



FWR-2105-WF-G SERIES

4 ports 10/100Mbps RJ-45, built-in IEEE 802.11b/g WiFi and 1 port 100Mbps fiber optics uplink Triple Play Gateway

FWR-2105-WF-N SERIES

4 ports 10/100Mbps RJ-45, built-in IEEE 802.11 n draft WiFi and 1 port 100Mbps fiber optics uplink Triple Play Gateway

FWR-2105-WF-G-RF

4 ports 10/100Mbps RJ-45, built-in IEEE 802.11b/g WiFi and 1 port 100Mbps fiber optics uplink Triple Play Gateway with CATV RF receiver

FWR-2105-WF-N-RF

4 ports 10/100Mbps RJ-45, built-in IEEE 802.11 n draft WiFi and 1 port 100Mbps fiber optics uplink Triple Play Gateway with CATV RF receiver

Network Management

User's Manual

Version 0.98

Trademarks

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

Trademarks

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

Copyright Statement

Copyright © 2010 Connection Technology Systems Inc.
This publication may not be reproduced as a whole or in part, in any way whatsoever unless prior consent has been obtained from Connection Technology Systems Inc.

FCC Warning

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into 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.

Copyright © 2010 All Rights Reserved.

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

Trademarks:

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

Table of Contents

1. INTRODUCTION	5
1.1 Front, Rear and Front-Top Panel.....	6
1.2 Management Options	7
1.3 Interface Description	8
1.4 Connecting the Wireless Gateway	8
1.5 RF over Fiber (With RF Receiver only)	9
1.6 LED Description	9
2. WEB MANAGEMENT	10
2.1 Web Management Overview	10
2.1.1 The Concept of IP Address	10
2.1.2 Start Configuring	11
2.1.3 Introduction to Sub-Menus.....	12
2.2 Information	13
2.2.1 System Information.....	13
2.2.2 Syslog Table	16
2.3 Network Management	17
2.3.1 WAN Setting	17
2.3.2 LAN Settings.....	20
2.3.3 WLAN Settings	22
2.3.4 WLAN Access Policy Setting	25
2.3.5 Static Route	25
2.3.6 NAT.....	26
2.3.7 Packet Filter.....	28
2.3.8 URL Filter.....	30
2.3.9 UPnP	30
2.3.10 DDNS	31
2.3.11 SNMP.....	32
2.4 Switch Management.....	33
2.4.1 Port Configuration.....	33
2.4.2 Bandwidth Control	34
2.4.2.1 Egress Bandwidth Control.....	34
2.4.2.1.1 By Port Only	34
2.4.2.1.2 By Port with Queue.....	35

2.4.2.1.3 By DSCP	35
2.4.2.1.4 By 802.1p	36
2.4.2.1.5 By Application	37
2.4.2.2 Ingress Bandwidth Setting.....	38
2.4.2.3 Traffic Flow for Bridge & NAT Mode	39
2.5.2.4 Bandwidth Control Setup Examples	40
2.4.3 Configure VLAN.....	52
2.5.4 Configure Q-in-Q	53
2.4.5 IGMP Control	56
2.5 Switch Monitor.....	58
2.5.1 Switch Port State	58
2.6 CATV Setting (Only available for RF module)	59
2.7 Management	59
2.7.1 Administrator Account.....	59
2.7.2 System Log.....	61
2.7.3 Date/Time	62
2.7.4 Ping Test.....	63
2.7.5 Save/Restore	63
2.7.6 Factory Default	64
2.7.7 Firmware Upgrade	64
2.8 Save & Logout.....	65
3. SNMP NETWORK MANAGEMENT	66
APPENDIX A: Set Up DHCP Auto-Provisioning.....	67
APPENDIX B: DHCP Text Sample.....	72

1. INTRODUCTION

Thank you for purchasing the Wireless Gateway that is designed to aim at FTTX applications. The Wireless Gateway provides four TP ports for LAN applications, one fiber port for WAN and built-in IEEE 802.11b/g or 802.11 b/g/n wireless LAN. The built-in management module allows you to configure and monitor this managed Wireless Gateway and its operation status locally or remotely through the network.

The wireless function of this Gateway conforms to IEEE 802.11b/g/n standards that can provide speed rate up to 30Mbps or 80Mbps when used with other 802.11b/g/n wireless products (the speed rate varies depends on the model that your purchase). To enhance wireless connections to reach further, detachable SMA 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 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 design of Wireless Gateway is dedicated to the FTTX broadband service providers who look for a way of delivering multiple IP service to home and SOHO users. The fiber-optic port supports a connection distance of from 2KM to 20KM, or more than 100KM by multi-mode optical fiber (MMF), single-mode optical fiber (SMF), or bi-direction SMF that can be used in apartments, houses, or schools.

The web management interface is easy for users to configure their needed settings, manage the Wireless Gateway, and upgrade the latest firmware for convenient maintenance. The NAT and DHCP server features also allow you to use an Ethernet hub or switch to establish a private network that enables multiple computers to share a single Internet connection. Additionally, Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example, a private IP address used in a local network) to a different IP address known within another network (for example, a public IP address used on the Internet). The Wireless Gateway's feature-designed patented compact case with a cable tray is for quick and easy installation and also wall-mountable. See below for the detailed hardware descriptions.

1.1 Front, Rear and Front-Top Panel

Both 802.11b/g and draft 802.11n models have same front and top panels. Figure 1-1~1-5 show the front and top views of 802.11b/g and draft 802.11n device:

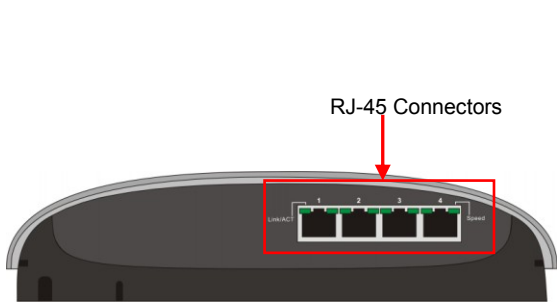


Figure 1-1. Front Panel

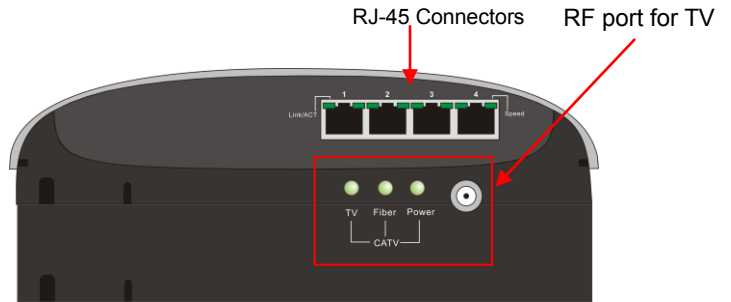


Figure 1-2. Front Panel with RF module

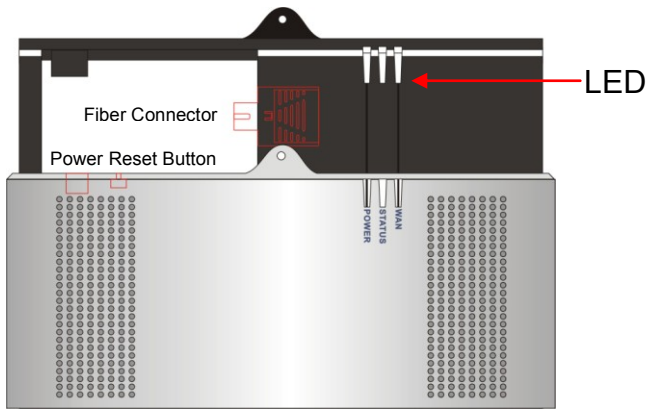


Figure 1-3. Top Panel with Cover Opened

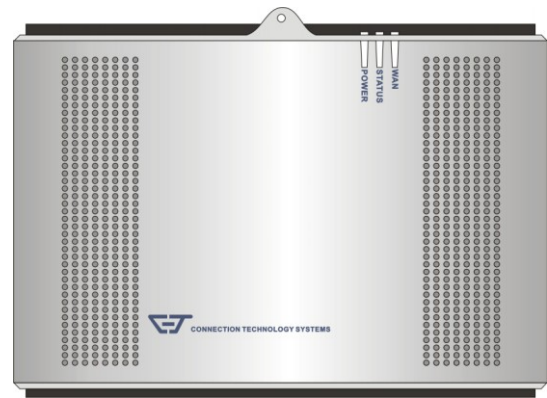


Figure 1-4. Top Panel with Cover Closed

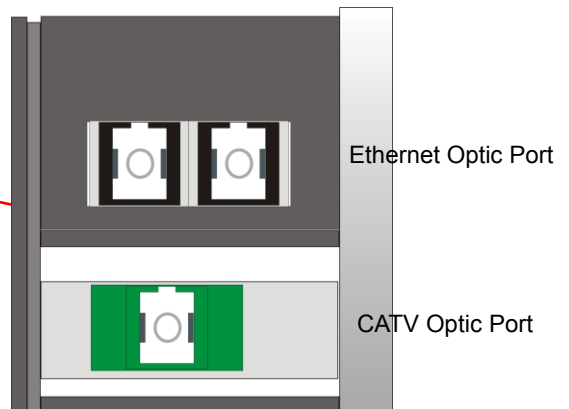
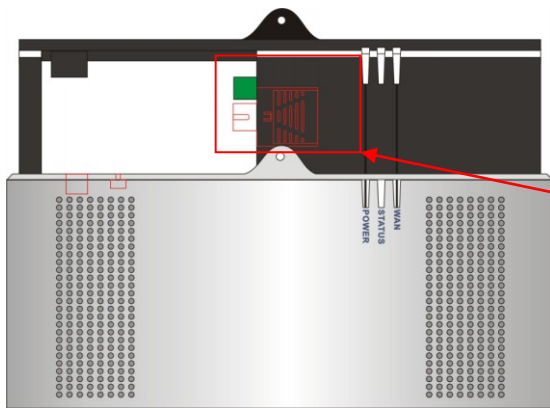


Figure 1-5. Fiber Port Close-up

802.11b/g and draft 802.11n models have different rear panels. Figure 2-1~2-4 show rear panel views of 802.11b/g and 802.11n model.

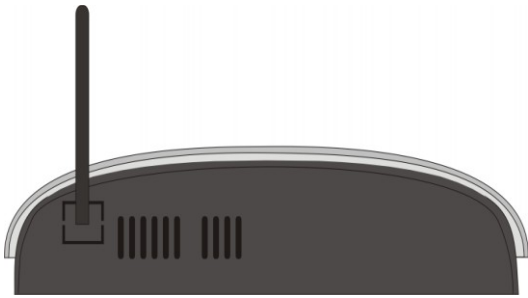


Figure 2-1. Rear Panel for 802.11b/g models

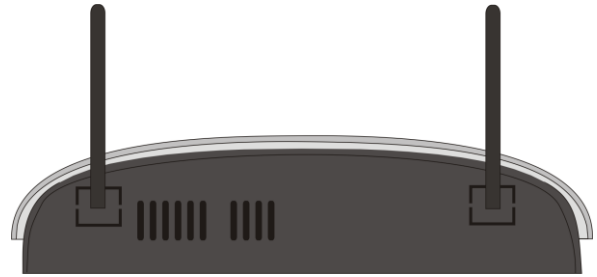


Figure 2-2. Rear Panel for 802.11n models

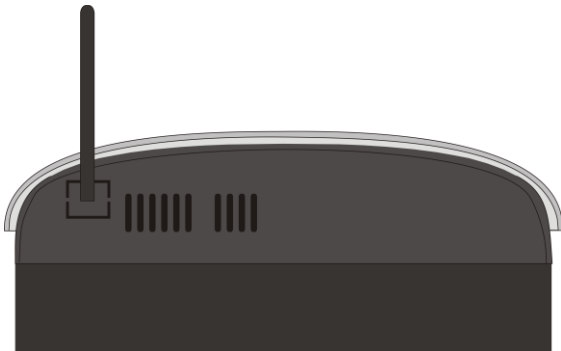


Figure 2-3. Rear Panel for 802.11b/g models with RF module

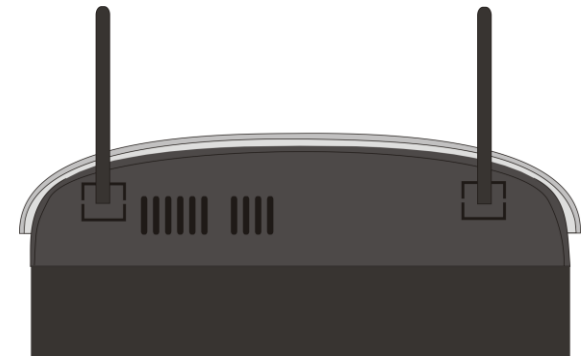


Figure 2-4. Rear Panel for 802.11n models with RF module

1.2 Management Options

Management options available in this Wireless Gateway are listed below:

- **Web Management**
Web Management is of course done over the network. Once the Wireless 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 Wireless Gateway to set up the needed IP, can also be done through any of the four 10/100Base-TX 8-pin RJ-45 ports located at the front panel of the Wireless Gateway. Direct RJ45 LAN cable connection between a PC and Wireless Gateway is required for this.
- **SNMP Management** (See [3. SNMP NETWORK MANAGEMENT](#) for detailed descriptions.)

1.3 Interface Description

It is very important that the proper cables with the correct pin arrangement are used when connecting the Wireless Gateway to other devices such as switch, hub, workstation, etc.

- **WAN 100Base-FX Fiber Port**

One 100Base-FX Fiber port is located at the back of the Wireless Gateway. This port is primarily used for up-link connection and will always operate at 100M/Full Duplex mode. Duplex SC, WDM Simplex SC, and SFP types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with other Ethernet Fiber port.

- **LAN 10/100Base-TX RJ-45 Port**

Four 10/100Base-TX RJ-45 ports are located at the front of the Wireless Gateway. These RJ-45 ports allow users to connect their traditional copper based Ethernet/Fast Ethernet devices to 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 Wireless Gateway, any of these 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 Wireless Gateway and a RJ-45 LAN cable for PC connections are required to connect the Wireless Gateway and a PC. Through these, the user then can configure and check the Wireless Gateway even when the network is down.

1.4 Connecting the Wireless Gateway

Before starting to configure the Wireless Gateway, you have to connect your devices correctly.

- Connect the power adaptor to the power port of the Wireless Gateway at the back panel, and the other side into a wall outlet. The Power LED indicator should be ON.
- The system starts to initiate. After completing the system test, the Status LED will light up.
- Connect one end of an Ethernet patch cable (RJ-45) to one of the LAN ports of Wireless Gateway and the other end of the patch cable (RJ-45) to the Ethernet port on the administrator computer for the first-time configuration. The LED indicator of the connected LAN port on the front panel will light up.
- Connect the Fiber cable provided from the service provider to the WAN Fiber port, the WAN LED indicator will light up and blink when data are transmitted.

1.5 RF over Fiber (With RF Receiver only)

Fiber Optic RF Receiver with SC/APC connector is located within the upper-left corner of the top-front of the Wireless Gateway. This port is primarily used for CATV RF link connection and will operate at output level greater than 24dBmV@-5dBm of optical input with 77 NTSC or 60 PAL channels of loading. Use proper RF optical fiber to connect this port with other fiber port at the CATV head end. Also use TV Coaxial Cable to connect the TV with the TV coaxial cable female connector located in the front of the Wireless Gateway. There are three LEDs beside the TV coaxial cable connector to indicate the status of TV/RF Output, RF Fiber Link status, and Power status respectively. See next section for CATV LED descriptions.

