 — Specify the IP address of the primary DNS server of the WAN interface. (This parameter is only available for the data interface.)

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.)

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.)

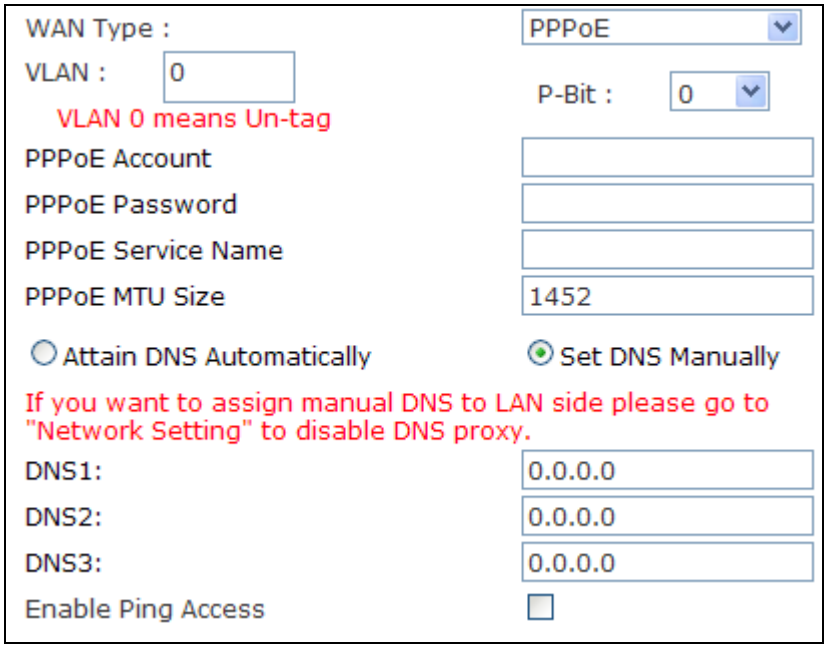
DNS1 — If you choose to set the DNS manually, please specify the IP address of the primary DNS server of this interface. (This parameter is only available for the data interface.)

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.)

PPPoE

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



PPPoE Account — Specify the user name or PPPoE account provided by your ISP.

PPPoE Password — Specify the PPPoE password provided by your ISP.

PPPoE Service Name — Specify the PPPoE service name provided by your ISP.

PPPoE MTU size — Specify the maximal size of the PPPoE packets for optimal performance.

PPPoE MTU — You can change the PPPoE MTU for optimal performance. 1492 is the default MTU.

Attain DNS Automatically & ***Set DNS Manually*** —Choose one of the two options - Manually or Automatically.

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

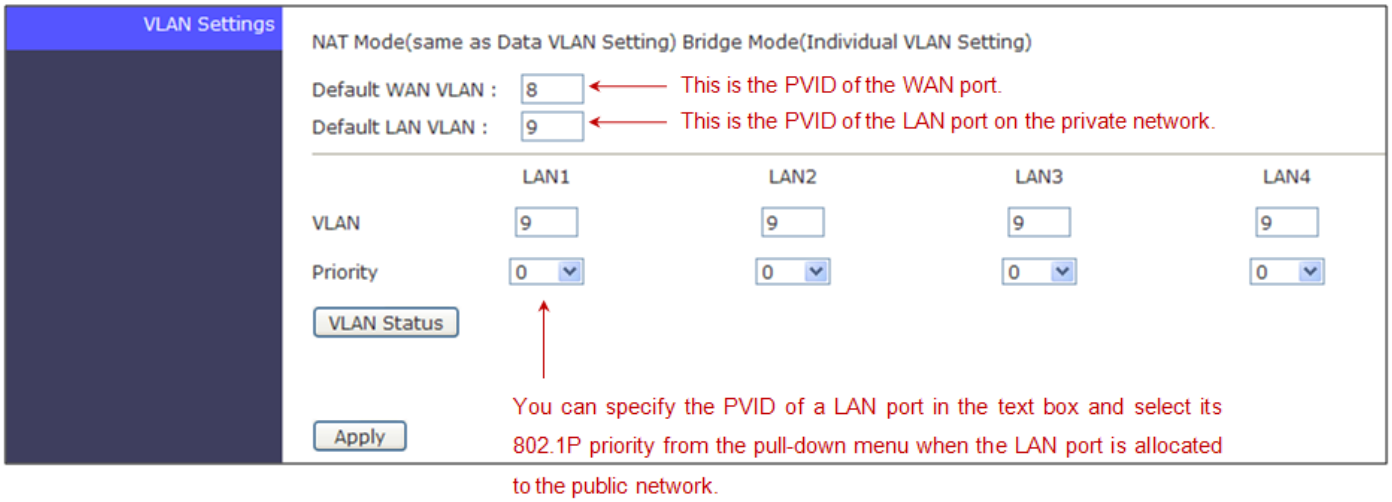
DNS2 — If you want to choose to set the DNS manually, please specify the IP address of the secondary DNS server of the WAN interface. (This field is only available for the data interface.)

DNS3 — If you want to choose to set the DNS manually, please 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 — Tick the checkbox to allow the WAN interface to reply the ICMP echo requests which it receives from the public network.

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

VLAN Settings This section enables you to assign a PVID and a P-Bit to each port of the Residential Gateway. And below is a description for the VLAN settings and the VLAN behaviors of the Residential Gateway.



- Packets will always be untagged when they leave the Residential Gateway from its LAN port.

- 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 tagged packets enter the Residential Gateway from a LAN port on the private network and leave from the WAN port, the Residential Gateway will process the packets according to their original VLAN tags. If their VLAN tags are the same as the PVID of the WAN interface from which they leave, the packets will be untagged. Otherwise, the packets will keep their original VLAN tags when they leave the Residential Gateway.

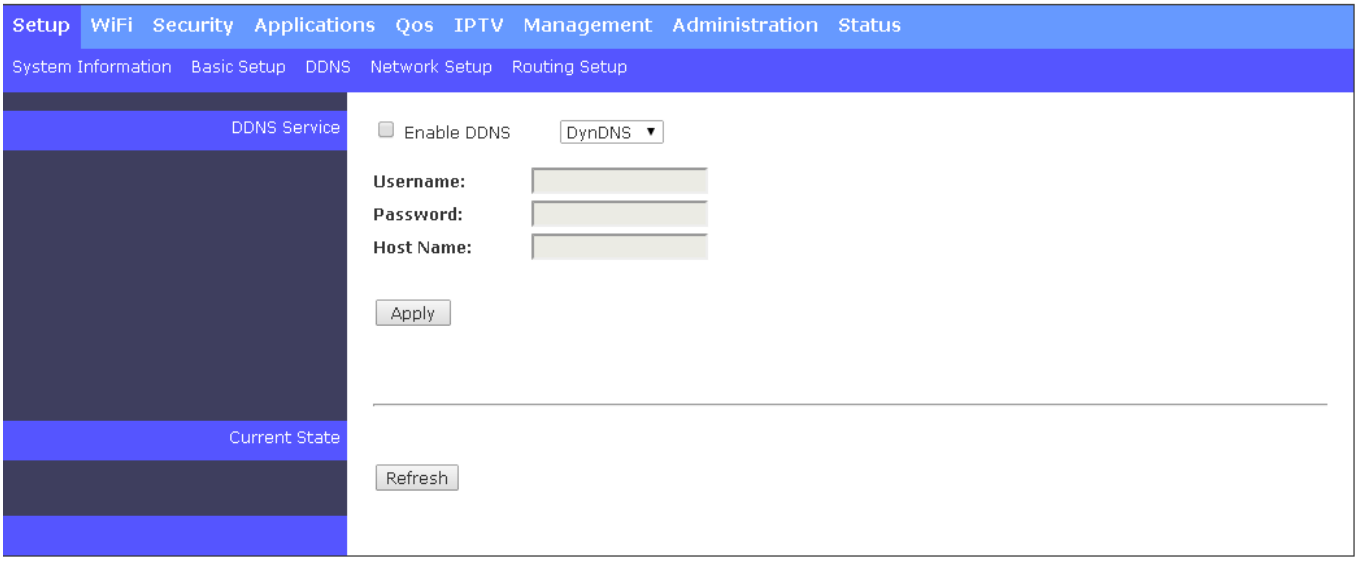
- When a LAN port is allocated to the public network, you can specify its VLAN ID in the text box and select its P-Bit value in the pull-down menu. But when a LAN port is allocated to the private network, its VLAN ID and P-Bit value cannot be changed.

Click *VLAN Status* to view the VLAN table or check members of the VLAN groups of the Residential Gateway.

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

2.4.3 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.



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.

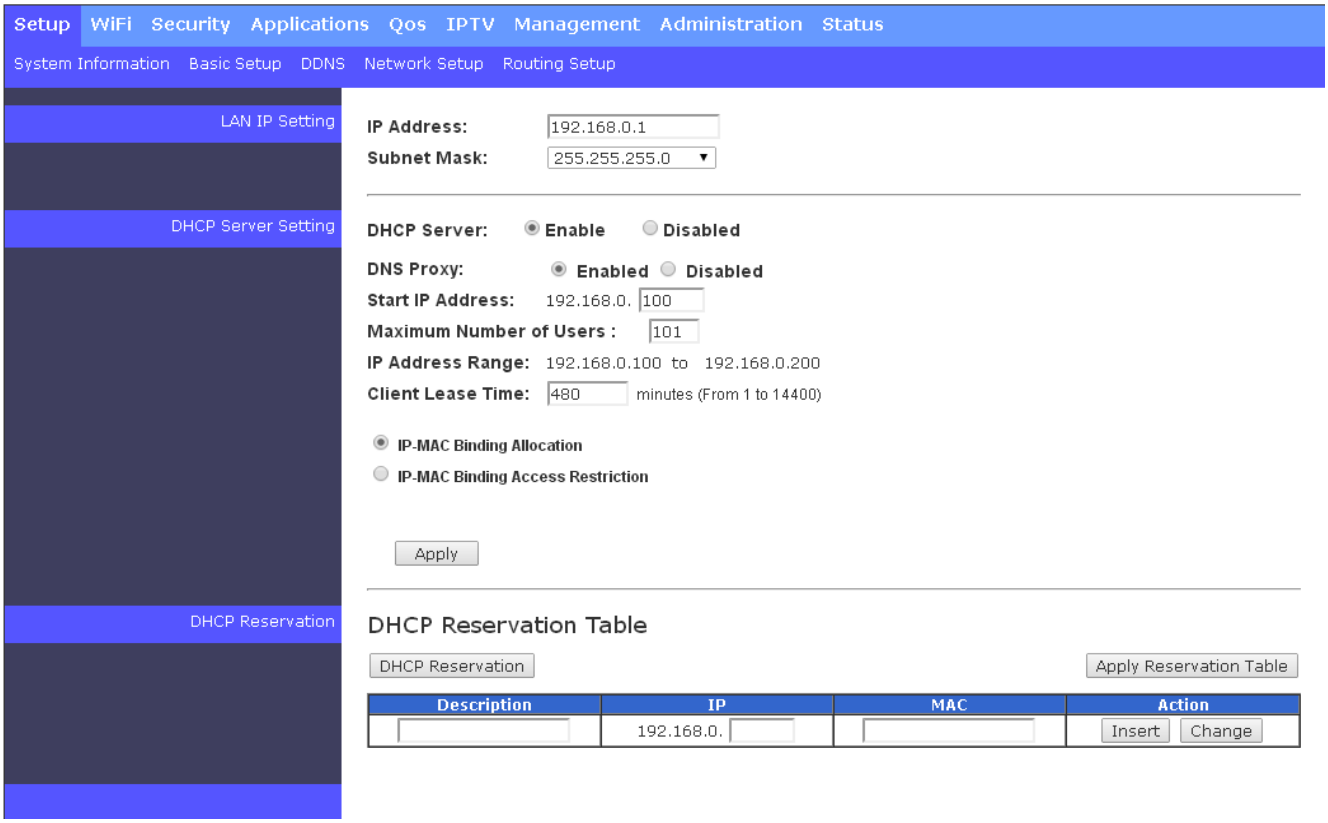
Host Name — Enter the DDNS URL assigned by the DDNS server..

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

Current Status 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.

2.4.4 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:



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

LAN IP Setting 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.

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.

DHCP Server Setting 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 or disable the DHCP server function of the Residential Gateway.

DNS Proxy — Enable or disable the DNS proxy function of the Residential Gateway. When it is enabled, the DHCP clients will regard the Residential Gateway as its DNS server. And when it is disabled, the DHCP clients on the private network will use the same DNS server on the public network as the Residential Gateway does.

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.

IP-MAC Binding Allocation & ***IP-MAC Binding Access Reservation*** — Select *IP-MAC Binding Allocation* for the Residential Gateway to assign IP addresses in the ***IP Address Range*** field to the DHCP clients. Or select *IP-MAC Binding Allocation Reservation* for

the Residential Gateway to only assign IP addresses which are in the ***DHCP Reservation Table***.

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

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***.

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 *Insert* to add a new entry after you configure it in the textboxes of the table. Click *Edit* to modify this entry in the text boxes. And after you modify it, click *Change* to replace the previous settings with the new one. Or click *Del* to remove an entry in this table.

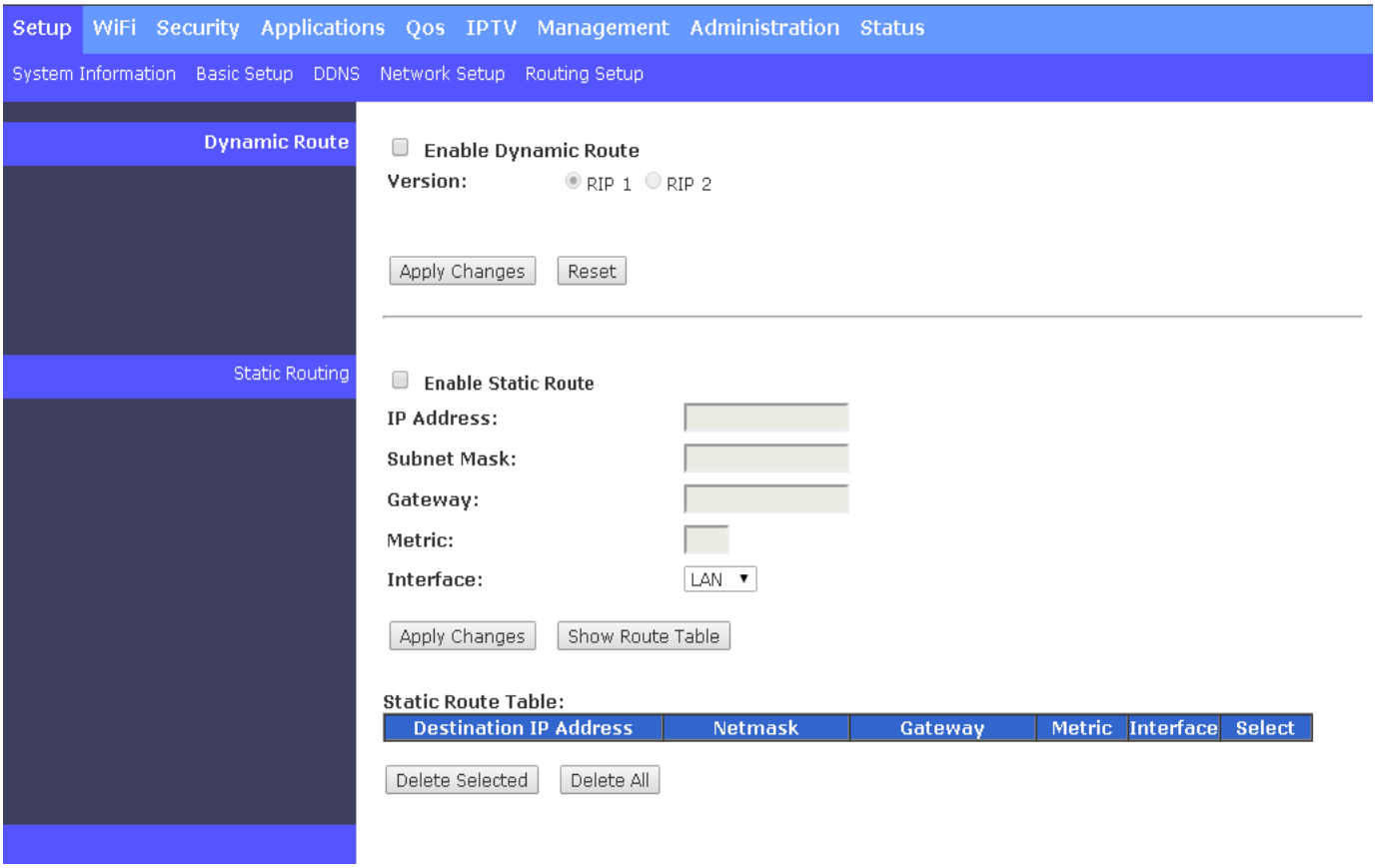
Click ***DHCP Reservation*** and the ***DHCP Client List*** will show up in the pop-out window. The list displays information such as the hostname, the IP address, the type of the IP address, the MAC address and the expire time of the leased IP address.

Click *Refresh* to update the DHCP client list. Or click *Close* to close the pop-out window. You can select an entry and click *add* to edit it in the text boxes of the ***DHCP Reservation Table***. After you finish editing this entry, you can click *Insert* to add this new entry to the ***DHCP Reservation Table***.

Click *Apply Reservation Table* to submit your settings after you finish configuring this table.

2.4.5 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:



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

NAT This section allows you to enable or disable the NAT function of the Residential Gateway. NAT stands for **"**Network Address Translation". Due to this function, the Residential Gateway can replace the private IP address in the header of a packet with a public IP address or vice versa.

***Note**: If you disable the NAT function, the firewall protection of the Residential Gateway will be disabled as well. So you should be cautious if you want to disable this function.*

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.

Enable Static Route — Enable or disable this static route.

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

Subnet Mask — 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 Changes* to submit your settings. Or click *Show Routing Table* to view the routing table of the Residential Gateway in the pop-out window. If you want to update the routing table, click *Refresh* in the pop-out window. And to close the pop-out window, click *Close*.

Static Routing Table - This table displays all the static routes created on the Residential Gateway. If you want to remove an entry in this table, click the checkbox in the last column of this table to select it. Then, click *Delete Selected* to remove the selected entry. And if you want to clear all the entries in the table, click *Delete All*.

Here is an example for how the packets follow the static route to reach the destination network. Suppose the following entry is created in the ***Static Routing Table*** of the Residential Gateway.

