



CONNECTION TECHNOLOGY SYSTEMS

VRG-21412-WF-G SERIES

4 ports 10/100Mbps RJ-45; 2 ports VoIP FXS, built-in IEEE 802.11b/g WiFi and 1 Port 100Mbps fiber optics uplink VoIP Residential Gateway

VRG-21412-WF-N SERIES

4 ports 10/100Mbps RJ-45; 2 ports VoIP FXS, built-in IEEE802.11n draft WiFi and 1 port 100Mbps fiber optics uplink VoIP Residential Gateway

VRG-21412-WF-G-RF

4 ports 10/100Mbps RJ-45; 2 ports VoIP FXS, built-in IEEE 802.11b/g WiFi and 1 Port 100Mbps fiber optics uplink VoIP Residential Gateway with CATV RF receiver

VRG-21412-WF-N-RF

4 ports 10/100Mbps RJ-45; 2 ports VoIP FXS, built-in IEEE802.11n draft WiFi and 1 port 100Mbps fiber optics uplink VoIP Residential 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 © 2009 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 © 2009 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	6
1.1 Front, Rear and Top-Front Panel.....	7
1.2 Management Options	8
1.3 Interface Descriptions.....	9
1.4 Connecting the Residential Gateway	9
1.5 RF over Fiber (With RF Receiver only)	10
1.6 LED Descriptions.....	10
2. WEB MANAGEMENT	11
2.1 The Concept of IP address.....	11
2.2 Start Configuring.....	11
2.3 Introduction to Sub-Menus	13
2.4 Information	14
2.4.1 System Information.....	14
2.4.2 Line Status	17
2.4.3 CDR.....	18
2.4.4 Syslog Table	19
2.5 Network Management	19
2.5.1 WAN Setting	19
2.5.2 LAN Setting	23
2.5.3 WLAN Setting	25
2.5.4 WLAN Access Policy	27
2.5.5 Static Route	28
2.5.6 NAT.....	29
2.5.7 Packet Filter.....	31
2.5.8 URL Filter.....	33
2.5.9 UPnP	34
2.5.10 DDNS	35
2.5.11 SNMP.....	36
2.6 Switch Management.....	36
2.6.1 Port Configuration.....	36
2.6.2 Bandwidth Configuration.....	37
2.6.2.1 Egress Bandwidth Control.....	38

2.6.2.1.1 By Port Only	38
2.6.2.1.2 By Port with Queue.....	38
2.6.2.1.3 By DSCP	39
2.6.2.1.4 By 802.1p	39
2.6.2.1.5 By Application.....	40
2.6.2.2 Ingress Bandwidth Setting.....	41
2.6.3 Configure VLAN.....	41
2.6.4 Traffic Flow for Bridge & NAT Mode.....	43
2.6.5 Bandwidth Control Setup Examples	44
2.6.6 Configure Q-in-Q	58
2.6.7 IGMP Control.....	61
2.7 Switch Monitor.....	62
2.8 SIP Management.....	63
2.8.1 Basic Setting.....	63
2.8.2 Account Setting.....	64
2.8.3 Server Setting.....	65
2.9 VoIP Management.....	66
2.9.1 Voice Setting.....	66
2.9.2 Call Service	68
2.9.3 FXS Port Setting.....	70
2.9.4 FAX Setting.....	72
2.9.5 General Dialing Setting.....	72
2.9.6 Phone Book	74
2.9.7 Dialing Plan	75
2.10 CATV Setting (Only available for RF module)	76
2.11 Management.....	76
2.11.1 Administrator Account	76
2.11.2 System Log	78
2.11.3 Date/Time	79
2.11.4 Ping Test.....	80
2.11.5 Save/Restore	80
2.11.6 Factory Default.....	81
2.11.7 Firmware Upgrade	81
2.12 Save & Logout.....	82

3. SNMP NETWORK MANAGEMENT 83
APPENDIX A: Set Up DHCP Auto-Provisioning 84
APPENDIX B: DHCP Text Sample 89

1. INTRODUCTION

Thank you for purchasing the WLAN Residential Gateway which is designed to aim at FTTX applications. This WLAN Residential Gateway provides four TP ports for LAN applications, one fiber optic or TP port for WAN, two sets of FXS telephony ports and built-in IEEE 802.11b/g or 802.11b/g/n wireless LAN (To use CATV application, please purchase the WLAN Residential Gateway with RF module installed). The combination of wireless and VoIP function provides users not only more flexible ways to enjoy bandwidth-intensive services but also more secure internet network connections by implementing packet or URL filtering policies.