1.6 LED Description

Model	LED	Color	Operation
Wireless Gateway	Power	Off	Power is off.
		Green	Power is functioning in normal operation.
	WAN	Orange	Fiber port link is off or down.
		Green	Fiber port link is up.
	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.
	Link/ACT	Off	Copper port link is off.
		Green	Copper port link is up.
		Green blinking	Blinking when traffic is present.
	Speed	Off	Copper port link is off or link is in 10Mbps.
		Green	Copper port link is in 100Mbps.
With RF Module Installed	Power	Off	System 12V DC power is off or down.
		Green	System 12V DC power is ready.
	Fiber port	Off	Lights off if the Fiber link is down because optical input power is < -8 dBm.
		Green	Lights on if the Fiber link is up with optical input power > -8 dBm.
	TV (RF) port	Off	Lights off when RF output is being shut off (or failed).
Orange		Lights on when RF output is normal.	

2. WEB MANAGEMENT

The Wireless Gateway provides two management options, these are: “**Web Management**” and “**SNMP Management**”. This chapter describes how to manage and monitor the Wireless Gateway through a web browser.

2.1 Web Management Overview

Once the Wireless Gateway is on the network, you can login and monitor the status remotely or locally by a web browser. Local console-type Web management is especially for the first time user of Wireless Gateway to set up the needed IP and can also be done through one of the four 10/100Base-TX RJ-45 ports located on the front panel of the Wireless Gateway.

2.1.1 The Concept of IP Address

IP addresses have the format n.n.n.n, (The factory default setting is 192.168.0.1).

IP addresses are made up of two parts:

- The first part (for example 168.168.n.n) refers to network address that identifies the network in 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 (for example n.n.8.100) 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 with the allocation organization where your IP addresses were obtained.

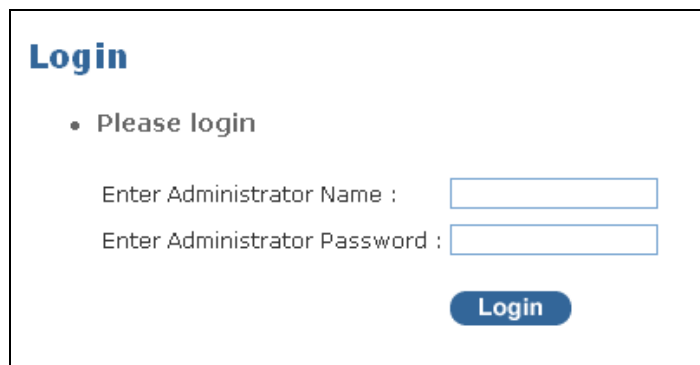
Remember that none of the two devices on a network can have the same address. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not be performed.

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.

2.1.2 Start Configuring

You can manage the Wireless Gateway via a web browser. However, you must first assign a unique IP address to the Wireless Gateway before doing so. When you use the Wireless Gateway for the first time or reload its factory default setting, follow the steps below to login to the Wireless Gateway and set up the IP address. (The Wireless Gateway's default IP is "192.168.0.1". You can change the IP to the needed one in the "WAN Settings" under the **Network Configuration** menu.)

1. Connect one end of RJ-45 LAN cable to one of the RJ-45 ports at the front panel of Wireless Gateway and the other end to the administrator computer as the temporary RJ-45 Management port.
2. Run a web browser and specify the Wireless Gateway's IP address to reach it. (The default IP of Wireless Gateway is "192.168.0.1" before any changes.)
3. Once you gain access, a Login window appears like the following:



Login

- Please login

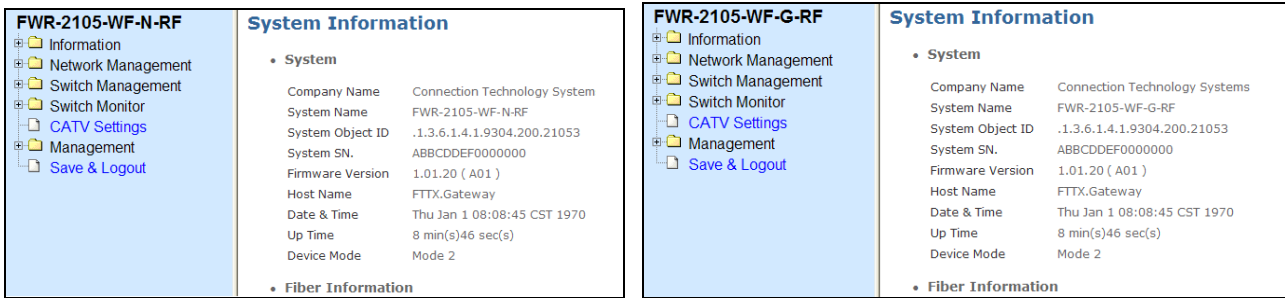
Enter Administrator Name :

Enter Administrator Password :

Login

4. Enter the administrator name and password then click "Login" to reach the main screen page. By default, the administrator name is **admin** without a password (leave the password field blank).
5. After a successful login, the following Wireless Gateway Main Menu screen appears.

NOTE: By default, the remote access to the WLAN Residential Gateway is disabled. If you would like to login the WLAN Residential Gateway from WAN port, you must enable "Remote Administration" option in **Administrator Account** under the **Management Menu** and then add IP address (optional) and specify Http port number (required) for remote login. Once completed, you can type in the specified IP address and Http port number in URL field of your web browser like this "192.168.1.198:8888" to access to web management.

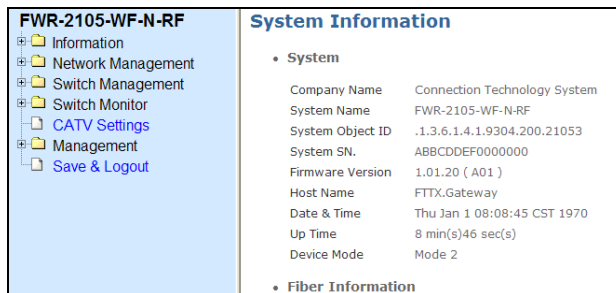


System Information page for 802.11n models System information page for 802.b/g models

Both 802.11n & 802.11b/g models have same software functions except that 802.11n models provide users to use 802.11n wireless mode that can achieve higher speed rate. In this user's manual, we will use screenshots from 802.11n model consistently to explain software functions. Differences in software functions between 802.11b/g and 802.11n models will also be pointed out in this user's manual.

2.1.3 Introduction to Sub-Menus

When you successfully login to the web management, you will be directed to the Main Menu. On the right pane of the Main Menu, it shows system information including detailed information about your device, fiber information, etc. On the left pane, there are several sub-menus that enable you to configure the basic and advanced software functions. Below is the brief description for each sub-menu. For detailed function explanations, please refer to the individual section.



Information: To display the current system set-up information, including the system information (e.g. location, firmware version, WAN, LAN status, etc.) and syslog table.

Network Management: To configure the Wireless Gateway settings, including WAN and LAN Settings, DHCP, NAT, DDNS, etc.

Switch Management: To configure Wireless Gateway Ethernet settings, including Port Configuration, Bandwidth Control, VLAN and IGMP settings.

Switch Monitor: To show each port's status.

CATV Settings: Enable or disable CATV function.

Management: This Menu including Administrator Account, Date/Time setting, Ping test, Save/Restore and Firmware Update.

Save & Logout: To save all configuration changes to the system, logout from the web management and reboot the device.

2.2 Information

Select **Information** from the **Main Menu**, then the sub-items **System information** and **Syslog Table** will show up.

2.2.1 System Information

Select **System Information** from the **Information** menu, then **System Information** screen page appears.

System

• System	
Company Name	Connection Technology System
System Name	FWR-2105-WF-N-RF
System Object ID	.1.3.6.1.4.1.9304.200.21053
System S/N.	ABBCCDEF0000000
Firmware Version	1.01.00 (A01)
Host Name	FTTX.Gateway
Date & Time	Thu Jan 1 08:08:45 CST 1970
Up Time	8 min(s)46 sec(s)
Device Mode	Mode 2

Company Name: View-only field that shows the manufacturer of this device.

System Name: View-only field that shows this Wireless Gateway's system name.

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

System S/N.: View-only field that shows this Wireless Gateway's serial number.

Firmware Version: View-only field that shows the Firmware version of this Wireless Gateway.

Host name: View-only field that shows the host name of this Wireless Gateway.

Date & Time: View-only field that shows the system's current date and time.

Up Time: View-only field that shows how long the system has been up.

Device mode: View-only field that shows the Wireless Gateway's operational mode.

Fiber Information

• Fiber Information		
Connector	ST	
Speed	100	
Wave Length	Tx : 1310	Rx : 1310
Distance	2 KM	

Connector: View-only field that shows the connector type of this fiber port.

Speed: View-only field that shows the speed of this fiber port.

Wave Length: View-only field that shows the transmitting and receiving wave length of this fiber port.

Distance: View-only field that shows the maximum distance of this fiber port.

WAN

• WAN	
WAN Type	DHCP
MAC Address	00:06:19:12:34:56
IP Address	N/A
Subnet Mask	N/A
Default Gateway	N/A
MTU	1500
Packet Info.	RX packets:0 TX packets:8
DNS 1	0.0.0.0
DNS 2	0.0.0.0

WAN Type: View-only field that shows the WAN port type (Static IP, DHCP assigned, or PPPoE) of this Wireless Gateway.

MAC Address: View-only field that shows the unique and permanent MAC address in WAN assigned to the Wireless Gateway. The default MAC address of your Wireless Gateway can not be changed.

IP Address: View-only field that shows the unique WAN IP address of this Wireless Gateway. You can use the default IP address or specify a new one in **Network Management** when the address conflict occurs or the address does not match up with your network.

Subnet Mask: View-only field that specifies the subnet mask to be used with the Wireless Gateway IP address. The default subnet mask values for the three Internet address classes are as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Default Gateway: View-only field that specifies the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the Wireless Gateway. This address is required if the Wireless Gateway and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and Wireless Gateway are on the same network.

MTU: View-only field that shows the Ethernet packet MTU (Maximum Transmission Unit) of the Wireless Gateway.

Packet Info.: View-only field that shows the number of packets received and transmitted.

DNS 1: View-only field that shows the IP address of the first DNS server which has been assigned dynamically by your ISP or specified by you.

DNS 2: View-only field that shows, if any, the IP address of the second DNS server which has been assigned dynamically by your ISP or specified by you.

LAN

• LAN	
MAC Address	00:06:19:12:34:57
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Packet Info.	RX packets:83 TX packets:99
DHCP Server	Enabled

MAC Address: View-only field that shows the unique and permanent MAC address in LAN assigned to the Wireless Gateway. The default MAC address of your Wireless Gateway can not be changed.

IP Address: View-only field that shows the unique LAN IP address of this Wireless Gateway. You can use the default IP address or specify a new one in **Network Management** when the address conflict occurs or the address does not match up with your network.

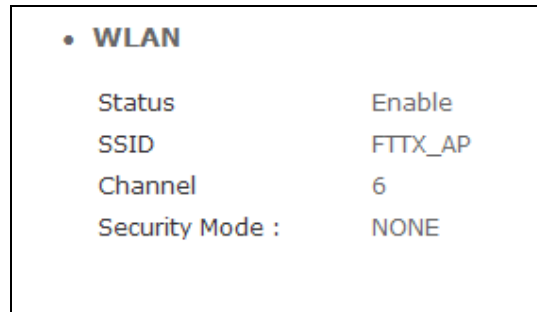
Subnet Mask: View-only field that shows the subnet mask to be used with the Wireless Gateway IP address. The default subnet mask values for the three Internet address classes are as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Packet Info.: View-only field that shows the number of packets received and transmitted.

DHCP Server: View-only field that shows whether the LAN port's DHCP server is enabled or disabled.

WLAN



• WLAN	
Status	Enable
SSID	FTTX_AP
Channel	6
Security Mode :	NONE

Status: View-only field that shows whether wireless function is enabled or not.

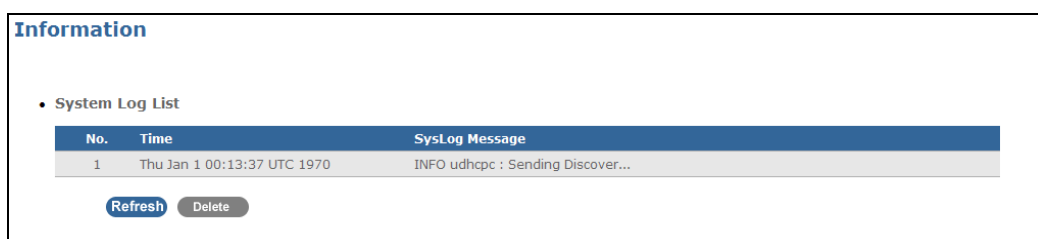
SSID: View-only field that shows the SSID broadcasted by VoIP & Wireless Residential Gateway.

Channel: View-only field that shows the channel used for wireless communication.

Security Mode: View-only field that shows the operating security mode.

2.2.2 Syslog Table

Select **Syslog Table** from the **Information** menu, then **Syslog Table** screen page appears.



Information		
• System Log List		
No.	Time	SysLog Message
1	Thu Jan 1 00:13:37 UTC 1970	INFO udhcp: Sending Discover...
<input type="button" value="Refresh"/> <input type="button" value="Delete"/>		

Time: View-only field that shows the time when syslog messages are recorded.

Syslog Message: The Syslog Table lists the latest 500 system log messages. The user can select what information will be shown in this Syslog Table in **System Log** under the **Management** menu.

Click the **“Refresh”** button to update the Syslog Table.

Click the **“Delete”** button to clear all log messages from the Syslog Table.

2.3 Network Management

Select **Network Management** from the **Main Menu**, then sub-items - **WAN Settings**, **LAN Settings**, **Static Route**, etc – will show up.

2.3.1 WAN Setting

Select **WAN Setting** from the **Network Management** menu, then **WAN Settings** screen page appears.

Network Management

- **WAN Setting**
 - NAT / Bridge Mode: Mode 4:1 WAN & 4 LAN
 - After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode).
 - WAN Port IP Assignment: Static IP DHCP PPPoE
 - Host Name: FTTX . Gateway
 - DHCP MTU: 1500 bytes
 - DHCP MRU: 1500 bytes
 - Set DNS server: Manually Automatically
 - Ping from WAN: Allowed

Submit **Reset**

NAT / Bridge Mode: There are five modes (Mode 0 ~ Mode 4) available from the drop-down menu. According to the application attached to this Wireless Gateway, you can select the appropriate mode by referring to the table below:

Mode	Bridge	NAT
0	Pure 4-port switch mode without VLAN and NAT functions	
1	WAN + LAN 1	LAN 2~4
2	WAN + LAN 1 + LAN 2	LAN 3~4
3	WAN + LAN 1 + LAN 2 + LAN 3	LAN 4
4	WAN	LAN 1~4

The default setting is Mode 4.

NOTE: After you switch between Bridge and NAT mode, the ARP table must be cleared by using the “arp -d” command (under PC MS-DOS Mode).

WAN Port IP assignment: Choose one of the three options – **Static IP**, **DHCP** or **PPPoE**.

1. **Static IP:** If you choose Static IP, you will need to specify the IP address, subnet mask, default gateway address, and DNS server for WAN setting. The **Static IP** screen page appears as follows:

Network Management

- WAN Setting

NAT / Bridge Mode Mode 2:3 WAN & 2 LAN ▾

After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode).

WAN Port IP Assignment Static IP DHCP PPPoE

Host Name FTTX . Gateway

IP Address 192.168.1.198

Subnet Mask 255.255.255.0 ▾

Default Gateway 192.168.1.254

Static IP MTU 1500 bytes

Primary DNS Server 192.168.0.1

Secondary DNS Server 0.0.0.0

Ping from WAN Allowed

Submit
Reset

Host Name: The Host Name is optional but may be required or defined by the user. The default host name is the name of this Wireless Gateway.

IP Address: If you choose to specify IP address, enter a unique IP address for this Wireless Gateway.

Subnet Mask: Specify the subnet mask of this Wireless Gateway IP address. The default subnet mask values for the three Internet address classes are as follows:

- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

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

Static IP MTU: Static IP MTU (Maximum Transmission Unit) can be changed based on your bandwidth to achieve optimal performance. When data larger than the size specified here are being sent, they will be divided into smaller packets. 1500 is the default MTU.