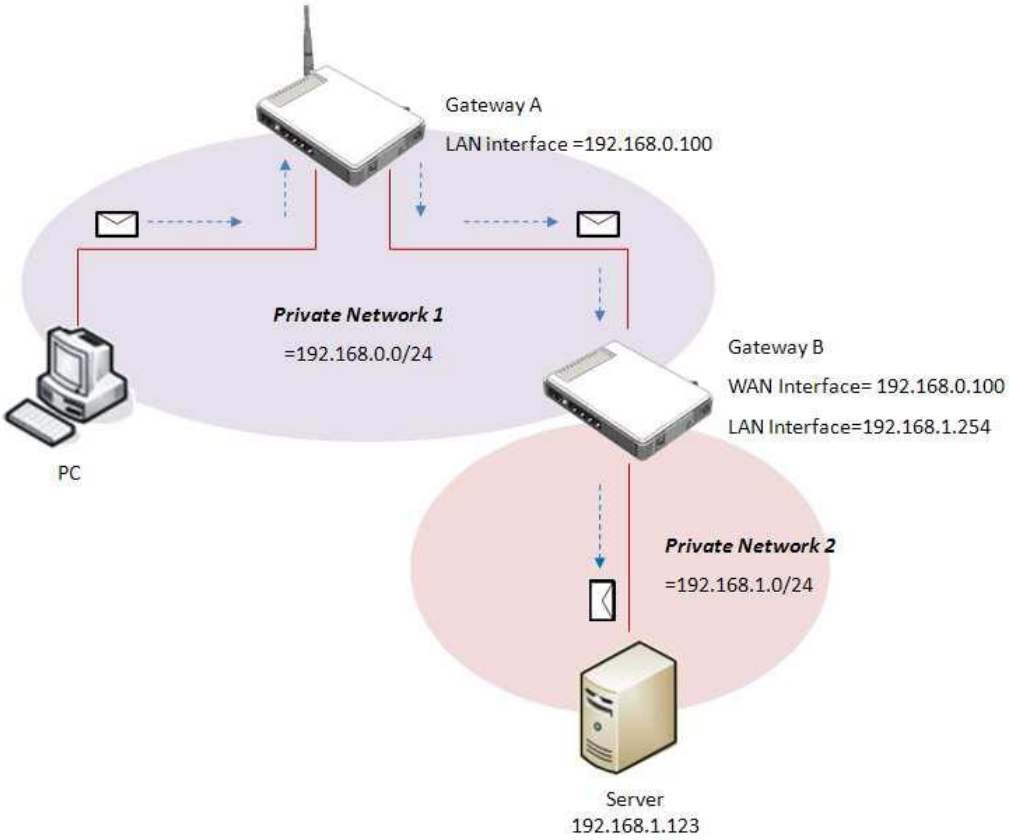
Static Route Table:

Destination IP Address	Netmask	Gateway	Metric	Interface	Select
192.168.1.0	255.255.255.0	192.168.0.100	2	LAN	☐

Delete Selected Delete All

Then, when the Residential Gateway receives packets whose destination IP addresses belongs to the network 192.168.1.0 from its LAN interface, the Residential Gateway will redirect the packets to the specified destination 192.168.0.100.

The picture below illustrates how the Residential Gateway will follow the static routes in the ***Static Routing Table***.

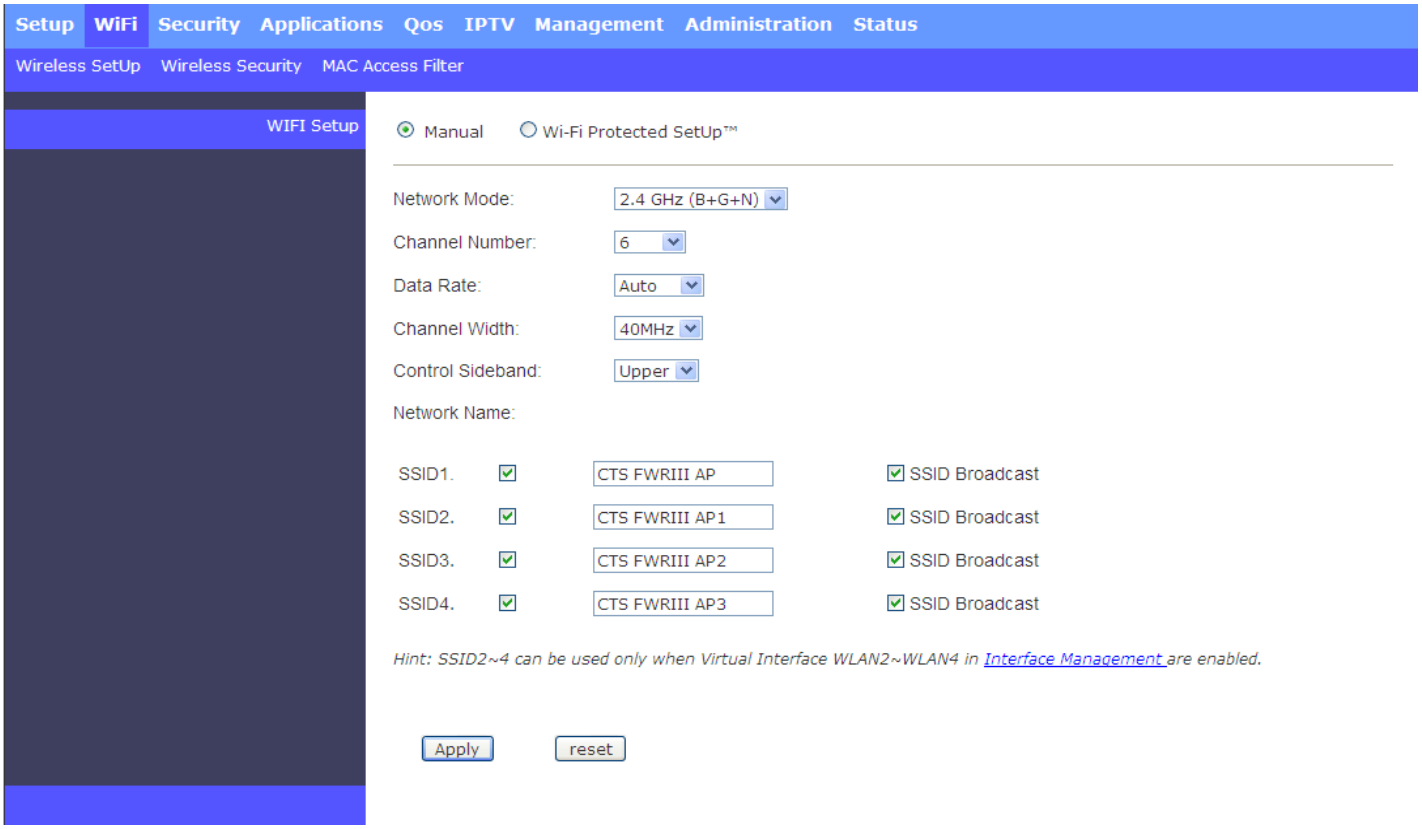


2.5 WiFi

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

2.5.1 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:

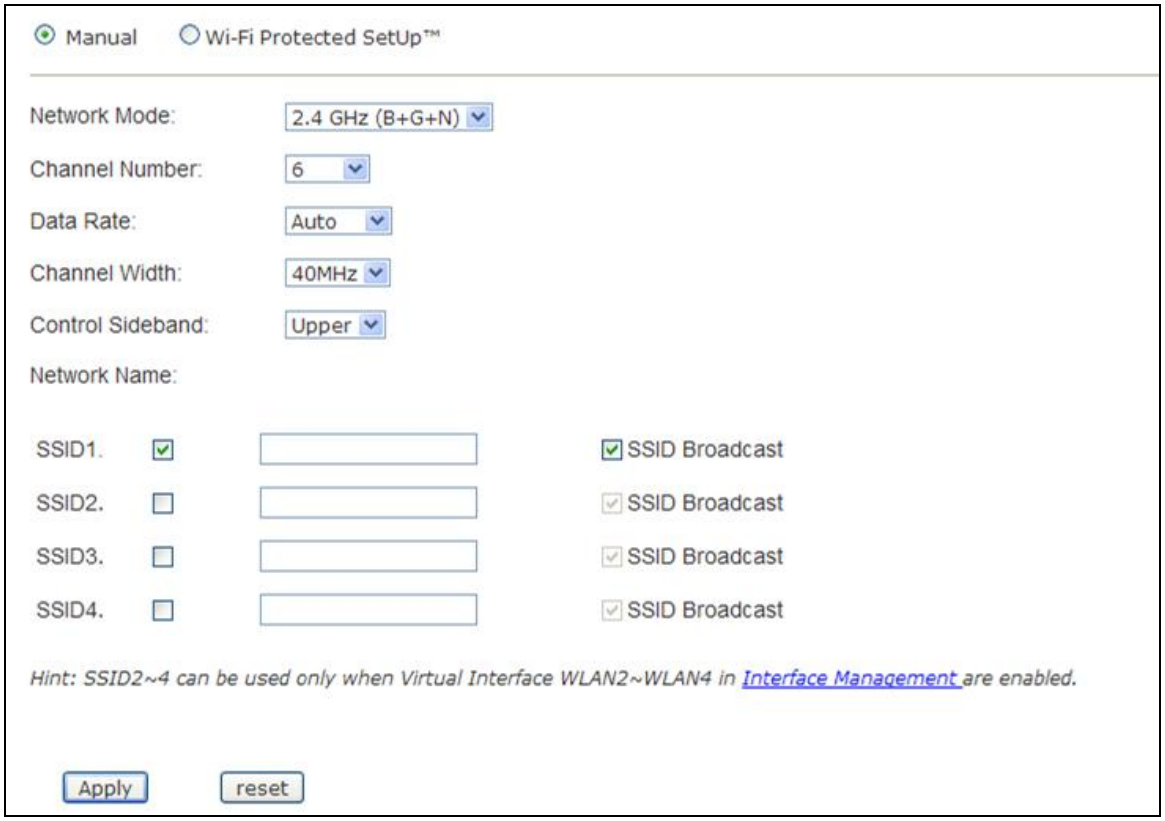


For details on the settings of this page, please refer to the description of the individual section below.

WiFi Setup This section offers you two approaches to set up the wireless network of the Residential Gateway. Select *Manual* to set up the wireless network manually. Or select *WiFi Protected Setup™* to allow the wireless clients to connect to the WLAN with WPS. WPS stands for "Wi-Fi Protected Setup". It is a standard which makes the WiFi security simpler and easier. Below is the description of configuration parameters for the two approaches.

Manual

If you want to set up the wireless network manually, please specify the values of the following parameters.



Network Mode — Select one of the following modes for your wireless network.

Network Mode	Description
2.4 GHz (B)	In this mode, the Residential Gateway will only support 802.11b standard.
2.4 GHz (G)	In this mode, the Residential Gateway will only support 802.11g standard.
2.4 GHz (N)	In this mode, the Residential Gateway will only support 802.11n standard.
2.4 GHz (B+G)	In this mode, the Residential Gateway will support both 802.11b and 802.11g standards.
2.4 GHz (G+N)	In this mode, the Residential Gateway will support both 802.11g and 802.11n standards.
2.4 GHz (B+G+N)	In this mode, the Residential Gateway will support 802.11b, 802.11g and 802.11n standards.

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* for the Residential Gateway to choose a WiFi channel automatically.

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

Channel Width — Select *20MHz* for the Residential Gateway to support the link speed of 802.11n mode up to 150Mbps. Or select *40MHz* for the Residential Gateway to support the link speed of 802.11n mode up to 300Mbps. Note that 40MHz will only operate when the WiFi Channel is 5-11. (*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).*)

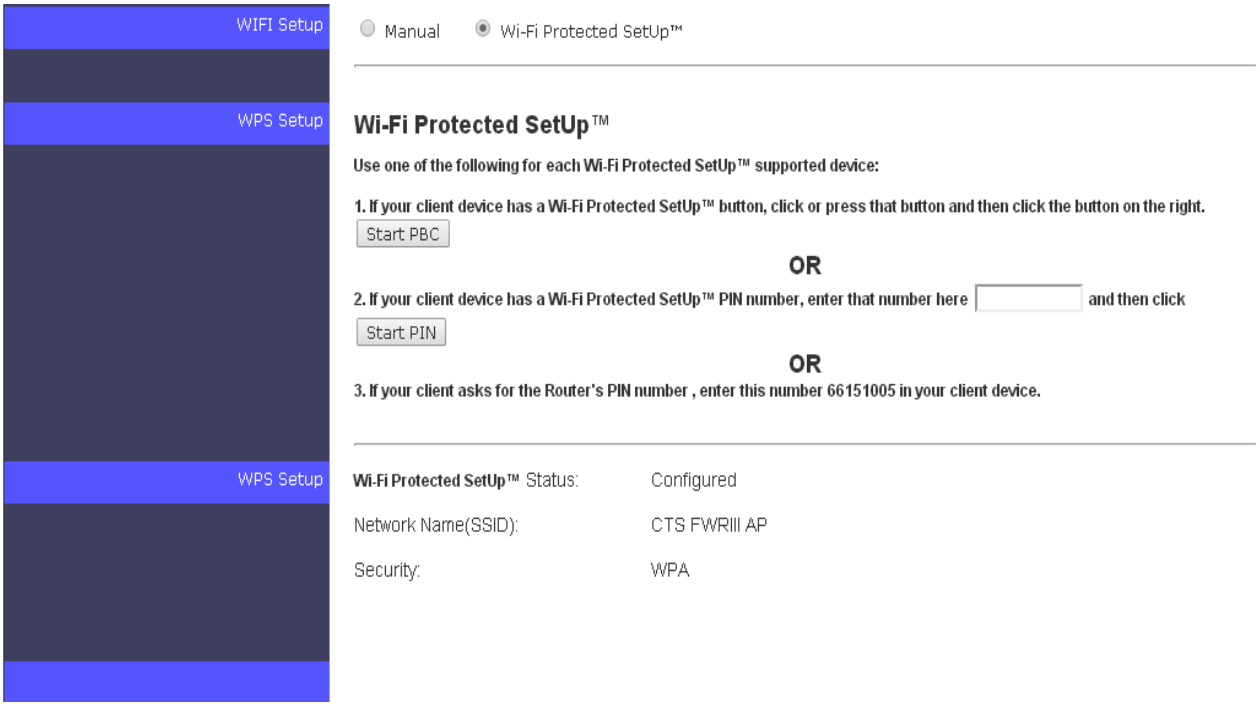
Control Sideband — The extra bandwidth will be available when the channel bandwidth is 40MHz. If you select *Upper*, the extra bandwidth will be extended in the upper sideband. (*This field is only available when the network mode is 2.4 GHz (N), 2.4 GHz (G+N), or 2.4 GHz (B+G+N).*)

Network Name — To enable a WLAN of the Residential Gateway, tick the checkbox of its SSID. And specify the SSID in the text box as the name of the WLAN. The Residential Gateway provides four WLANs. The WLANs should be distinguished from each other by their SSIDs. You can find the SSID in the wireless control panel of the wireless client devices to set up the wireless connection to the Residential Gateway. And if you do not want the SSID of this WLAN to be displayed on the wireless control panel of the wireless client devices, unselect the checkbox for *SSID Broadcast*.

Click *Apply* to submit your changes. Or click *reset* to clear all values in the text boxes.

WiFi Protected Setup™

If you want to set up a wireless network of the Residential Gateway via WPS, please specify the values of the following parameters.



WPS Setup This section allows you to decide how the WPS clients shall set up the wireless connection to the Residential Gateway. Choose one of the three methods below for WPS clients to connect to the wireless network of the Residential Gateway.

- Push the WPS buttons on the Residential Gateway and the WPS client device. And click *Start PBC* to set up the wireless connection.

- Enter the PIN number generated by the WPS client device in the text box. And click *Start PIN* to set up the wireless connection.

- Enter the PIN number generated by the Residential Gateway here on the WPS clients. And after the PIN number is entered on the WPS clients, the wireless connection will be set up.

WPS Setup This is a view-only section which displays information about the WPS connection status.

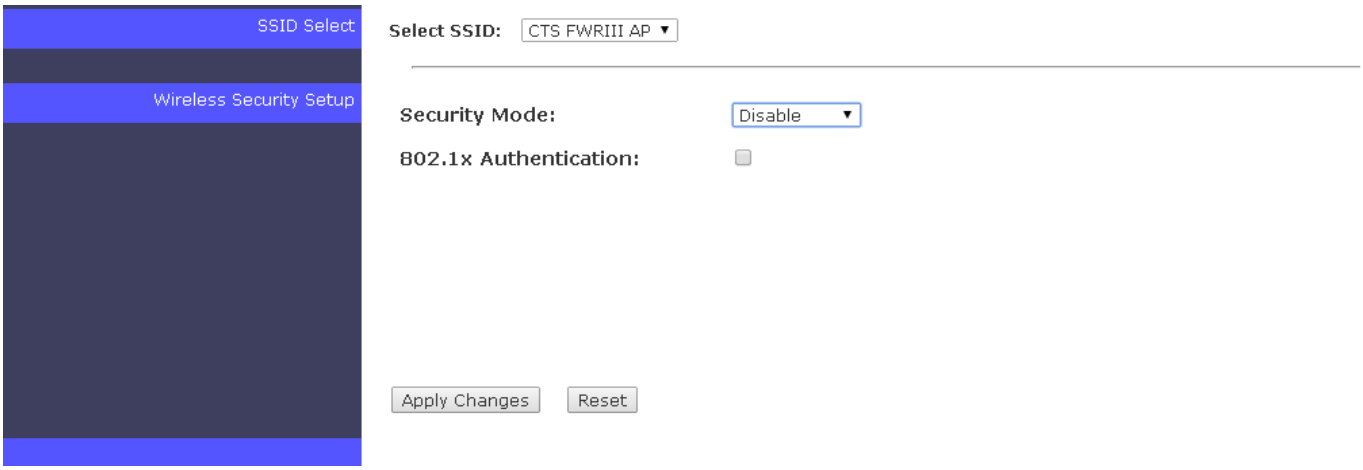
WiFi Protected Setup™ Status — It is *Configured* when the WPS connection has not been set up. And it is *Unconfigured* when the WPS connection has been set up successfully.

Network Name(SSID) — This is a network name (SSID) automatically set up by the Residential Gateway.

Security — This shows the current security mode used.

2.5.2 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:



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

SSID Select Select the SSID of a WLAN from the pull-down menu to set its authentication type in the following section.

Wireless Security Setup 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.