DNS (Domain Name System): DNS is used to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important. Without it, you must know the IP address of a computer before you can access it. The Wireless Gateway uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.

Primary DNS Server: Specify the primary DNS server address.

Secondary DNS Server: Specify the secondary DNS server address.

Ping from WAN: Tick this checkbox to allow the WAN port to be "pinged". Uncheck the box (disable the Ping function) may provide extra security to avoid hackers' attacks.

- DHCP:** Choose DHCP to obtain the IP address automatically from DHCP server. The **DHCP** screen page appears as follows:

The screenshot shows the 'Network Management' interface with the 'WAN Setting' section expanded. The 'NAT / Bridge Mode' is set to 'Mode 2:3 WAN & 2 LAN'. Below this, a note states: 'After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode)'. The 'WAN Port IP Assignment' is set to 'DHCP' (selected with a radio button). The 'Host Name' is 'FTTX' and the 'Gateway' is empty. The 'DHCP MTU' is set to '1500' bytes. The 'Set DNS server' is set to 'Automatically' (selected with a radio button). The 'Ping from WAN' checkbox is checked and labeled 'Allowed'. At the bottom, there are 'Submit' and 'Reset' buttons.

DHCP MTU: DHCP MTU (Maximum Transmission Unit) can be changed based on your bandwidth to achieve optimal performance. When data larger than the size specified here are being sent, they will be divided into smaller packets. 1500 is the default MTU.

Set DNS server: Choose either **Manually** or **Automatically**. If you choose **Manually**, the IP address of the DNS Server needs to be set up.

Primary DNS Server: Specify the IP address of the primary DNS server.

Secondary DNS Server: Specify the IP address of the secondary DNS server.

Ping from WAN: Tick this checkbox to allow the WAN port to be “pinged”. Uncheck the box (disable the Ping function) may provide extra security to avoid hackers’ attacks.

- PPPoE:** Choose PPPoE to obtain WAN IP address information. The **PPPoE** screen page appears as follows:

The screenshot shows the 'Network Management' interface with the 'WAN Setting' section expanded. The 'NAT / Bridge Mode' is set to 'Mode 2:3 WAN & 2 LAN'. Below this, a note states: 'After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode)'. The 'WAN Port IP Assignment' is set to 'PPPoE' (selected with a radio button). The 'Host Name' is 'FTTX' and the 'Gateway' is empty. The 'PPPoE Username' is 'PPPOE_USERNAME' and the 'PPPoE Password' is masked with dots. The 'PPPoE MTU' is set to '1492' bytes. The 'Set DNS server' is set to 'Automatically' (selected with a radio button). The 'Ping from WAN' checkbox is checked and labeled 'Allowed'. At the bottom, there are 'Submit' and 'Reset' buttons.

PPPoE Username: Enter the PPPoE username provided by your ISP.

PPPoE Password: Enter the PPPoE password provided by your ISP.

Max Idle Time: Enter the maximum idle time. The WAN port connection will be maintained within inactivity period that you specify here.

PPPoE MTU: PPPoE MTU (Maximum Transmission Unit) can be changed based on your bandwidth to achieve optimal performance. When data larger than the size

specified here are being sent, they will be divided into smaller packets.1492 is the default MTU.

Set DNS server: Choose either **Manually** or **Automatically**. If you choose **Manually**, the IP address of the DNS Server needs to be set up.

Primary DNS Server: Specify the IP address of the primary DNS server.

Secondary DNS Server: Specify the IP address of the secondary DNS server.

Ping from WAN: Tick this checkbox to allow the WAN port to be “pinged”. Uncheck the box (disable the Ping function) may provide extra security to avoid hackers’ attacks.

2.3.2 LAN Settings

Select **LAN Settings** from the **Network Management** menu, then **LAN Settings** screen page appears as follows.

Network Management

- LAN Settings
 - LAN IP Address:
 - Subnet Mask:
 - DNS Proxy: Enable
- DHCP Server Settings
 - DHCP Server: Enable
 - Assigned DHCP IP Address
 - Start IP: 192.168.0.
 - End IP: 192.168.0.
 - DHCP IP Lease Time: seconds (60..864000)
 -
- DHCP Static Map

MAC	IP	Description	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
- DHCP Client List

Type	Hostname	MAC	IP	Expire Time
------	----------	-----	----	-------------

LAN Settings

LAN IP Address: Specify a unique IP address for this Wireless Gateway in LAN.

Subnet Mask: Specify the subnet mask to be used with the Wireless Gateway IP address. The available subnet mask values are listed from the drop-down menu. Options include 255.255.255.0, 255.255.255.128, 255.255.255.192, 255.255.255.224, 255.255.255.240, 255.255.255.248, 255.255.255.252.

DNS Proxy: Tick this checkbox if you would like to relay clients’ DNS requests to a real DNS server IP address.

DHCP Server Settings

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure this gateway as a DHCP server or disable it. When the gateway is configured as a server, it provides the TCP/IP configuration for clients. If DHCP service is disabled, you must have another DHCP server on your LAN; otherwise, the computer must be manually configured.

Tick “**DHCP server**” checkbox to enable or disable the DHCP server. If **Enable** is checked and a DHCP server is available on the network, the Wireless Gateway will automatically get the IP address from the DHCP server. Otherwise (Disabled), the user needs to specify the IP address, Subnet Mask and Gateway. When DHCP is used, the following items need to be set as well.

Start IP Address: The starting IP address which can be assigned to this Wireless Gateway when a DHCP server is enabled and available on the network.

End IP Address: The ending IP address which can be assigned to this Wireless Gateway when a DHCP server is enabled and available on the network.

DHCP Leased Time: Enter the length of lease time in seconds for the automatically-assigned IP address. When the leased time is expired, the user has to get the automatically-assigned IP address from the DHCP server again.

Click the “**Submit**” button to make your settings effective.

Click the “**Reset**” button to clear settings that you have entered.

NOTE: *This Residential Gateway supports DHCP auto-provisioning function that enables DHCP clients to automatically download the latest Firmware and Configuration image. For information about how to set up a DHCP server, please refer to [APPENDIX A](#).*

DHCP Static Map

MAC: Enter the MAC address of the devices. Maximum ten MAC addresses can be set up with specific IP addresses.

IP: Enter the IP address that you would like to assign to the corresponding MAC address.

Description: Enter the brief description for this entry.

Action: Insert - To add a new entry to DHCP Client List below. Change - To modify current DHCP static map setting.

DHCP Client List

Type: When your device obtains the IP address from the DHCP server, this view-only field displays “Dynamic”.

Hostname: View-only field that shows the DHCP client’s computer name.

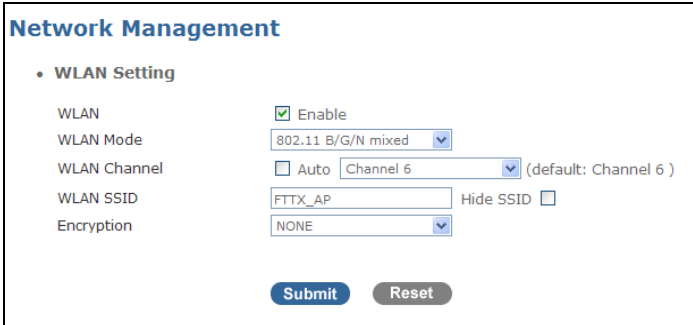
MAC: View-only field that shows the DHCP client’s MAC.

IP: View-only field that shows the DHCP client’s IP address.

Expire Time: View-only field that shows the DHCP client’s expire time.

2.3.3 WLAN Settings

Select **WLAN Settings** from the **Network Management** menu, then **WLAN Settings** screen page appears as follows.



The screenshot shows the 'Network Management' interface with the 'WLAN Setting' section expanded. The settings are as follows:

- WLAN: Enable
- WLAN Mode: 802.11 B/G/N mixed
- WLAN Channel: Auto Channel 6 (default: Channel 6)
- WLAN SSID: FTTX_AP Hide SSID
- Encryption: NONE

Buttons: Submit, Reset

WLAN: Enable or disable wireless LAN function. By default, wireless function is enabled.

WLAN Mode: There are six WLAN modes available from the pull-down menu.

802.11 B/G mixed: The Residential Gateway supports both 802.11b and 802.11g standard.

802.11 B only: The Residential Gateway only supports 802.11b standard.

802.11 G only: The Residential Gateway only supports 802.11g standard.

802.11 N only: (This mode is only available in 802.11n models) The Residential Gateway only supports 802.11n standard.

802.11G/N mixed: (This mode is only available in 802.11n models) The Residential Gateway supports both 802.11g and 802.11n standard.

802.11 B/G/N mixed: (This mode is only available in 802.11n models) The Residential Gateway supports 802.11b, 802.11g and 802.11n standard.

WLAN Channel: Select the channel for wireless communication from the pull-down menu or

tick the “**auto**” checkbox to allow the router to automatically search the available channel. The default WLAN channel is Channel 6 (2.437 GHZ).

WLAN SSID: Specify the unique name for your WLAN, up to 32 characters long. This will allow client devices with the same SSID as you defined here to connect to the Access Point. Tick the “**Hide SSID**” checkbox when you do not want the specified SSID to be broadcasted.

Encryption: There are four encryption options available in the drop-down menu. Select “**NONE**” if you prefer no encryption with your data; otherwise, choose “**WEP**”, “**WPA**” or “**WPA2**” as your encryption method.

The screenshot shows the 'WLAN Setting' configuration page. It includes the following fields and options:

- WLAN:** Enable
- WLAN Mode:** 802.11 B/G/N mixed
- WLAN Channel:** Auto | Channel 6 (default: Channel 6)
- WLAN SSID:** FTTX_AP | Hide SSID
- Encryption:** WEP
- Authentication:** Open System
- WEP Key Length:** 64-bit WEP

Below these fields, there are instructions for WEP keys:

- 64-bit WEP: Enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each Key (1-4).
- 128-bit WEP: Enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each Key (1-4).

There are four key input sections, each with a radio button for 'Key 1' through 'Key 4' and options for 'HEX' or 'ASCII' characters.

At the bottom, there are 'Submit' and 'Reset' buttons.

1. WEP Encryption: WEP (Wired Equivalent Privacy) is based on IEEE 802.11 standard and uses the RC 4 encryption algorithm to encrypt data over the wireless network so as to protect your data from unauthorized accesses or intruders. When connecting to a WEP network, the user has to know a key that can be either 64-bit or 128 bit with ASCII characters or hexadecimal characters.

Authentication: There are two options available for authentication; these are, “Open System” and “Share Key”. For more secure protection, you should choose “Share Key” option which requires wireless clients have the same key positions with the VoIP & Wireless Residential Gateway.

WEP Encryption Length: Select either 64-bit WEP or 128-bit WEP. 128-bit WEP requires a longer key than 64-bit WEP. Your wireless clients must have the same WEP encryption length as this Residential Gateway; otherwise, the connection will not be established.

Key 1 ~ 4: Enter values for Key 1 to Key 4 with either HEX or ASCII characters.

If you choose 64-bit WEP as your WEP encryption length, enter 5 ASCII characters or 10 hexadecimal characters (“0-9”, “A-F”) for each Key (1~4). If you choose 128-bit WEP, enter 13 ASCII characters or 26 hexadecimal characters (“0-9”, “A-F”) fro each Key (1~4).

Network Management

- **WLAN Setting**
 - WLAN Enable
 - WLAN Mode 802.11 B/G/N mixed
 - WLAN Channel Auto Channel 6 (default: Channel 6)
 - WLAN SSID FTTX_AP Hide SSID
 - Encryption WPA(Pre-Shared-Key)
 - WPA Cipher suite TKIP
 - WPA Pre-Shared Key (8~63 ASCII or 64 HEX characters)

Submit Reset

2. **WPA:** WPA stands for Wi-Fi Protected Access and intends to improve the security functions of WEP by using two security-enhanced types to encrypt data, these are: TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard).

WPA Cipher Suite: Select either “TKIP” or “AES” (AES is a stronger encryption method than TKIP).

WPA Pre-Shared Key: Enter the pre-shared key value which can be between 8 and 63 characters long or 64 HEX characters long. Symbols and spaces can also be used.

Network Management

- **WLAN Setting**
 - WLAN Enable
 - WLAN Mode 802.11 B/G/N mixed
 - WLAN Channel Auto Channel 6 (default: Channel 6)
 - WLAN SSID FTTX_AP Hide SSID
 - Encryption WPA2(Pre-Shared-Key)
 - WPA Cipher suite TKIP
 - WPA Pre-Shared Key (8~63 ASCII or 64 HEX characters)

Submit Reset

3. **WPA2:** WPA2, based on 802.11i, provides stronger wireless security than WPA to protect your network from malicious intruders.

WPA Cipher Suite: Choose either TKIP or AES.

WPA Pre-Shared Key: Enter the pre-shared key value which can be between 8 and 63 characters long or 64 HEX characters long. Symbols and spaces can also be used.

2.3.4 WLAN Access Policy Setting

Select **WLAN Access Policy Setting** from the **Network Management** menu, then **WLAN Access Policy Setting** screen page appears.

Network Management

- Access Policy Setting

Access Policy:

Access Control List:

--

Access Policy: To disable Access Policy function or to select “**Allow all**” or “**Reject all**” accesses from the control list.

Access Control List: Enter MAC addresses (with the AA:AA:AA:AA:AA:AA format) that you would like to add to the access control list. A total of 50 MAC addresses can be added to the access control list.

Insert to list: Once you have entered a MAC address, press “**Insert to list**” to add it to the list.

Delete from list: Select a MAC address from the access control list and press “**Delete from list**” to remove it from the list.

2.3.5 Static Route

The Wireless Gateway uses IP or Host name to communicate with management computers, for example using HTTP, telnet, SSH, or SNMP. Using IP static routes allows the Wireless Gateway to respond to remote management stations that are not reachable through the default gateway. The Wireless Gateway can also use static routes to send data to a server or device that is not reachable through the default gateway, for instance when sending SNMP traps or using ping to test IP connectivity.

Select **Static Route** from the **Network Management** menu, then **Static Route** screen page appears.

Network Management

- Static Route

Enable	Type	Target	Netmask	Gateway	Action
<input type="checkbox"/>	Net	<input type="text"/>	255.255.255.0	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Enable: Tick the checkbox to turn on static route function.

Type: Specify the Type to be used with the Wireless Gateway IP address. The types available are listed in the drop-down menu with the following options – NET (IP address), Host (Host name).

Target: Specify the IP network address or Host name of the final destination. Routing is always based on network number.

Netmask: Enter the subnet mask for this destination.

Gateway: Enter the gateway address for this destination.

Action: Insert - To add a new static route to the Wireless Gateway. Change - To modify the current setting.

2.3.6 NAT

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example, a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

Select **NAT** from the **Network Management** menu and tick the “**Network Address Translation**” checkbox, then the **NAT** screen page appears as follows.

The screenshot displays the 'Network Management' interface with the following sections:

- NAT Setting:** A list of settings with checkboxes and input fields:
 - Network Address Translation: Enable
 - DMZ: Enable
 - DMZ LAN IP:
 - DDOS Protection: Enable
 - Detection Frequency:Buttons for 'Submit' and 'Reset' are located below these settings.
- Virtual Server Mapping:** A table with columns: Enable, WAN Port, Protocol, LAN IP, LAN Port, and Action.

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	Insert Change
- Port Trigger:** A table with columns: Enable, Trigger Port, Trigger Type, Public Port, Public Type, and Action.

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	TCP	Insert Change

NAT Setting

Network Address Translation: If you would like to activate NAT function, tick the enable checkbox.

A **DMZ (Demilitarized Zone)** host is a computer without the protection of the firewall. If you have a client PC that cannot run Internet applications properly from the Wireless Gateway, you can set the client up for unrestricted Internet access. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks. Therefore,

enable this function when necessary.

DMZ: Enable DMZ if checked.

DMZ LAN IP: Enter the IP address that you would like to open all ports to.

DDoS Protection: Tick the checkbox to enable Wireless Gateway to detect SYN flooding attacks. By default, this function is disabled which makes your device vulnerable to attacks. To prevent your Wireless Gateway from open malicious attacks, you should enable DDoS Protection manually.

Detection Frequency: Specify the frequency of attack requests to Wireless Gateway. When Wireless Gateway detects malicious SYN attacks, it will clear streams occupied by the source host.

Virtual Server Mapping

Virtual Server is used to set up public services on your network. When users from the Internet make certain requests on your network, the Wireless Gateway can forward those requests to computers to handle the requests. For example, when you set the port number 80 (HTTP) to be forwarded to IP Address 192.168.1.2, all HTTP requests from outside users will be forwarded to 192.168.1.2. You may use this function to establish a Web server or FTP server via an IP Gateway. Be sure that you enter a valid IP Address. (You may need to establish a static IP address in order to properly run an Internet server.)

For added security, Internet users can communicate with the server, but they will not actually be connected. The packets will simply be forwarded through the Wireless Gateway.

Enable: Tick the checkbox to enable this rule.

WAN Port: Specify the WAN port number (1~65535).

Protocol: Choose TCP, UDP or Both as your desired protocol.

LAN IP: Specify the LAN IP - 192.168.0.xxx, where xxx is editable.

LAN Port: Specify the port LAN port number (1~65535).

Action: Insert- To insert a new Virtual Server setting to the Wireless Gateway. Change-To modify the current setting.

Port Trigger

Enable: Tick the checkbox to enable this rule.

Trigger Port: Enter the port number used by the application to establish an open service port.

Trigger Type: Choose either TCP or UDP.

Public Port: Enter the port number to be allowed to pass through when trigger packets are detected.

Public Type: Choose either TCP or UDP.

Action: Insert - To add a new port trigger to the Wireless Gateway. Change - To modify the current setting.

2.3.7 Packet Filter

This Wireless Gateway supports WAN, LAN port and MAC address filtering that allow users to create and enforce WAN and LAN port access policies tailored to your needs.

Select **Packet Filter** from the **Network Management** menu and tick **Enable** box of WAN, LAN, and MAC, then **Packet Filter** screen page appears as follows.

Network Management

- Packet Filter
 - WAN Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	TCP	Always	All	00:00 ~ 00:00	Insert Change
 - LAN Enable

Enable	Source IP	Dest. Port	Protocol	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	TCP	Always	All	00:00 ~ 00:00	Insert Change
 - MAC Enable

Enable	MAC Address	Block	Day	Time	Action
<input type="checkbox"/>	<input type="text"/>	Always	All	00:00 ~ 00:00	Insert Change

WAN: Enable WAN port packet filter, if checked.

Enable: Enable this filtering rule, if checked. The total number of rules can be created in WAN Packet Filter is 20.

Public IP: Enter the public source IP address.

Dest. Port: Enter the UDP or TCP destination port number (1~65535).

Protocol: Select the filtering protocol (UDP or TCP) from pull-down menu.

Block: Select the block function from pull-down menu.

- Always (always block which means that access to the requested service will be denied)
- By schedule (follow "Day" and "time" field setting)

Action: Insert- To add a new filtering rule. Change-To modify the current filtering rule's setting.

LAN: Enable LAN port packet filter, if checked.

Enable: Enable this filtering rule, if checked. The total number of rules can be created in LAN Packet Filter is 20.

Source IP: Enter the device's source IP address resided in LAN.

Dest. Port: Enter the UDP or TCP destination port number (1~65535).

Protocol: Select the filtering protocol (UDP or TCP) from pull down menu.

Block: Select the block function from pull-down menu.

- Always (always block which means that access to the requested service will be denied)
- By schedule (follow "Day" and "time" field setting)

Action: Insert- To add a new filtering rule. Change-To modify the current filtering rule's setting.

MAC: Enable MAC address filter, if checked.

Enable: Enable this filtering rule, if checked. The total number of rules can be created in MAC Packet Filter is 20.

MAC address: Specific the device's MAC address (source MAC address) resided in LAN.

Block: Select the block function from pull-down menu.

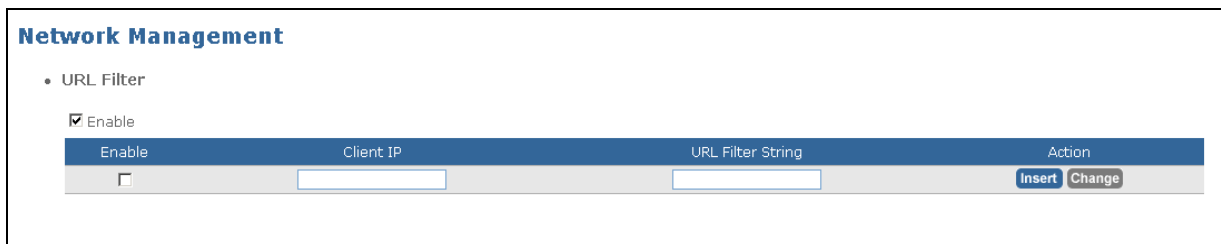
- Always (always block which means that access to the requested service will be denied)
- By schedule (follow "Day" and "time" field setting)

Action: Insert- To add a new filtering rule. Change-To modify the current filtering rule's setting.

2.3.8 URL Filter

This feature allows users to create a list of websites or client IP addresses that you would like to deny users' access. For example, in some companies, they may restrict their employees to access undesirable websites or contents on the Internet.

Select **URL Filter** from the **Network Management** menu and tick the **Enable** box, then **URL Filter** screen page appears as follows.



The screenshot shows the 'Network Management' interface with the 'URL Filter' section expanded. It includes an 'Enable' checkbox (checked), a table with columns for 'Enable', 'Client IP', 'URL Filter String', and 'Action', and 'Insert' and 'Change' buttons.

Enable	Client IP	URL Filter String	Action
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>

Enable: Enable Global URL filter function, if checked.

Enable: Enable this URL filtering rule, if checked. The total number of rules can be created in URL Filter is 20.

Client IP: Enter the client IP address. Traffic from this client IP address, requesting the specified service, will be denied.

URL Filter string: Enter a specific keyword or domain name that you want to block. For example, if you would like to restrict a client to access www.yahoo.com, you can type in the keyword "yahoo" or the website www.yahoo.com.

Action: Insert- To add a new filtering rule. Change-To modify the current filtering rule's setting.

2.3.9 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. Apart from that, a device can leave a network smoothly and automatically.

Select **UPnP** from the **Network Management** menu and tick the **Enable** box, then **UPnP** screen page appears as follows.

The screenshot shows a 'Network Management' interface. Under 'UPnP Setting', there is a section for 'UPnP Internet Gate Device' with an 'Enable' checkbox checked. Below this are 'Submit' and 'Reset' buttons. Below that is a 'UPnP Map' section with a table header and a 'Refresh' button.

Remote Host	External Port	Internal Client	Internal Port	Protocol	Duration	Description
Refresh						

UPnP Setting

UPnP Internet Gate Device: Tick Enable checkbox then click Submit button to enable UPnP feature. UPnP provides compatibility with networking devices, software and peripherals.

UPnP Map

Remote Host: View-only field that shows the remote IP address whose packets will be transferred to the internal client.

External Port: View-only field that shows which port on Wireless Gateway will be allowed to transfer packets to the internal client.

Internal Client: View-only field that shows the internal client IP address that will receive packets.

Internal Port: View-only field that shows the port number of the internal client.

Protocol: View-only field that shows the protocol used for this rule.

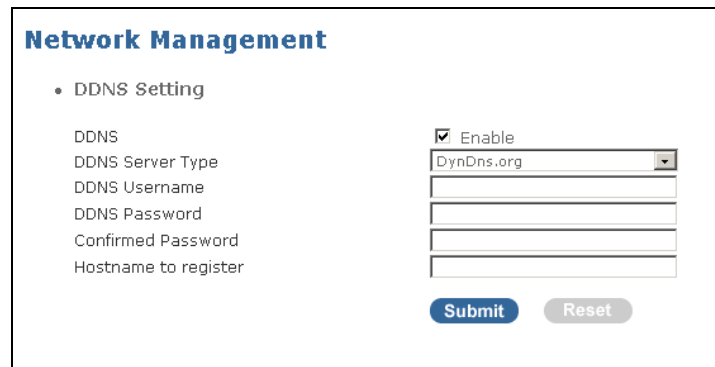
Duration: View-only field. This rule will be disabled when the duration is timeout.

Description: View-only field that shows the description for this rule.

2.3.10 DDNS

The Wireless Gateway supports DDNS (Dynamic Domain Name Service) that enables a dynamic public IP address to be associated with a static host name in any domains and allows access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form "hostname.dyndns.org". Many ISPs assign public IP addresses using DHCP; therefore, it is difficult to locate a specific host on the LAN using standard DNS. For example, when you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS providers.

Select **DDNS** from the **Network Management** menu and tick the **Enable** box, then **DDNS** screen page appears as follows.



The screenshot shows a web interface titled "Network Management" with a sub-section "DDNS Setting". It contains the following fields and controls:

- DDNS**: A checkbox labeled "Enable" which is checked.
- DDNS Server Type**: A dropdown menu with "DynDns.org" selected.
- DDNS Username**: A text input field.
- DDNS Password**: A text input field.
- Confirmed Password**: A text input field.
- Hostname to register**: A text input field.
- At the bottom, there are two buttons: "Submit" (highlighted in blue) and "Reset" (greyed out).

DDNS: Tick the checkbox to enable DDNS global setting.

DDNS Server type: Select one of the DDNS registration organizations from those listed in the drop-down menu. Available servers include Dyn.Dns.org and no-ip.com.

DDNS Username: Enter the username given by your DDNS server.

DDNS password: Enter the password or key given by your DDNS server.

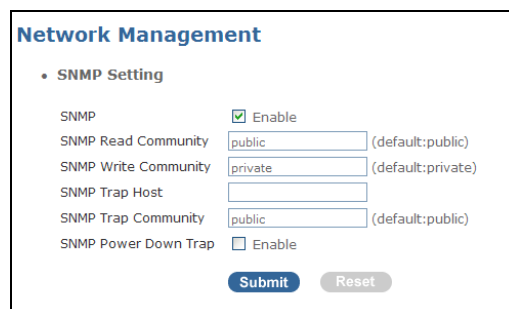
Confirmed password: Re-enter DDNS password to confirm.

Hostname to register: Enter the host name of the DDNS server.

2.3.11 SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Wireless Gateway through the network via SNMP version one (SNMPv1), SNMP version 2c.

Select **SNMP** from the **Network Management** menu, then **SNMP** screen page appears.



The screenshot shows a web interface titled "Network Management" with a sub-section "SNMP Setting". It contains the following fields and controls:

- SNMP**: A checkbox labeled "Enable" which is checked.
- SNMP Read Community**: A text input field with "public" and "(default:public)" to its right.
- SNMP Write Community**: A text input field with "private" and "(default:private)" to its right.
- SNMP Trap Host**: A text input field.
- SNMP Trap Community**: A text input field with "public" and "(default:public)" to its right.
- SNMP Power Down Trap**: A checkbox labeled "Enable" which is unchecked.
- At the bottom, there are two buttons: "Submit" (highlighted in blue) and "Reset" (greyed out).

SNMP: Enable or disable SNMP service.

SNMP Read Community: Specify the Read Community.

SNMP Write Community: Specify the Write Community.

SNMP Trap Host: Specify the SNMP trap host (IP address) to which trap messages will be sent.

SNMP Trap Community: Specify the Trap Community.

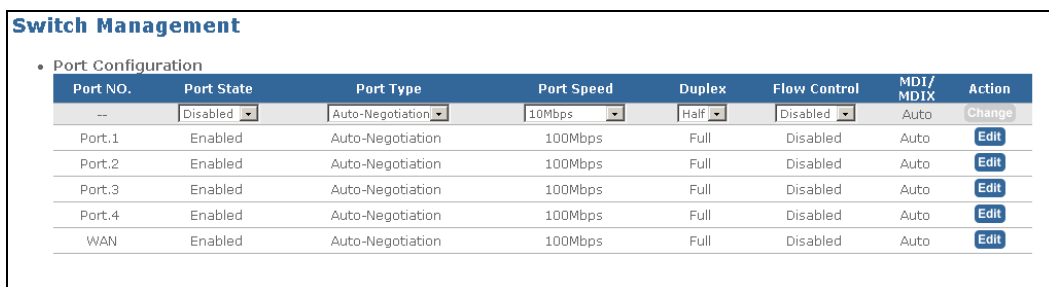
SNMP Power Down Trap: If enabled, a trap or notice will be sent when power supply is down.

2.4 Switch Management

Select **Switch Management** from the **Main Menu**, the sub-items **Port Configuration**, **Bandwidth Control**, **QoS Priority**, and **Configure VLAN** will show up.

2.4.1 Port Configuration

Select **Port Configuration** from the **Switch Management** menu, then **Port Configuration** screen page appears.



The screenshot shows a web interface titled "Switch Management" with a sub-section "Port Configuration". It contains a table with columns: Port NO., Port State, Port Type, Port Speed, Duplex, Flow Control, MDI/MDIX, and Action. The first row is a header with dropdown menus for Port State, Port Type, Port Speed, and Duplex, and a "Change" button. The following rows list ports Port.1 through Port.4 and WAN, each with a status of "Enabled", "Auto-Negotiation" type, "100Mbps" speed, "Full" duplex, "Disabled" flow control, and "Auto" MDI/MDIX. Each row has an "Edit" button.

Port NO.	Port State	Port Type	Port Speed	Duplex	Flow Control	MDI/MDIX	Action
--	Disabled	Auto-Negotiation	10Mbps	Half	Disabled	Auto	Change
Port.1	Enabled	Auto-Negotiation	100Mbps	Full	Disabled	Auto	Edit
Port.2	Enabled	Auto-Negotiation	100Mbps	Full	Disabled	Auto	Edit
Port.3	Enabled	Auto-Negotiation	100Mbps	Full	Disabled	Auto	Edit
Port.4	Enabled	Auto-Negotiation	100Mbps	Full	Disabled	Auto	Edit
WAN	Enabled	Auto-Negotiation	100Mbps	Full	Disabled	Auto	Edit

Port NO.: The number of each port.

Port State: Enable or disable the status of each port.

Port Type: Each port's Auto-Negotiation configuration.

Port Speed: Each port's speed configuration (10/100Mbps).

Duplex: Each port's Duplex mode (Full or Half) configuration.

Flow Control: Each port's flow control configuration.

MDI/MIDX: View-only field (always auto).

Click the “**Edit**” button on the port that you would like to make some changes. When the selected port is highlighted in blue, users can make some changes by selecting from the drop-down menu.

Click the “**Change**” button to apply the changes.

2.4.2 Bandwidth Control

Select **Bandwidth Control** from the **Switch Management** menu, then **Bandwidth Control** screen page appears.

Switch Management

- Bandwidth Range
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress Bandwidth Control
Bandwidth Mode: OFF
- Ingress Bandwidth Control

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	10240 (K)	10240 (K)	10240 (K)	10240 (K)	10240 (K)

Submit Reset

Bandwidth Range: There are 3 different bandwidth ranges in drop-down menu for selection: 1024k~100M (Min. unit size 1024k), 64K~100M (Min. unit size 128k) and 16K~32M (Min. unit size 16k). If you select “1024k~100M (Min. unit size 1024k)”, the minimum bandwidth that can be entered and bandwidth range for Egress and Ingress traffic is 1024. For example, if you enter a value that is lower than 1024k or higher than 1024k but lower than 2048k, then the bandwidth will be adjusted to 1024k automatically. The next bandwidth that can be used is 2048k.

2.4.2.1 Egress Bandwidth Control

There are six modes in the drop-down menu for selection: **OFF/ By Port Only/ By Port with Queue/ By DSCP/ By 802.1p/ By Application**. Except “OFF” mode, the advanced configurations will be displayed when the appropriate mode is selected according to the network application with this gateway installed.

2.4.2.1.1 By Port Only

Selecting “By Port Only” enables users to allocate transmission bandwidth to each LAN and WAN port.