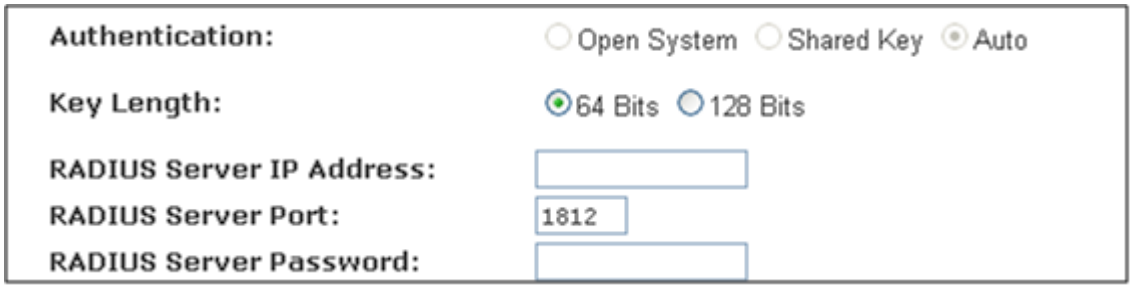
Security Mode — The Residential Gateway supports four types of encryptions — *WEP*, *WPA*, *WPA2* and *WPA-Mixed*. Select one of them in the drop-down menu as the encryption of this WLAN. Or select *Disabled* if you don't want any data encryption for this WLAN.

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:



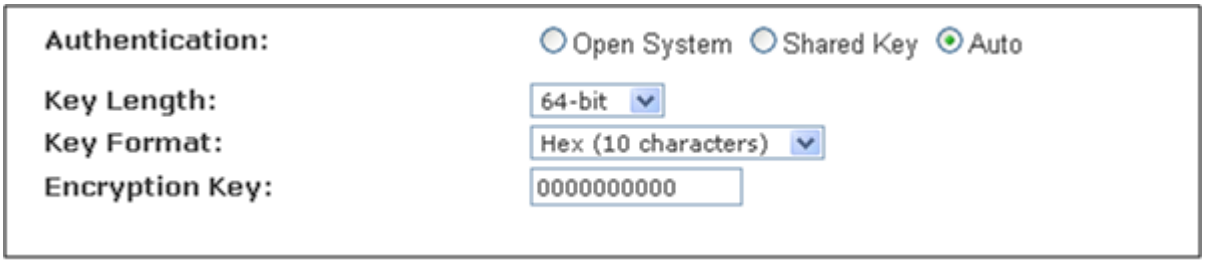
Key Length — Select *64 bits* or *128 bits* from the pull-down menu. The wireless client devices must have the same WEP encryption length as the Residential Gateway.

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:



Authentication — 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.

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.

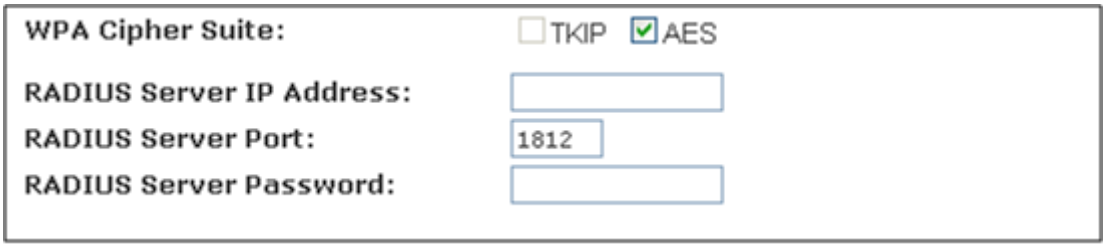
Key Format — Select **ASCII (5 characters)** or **HEX (10 characters)** from the pull-down menu as the format of the key.

Encryption Key — Specify the 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.



WPA Cipher Suite & ***WPA2 Cipher Suite*** — Select *TKIP* or *AES* in the pull-down menu.

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.

WPA Cipher Suite & ***WPA2 Cipher Suite*** — Select *TKIP* or *AES* in the pull-down menu.

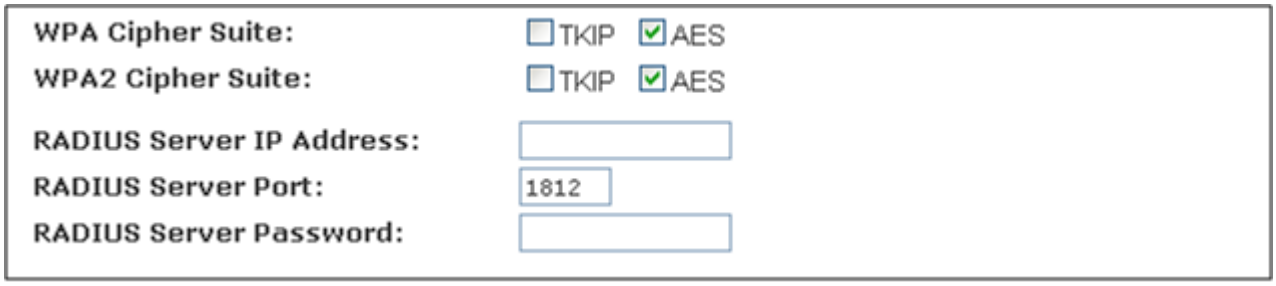
Pre-Shared Key Format — Select *Passphrase* (alphanumeric format) or *Hex(64characters)* (“A-F”, “a-f” and “0-9”) in the pull-down menu.

WPA Pre-Shared Key — Specify the pre-shared 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.



WPA Cipher Suite — Select *TKIP* or *AES* in the pull-down menu.

WPA 2 Cipher Suite — Select *TKIP* or *AES* in the pull-down menu.

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.

WPA Cipher Suite — Select *TKIP* or *AES* in the pull-down menu.

WPA 2 Cipher Suite — Select either *TKIP* or *AES* in the pull-down menu.

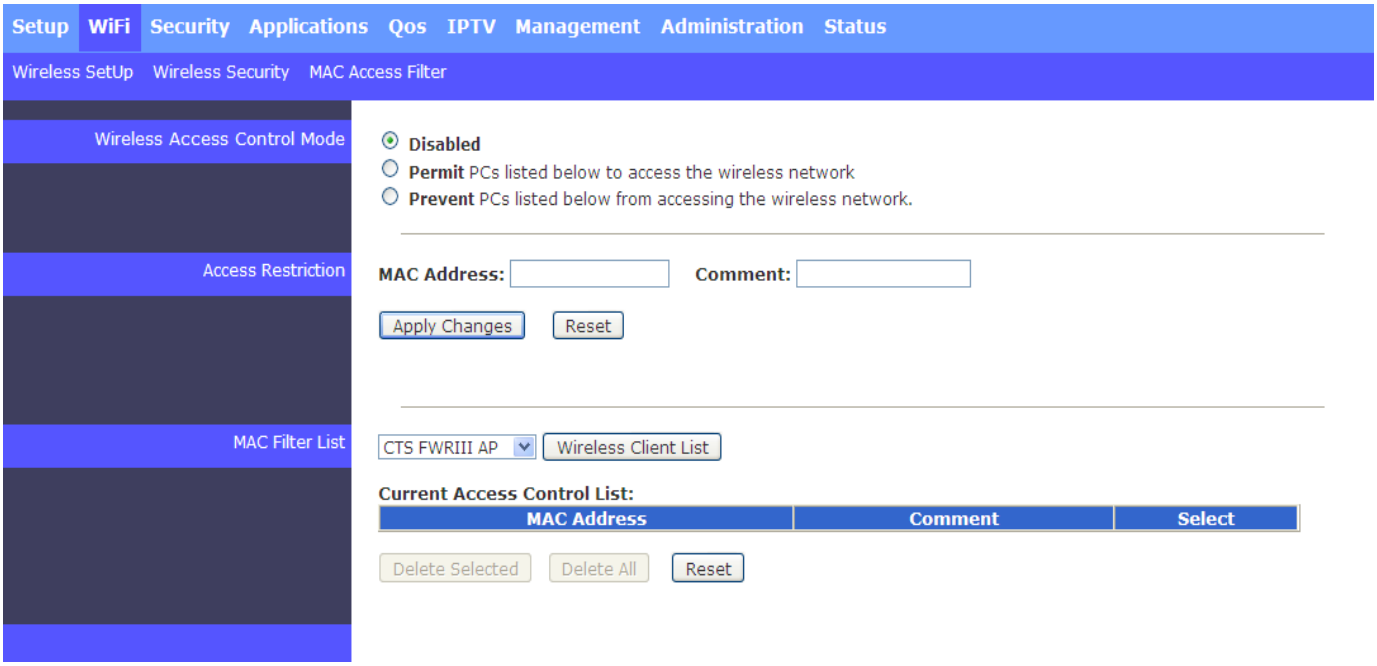
Pre-Shared Key Format — Select either *Passphrase* (alphanumeric format) or *Hex(64characters)* ("A-F", "a-f" and "0-9") in the pull-down menu.

Pre-Shared Key — Specify the pre-shared 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 Change* to submit the settings after you finish configuring this page

2.5.3 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:



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

Wireless Access Control Mode This section allows you to decide whether the Residential Gateway should deny or allow wireless connection from the MAC addresses in the ***Current Access Control List*** below.

- Select *Disabled* to deactivate the MAC access filter feature.
- Select *Permit PCs listed below to access the wireless network* to open the WiFi service of the Residential Gateway only to the wireless clients in the list.
- Select *Prevent PCs listed below from accessing the wireless network* to open the WiFi service of the Residential Gateway to any wireless clients except those in the list.

Access Restriction This section enables you to create or modify an entry in the ***Current Access Control List*** in the next section. Please 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 *Apply Changes* to apply the changes in the text boxes to the list. Or click *Reset* to clear all the values in the text boxes.

MAC Filter List This section contains the ***Current Access Control List*** of each WLAN. Select the SSID of the WLAN from the pull-down menu in this section to check its control list.

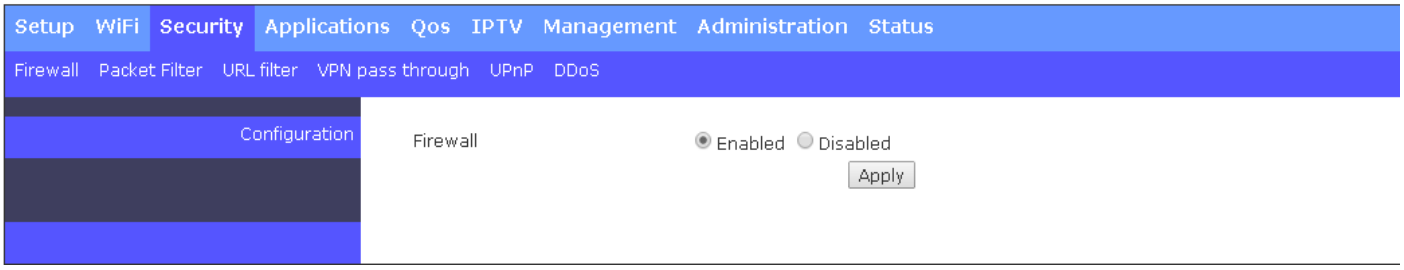
To remove an entry from the list, select it in its checkbox in the last column. And click *Delete Selected* to remove it from the list. Or if you want to delete all entries in the list, click *Delete All*. Click *Wireless Client List* to view the Active Wireless Client Table in the pop-out window.

2.6 Security

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

2.6.1 Firewall

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



Configuration 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.

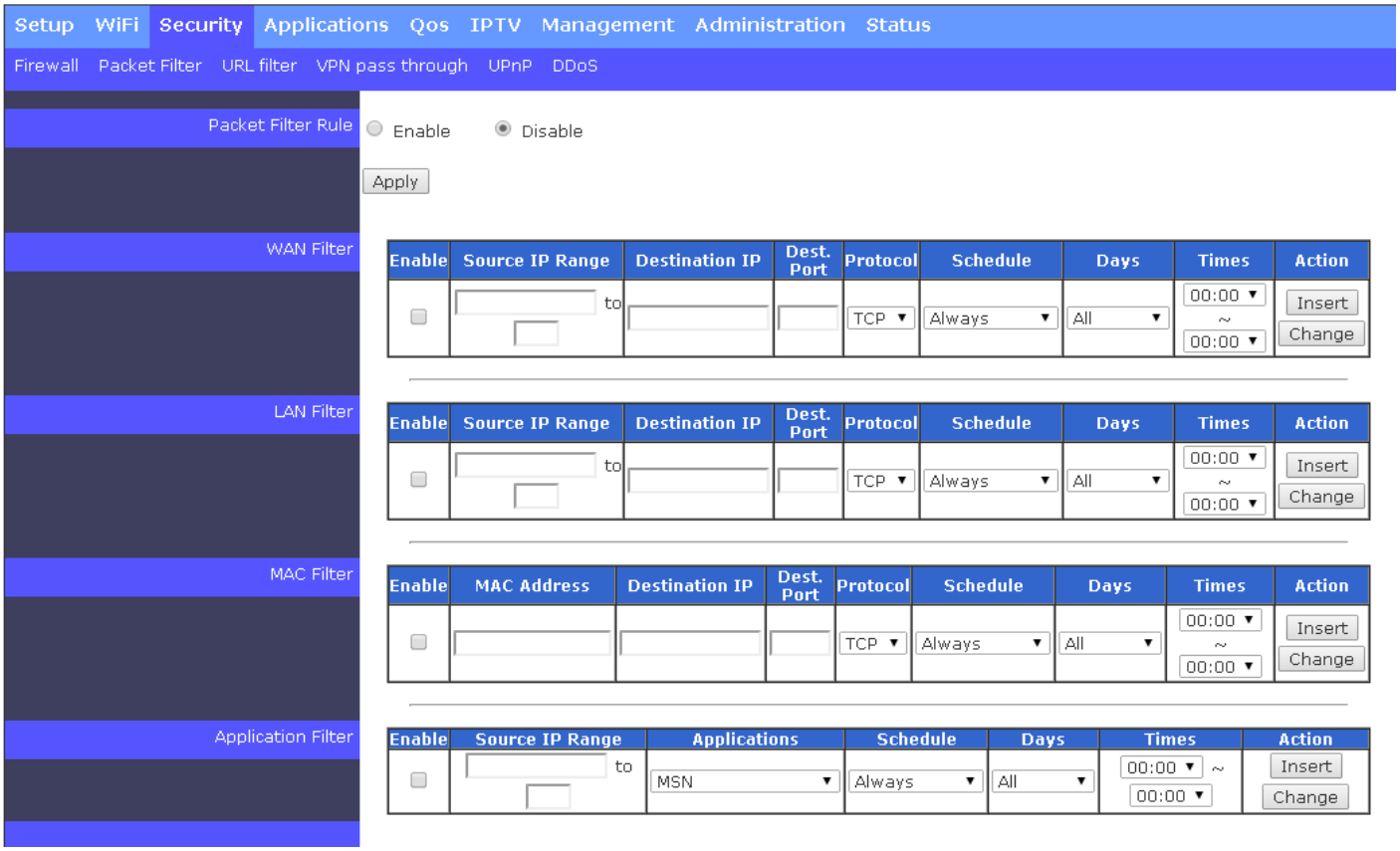
Note: *When you disable the firewall protection, the security features such as "Packet Filter", "URL Filter", "VPN Passthrough" and "DDoS" will stop working.*

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

2.6.2 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 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 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.
as the communication protocol of the packets which the WAN filter rule will block.

Schedule — Select *Always* for the Residential Gateway to always execute this rule. Or select *By Schedule* for the Residential Gateway to follow the schedule stipulated in the ***Days*** and ***Time*** fields to execute this rule.

Days — Select the days on which you want this rule to be executed in a week.

Time — Specify a time period of a day in which this rule will be executed.

Actions — Click *Insert* to create a new rule which you configure in the text boxes. And if you want to modify an entry in the rule table, click *Edit* to modify it in the text boxes. Then, click *Change* to submit the new settings. And if you want to remove an entry in the rule table, click *Del*.

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.

Schedule — Select *Always* for the Residential Gateway to always execute this rule. Or select *By Schedule* for the Residential Gateway to follow the schedule stipulated in the ***Days*** and ***Time*** fields to execute this rule.

Days — Select the days on which you want this rule to be executed in a week.

Time — Specify a time period of a day in which this rule will be executed.

Actions — Click *Insert* to create a new rule which you configure in the text boxes. And if you want to modify an entry in the rule table, click *Edit* to modify it in the text boxes. Then, click *Change* to submit the new settings. And if you want to remove an entry in the rule table, click *Del*.

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.

Schedule — Select *Always* for the Residential Gateway to always execute this rule. Or select *By Schedule* for the Residential Gateway to follow the schedule in the ***Days*** and ***Time*** fields to execute this rule.

Days — Select the day on which you want this rule to be executed.

Time — Specify a time period of a day in which you want this rule to be executed.

Actions — Click *Insert* 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 *Edit*. Then, click *Change* to submit the new settings. If you need to remove any entry from this table, click *Del*.

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 *MSN*, *YAHOO Messenger*, *FTP*, *SSH*, *Telnet*, *SMTP*, *DNS*, *HTTP*, *POP*, *NNTP*, *IMAP*, *SNMP*, and *HTTPS*. Select an application whose packets will be denied by this filter rule.

Schedule — Select *Always* for the Residential Gateway to always execute this rule. Or select *By Schedule* for the Residential Gateway to follow the schedule in the ***Days*** and ***Time*** fields to execute this rule.

Days — Select the day on which you want this rule to be executed.

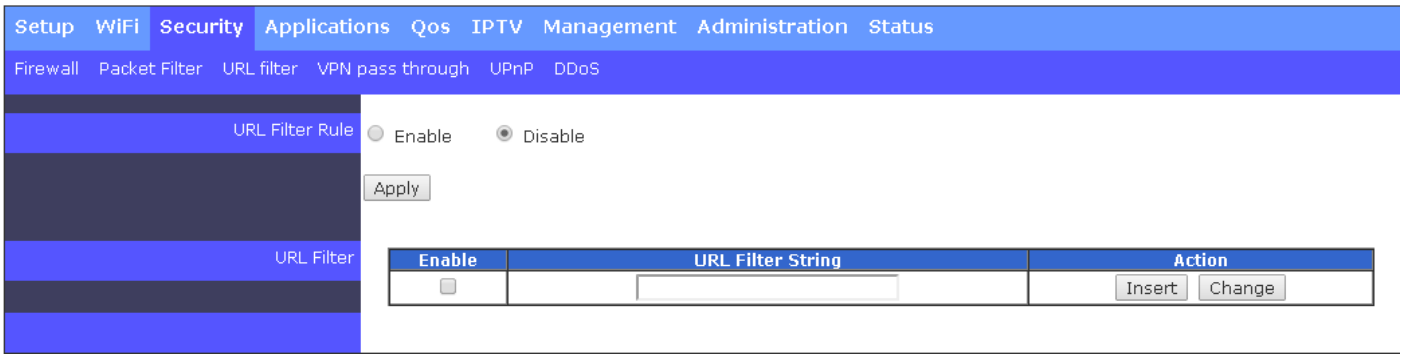
Time — Specify a time period of a day in which you want this rule to be executed.

Actions — Click *Insert* 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 *Edit*. Then, click *Change* to submit the new settings. If you need to remove any entry from this table, click *Del*.