Switch Management

- **Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: By Port Only

Port	Port.1	Port.2	Port.3	Port.4	NAT Download stream	NAT Upload stream	WAN
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)

NAT Download & Upload Stream: These two ports determine bandwidth for downstream traffic and upstream traffic for ports assigned in NAT mode.

Bandwidth: Specify reserved bandwidth for each port.

2.4.2.1.2 By Port with Queue

For each WAN and LAN port, users can designate each port's specific priority queue and allocate transmission bandwidth to each queue.

Switch Management

- **Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: By Port with Queue

Port	Port.1	Port.2	Port.3	Port.4	WAN
Map to Q	Q0	Q1	Q2	Q3	Q3

Reserve Min. Egress Bandwidth of Queue				
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	102400 (K)	102400 (K)	102400 (K)	102400 (K)

By Port Map to Q: Select priority queue mapping for LAN port 1~4 and WAN from the drop-down menu. The queue priority is Q3>Q2>Q1>Q0.

Reserve BW: Specify reserved bandwidth for each queue (Queue-0 ~ Queue-3).

2.4.2.1.3 By DSCP

Differentiated Service Code Point (DSCP) provides a means for users to specify different priority levels to different applications that uses 6-bit of the DS field to select Per Hop Behavior (PHB). As defined by the IETF, PHB values are written using a prefix that identifies the way forwarding should be handled: expedited forwarding (EF) or assured forwarding (AF). Once DSCP marking is assigned, it can map to a queue for setting up preferred egress bandwidth.

Switch Management

- Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control**
Bandwidth Mode: By DSCP
By DSCP
DSCP Map: DSCP(0) --> Q0

Q0-DSCP	0~63
Q1-DSCP	
Q2-DSCP	
Q3-DSCP	

Reserve Min. Egress Bandwidth of Queue				
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	102400 (K)	102400 (K)	102400 (K)	102400 (K)

DSCP Map: Select priority queue mapping for the DSCP field within every IP Packet from the drop-down menu. The DSCP includes DSCP (0) to DSCP (63), and the priority queue includes Q0, Q1, Q2 and Q3. The queue priority is Q3>Q2>Q1>Q0.

Reserve BW: Specify reserved bandwidth for each queue (Queue-0 ~ Queue-3).

2.4.2.1.4 By 802.1p

IEEE 802.1p is a standard that provides traffic class expediting and dynamic multicast filtering. Essentially, it provides a mechanism for implementing Quality of Service (QoS) at the MAC (Media Access Control) level.

Eight priority bits are available, expressed through the 3-bit user_priority field in an IEEE 802.1q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation.

Switch Management

- Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control**
Bandwidth Mode: By 802.1p
By 802.1p

Value	P-Bit 0	P-Bit 1	P-Bit 2	P-Bit 3	P-Bit 4	P-Bit 5	P-Bit 6	P-Bit 7
Map to Q	Q3	Q3	Q3	Q3	Q3	Q3	Q3	Q3

Reserve Min. Egress Bandwidth of Queue				
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	102400 (K)	102400 (K)	102400 (K)	102400 (K)

By 802.1p Map to Q: Select priority bit and queue mapping for P-Bit-0 to P-Bit-7 from the drop-down menu. The queue priority is Q3>Q2>Q1>Q0.

Reserve BW: Specify reserved bandwidth for each queue (Queue-0 ~ Queue3).

2.4.2.1.5 By Application

“By Application” mode allows users to define a range of port number or a port number in terms of destination or source port. If conditions are fulfilled, the queue and bandwidth settings will be applied.

• Egress QoS Control

Bandwidth Mode By Application

By Application

No	Compare	Port Start	Port End	Queue
1	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
2	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
3	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
4	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
5	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
6	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
7	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0
8	Doesn't Compare	<input style="width: 40px;" type="text" value="0"/>	<input style="width: 40px;" type="text" value="0"/>	Q0

Reserve Min. Egress Bandwidth of Queue

Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	<input style="width: 40px;" type="text" value="102400"/> (K)	<input style="width: 40px;" type="text" value="102400"/> (K)	<input style="width: 40px;" type="text" value="102400"/> (K)	<input style="width: 40px;" type="text" value="102400"/> (K)

No.: The total of eight rules can be set up. The comparison process will start from rule No. 1 to No. 8. If the rule No. 1 is fulfilled, then the assigned queue and reserved bandwidth will be applied. If not, each rule will be checked one by one.

Compare: Four options are available for selection.

Doesn't Compare: This rule is disabled.

Source: Use TCP source port to compare.

Destination: Use TCP destination port to compare.

Destination & Source: Use both TCP destination and source port to compare.

Port Start: Specify the starting TCP port number from 0 to 65535.

Port End: Specify the ending TCP port number from 0 to 65535.

NOTE: The range of starting and ending TCP port number should not be over 255. Otherwise, an error message will pop-up when you click “**Submit**” button.

Reserve BW: Specify reserved bandwidth for each queue (Queue-0 ~ Queue3).

2.4.2.2 Ingress Bandwidth Setting

This section describes how to setup the ingress bandwidth for LAN-1 ~ 4 port and WAN port.

• Ingress Bandwidth Control

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Bandwidth	<input type="text" value="10240"/> (K)	<input type="text" value="10240"/> (K)	<input type="text" value="10240"/> (K)	<input type="text" value="10240"/> (K)	<input type="text" value="10240"/> (K)

Enabler: Disable or enable bandwidth control function for Port 1 ~ 4 and WAN port.

Bandwidth: Specify bandwidth for each port (Port 1~4 and WAN port).

2.4.2.3 Traffic Flow for Bridge & NAT Mode

The Wireless Gateway provides four physical 10/100Base-TX ports located on the front panel and one physical WAN port inside the device (interfaces vary depending on the model that you purchased). However, there are two more ports that are not explicitly shown in the interface but might largely affect the traffic flow when you use Bridge/NAT mode; these are Upstream port and Downstream port.

In normal operations, when packets received from the WAN port and destined for ports assigned in Bridge Mode, they will be delivered directly to these ports. On the other hand, for traffic flow destined for ports assigned in NAT mode, they will be delivered to Downstream port (WAN CPU) first and then to Upstream port (LAN CPU) for delivering traffic to NAT ports. For example, if you set NAT/Bridge Mode to “Mode 2: 3 WAN & 2 LAN”, the traffic flow from the WAN port to two Bridge ports are illustrated below in Figure 1 and the traffic flow from the WAN port to two NAT ports are illustrated in Figure 2.

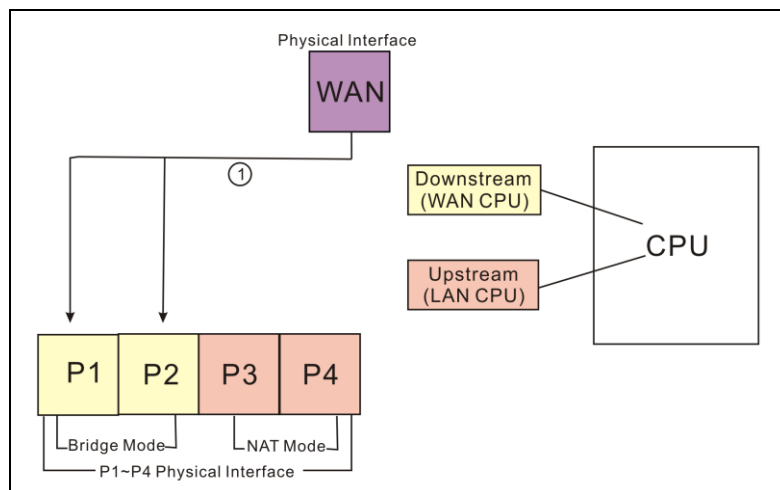


Figure 1: Traffic Flow for Bridge Mode

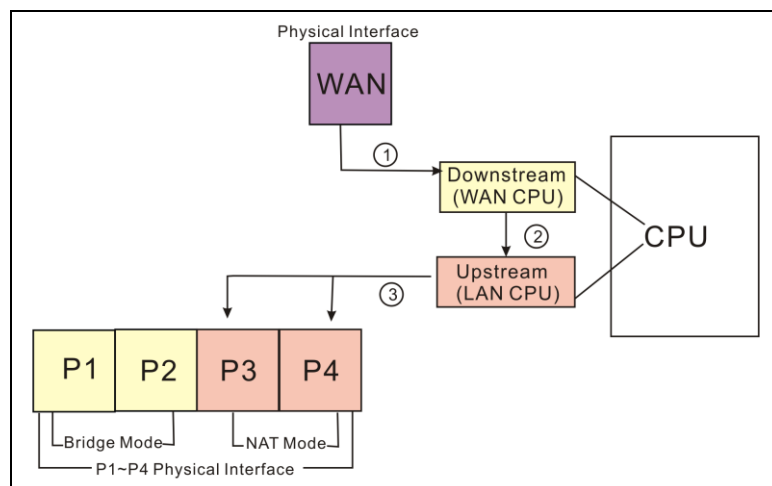


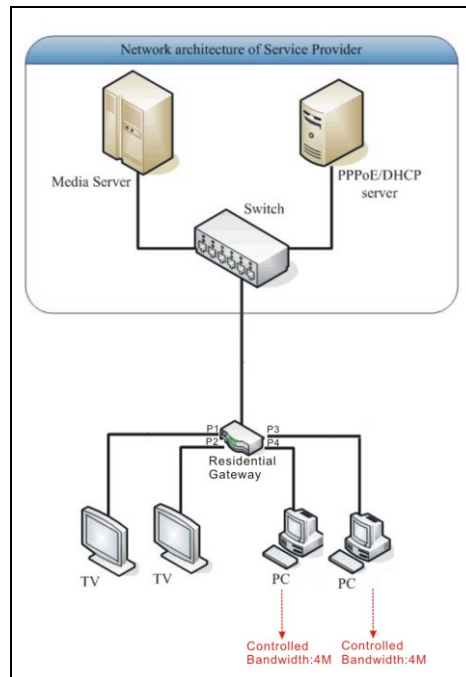
Figure 2: Traffic Flow for NAT Mode

When setting up the desired bandwidth for each port or queue in your networking environment, it is strongly recommended to consider the traffic flow for ports assigned in Bridge and NAT Mode.

2.5.2.4 Bandwidth Control Setup Examples

Scenario I:

In this scenario, the Residential Gateway supports both IPTV applications and internet access. As illustrated below, IPTV applications are connected to Port 1 (P1) and Port 2 (P2); whereas, PC devices are connected to Port 3 (P3) and Port 4 (P4) to access the internet. If you would like the Residential Gateway to control how much egress traffic gets forwarded for Internet access as wished (4Mbps for P3 and P4 each), you can follow the suggested setup steps below.



Step 1. Set Up NAT/Bridge Mode

Network Management > WAN Setting

Network Management

- WAN Setting

NAT / Bridge Mode: Mode 2:3 WAN & 2 LAN

After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode).

WAN Port IP Assignment: Static IP DHCP PPPoE

Host Name: FTTX - Gateway

IP Address: 192.168.1.198

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Static IP MTU: 1500 bytes

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Ping from WAN: Allowed

In the scenario provided, "Mode 2: 3 WAN & 2 LAN" can be selected to group the WAN port, Port 1 & 2 to Bridge Mode and Port 3 & 4 to NAT Mode.

Step 2. Set Up Default VLAN ID

Switch Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Submit](#) [Reset](#)

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit

- Set up WAN's Default VLAN ID to 24 then NAT Interface's will be changed to the same one automatically.
- Set up Port 1 and Port 2's Default VLAN ID to 1100.
- Click the "Submit" button to apply the settings.

Step 3. Set Up VLAN Forwarding Table

Switch Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Submit](#) [Reset](#)

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit
24	0	U	T	-	-	Edit Delete
1100	0	-	T	U	U	Edit Delete

- According to the scenario provided, VID 24 should have NAT Interface untagged and WAN tagged.
- According to the scenario provided, VID 1100 should have WAN tagged and Port 1 and Port 2 untagged.

Step 4. Set Up Egress QoS Control

In this scenario, “Bandwidth Control” can be configured to control the outbound (egress) bandwidth to PC devices. To limit the bandwidth to 4Mbps for both Port 3 and Port 4, “By Port Only” Bandwidth Mode can be used to achieve this goal.
Switch Management > Bandwidth Control

Switch Management

- Bandwidth Range
 - Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control
 - Bandwidth Mode: OFF (dropdown menu highlighted with a red box)
- Ingress Bandwidth Control

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)

Buttons: Submit, Reset

Select “By Port Only”:

Switch Management

- Bandwidth Range
 - Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control
 - Bandwidth Mode: By Port Only (dropdown menu highlighted with a red box)
- Ingress Bandwidth Control

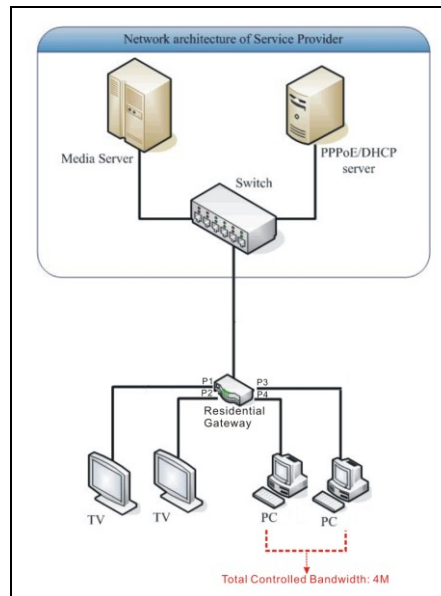
Port	Port.1	Port.2	Port.3	Port.4	NAT Download stream	NAT Upload stream	WAN
Bandwidth	102400 (K)	102400 (K)	4096 (K)	4096 (K)	8192 (K)	8192 (K)	102400 (K)

Buttons: Submit, Reset

- Set up Port 3 & Port 4’s egress bandwidth to 4096K and Download and Upload stream’s bandwidth to 8192K. In this way, both Port 3 & Port 4 are each allocated 4096K bandwidth.

Scenario II:

In this scenario, the Residential Gateway supports both IPTV applications and internet access. As illustrated in Figure 3, IPTV applications are connected to Port 1 (P1) and Port 2 (P2); whereas, PC devices are connected to Port 3 (P3) and Port 4 (P4) to access the internet. If you would like the Residential Gateway to control how much traffic gets forwarded for Internet access as wished (the total bandwidth for Port 3 and Port 4 is 4Mbps), you can follow the suggested setup steps below.



Step 1. Set Up NAT/Bridge Mode

Network Management > WAN Setting

Network Management

- **WAN Setting**

NAT / Bridge Mode: Mode 2:3 WAN & 2 LAN

After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode)

WAN Port IP Assignment: Static IP DHCP PPPoE

Host Name: FTX . Gateway

IP Address: 192.168.1.198

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Static IP MTU: 1500 bytes

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Ping from WAN: Allowed

Submit **Reset**

In the scenario provided, "Mode 2: 3 WAN & 2 LAN" can be selected to group the WAN port, Port 1 & 2 to Bridge Mode and Port 3 & 4 to NAT Mode.

Step 2. Set Up Default VLAN ID

Network Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Submit](#) [Reset](#)

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit

- Set up WAN's Default VLAN ID to 24 then NAT Interface's will be changed to the same one automatically.
- Set up Port 1 and Port 2's Default VLAN ID to 1100.
- Click the "Submit" button to apply the settings.

Step 3. Set Up VLAN Forwarding Table

Network Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

[Submit](#) [Reset](#)

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit
24	0	U	T	-	-	Edit Delete
1100	0	-	T	U	U	Edit Delete

- According to the scenario provided, VID 24 should have NAT Interface untagged and WAN tagged.
- According to the scenario provided, VID 1100 should have WAN tagged and Port 1 and Port 2 untagged.

Step 4. Set Up Egress QoS Control

In this scenario, “Bandwidth Control” can be configured to control the outbound (egress) bandwidth to PC devices. To allow the total bandwidth for Port 3 and Port 4 to 4Mbps, “By Port Only” and “By Port with Queue” Bandwidth Mode can be used to achieve this goal.