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

2.6.3 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:



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 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.

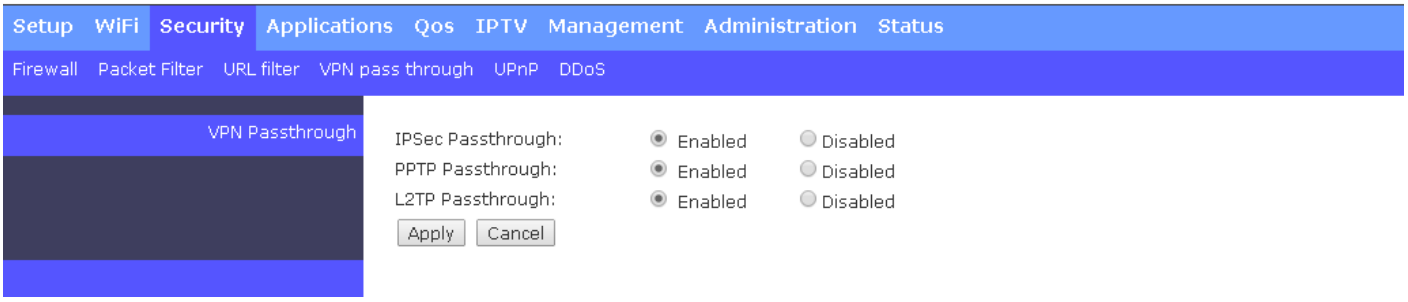
URL Filter String — Specify the URL address which this rule will allow or deny.

Action — Click *Insert* 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 *Edit*. Then, click *Change* to submit the new settings. If you need to remove any entry from this table, click *Del*.

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

2.6.4 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. Select **VPN pass through** from the **Security** sub menu bar. Then, **VPN pass through** screen page appears as follows:



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

VPN Passthrough The Residential Gateway supports VPN passthrough 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 Passthrough — Enable or disable 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.

PPTP Passthrough — Enable or disable 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.

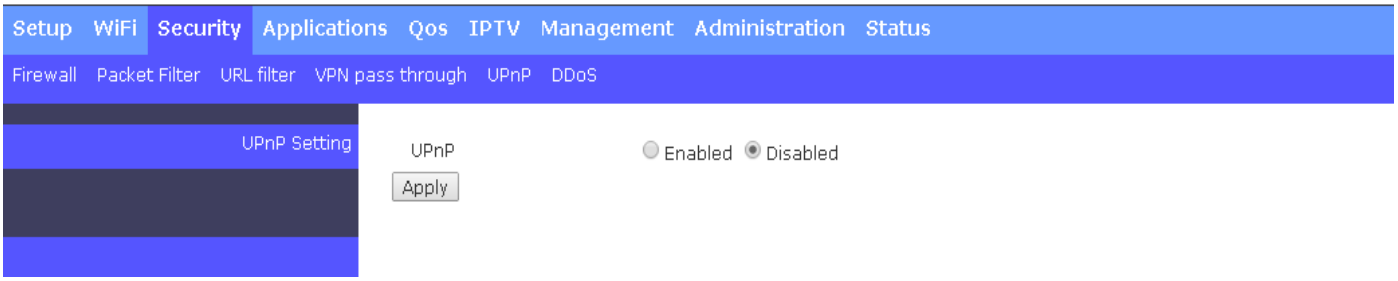
L2TP Passthrough — Enable or disable the PPTP passthrough on the Residential Gateway. L2TP stands for “Layer 2 Tunneling Protocol”. It is used to enable Point-to-Point sessions via the Internet on the Layer 2 level.

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

2.6.5 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.

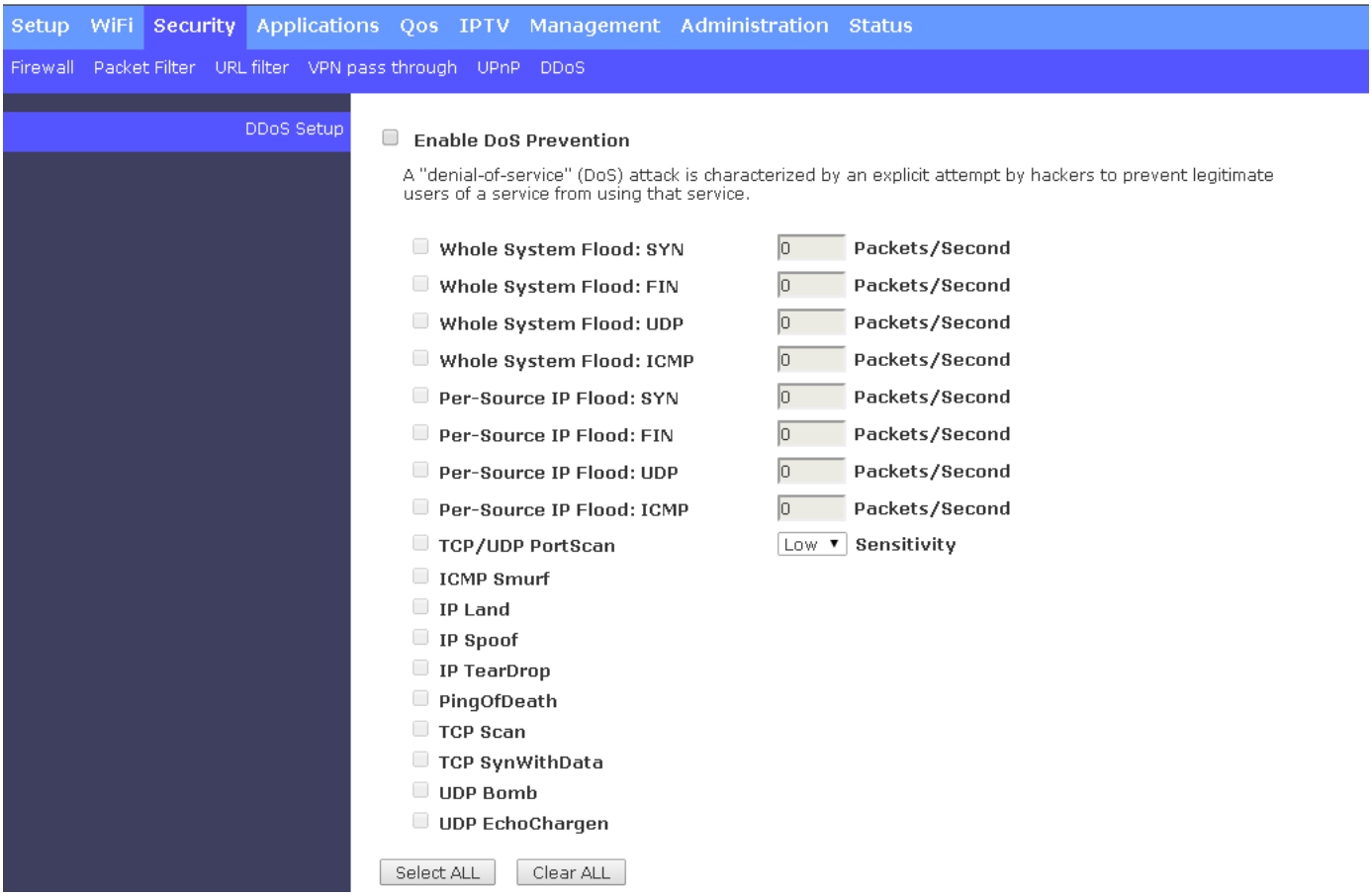
Select **UPnP** from the **Security** sub menu bar. Then, this screen page appears as follows:



UPnP Setting Tick this checkbox then click Submit button to enable UPnP feature. UPNP provides compatibility with networking equipment, software and peripherals.

2.6.6 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:



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

DDoS Setup 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.

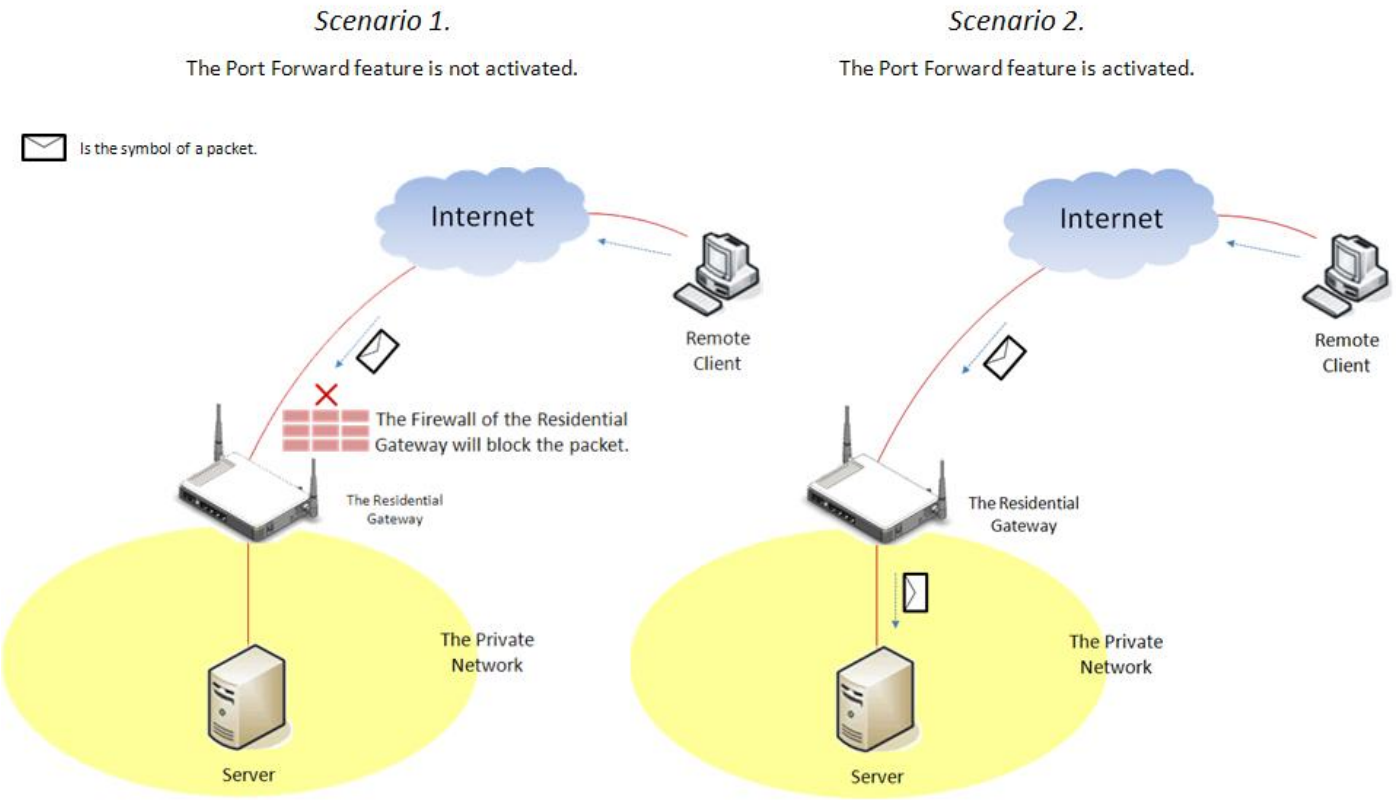
Click *Apply Changes* to submit your settings after you finish configuring this page.

2.7 Application

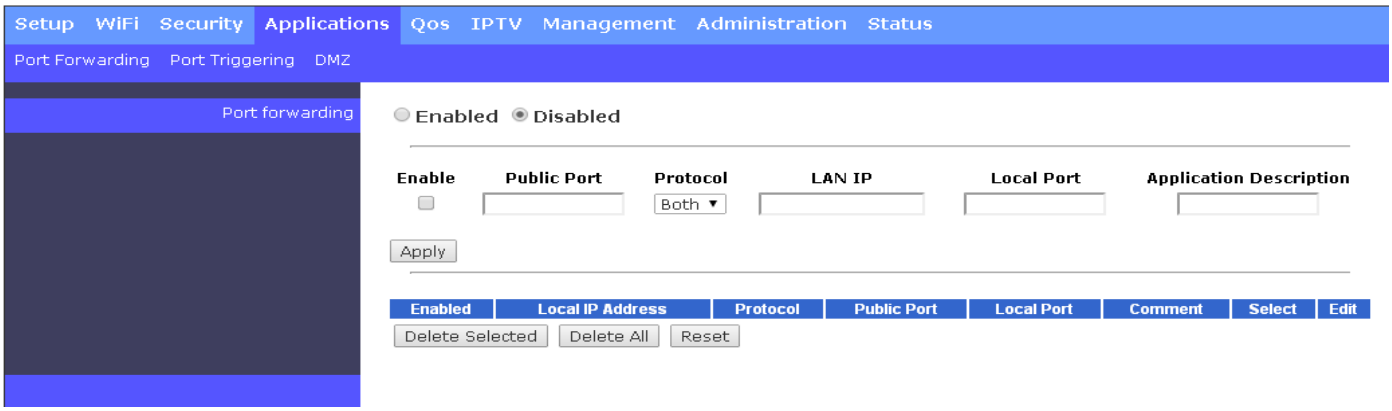
Select **Application** in the Main Menu bar. And the sub-items – **Port Forwarding**, **Port Triggering** and **DMZ** – will show up on the sub menu bar.

2.7.1 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 compare the two scenarios when the Port Forwarding feature is enabled and when it is not.



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



Port Forwarding 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.

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

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

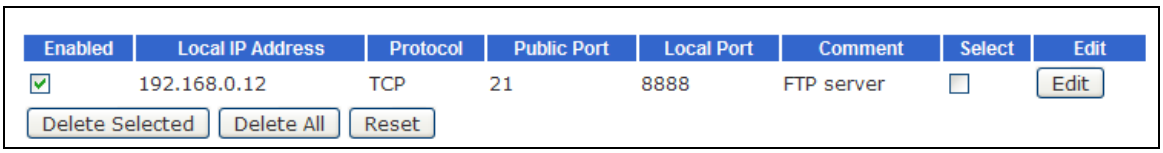
LAN IP — Specify the IP address of the server on the private network.

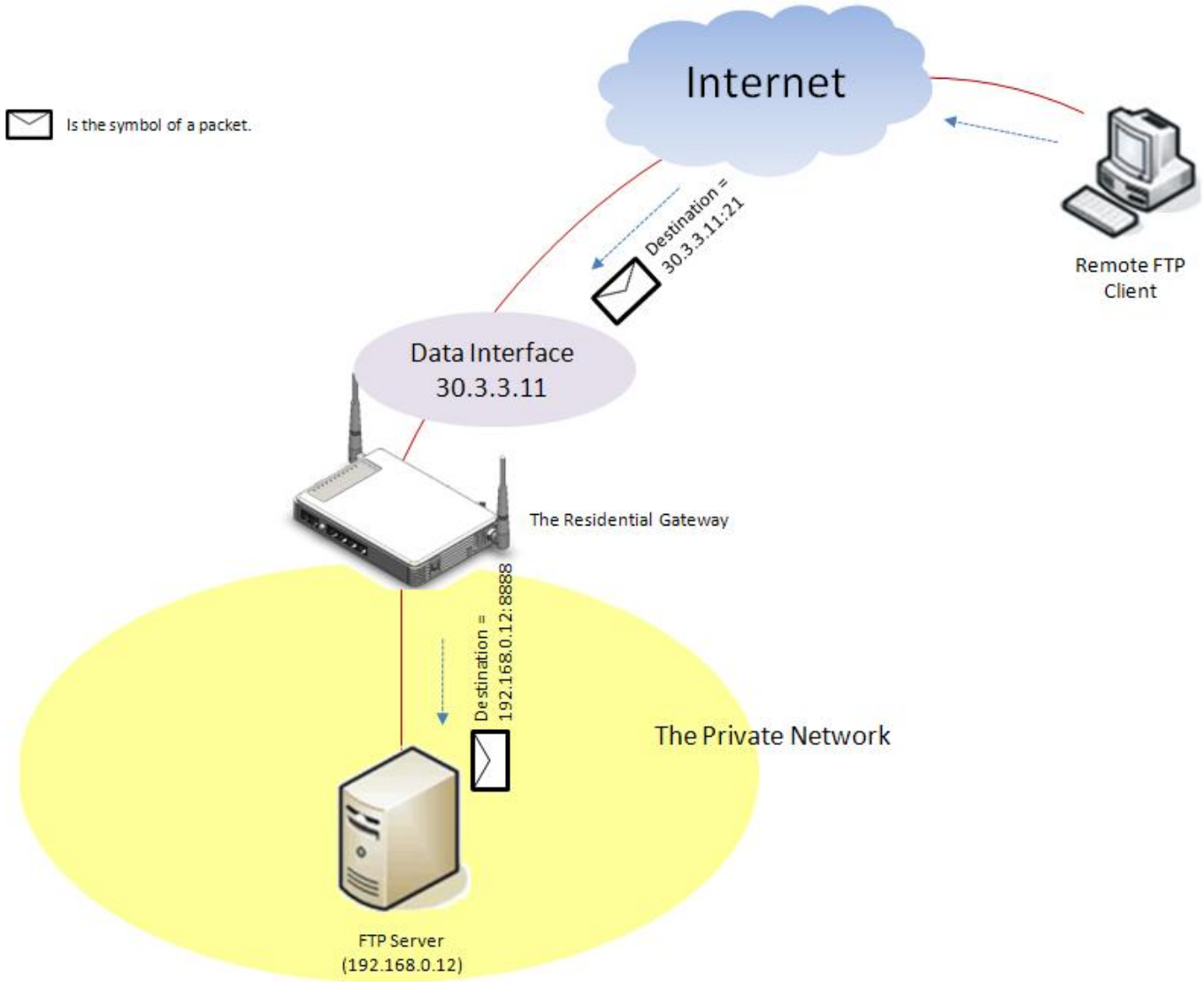
Local Port — Specify the port number which the packets are destined to (1~65535).

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

Click *Apply* 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.