Switch Management > Bandwidth Control

Switch Management

- Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control**
Bandwidth Mode: OFF (dropdown menu open showing: OFF, By Port Only, By Port with Queue, By DSCP, By 802.1p, By Application, Disable)
- Ingress Bandwidth Control**

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)

Buttons: Submit, Reset

Select “By Port Only”:

Switch Management

- Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- Egress QoS Control**
Bandwidth Mode: By Port Only
- Ingress Bandwidth Control**

By Port Only

Port	Port.1	Port.2	Port.3	Port.4	NAT Download stream	NAT Upload stream	WAN
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)	4096 (K)	4096 (K)	102400 (K)

Ingress Bandwidth Control

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)	102400 (K)

Buttons: Submit, Reset

- Set up Download and Upload stream’s bandwidth to 4096K and leave Port 3 and Port 4’ bandwidth setting to their default values. In this way, the total egress bandwidth for Port 3 and Port 4 is 4096K. For example, if Port 3 consumes 1024K bandwidth, Port 4’s allowed egress bandwidth is 3072K.

Select “By Port with Queue”:

Switch Management

- Bandwidth Range
 - Min. Bandwidth Unit
- Egress QoS Control
 - Bandwidth Mode
 - By Port with Queue

Port	Port.1	Port.2	Port.3	Port.4	WAN
Map to Q	<input type="text" value="Q0"/>	<input type="text" value="Q0"/>	<input type="text" value="Q0"/>	<input type="text" value="Q0"/>	<input type="text" value="Q1"/>
 - Reserve Min. Egress Bandwidth of Queue

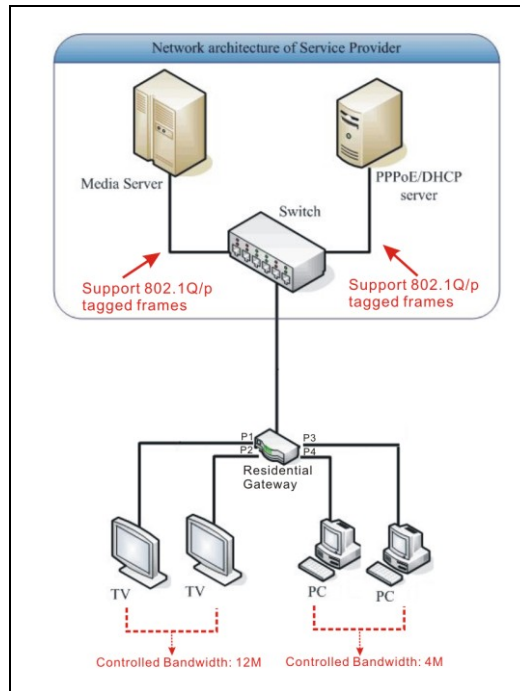
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	<input type="text" value="4096"/> (K)	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)
- Ingress Bandwidth Control

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>	<input type="text" value="Disable"/>
Bandwidth	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)	<input type="text" value="102400"/> (K)

- Select each port’s corresponding queue. Set Port 1, 2, 3, and 4’s queue to Q0 and WAN’s queue to Q1. **By default, when “By Port with Queue” bandwidth mode is selected, (Upstream & Downstream) CPU belongs to Q0 and this queue setting for CPU can not be modified. For LAN and WAN traffic flow, please refer to “Traffic Flow for Bridge & NAT Mode”.**
- Set up reserved egress bandwidth for each queue. Set Queue 0’s bandwidth to 4096 (K) and leave queue 1, 2 and 3 to their default setting. By doing so, the total egress bandwidth for Port 3 and Port 4 is 4Mbps.

Scenario III:

In this scenario, the Residential Gateway supports both IPTV applications and internet access. As illustrated in Figure 4, IPTV applications are connected to Port 1 (P1) and Port 2 (P2); whereas, PC devices are connected to Port 3 (P3) and Port 4 (P4) to access the internet. The media server sends out 802.1Q/p tagged frames. If you would like the Residential Gateway to control how much traffic gets forwarded for IPTV application and Internet access as wished (12Mbps for IPTV; 4Mbps for Internet), you can follow the suggested setup steps below.



Step 1. Set Up NAT/Bridge Mode

Network Management > WAN Setting

The screenshot shows the 'Network Management' configuration page. Under the 'WAN Setting' section, the 'NAT / Bridge Mode' dropdown is set to 'Mode 2:3 WAN & 2 LAN'. Below this, there is a note: 'After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode)'. The 'WAN Port IP Assignment' section has 'Static IP' selected. Other fields include Host Name (FTTX.Gateway), IP Address (192.168.1.198), Subnet Mask (255.255.255.0), Default Gateway (192.168.1.254), Static IP MTU (1500 bytes), Primary DNS Server (0.0.0.0), Secondary DNS Server (0.0.0.0), and Ping from WAN (checked/Allowed). 'Submit' and 'Reset' buttons are at the bottom.

In the scenario provided, "Mode 2: 3 WAN & 2 LAN" can be selected to group the WAN port, Port 1 & 2 to Bridge Mode and Port 3 & 4 to NAT Mode.

Step 2. Set Up Default VLAN ID

Switch Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	<input type="button" value="Insert"/> <input type="button" value="Change"/>
1	0	U	U	U	U	<input type="button" value="Edit"/>
2	0	-	-	-	-	<input type="button" value="Edit"/>

- Set up WAN's Default VLAN ID to 24 then NAT Interface's will be changed to the same one automatically.
- Set up Port 1 and Port 2's Default VLAN ID to 1100.
- Click the “**Submit**” button to apply the settings.

Step 3. Set Up VLAN Forwarding Table

Switch Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	24	24	1100	1100
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	<input type="button" value="Insert"/> <input type="button" value="Change"/>
1	0	U	U	U	U	<input type="button" value="Edit"/>
2	0	-	-	-	-	<input type="button" value="Edit"/>
24	4	U	T	-	-	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
1100	5	-	T	U	U	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

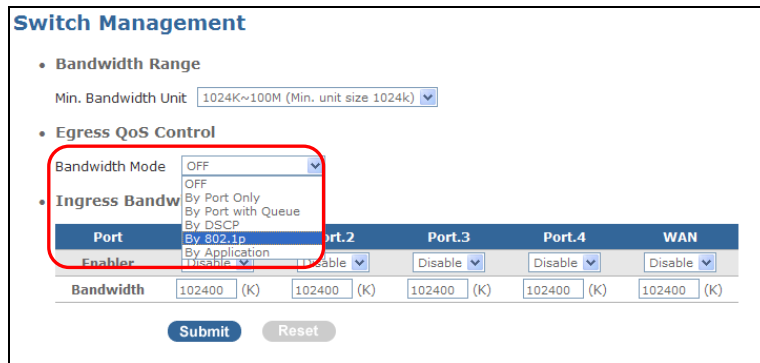
- According to the scenario provided, VID 24 should have NAT Interface untagged and WAN tagged.
- Since the WAN link carries 802.1Q/p tagged frames, for VID 24, P-Bit must be specified to mark packets as belonging to a specific level of service. Set VID 24's P-Bit to 4.
- According to the scenario provided, VID 1100 should have WAN tagged and Port 1 and Port 2 untagged.

- Since the WAN link carries 802.1Q/p tagged frames, for VID 1100, P-Bit must be specified to mark packets as belonging to a specific level of service. Set VID 1100's P-Bit to 5.

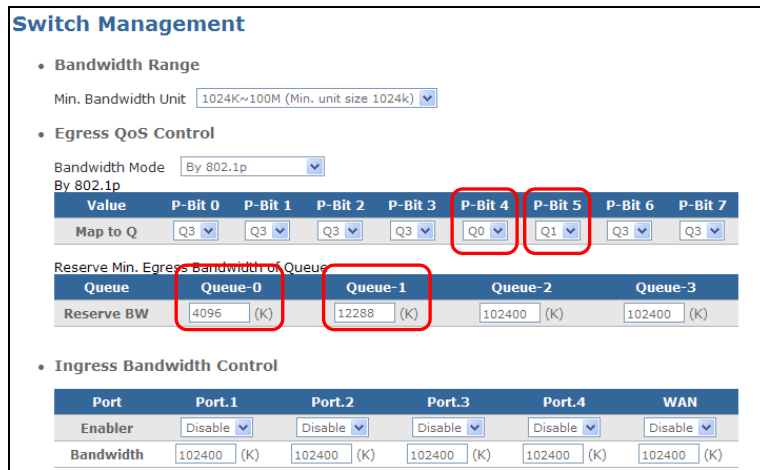
Step 4. Set Up Egress QoS Control

Egress QoS Control provides five bandwidth modes for users to set up the required bandwidth based on the actual networking environment. In this scenario, the bandwidth mode “By 802.1p” can be used to limit the egress bandwidth to 12Mbps for IPTV application and 4Mbps for Internet access.

Switch Management > Bandwidth Control



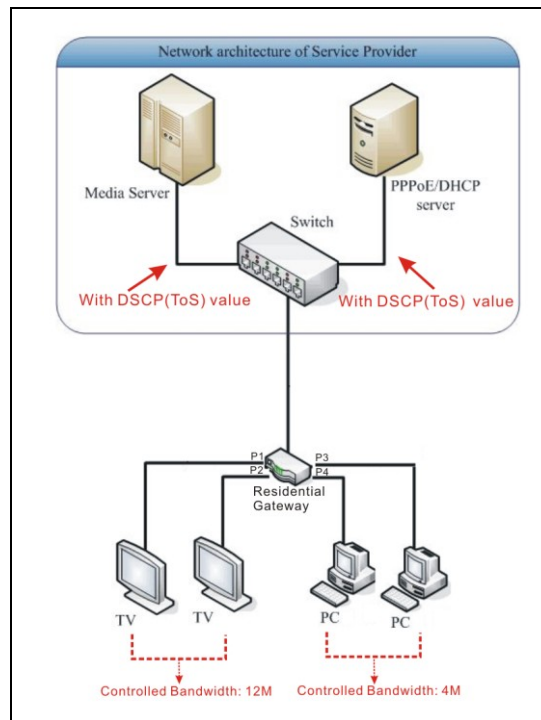
Select “By 802.1p”:



- Map P-bit 4 to Q0 and P-bit 5 to Q1.
- Set Queue 0's reserved bandwidth to 4096K and Queue 1's reserved bandwidth to 12288K.

Scenario IV:

In this scenario, the Residential Gateway supports both IPTV applications and internet access. As illustrated in Figure 5, IPTV applications are connected to Port 1 (P1) and Port 2 (P2); whereas, PC devices are connected to Port 3 (P3) and Port 4 (P4) to access the internet. The frames received from the WAN port are with a DSCP value. If you would like the Residential Gateway to control how much traffic gets forwarded for IPTV application and Internet access as wished (12Mbps for IPTV; 4Mbps for Internet), you can follow the suggested setup steps below.



Step 1. Set Up NAT/Bridge Mode

Network Management > WAN Setting

Network Management

- WAN Setting

NAT / Bridge Mode: Mode 2:3 WAN & 2 LAN
After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode).

WAN Port IP Assignment: Static IP DHCP PPPoE

Host Name: FTTX . Gateway

IP Address: 192.168.1.198

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.254

Static IP MTU: 1500 bytes

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Ping from WAN: Allowed

Submit Reset

In the scenario provided, "Mode 2: 3 WAN & 2 LAN" can be selected to group the WAN port, Port 1 & 2 to Bridge Mode and Port 3 & 4 to NAT Mode.

Step 2. Set Up Egress QoS Control

Egress QoS Control provides five bandwidth modes for users to set up the required bandwidth based on the actual networking environment. In this scenario, the bandwidth mode “By DSCP” can be used to limit the egress bandwidth to 12Mbps for IPTV application and 4Mbps for Internet access.

Switch Management > Bandwidth Control

Switch Management

- **Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: OFF (dropdown menu with options: OFF, By Port Only, By Port with Queue, By DSCP, By Application)
- **Ingress Bandwidth**

Port	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable
Bandwidth	102400 (K)	102400 (K)	102400 (K)	102400 (K)

Submit Reset

Select “By DSCP”:

Switch Management

- **Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: By DSCP
- By DSCP
DSCP Map: DSCP(47) --> Q1

Q0-DSCP	0~39,48~63
Q1-DSCP	40~47
Q2-DSCP	
Q3-DSCP	

Reserve Min. Egress Bandwidth of Queue

Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	4096 (K)	12288 (K)	102400 (K)	102400 (K)

- Set up Queue-DSCP mapping.
 - Set Q0-DSCP mapping to 0~39, 48~63. (This value should be changed based on your networking environment.)
 - Set Q1-DSCP mapping to 40~47. (This value should be changed based on your networking environment.)
- Set up Queue 0's reserved bandwidth to 4096K and Queue 1's to 12288K.

2.4.3 Configure VLAN

Select **Configure VLAN** from the **Switch Management** menu, then **Configure VLAN** screen page appears.

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text" value=""/>	<input type="text" value="0"/>	<input type="text" value="-"/>	<input type="text" value="-"/>	<input type="text" value="-"/>	<input type="text" value="-"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
1	0	U	U	U	U	<input type="button" value="Edit"/>
3	0	U	T	U	U	<input type="button" value="Edit"/> <input type="button" value="Search"/>

Default VLAN VID: Specify a default VID number (1~4095) to each port.

Ingress Double Tag: Enable or disable “Ingress Double Tag” function. When enabled, ingress traffic is added with a PVID. The Residential Gateway supports Q-in-Q (Double tag tunneling) for security via robust isolation of customer traffic and unburdening the service provider from configuration management of CPE.

VLAN Forwarding Table

VID: Specify a VID for new VLAN rule.

NOTE: By default, there are two VLANs in the VLAN Forwarding table; VLAN 1 is for WAN, VLAN 2 is for LAN. When you select your desired “**NAT/Bridge Mode**” in **WAN Settings**, the settings in VLAN 1 and VLAN2 will be changed accordingly and automatically.

P-Bit: Select a priority value from the drop-down menu for this VLAN rule.

Port: T (Tag, a member in this VLAN rule), U (Un-tag, a member in this VLAN rule), – (Not a member in this VLAN rule).

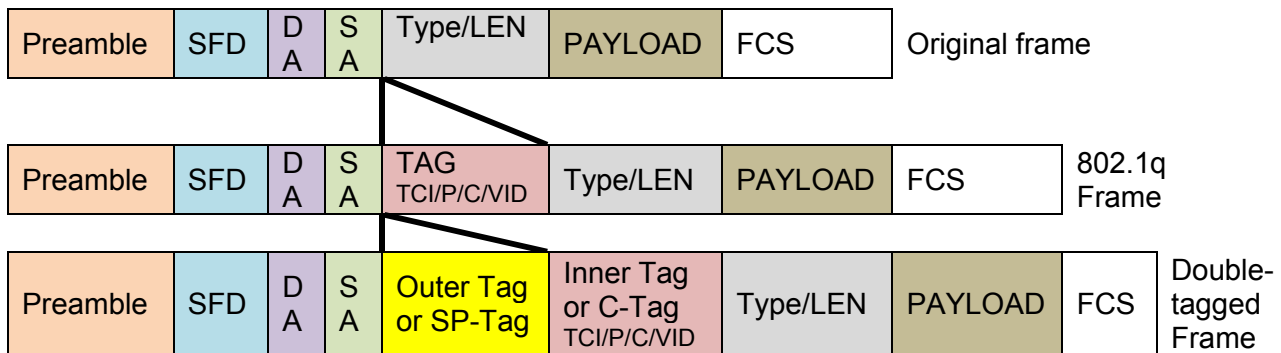
Click the “**Insert**” button to add this new rule to the VLAN table below after you enter the new VID and select appropriate settings from the drop-down menu

Click the “**Edit**” button on the VLAN rule that you would like to make some changes. When the selected port is highlighted in blue, users can make some changes by selecting from the drop-down menu.

Click the “**Change**” button to apply the changes. The modified changes will apply to the VLAN table immediately.

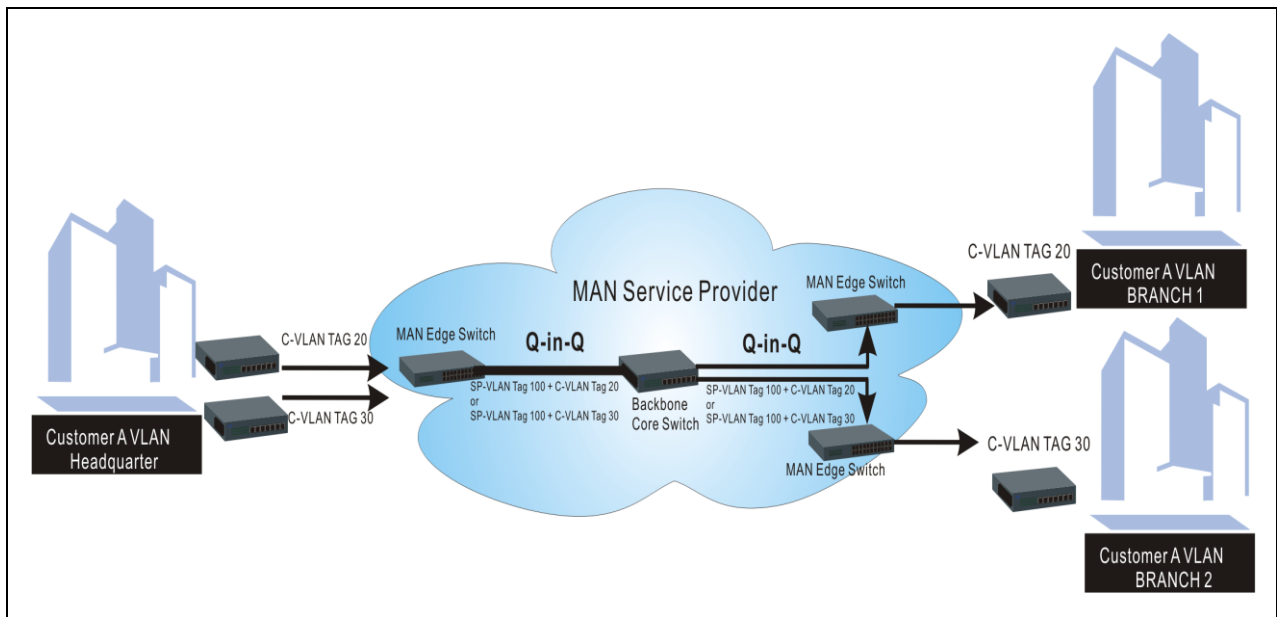
2.5.4 Configure Q-in-Q

The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As shown below in “Double-Tagged Frame” illustration, an outer tag is added between source destination and inner tag at the provider network’s edge. This can support C-VLAN (Customer VLAN) over Metro Area Networks and ensure complete separation between traffic from different user groups. Moreover, the addition of double-tagged space increases the number of available VLAN tags which allow service providers to use a single SP-VLAN (Service Provider VLAN) tag per customer over the Metro Ethernet network.



Double-Tagged Frame

As shown below in “Q-in-Q Example” illustration, Headquarter A wants to communicate with Branch 1 that is 1000 mile away. One common thing about these two locations is that they have the same VLAN ID of 20, called C-VLAN (Customer VLAN). Since customer traffic will be routed to service provider’s backbone, there is a possibility that traffic might be forwarded insecurely, for example due to the same VLAN ID used. Therefore, in order to get the information from Headquarter to Branch 1, the easiest way for the carrier to ensure security to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as SP-VLAN (Service Provider VLAN) that is added as data enters the service provider’s network and then removed as data exits. Eventually, with the help of SP-Tag, the information sent from Headquarter to Branch 1 can be delivered with customers’ VLANs intact and securely.



Q-in-Q Example

Q-in-Q Setup Steps:

Step 1. Set up Bridge/NAT Mode

Network Management > WAN Setting

Network Management

- WAN Setting

NAT / Bridge Mode Mode 2:3 WAN & 2 LAN

After you switch between Bridge and NAT mode, please clear up your ARP table by using the "arp -d" command (under PC MS-DOS Mode).

WAN Port IP Assignment Static IP DHCP PPPoE

Host Name .

IP Address

Subnet Mask

Default Gateway

Static IP MTU bytes

Primary DNS Server

Secondary DNS Server

Ping from WAN Allowed

- Q-in-Q only works in ports that belong to Bridge Mode. Before going any further, please make sure that the appropriate mode is selected.
- Please make sure that packets received from Bridged ports already carry a tag (C-tag). In this way, a second tag (SP-tag) can be added.

Step 2. Enable Ingress Double Tag

Switch Management > Configure VLAN

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	1	1	100	1
Ingress Double Tag		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
	0	-	-	-	-	<input type="button" value="Insert"/> <input type="button" value="Change"/>
1	0	U	U	U	U	<input type="button" value="Edit"/>
2	0	-	-	-	-	<input type="button" value="Edit"/>

Enable Ingress Double Tag on Bridged ports that you would like to add an additional tag (SP-tag).

Step 3. Set up PVID

Switch Management

• Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	1	1	100	1
Ingress Double Tag		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
	0	-	-	-	-	<input type="button" value="Insert"/> <input type="button" value="Change"/>
1	0	U	U	U	U	<input type="button" value="Edit"/>
2	0	-	-	-	-	<input type="button" value="Edit"/>

Set up a PVID. When packets received with a tag, the PVID will be added. In this example, PVID 100 will be added (Inner tag+ PVID 100).

Step 4. Set up Egress Forwarding Table

The screenshot shows the 'Switch Management' interface. Under the 'Configure VLAN' section, there is a table for VLAN configuration:

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Ingress Double Tag	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Below this table are 'Submit' and 'Reset' buttons. A note states: 'VID 2 is reserved for internal use.' Below the note is the 'Egress Forwarding Table' with the following columns: VID, P-Bit, NAT Interface, WAN, Port .1, Port .2, and Action.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
<input type="text"/>	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit
100	0	-	T	T	-	Edit Delete

The row for VID 100 is highlighted with a red border.

Set up VID 100's Egress Forwarding Table. WAN port must set to "T" (Tagged) to enable the Gateway to deliver double-tagged packets. If "U" is assigned to WAN port, PVID will be removed; therefore, packets with one tag are forwarded.

2.4.5 IGMP Control

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

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

IGMP snooping can effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. This router using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduces the packet processing at the gateway and the workload at the end hosts.

Select **IGMP Control** from the **Switch Configuration** menu, then **IGMP Control** screen page shows up.

The screenshot shows the 'Switch Management' interface with the 'IGMP Control' section selected. The settings are as follows:

- NAT IGMP Proxy: Enable
- Bridge IGMP Snooping: Enable
- Snooping Fast Leave: Enable
- Snooping Congestion Control: Enable report suppression and join aggregation, Enable report suppression, Transparent mode

At the bottom are 'Submit' and 'Reset' buttons.

NAT

IGMP Proxy: Enable or disable IGMP Proxy. When enabled, all clients attached to the Residential Gateway will receive multicast data. Please note that IGMP Proxy and IGMP Snooping can not be selected at the same time.

Proxy Fast Leave: Enable or disable Proxy Fast Leave. When enabled, the Residential Gateway removes the interface from the forwarding table immediately when the leave message is received. Please ensure that only one host is attached to the each interface when Fast Leave is enabled; otherwise, multicast traffic to other hosts attached to the interface will be dropped.

Bridge

IGMP Snooping: Enable or disable IGMP Snooping. When enabled, all clients that respond with a join message will receive multicast data. Please note that IGMP Proxy and IGMP Snooping can not be selected at the same time.

Snooping Fast Leave: Enable or disable Snooping Fast Leave. When enabled, the Residential Gateway removes the interface from the forwarding table immediately when the leave message is received. Please ensure that only one host is attached to the each interface when Fast Leave is enabled; otherwise, multicast traffic to other hosts attached to the interface will be dropped.

Snooping Congestion Control: There are three modes available. However, when you enable MVR, the “Transparent Mode” is the only option that can be selected.

Enable report suppression and join aggregation: The Residential Gateway forwards only one (the first) IGMP report and join message from all hosts to multicast devices. Other reports or join messages sent will be filtered. Enabling report suppression can prevent the same reports from being sent to multicast devices.

Enable report suppression: The Residential Gateway forwards only one (the first) IGMP report from all hosts to multicast devices. Enabling report suppression can prevent the same reports from being sent to multicast devices.

Transparent Mode: All join and leave messages are forwarded to multicast devices.

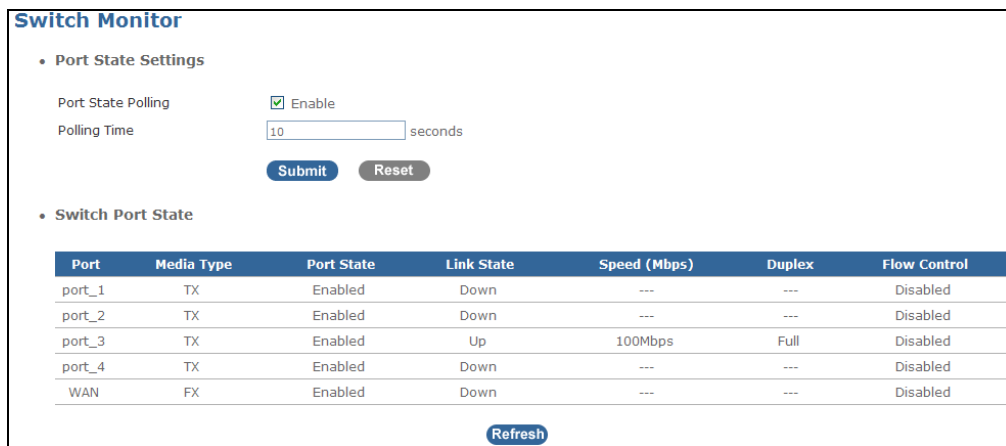
NOTE: *The Residential Gateway only supports IGMPv1 and IGMPv2.*

2.5 Switch Monitor

Select **Switch Monitor** from the **Main Menu**, the sub-item – **Switch port state** – will show up.

2.5.1 Switch Port State

Select **Switch Port State** from the **Switch Monitor** menu, then **Switch Port State** screen page appears.



The screenshot shows the 'Switch Monitor' interface. Under 'Port State Settings', there is a checkbox for 'Port State Polling' which is checked and labeled 'Enable'. Below it is a 'Polling Time' input field with the value '10' and the unit 'seconds'. There are 'Submit' and 'Reset' buttons. Below this is the 'Switch Port State' section, which contains a table with the following data:

Port	Media Type	Port State	Link State	Speed (Mbps)	Duplex	Flow Control
port_1	TX	Enabled	Down	---	---	Disabled
port_2	TX	Enabled	Down	---	---	Disabled
port_3	TX	Enabled	Up	100Mbps	Full	Disabled
port_4	TX	Enabled	Down	---	---	Disabled
WAN	FX	Enabled	Down	---	---	Disabled

At the bottom of the table is a 'Refresh' button.

Port State Polling: Tick the checkbox to automatically refresh port status.

Polling Time: Specify time interval in seconds to automatically refresh port status.

Media Type: View-only field that shows whether each port is a copper port or fiber port.

Port State: View-only field that shows whether each port is enabled or not.

Link State: View-only field that shows whether each port is link up or down.

Speed (Mbps): View-only field that shows the speed of the link-up port(s).

Duplex: View-only field that shows whether the link-up port is full or half duplex mode.

Flow Control: View-only field that shows whether each port's flow control function is enabled or disabled.

2.6 CATV Setting (Only available for RF module)

Select **CATV Setting**, then **CATV Settings** screen page appears.

CATV Setting: The default setting of CATV-RF module is enabled. Select “Disable” from the pull-down menu to disable CATV-RF module.

2.7 Management

In this session you will be able to set up web management authority, username and password for the authentication of configuration and maintenance, and upgrade firmware.

Select **Management** from the **Main Menu**, the sub-items – **Administrator Account**, **Date/Time**, **Ping test**, **Save/Restore**, **Factory Default**, and **Firmware Update** - will show up.

2.7.1 Administrator Account

Select **Administrator Account** from the **Management** menu, then **Administrator Account** screen page appears.

Account: Up to ten login accounts can be created.

Admin: Tick the checkbox if you would like this account to have administrator privilege. Uncheck the checkbox if you would like to set up an account with limited privilege.

Account	Privilege
Administrator	Can view all Information pages Can set up all functions' configurations
User	Can view all Information pages Can set up functions in Network Management and Management folder (except Administrator Account &

	Save / Restore)
--	-----------------

User Name: Specify the authorized user login name, up to 31 alphanumeric characters.

Password: Enter the desired user password for this account.

Confirm Password: Re-type the desired user password to confirm.

Click the “**Insert**” button to add a new account.

Click the “**Edit**” button on the account that you would like to make some changes. When the selected line is highlighted in blue, users can make some changes to username and password fields.

Click the “**Change**” button to apply the changes.

Click the “**Delete**” button to remove an account. To avoid incorrect operations, you can not delete your own account.

NOTE: When you set up your new administrator name and password to login to Web Management, please remember login information by heart or keep it in a safe place. If you forget your login information or every login retry fails, you can press the Reset button for about 10 seconds to reset the device to factory defaults. In this way, you can use the default login information to login to Web Management.

Remote Administration

Remote administration: If enabled, the Residential Gateway could be accessed from WAN port.

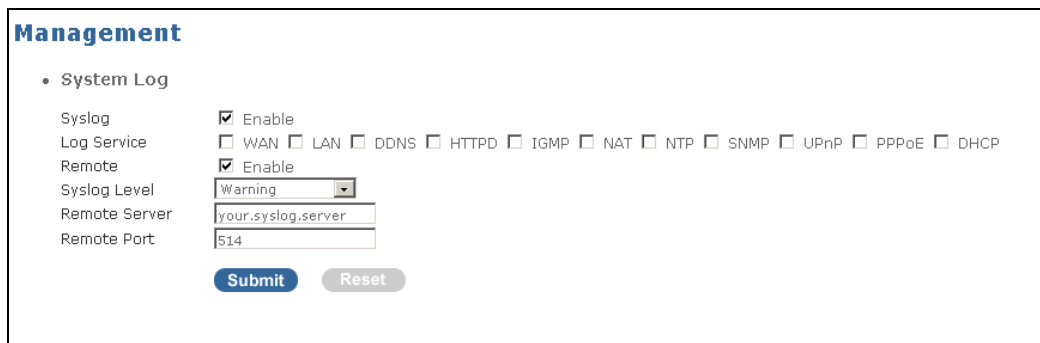
Http port for remote: Specify the port number for remote access. The default http port number is 8888.

Remote administration only from IP: To limit the remote administration access IP address. Login access from the IP address other than the one specified will be restricted.

NOTE: If you would like to login the Residential Gateway from WAN port, you must enable “Remote Administration” option in **Administrator Account** under the **Management Menu** and then add IP address (if necessary) and specify Http port number for remote login. Once completed, you can type in the specified IP address and Http port number in URL field of your web browser like this “**192.168.1.198:8888**” to access to web management.

2.7.2 System Log

Select **System Log** from the **Management** menu, then **System Log** screen page appears.



The screenshot shows the 'Management' menu with 'System Log' selected. The configuration options are:

- Syslog**: Enable
- Log Service**: WAN LAN DDNS HTTPD IGMP NAT NTP SNMP UPnP PPPoE DHCP
- Remote**: Enable
- Syslog Level**: Warning (dropdown menu)
- Remote Server**: your.syslog.server (text input)
- Remote Port**: 514 (text input)

Buttons: **Submit** (blue), **Reset** (grey)

Syslog: Tick the checkbox to enable System Log function.

Log Service: When certain service checkboxes are ticked, you are able to view their system log messages in **Syslog Table** under the **Information** menu.

Syslog Level: There are eight syslog levels for users to choose from. If you choose a certain log level, the Residential Gateway will record log events at the chosen level and above. For example, if you choose Error, all error, critical, alert and emergency events will be recorded.