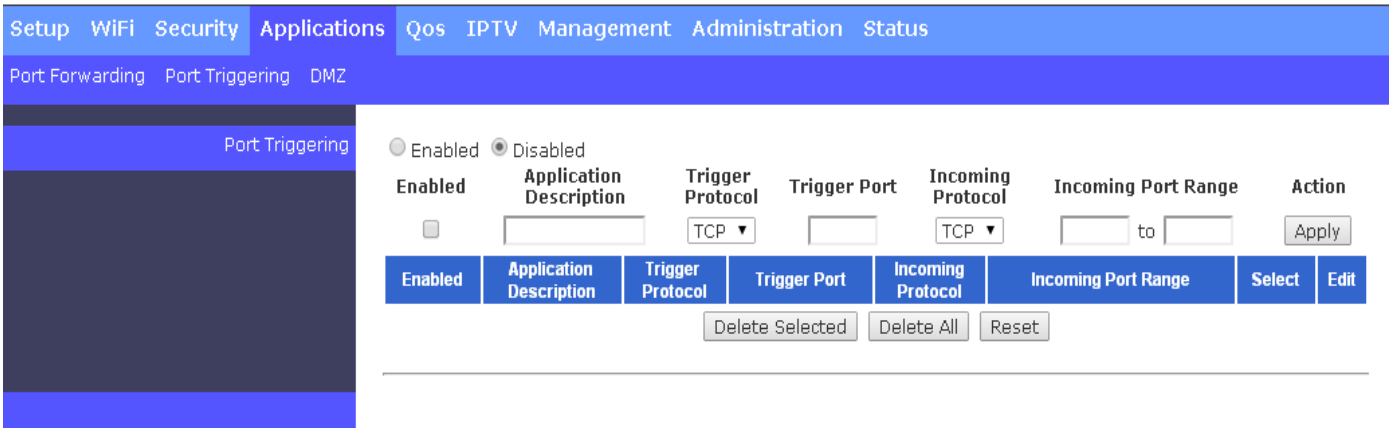




2.7.2 Port Triggering

Port Triggering is a more secure feature than port forwarding. It only allows transient port forwarding and does not always expose an Internet socket port to the Internet. When a packet which meets the precondition of a port triggering rule is received by the Residential Gateway from the private network, it will trigger the Residential Gateway to set up a temporary tunnel for an open service port. The tunnel will not be closed until the packets stop passing through the Residential Gateway for a period of time.

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



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

Port Triggering Select **Enabled** to activate port triggering feature on the Residential Gateway. Then, the Residential Gateway will execute the port triggering rules in the rule table below. Or select the **Disabled** radio button if you want to deactivate this feature. You can modify or create a port triggering rule in the text boxes according to your preferences. Below is a description of configuration parameters in this section.

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

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

Protocol — Choose *TCP*, *UDP* or *Both* in the pull-down menu as the protocol of the trigger packets

Trigger Port — Enter the destination port number of the trigger packet.

Incoming Port Range — Specify the range of destination port numbers of the packets which are allowed to pass through from the WAN interface to the private network when trigger packets are detected.

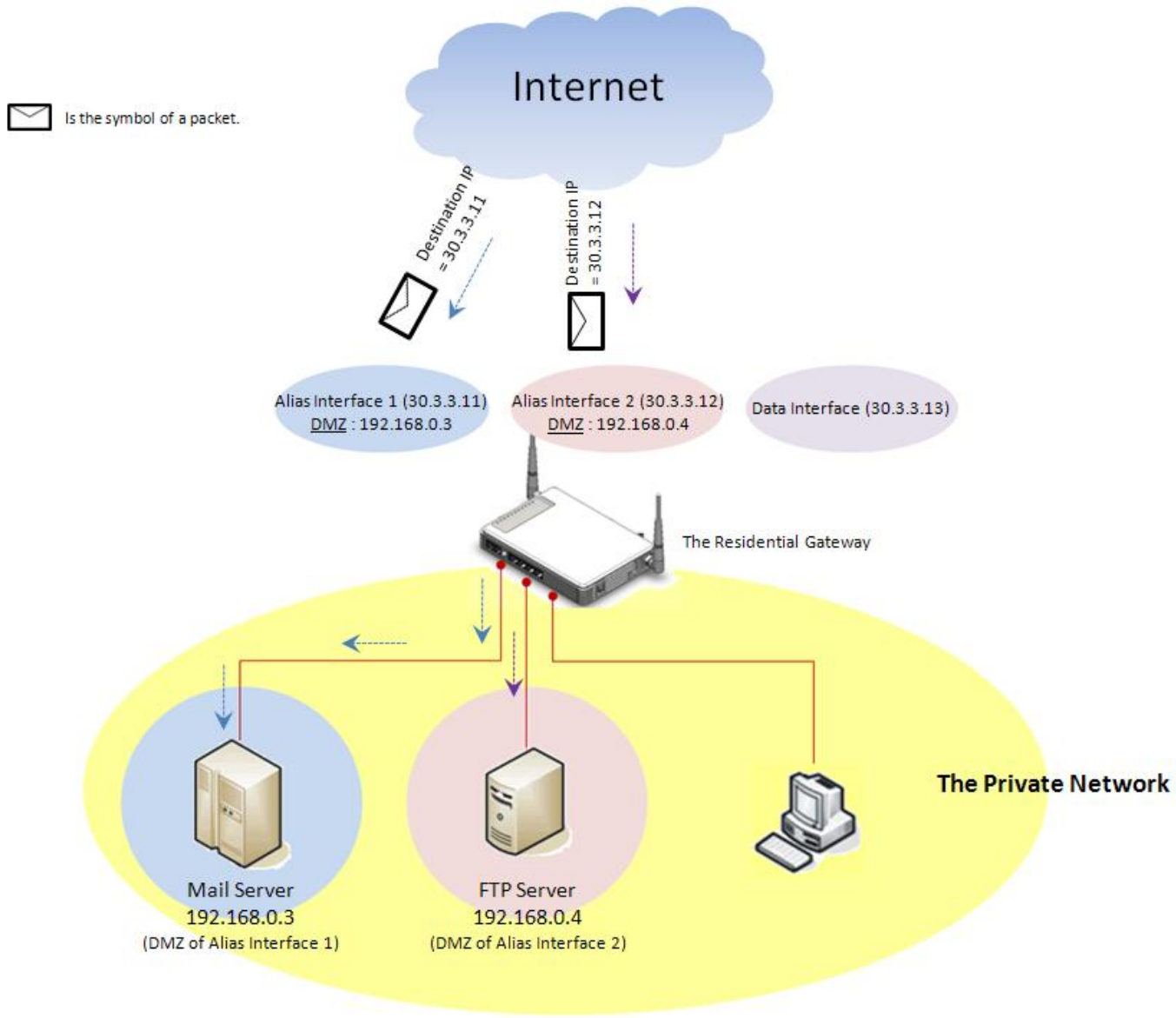
Action — Click *Apply* to submit the settings after you finish configuring a rule in the text boxes.

To modify an entry in the rule table, you can select *Edit* in the last column of the rule table to modify the entry in the text boxes. Or you can click *Reset* below the rule table to clear all the

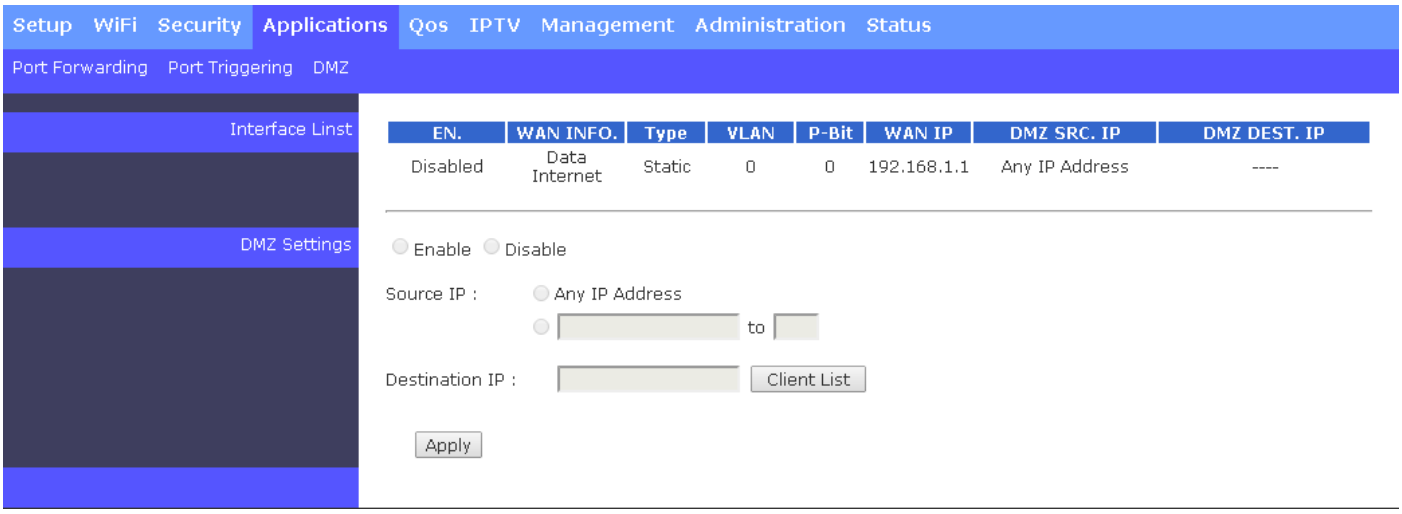
values in the text boxes. If you want to remove an entry in the rule table, please select the entry in the checkbox in the last column and click *Delete Selected* below the table. If you want to remove all entries in the table, please click *Delete All*.

2.7.3 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.



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



Interface List This section displays a list of the data interface and alias interfaces of the Residential Gateway. You can create a DMZ for each of the WAN interfaces in the list. And after a DMZ is created for an interface, this interface will redirect the packets received from the public network to its DMZ. Below is a description for each column of the table.

EN — This field displays if the WAN interface is enabled or disabled. You can click this field to create or edit its interface in the following section.

WAN INFO. — This is a view-only field which displays the type of the WAN interface.

Type — This is a view-only field which displays the Internet access type of this WAN interface.

VLAN — This is a view-only field. It displays the VLAN ID which the WAN interface will add to the untagged packets when the packets leave the Residential Gateway from this WAN interface.

P-Bit — This is a view-only field. It displays the 802.1p priority value which the WAN interface will add to the untagged packets along with its VLAN ID.

WAN IP — This is a view-only field which displays the IP address of this WAN interface.

DMZ SRC. IP — This is a view-only field. It displays an IP address range on the internet which the DMZ is open to.

DMZ DES. IP — This is a view-only field. It displays the private IP address which is on the DMZ of this WAN interface.

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.

Enable & ***Disable*** — 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 click *Client List* to view the DHCP client list in the pop-out window.

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

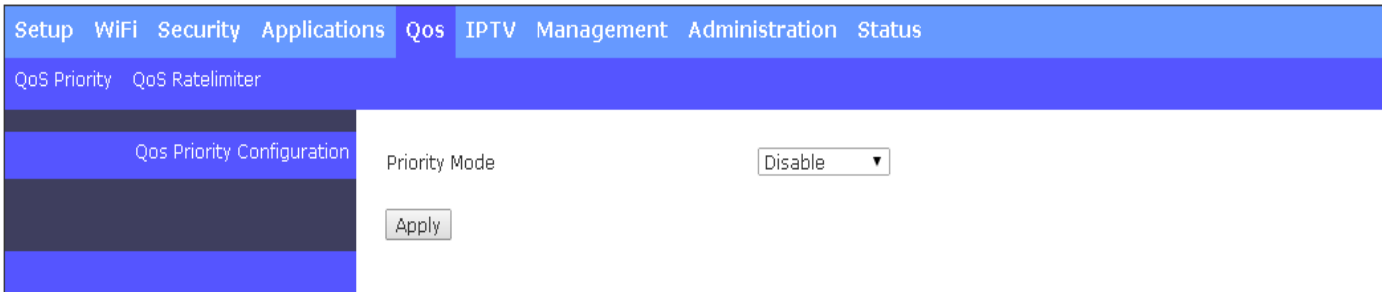
2.8 QoS

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

2.8.1 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:



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.

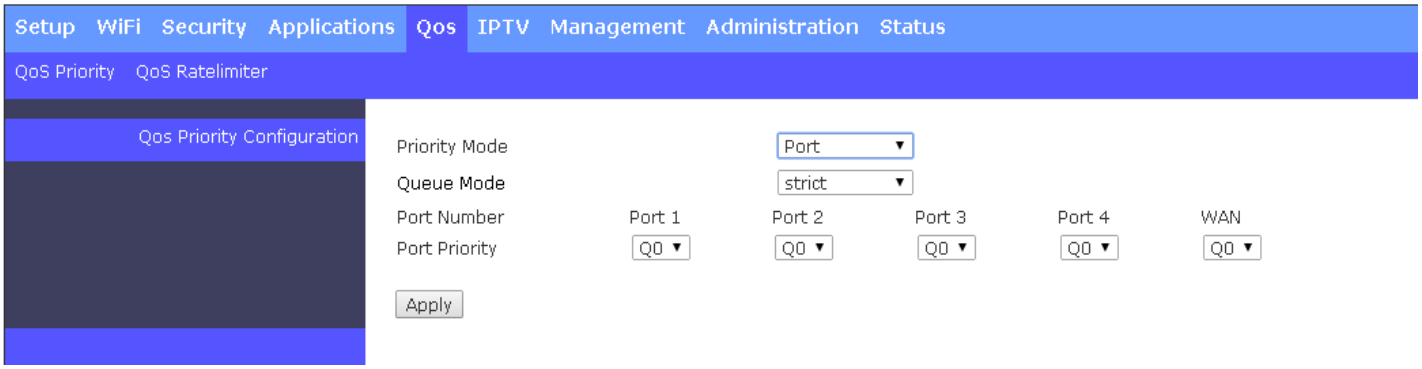
DSCP — Select this mode to bind the DSCP values of the packets with the designated

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**

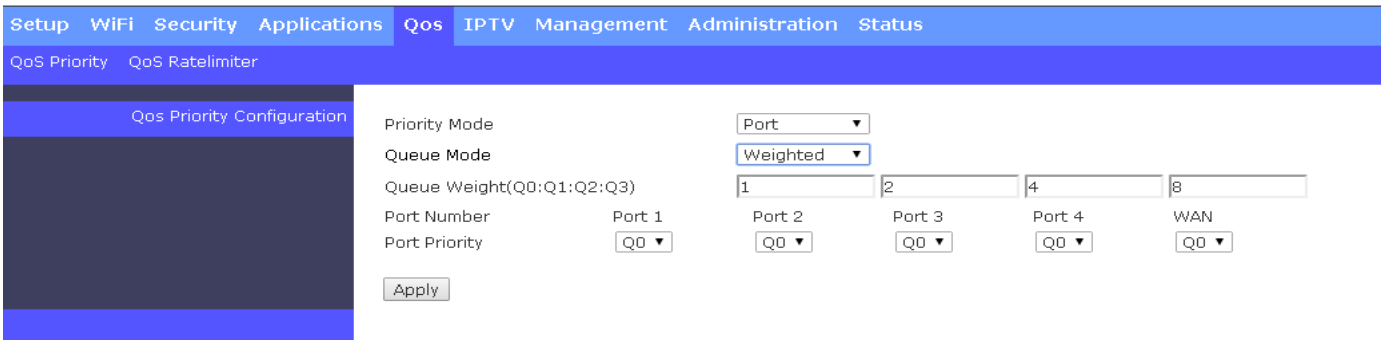
If you select *Port* for the ***Priority Mode*** and *strict* for the ***Queue Mode***, you need to decide how the ports of the Residential Gateway will be mapped to the queues.



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.

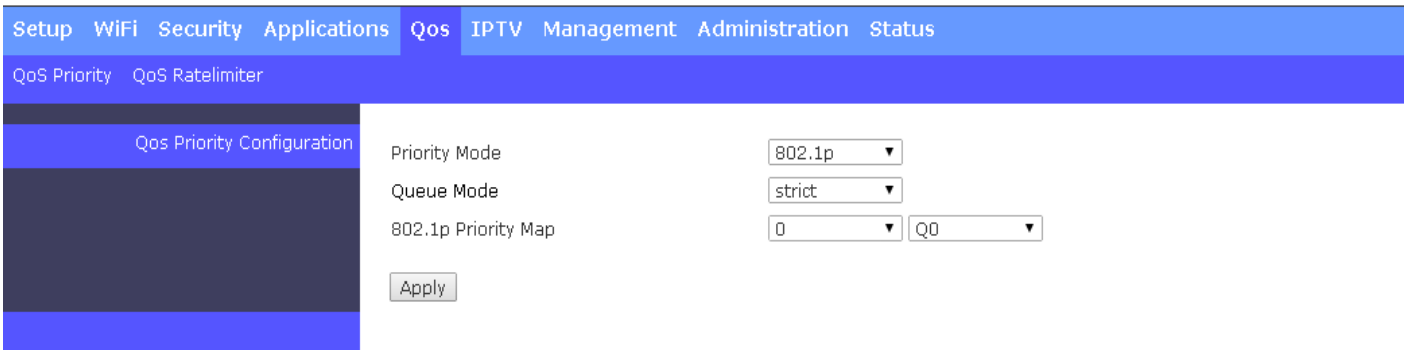


Queue Weight(Q0:Q1:Q2:Q3) — Specify the ratio of the transmission rates for queues in the text boxes.

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

802.1p Priority Mode > Strict Queue Mode

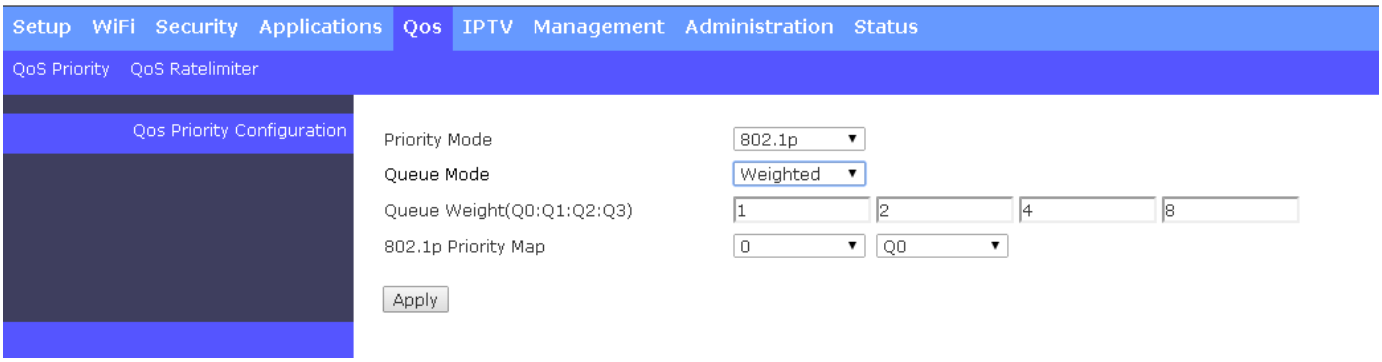
If you select *802.1p* for the ***Priority Mode*** and *strict* for the ***Queue Mode***, you need to determine how the 802.1p value will be mapped to the queues.



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.



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.

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.