Level 1 Emergency: System is unusable.

Level 2 Alert: Emergent actions that must be taken immediately.

Level 3 Critical: Critical conditions.

Level 4 Error: Error conditions.

Level 5 Warning: Warning conditions.

Level 6 Notice: Normal but significant conditions.

Level 7 Informational: Keep informational events message.

Level 8 Debug: Debug-level messages are logged.

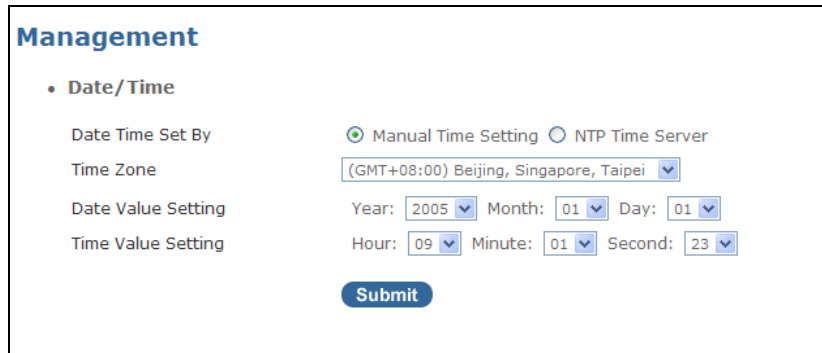
Remote: Enable the remote server, if checked.

Remote Server: Specify the remote log server IP address.

Remote Port: Specify the remote port. By convention, port 514 is used. However, you can specify the port number that suits your networking environment setup.

2.7.3 Date/Time

Select **Date/Time** from the **Management** menu, then **Date/Time** screen page appears.



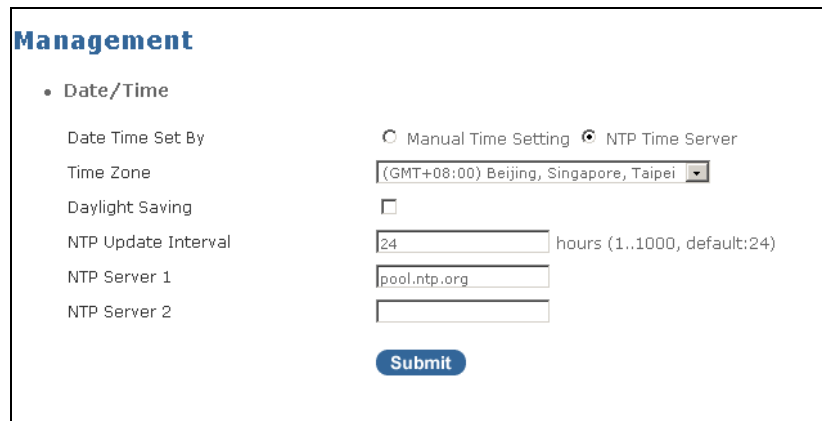
The screenshot shows the 'Management' menu with 'Date/Time' selected. The 'Date Time Set By' option is set to 'Manual Time Setting'. The 'Time Zone' is '(GMT+08:00) Beijing, Singapore, Taipei'. The 'Date Value Setting' is Year: 2005, Month: 01, Day: 01. The 'Time Value Setting' is Hour: 09, Minute: 01, Second: 23. A 'Submit' button is at the bottom.

Date Time Set by: The WLAN Residential Gateway provides two options for users to configure date and time settings; these are **Manual Time Setting** and **NTP Time Server**. The former option sets up the local time specified by the user; whereas, the later one synchronizes the local time with NTP server on the internet automatically.

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

Date Value Setting: Select the value from the year, month and day pull-down menu.

Time Value Setting: Select the value from the hour, minute and second pull-down menu.



The screenshot shows the 'Management' menu with 'Date/Time' selected. The 'Date Time Set By' option is set to 'NTP Time Server'. The 'Time Zone' is '(GMT+08:00) Beijing, Singapore, Taipei'. The 'Daylight Saving' checkbox is unchecked. The 'NTP Update Interval' is 24 hours (1..1000, default:24). The 'NTP Server 1' is pool.ntp.org. The 'NTP Server 2' is empty. A 'Submit' button is at the bottom.

NTP Update Interval: Specify how frequent to update system clock. The default setting is 24 hours.

NTP Server 1: Specify the primary NTP Server domain name or IP address.

NTP Server 2: Specify the NTP Server 2 domain name (optional).

2.7.4 Ping Test

Select **Ping Test** from the **Management** menu, then **Ping Test** screen page appears.

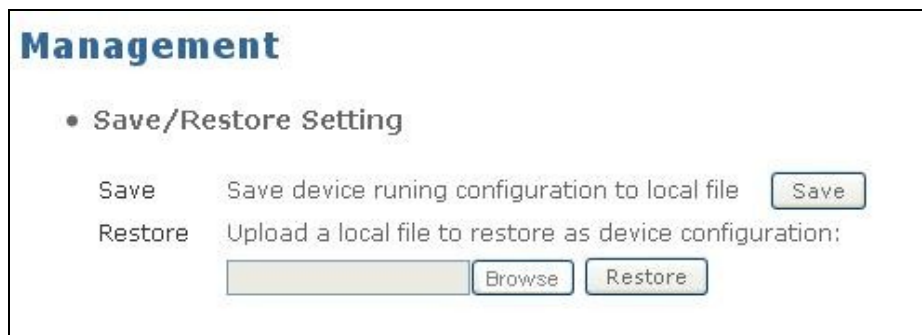


The screenshot shows a web interface titled "Management" with a sub-menu item "Ping Test". Below the sub-menu item, there is a label "Ping Destination" followed by a text input field and a blue "Ping" button.

Ping Destination: The Ping Test is used to send ICMP request packets to test if a computer is on the Internet. Specify the IP Address that you wish to Ping, and click the “**Ping**” button to test the connectivity of the destination address.

2.7.5 Save/Restore

Select **Save/Restore** from the **Management** menu, then **Save/Restore** screen page appears.



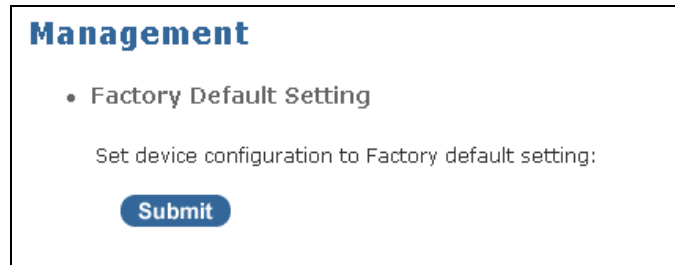
The screenshot shows a web interface titled "Management" with a sub-menu item "Save/Restore Setting". Below the sub-menu item, there are two sections: "Save" and "Restore". The "Save" section has a label "Save" and a description "Save device running configuration to local file" followed by a "Save" button. The "Restore" section has a label "Restore" and a description "Upload a local file to restore as device configuration:". Below the description, there is a text input field, a "Browse" button, and a "Restore" button.

Save: Save device configurations to a local file. The default filename is “metafile.dat”.

Restore: Upload a local file to restore the Wireless Gateway configurations. When the restore process is completed, a pop-up window will appear to notify the user.

2.7.6 Factory Default

Select **Factory Default** from the **Management** menu, then **Factory Default** screen page appears.




The screenshot shows a web interface titled "Management". Underneath, there is a bullet point for "Factory Default Setting". Below this, the text reads "Set device configuration to Factory default setting:". At the bottom of the section is a blue "Submit" button.

If you would like to set the Wireless Gateway back to Factory default settings, click the **“Submit”** button. When the loading process is completed, the Wireless Gateway will restart automatically to make the factory default settings effective.

2.7.7 Firmware Upgrade

Select **Firmware Upgrade** from the **Management** menu, then **Firmware Upgrade** screen page appears.



The screenshot shows a web interface titled "Firmware Upgrade". It has two main sections. The first is "Manual Firmware Upgrade", which includes a "Firmware File" label, an empty text input field, a "Browse" button, and an "Upload" button. The second section is "Ftp Firmware Upgrade", which includes four labels: "Absolute Path File Name", "IP or URL", "Ftp User Name", and "Ftp User Password", each followed by an empty text input field. At the bottom of the form is a blue "Submit" button.

Manual Firmware Upgrade

This Residential Gateway can upgrade firmware version by using local hard drive of your computer or via FTP. For manual upgrade, click on the **“Browse”** button to locate the firmware file to be used for the update. Then, click on the **“Upload”** button to start Firmware upgrade. When the upgrade is in process, please follow the instructions shown on the screen and do not turn off the power.

FTP Firmware Upgrade

Absolute Path File Name: Specify the firmware file name that you would like to upgrade.

IP or URL: Specify the FTP server's IP address or URL.

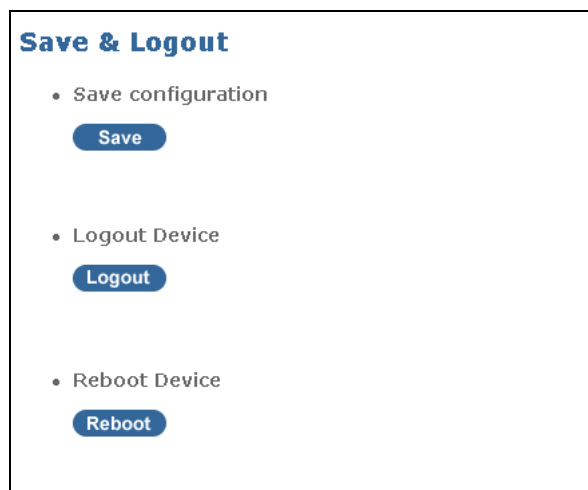
FTP User Name: Specify the FTP login user name.

FTP User Password: Specify the FTP login password.

NOTE: It will take approximately 200 seconds (3 minutes and 20 seconds) to upgrade your Residential Gateway with the new firmware. Please do not turn off the power while your device is upgrading new firmware. When firmware upgrade is complete, the login page will appear to prompt you to enter your username and password.

2.8 Save & Logout

Select **Save & Logout** from the **Management** menu, then **Save & Logout** screen page appears.



Click the **“Save”** button to save current configuration settings. If changed settings are not saved, all new configurations will be lost when you restart the Wireless Gateway.

Click the **“Logout”** button to Logout from the system.

Click the **“Reboot”** button to restart the system.

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.

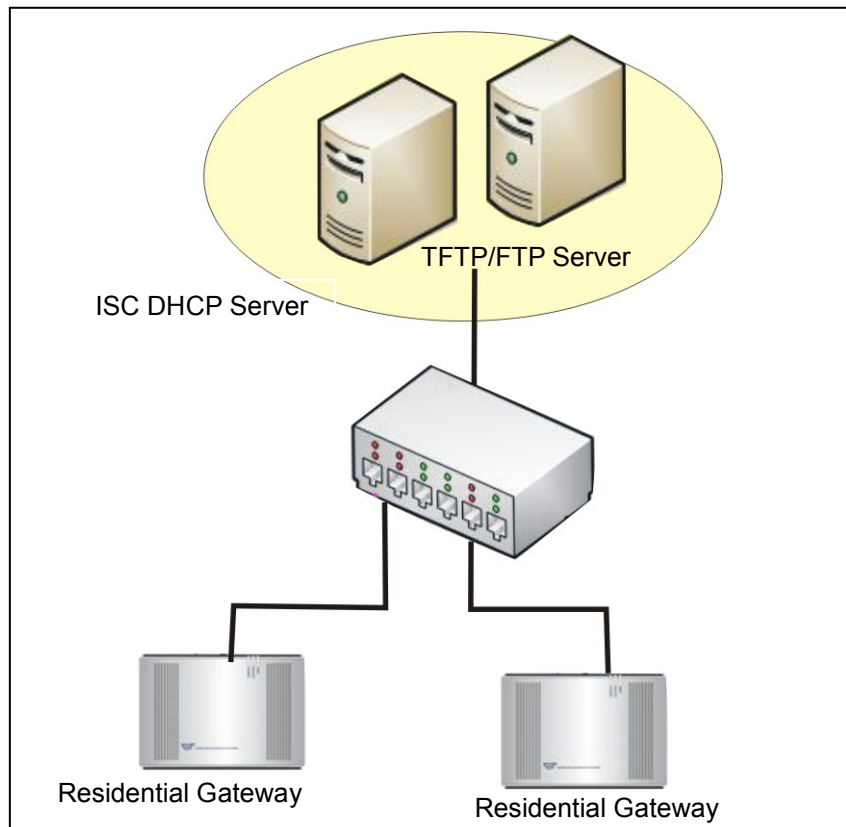
APPENDIX A: Set Up DHCP Auto-Provisioning

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 VoIP 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:ftp, 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" "VRG-21412-WF" {
    vendor-option-space SAMPLE;
#    option SAMPLE.firmware-file-name "VRG-21412-WF_9.99.99.bin";
#    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 "sq"; 5
option SAMPLE server-login-password "a12345A"; 6

subclass "vendor-classes" "VRG-21412-WF" { 7
    vendor-option-space SAMPLE;
# option SAMPLE firmware-file-name "VRG-21412-WF_9.99.99.bin"; 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 "metatile"; 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 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. Put a copy of Firmware and Configuration File in TFTP/FTP Server

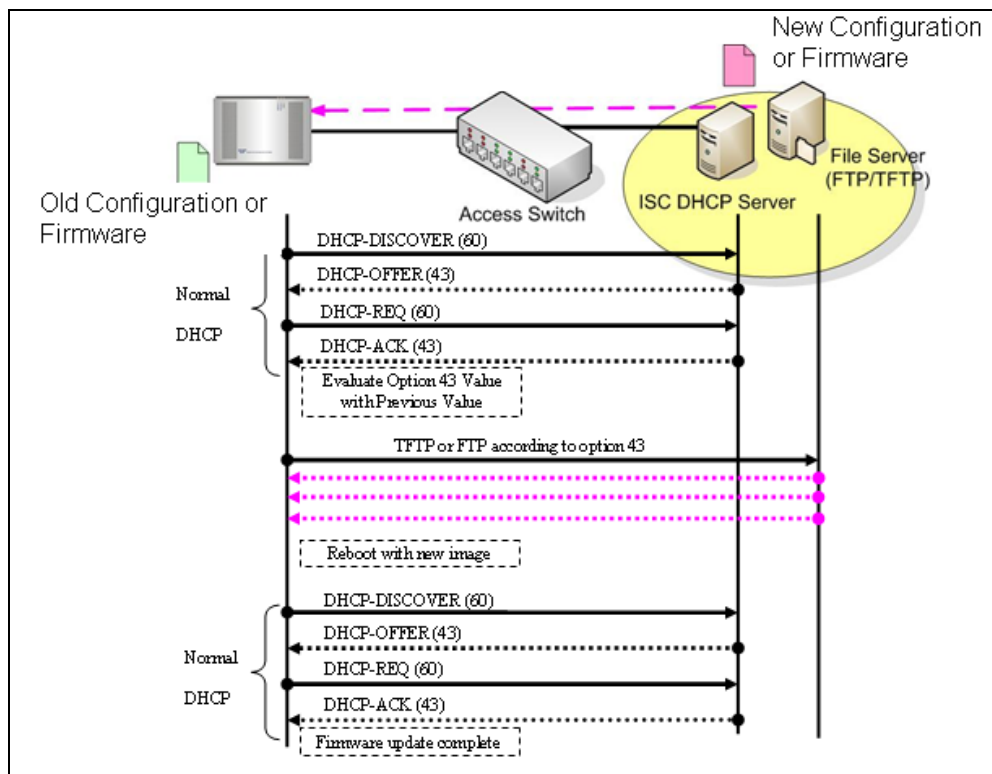
The TFTP/FTP File server should include the following items:

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" "VRG-21412-WF" {
    vendor-option-space SAMPLE;
# option SAMPLE.firmware-file-name "VRG-21412-WF_9.99.99.bin";
```



```
# 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.