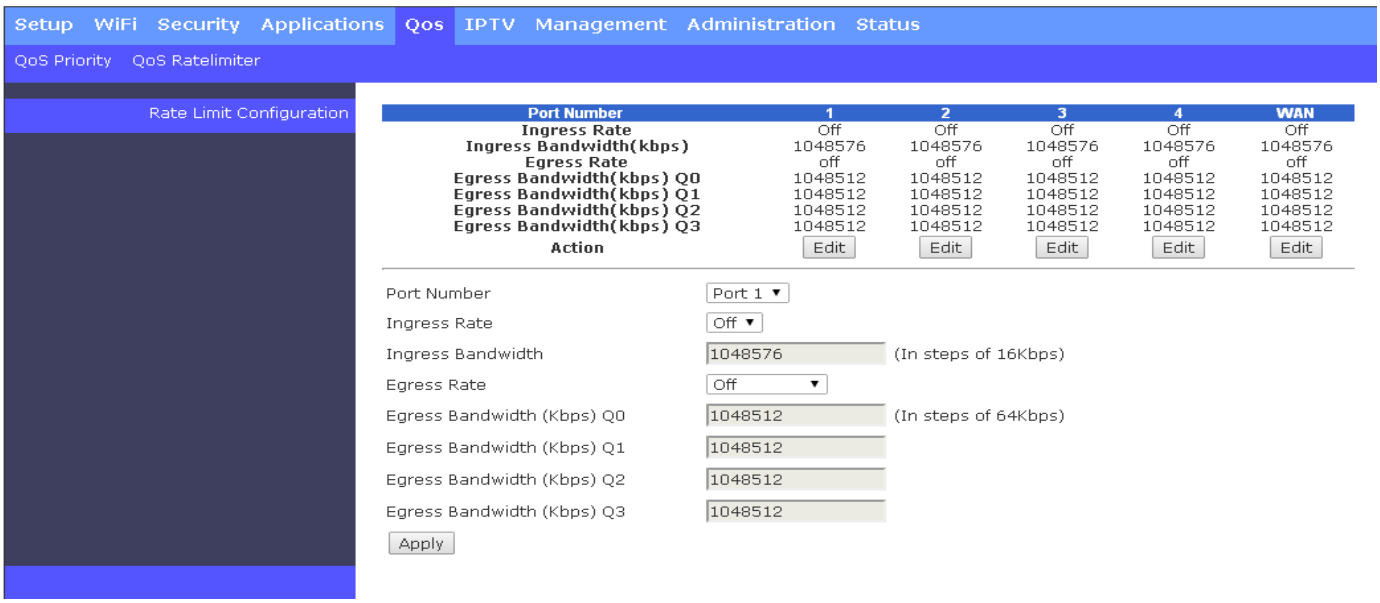
Queue Weight(Q0:Q1:Q2:Q3) — Specify the ratio of the transmission rate for queues in the text boxes.

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.

2.8.2 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:



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.

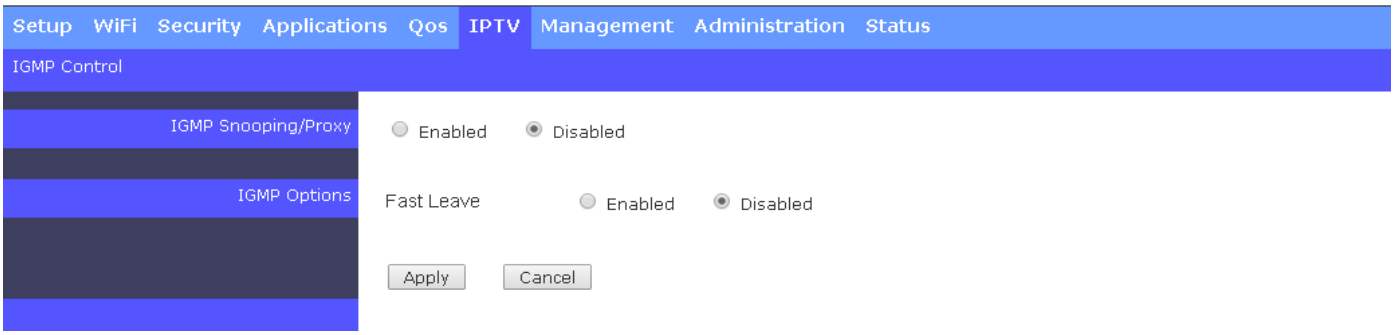
Click *Apply* to submit your settings after you finish configuring this page.

2.9 IPTV

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

2.9.1 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:



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

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.

IGMP Options This section allows you to set some values for other IGMP parameters.

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

2.10 Management

Select **Management** in the Main Menu bar. And the sub-items – **Auto-Provision (TR069/DHCP)** and **SNMP**– will show up on the sub menu bar.

2.10.1 Auto Provision (TR069/DHCP)

The Residential Gateway supports DHCP auto-provision and TR-069. The two functions are important for the network administrator who needs to manage many devices. They enable devices to automatically upgrade firmwares and configuration files from the server. So the network administrator can save much time and cost and does not have to configure each device manually. For details on the settings, please refer to the description of the individual section below.

Select **Auto-Provision (TR069/DHCP)** from the **Management** sub menu bar. And then the following screen page appears.

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

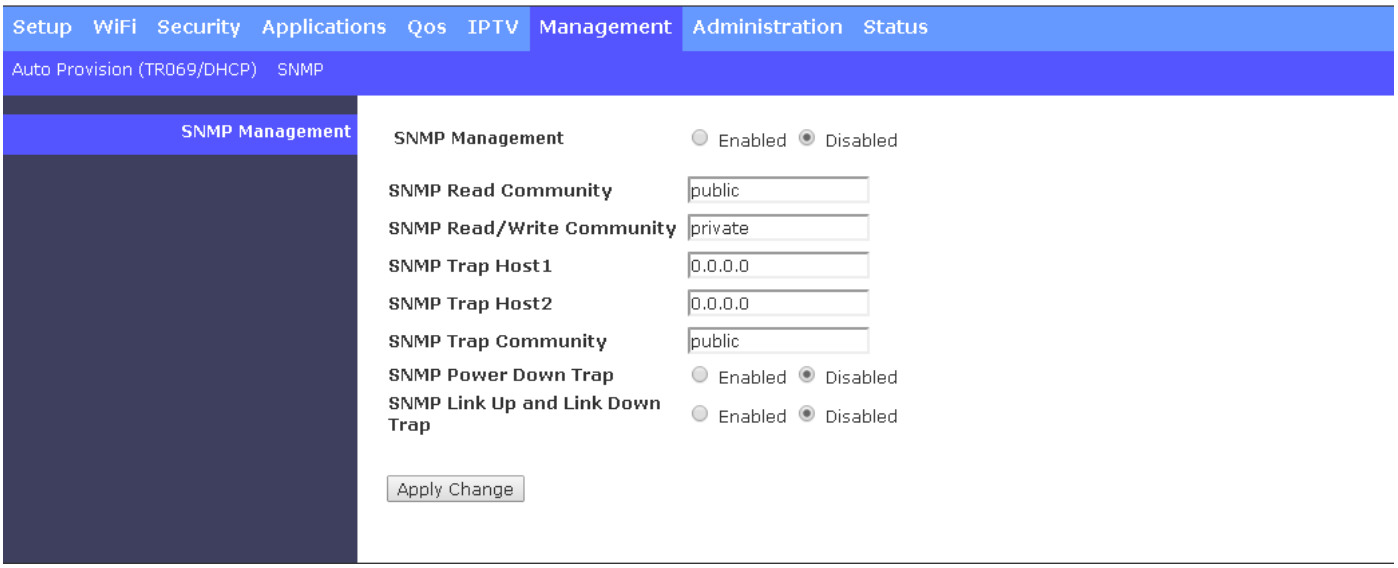
TR-069 This section allows you to enable or disable TR-069 management.

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

2.10.2 SNMP

The Residential Gateway supports SNMP management. SNMP stands for “Simple Network Management Protocol”. A brief introduction for SNMP will be found in Chapter 3 of this document.

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



SNMP Management This section allows you to make a 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.

SNMP Management — Enable or disable the SNMP service.

SNMP Read Community — Specify the Read Community.

SNMP Read/Write Community — Specify the Read/Write Community.

SNMP Trap Host 1 — Specify the IP address of the SNMP server to which the Residential Gateway will send the SNMP traps.

SNMP Trap Host 2 — Specify the IP address of the SNMP server to which the Residential Gateway will send the SNMP traps.

SNMP Trap Community — Specify the authorized SNMP community name.

SNMP Power Down Trap — Select *Enable* for the Residential Gateway to send the power down trap to the SNMP trap host.

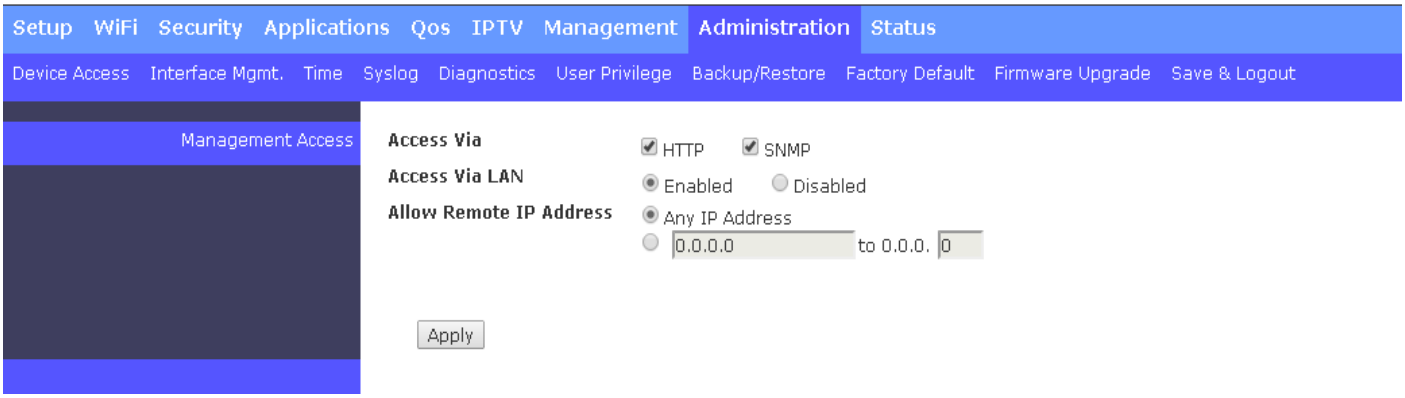
SNMP Link Up and Link Down Trap — Select *Enable* for the Residential Gateway to send the link up or link down trap to the SNMP trap host..

2.11 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.

2.11.1 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:



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

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.

Access Via — Tick the checkbox to enable the Residential Gateway to open the web UI for management.

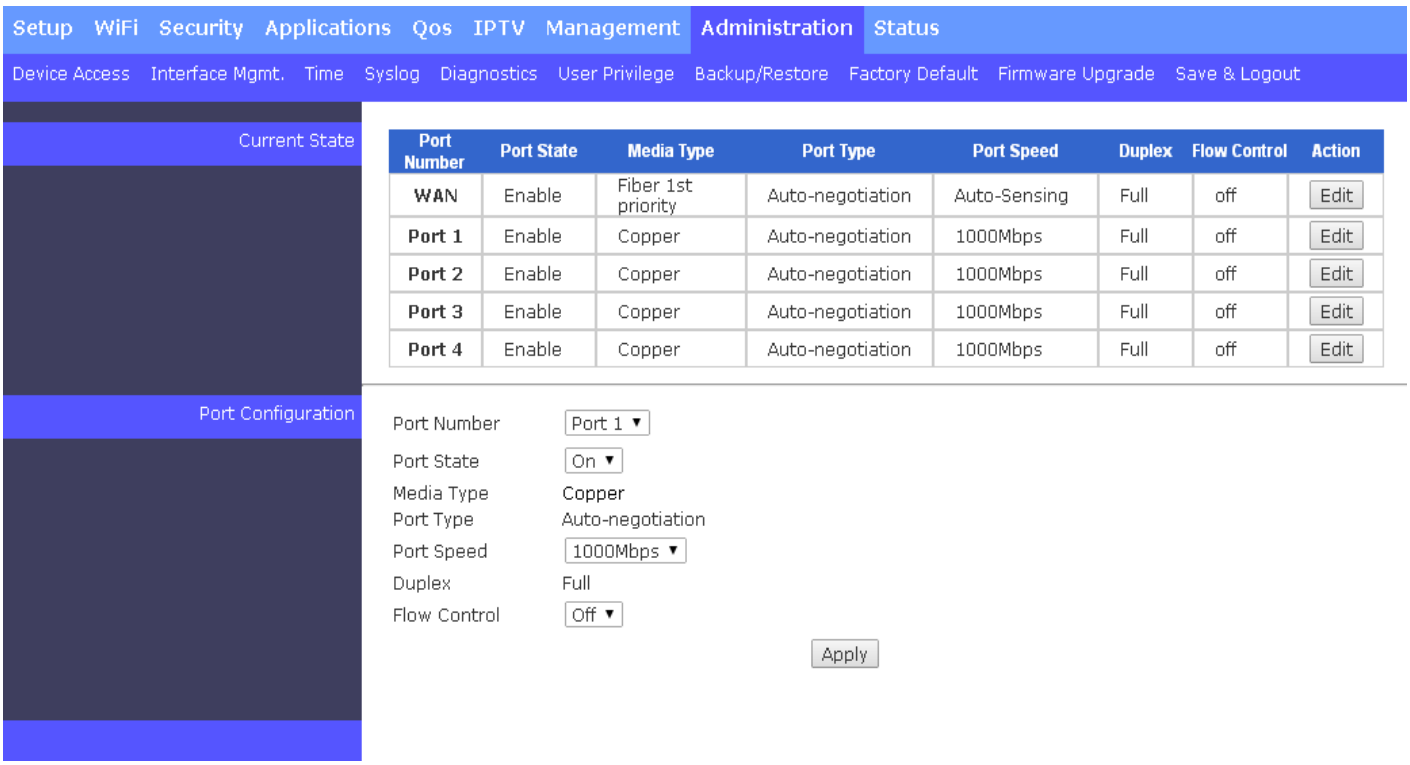
Access Via LAN — Select *Enabled* to permit the computers to manage the Residential Gateway from its LAN ports. Or select *Disabled* to deny the computers to manage the Residential Gateway from its LAN ports.

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.

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

2.11.2 Interface Mgmt.

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.



Current State This section displays the port state of the Residential Gateway. You can click *Edit* in the last 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 This section allows you to edit the port settings of the Residential Gateway.

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.

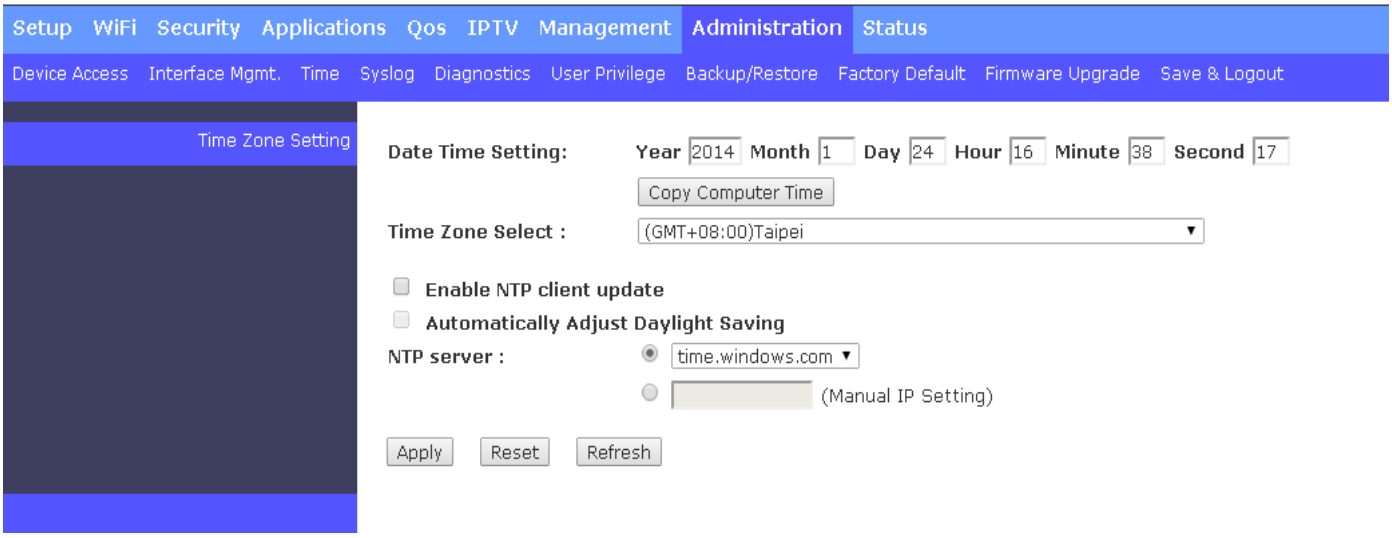
Duplex — This is a view only field. It indicates that the selected port is in the full duplex mode.

Flow Control — Enable or disable the flow control function.

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

2.11.3 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:



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

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.

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 Zone Select — Select your time zone from the pull-down menu.

Enable NTP client update — Tick the checkbox for the Residential Gateway to update its internal clock from a NTP server on the Internet.

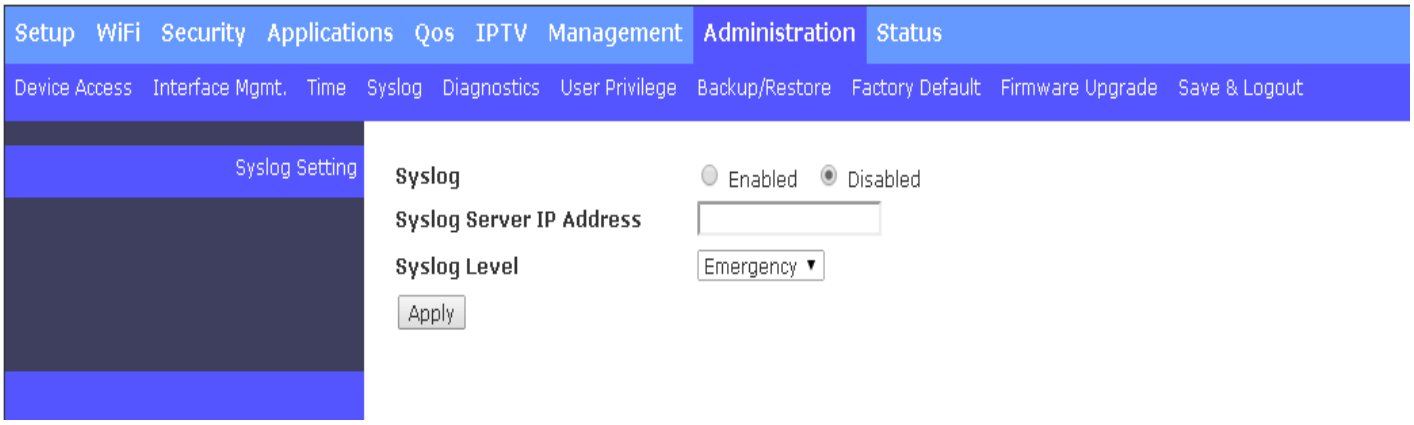
Automatically Adjust Daylight Saving — Tick the checkbox to enable the automatic daylight saving time function. It is a way of getting more daytime hour(s) by settings the time to be hour(s) ahead in the morning.

NTP Server — 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 first radio button and choose one of the default NTP servers from the pull-down menu. Or if you prefer a NTP server which is not available in the pull-down menu, select the second radio button and specify the IP address of the NTP server in the text box.

Click *Reset* to clear the unsaved values in the text boxes. Or click *Refresh* to update the date and time of the Residential Gateway. Click *Apply* to submit your settings after you finish configuring this page. And you can check the time of the Residential Gateway in the "System Information" page.

2.11.4 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 Settings Below is a description of the configuration parameters of this section.

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.

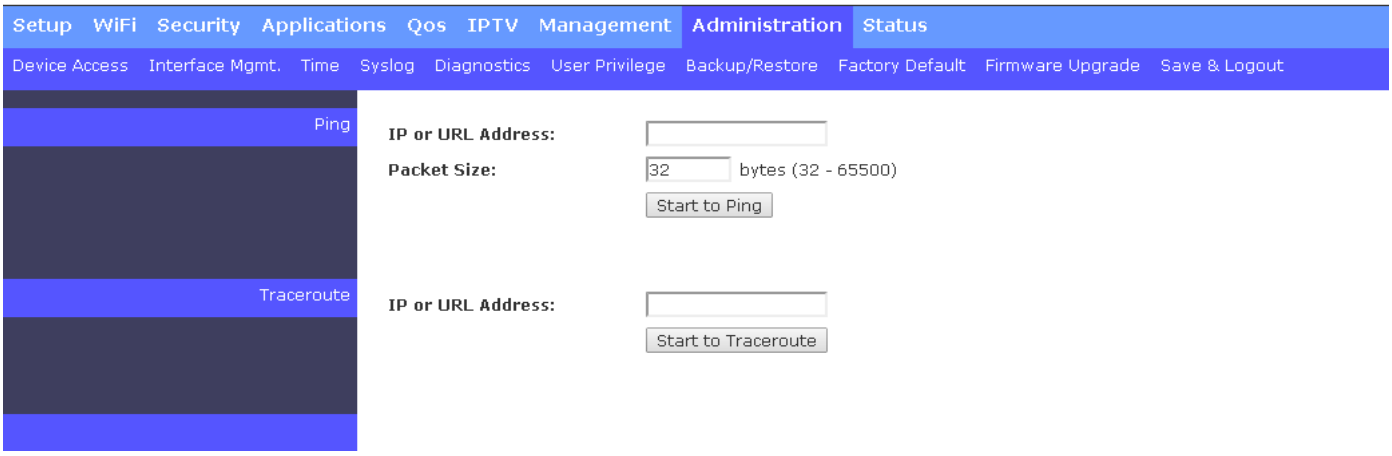
Syslog Level — Select one of the syslog levels from the pull down menu. The Residential Gateway will record log events at the chosen level and above. For example, if you choose *Error*, “error”, “critical”, “alert” and “emergency” events will be recorded.

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 *Apply* after you finish configuring the setting of this page.

2.11.5 Diagnostics

This page enables the network administrator to use ICMP and traceroute to check the network connectivity. The Residential Gateway supports the diagnostic tools such as ICMP and traceroute. It can emit ICMP Ping messages to a destination host on the Internet and see if it can receive the replies from the host. It can trace the path from the Residential Gateway to the destination host and display the list of routers between Residential Gateway to the destination host in this page. Select **Diagnostics** from **Administration** sub menu bar. Then, **Diagnostics** screen page will appear as follows:



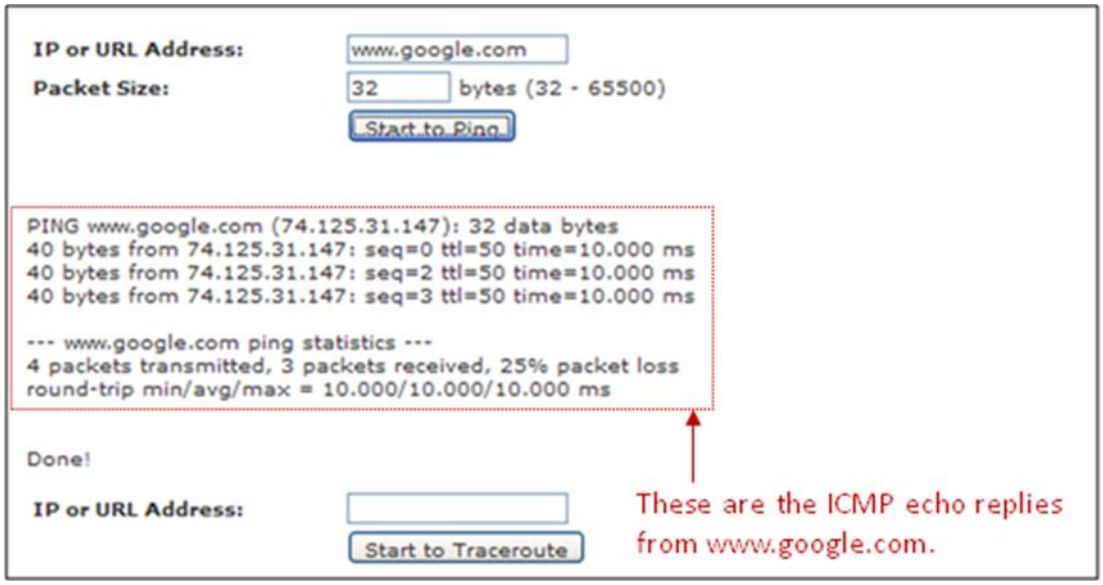
For details on the settings, please refer to the description of the individual section below.

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.

IP or URL Address — Specify an IP address or a URL address as the destination of the ICMP Ping packets.

Packet Size — Specify the size of the ICMP Ping packets.

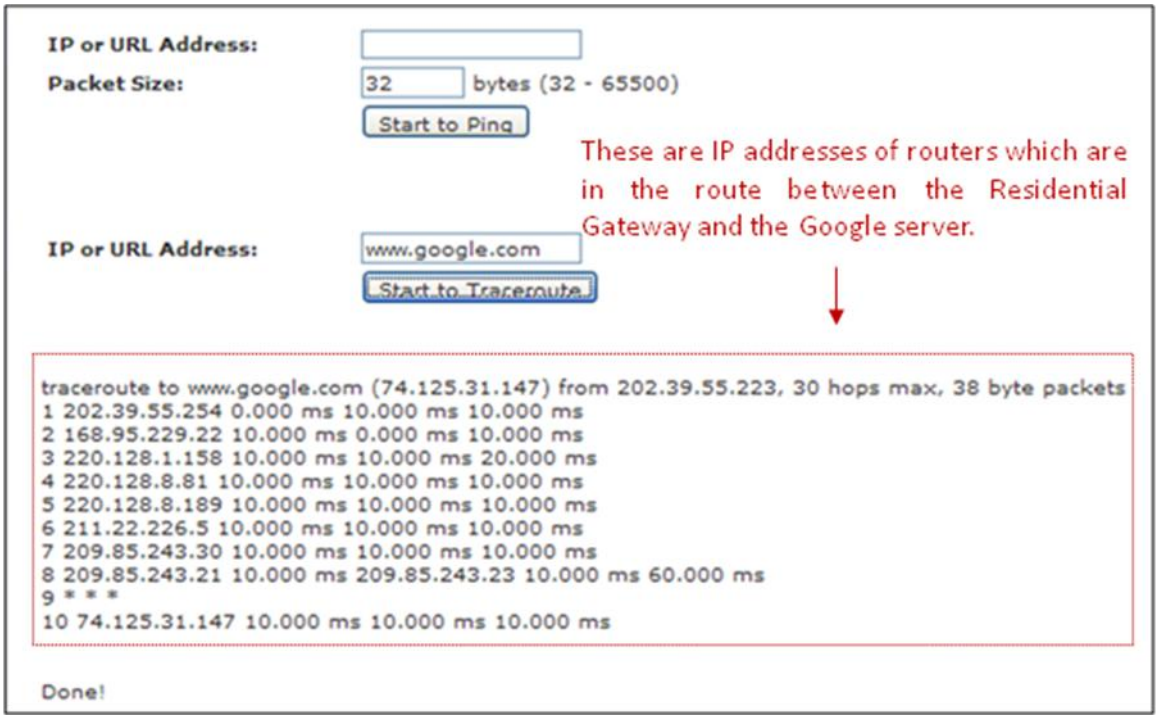
Click *Start to Ping* for the Residential Gateway to emit ICMP packets to the destination IP or URL address. And the ICMP replies from the destination host or any other ICMP messages will be displayed in this section.



Traceroute This section allows you to use traceroute function to find the path from the Residential Gateway to a destination host.

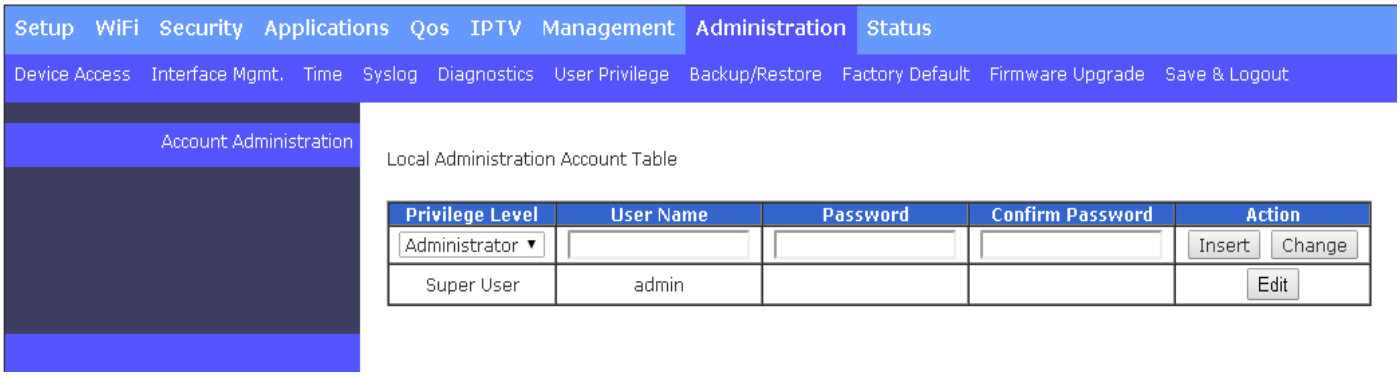
IP or URL Address — Specify the IP address or the URL address of the destination host.

Click *Start to Traceroute* for the Residential Gateway to use traceroute to find the routers between the Residential Gateway and the destination host. The Residential Gateway will display the IP addresses of the routers in this section.



2.11.6 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:



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

Account Administration This section contains the “Local Administration Account Table”. The local administration account table includes a list of user accounts which can access the management interface of the Residential Gateway. You can create a new account in the text boxes and add the new account in the table. Or you can select the entry in the table and modify it in the text boxes. Below is a description of each column in this table.

Privilege Level — The drop-down menu provides three privilege levels as follows.

Super User — This is the paramount privilege level which an account can have. And only one account in the table can have this privilege level. When an account is given this privilege level, it is allowed to read and write in every page of the UI. And it can also edit the local administration account table.

Administrator — This is the secondary paramount privilege level. More than one account can have this privilege level. And when an account is given this privilege level, it is allowed to read and write every page of the UI. But it is not authorized to modify the local administration account table.

Guest — This is the least paramount privilege level. More than one account can have this privilege level. It only enables the account to read the sub pages of “Status” in the main menu bar.

User Name — Specify a name for the user account in the text box.

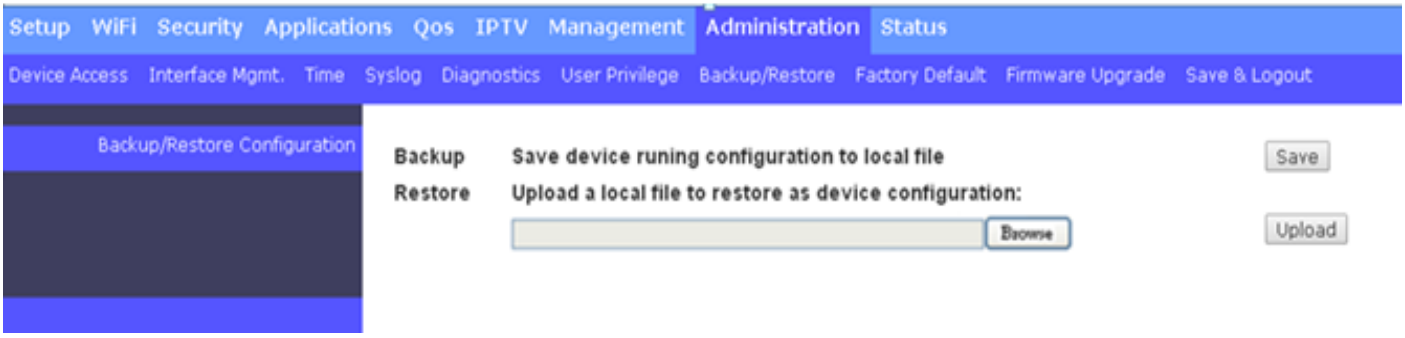
Password — Specify the password for this user account in the text.

Confirm Password — Specify the password for this user account in the text box again to confirm it.

Action — If you want to edit an entry in this table, click *Edit* in this column of that entry and edit it in the text boxes. Then, click *Insert* to create a new account or click *Change* to change the settings of an entry. If you want to remove an entry from this table, click *Del* in this column of the entry.

2.11.7 Backup/Restore

Select **Backup/Restore** from **Administration** sub menu bar. Then, **Backup/Restore** screen page will appear as follows:



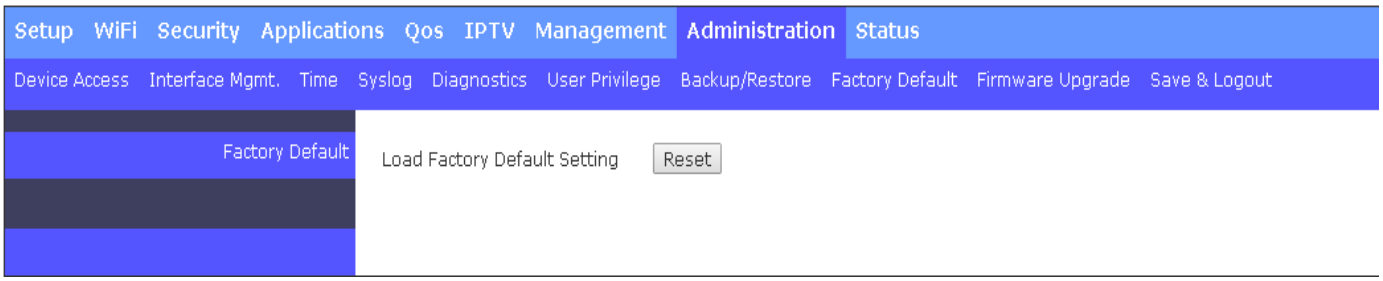
For details on the settings, please refer to the description of the individual section below.

Backup/Restore Configuration 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*** — Click *Save* to create a backup file for the current configuration of the Residential Gateway on the management computer.
>
> ***Restore*** — 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.

2.11.8 Factory Default

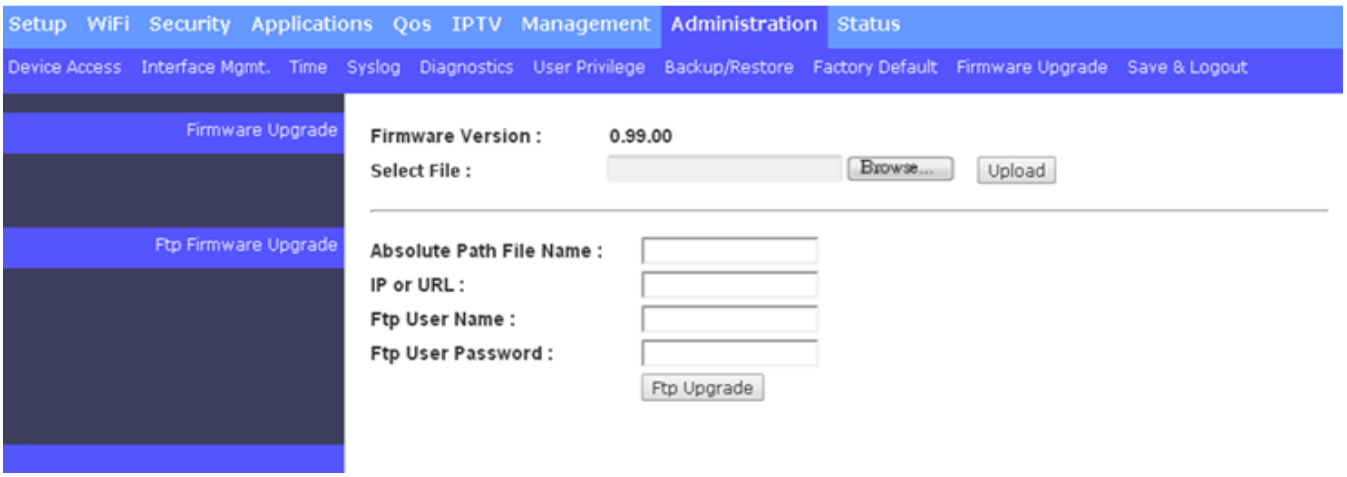
Select **Factory Default** from **Administration** sub menu bar. Then, **Factory Default** screen page will appear as follows:



Factory Default Click *Reset* to reset the Residential Gateway to the default settings.

2.11.9 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:



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

Firmware Upgrade This section enables you to upgrade the firmware of the Residential Gateway from the management computer. Below is a description of the configuration parameters of this section.

> ***Firmware Version*** — This is a view-only field which displays the current firmware version of the Residential Gateway.

Select File — Click *Browse* to find the path to the firmware in the pop-out window. And select the firmware in the pop-out window after you find its path in the management computer. Then, click *Upload* to load it to the Residential Gateway.

FTP Firmware Upgrade This section enables you to upgrade the firmware of the Residential Gateway from the FTP server. Below is a description of the configuration parameters of this section.

Absolute Path File Name — Specify the file name of the firmware in the FTP server.

IP or URL — Enter the IP address or the URL of the FTP server.

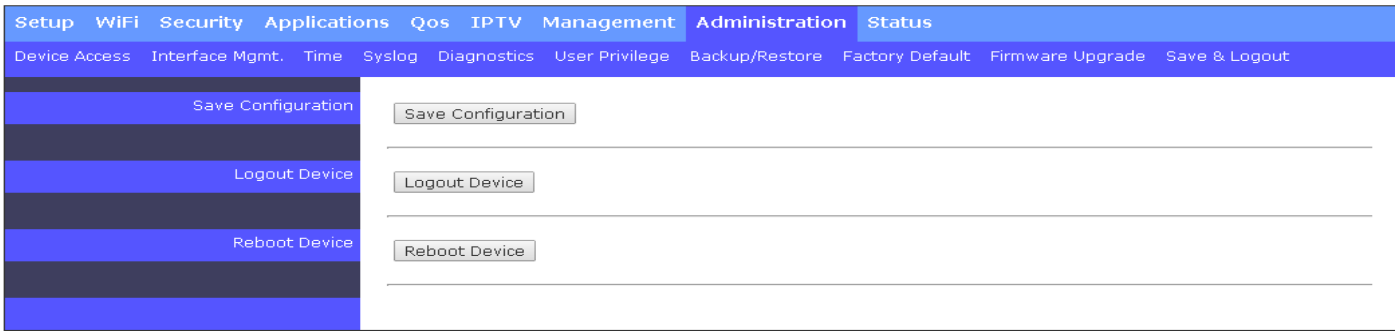
FTP User Name — Specify the user account of the FTP server.

FTP User Password — Specify the password for the FTP account.

Click *FTP Upgrade* to download the firmware from the FTP server to the Residential Gateway.

2.11.10 Save & Restore

Select **Save and Logout** from **Administration** sub menu bar. Then, **Save and Logout** screen page will appear as follows:



Save Configuration Click *Save Configuration* to save the current settings of the Residential Gateway.

Logout Device Click *Logout Device* to log out your account,

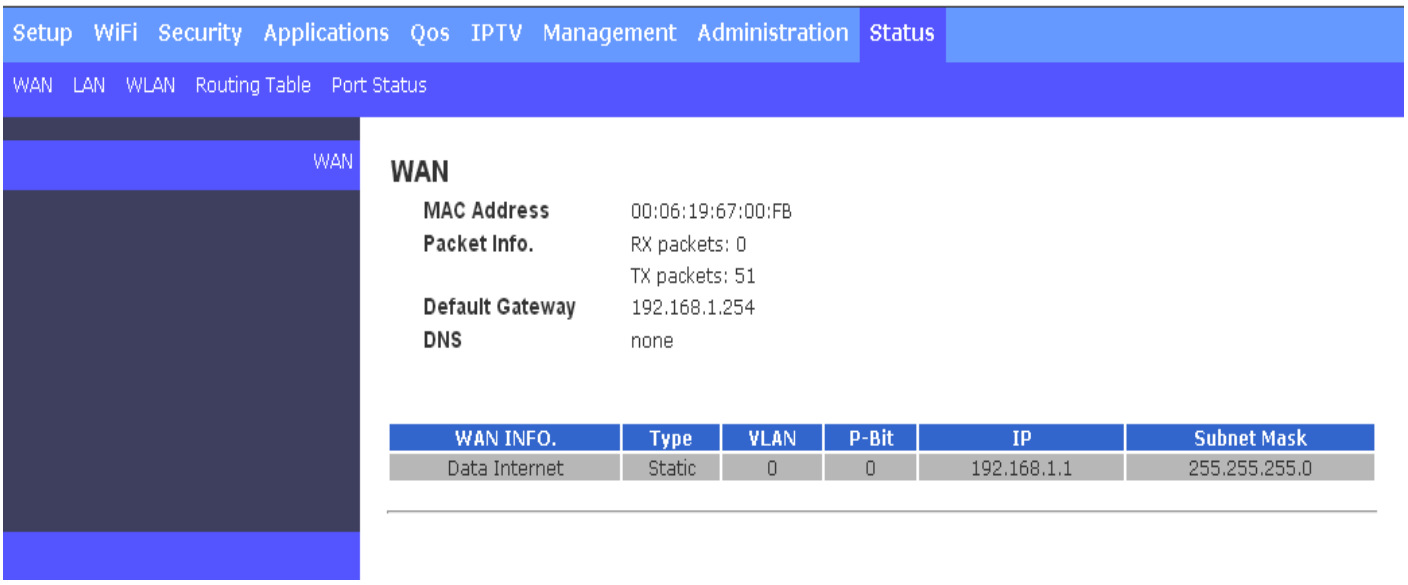
Reboot Device Click *Reboot Device* to restart the Residential Gateway.

2.12 Status

Select **Status** in the Main Menu bar. And the sub-items – **WAN**, **LAN**, **WLAN**, **Routing Table**, **Line Status**, and **Port Status**– will show up on the sub menu bar.

2.12.1 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:



WAN 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.

Packet Info — This is the numbers of the packets which are both transmitted (TX) and received (RX) by the WAN port.

Default Gateway — This is the default gateway which the Residential Gateway has on the public network.

DNS — 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 interfaces 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.

2.12.2 LAN

This page displays information of the Residential Gateway on the private network. Select **LAN** from the **Status** sub menu bar. Then, **WAN** screen page appears as follows:

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.

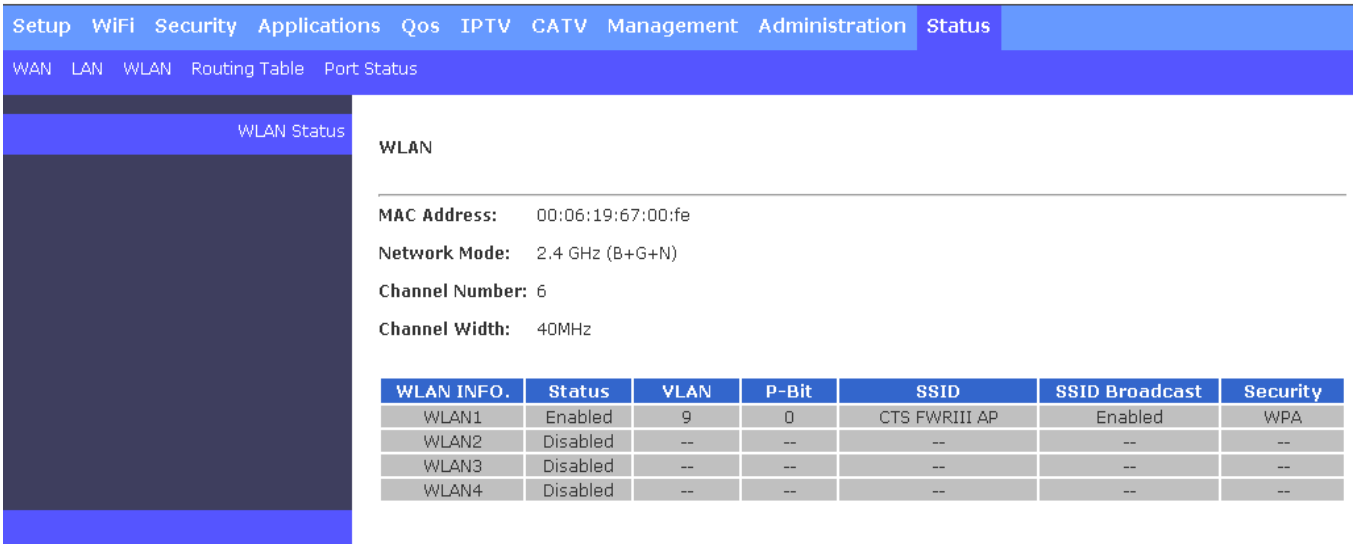
DNS Proxy — It is *Enabled* if the DNS proxy function of the Residential Gateway is activated. And it is *Disabled* if the DNS proxy of the Residential Gateway is deactivated.

IP-MAC Binding Mode — It is *IP-MAC Binding Allocation* if the Residential Gateway assigns IP addresses in the specified IP addresses range to the DHCP clients**.** And it is *IP-MAC Binding Access Restriction* if the Residential Gateway only assigns IP addresses in ***the DHCP reservation table*****.**

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.

2.12.3 WLAN

This page displays WLAN information of the Residential Gateway. Select **WLAN** from the **Status** sub menu bar. Then, **WLAN** screen page appears as follows:



And for more details, please refer to the description of the individual section below.

WLAN Status This is a view-only section which displays information about the wireless settings of the Residential Gateway. Below is a description of each item in this section.

MAC Address — It is the MAC address of the wireless card of the Residential Gateway.

Network Mode — It is the network mode of the wireless network of the Residential Gateway..

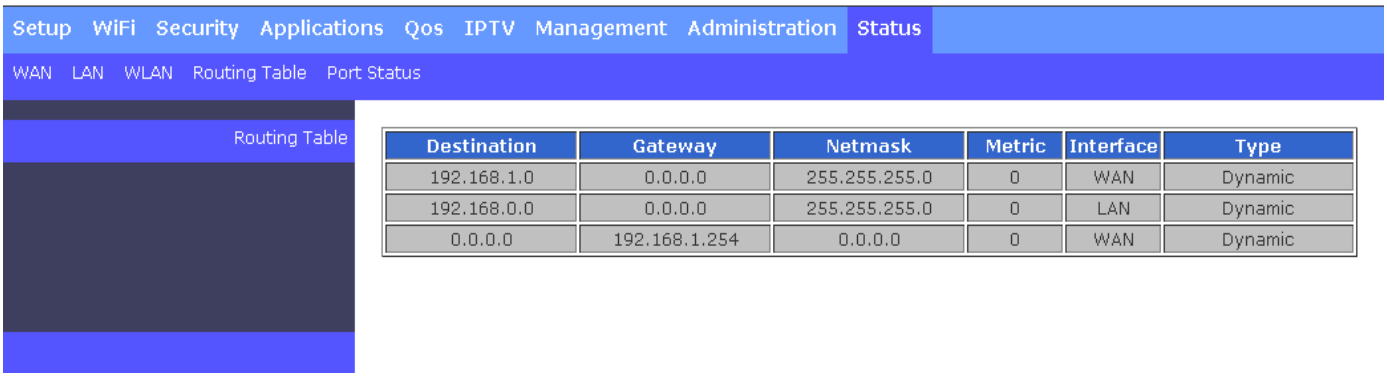
Channel Number — It is the channel of the wireless network of the Residential Gateway.

Channel Width — It is the wireless channel width of the Residential Gateway which is either 20 Hz or 40 Hz.

And the table in this section displays the current status of each WAN interfaces of the Residential Gateway. Below is the description for each column of this table.

2.12.4 Routing Table

Select **Routing Table** from the **Status** sub menu bar. Then, **Routing Table** screen page appears as follows:

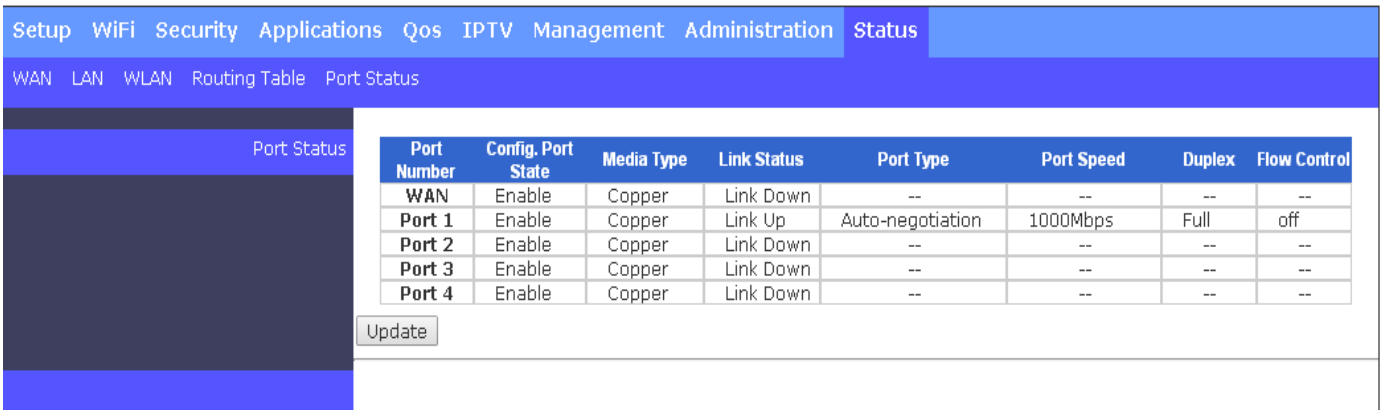


Destination	Gateway	Netmask	Metric	Interface	Type
192.168.1.0	0.0.0.0	255.255.255.0	0	WAN	Dynamic
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN	Dynamic
0.0.0.0	192.168.1.254	0.0.0.0	0	WAN	Dynamic

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).

2.12.5 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 Type	Port Speed	Duplex	Flow Control
WAN	Enable	Copper	Link Down	--	--	--	--
Port 1	Enable	Copper	Link Up	Auto-negotiation	1000Mbps	Full	off
Port 2	Enable	Copper	Link Down	--	--	--	--
Port 3	Enable	Copper	Link Down	--	--	--	--
Port 4	Enable	Copper	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 Type — It is the network mode of the wireless network of the Residential Gateway..

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 *on* or *off*.

3. 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.

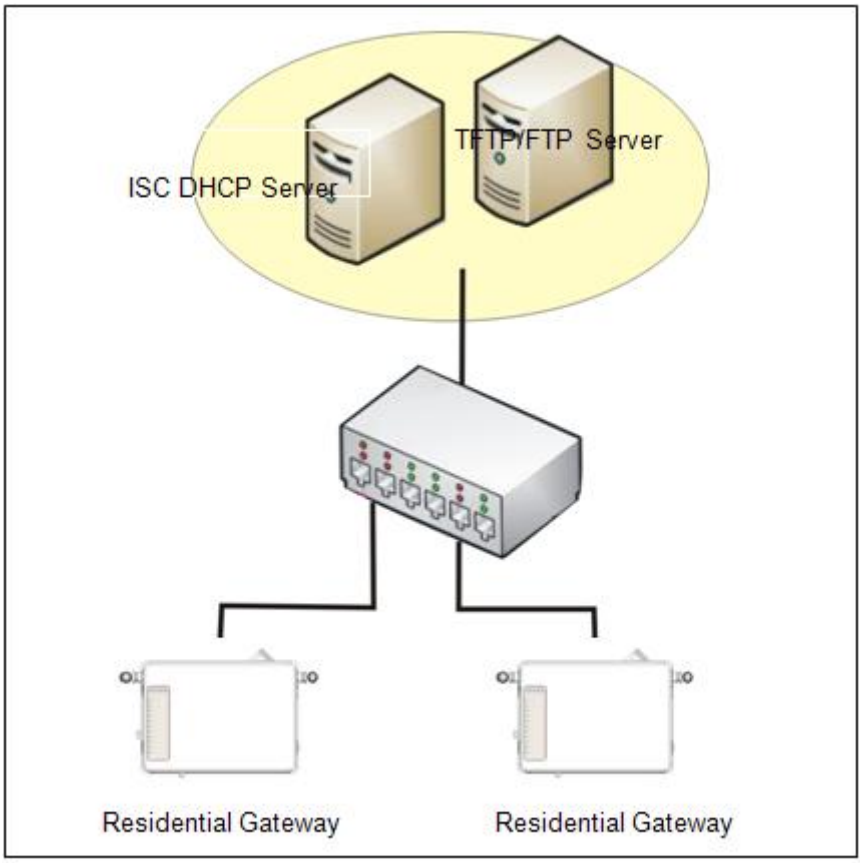
APPENDIX A: Set Up DHCP Auto-Provisioning

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;                                                    1
# 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;                                       2
        option SAMPLE.server-ip 192.168.2.1;                            3
#       option SAMPLE.server-login-name "anonymous";                    4
        option SAMPLE.server-login-name "sqa";                          5
        option SAMPLE.server-login-password "a12345A";                  6

    subclass "vendor-classes" "Host Name" {                             7
    vendor-option-space SAMPLE;
#    option SAMPLE.firmware-file-name "File Name";                      8
#    option SAMPLE.firmware-md5 d8:e2:f0:de:7d:a5:8e:2c:6e:4e:a7:5a:39:78:07:d8;   9
    option SAMPLE.configuration-file-name "metafile";                   10
    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

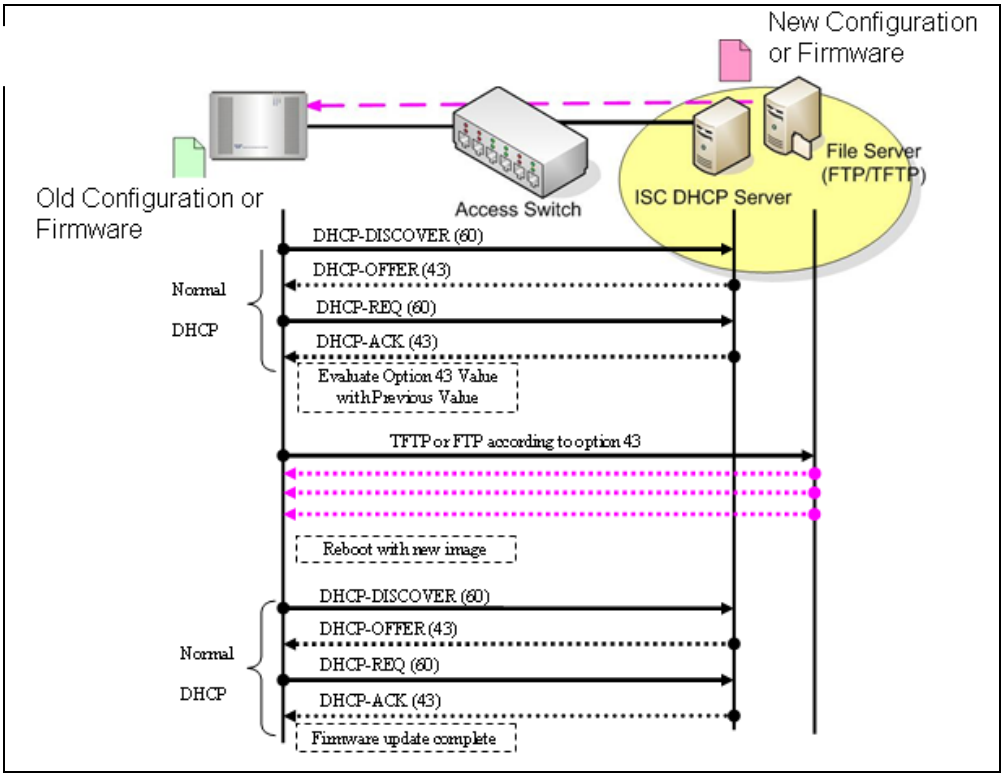
The TFTP/FTP File server should include the following items:

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.