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.

For VoIP applications, the internationally recognized standards, SIP (Session Initiation Protocol), have been employed to manage multimedia communication sessions so that users can use traditional analog telephones to make telephone calls to IP telephones over the Internet. Calls received from IP telephones work exactly the same as you would expect from the traditional telephone service. Other WLAN Residential Gateway's features are: Voice Activity Detection (VAD) / Silence Suppression which reduces the bandwidth that a call uses by not transmitting when you are not speaking; Comfort Noise Generation that is the background noise the device generates to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection); Echo Cancellation which is WLAN Residential Gateway's supporting G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

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

1.1 Front, Rear and Top-Front Panel

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:

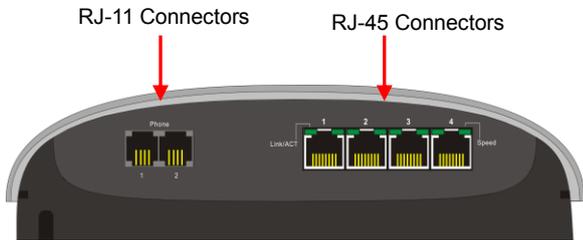


Figure 1-1. Front Panel

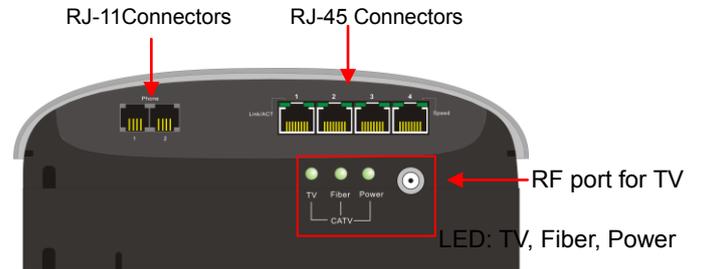


Figure 1-2. Front Panel with RF module

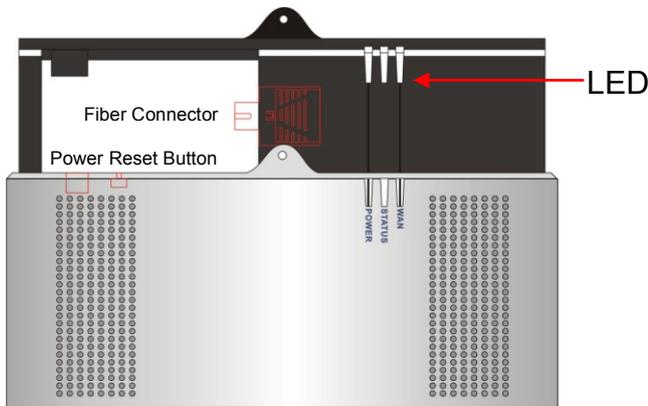


Figure 1-3. Top Panel with Cover Opened

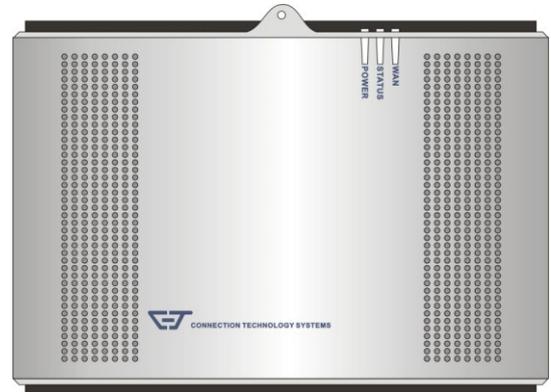


Figure 1-4. Top Panel with Cover Closed

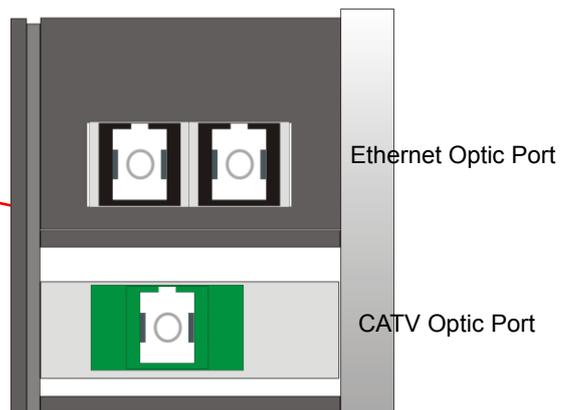
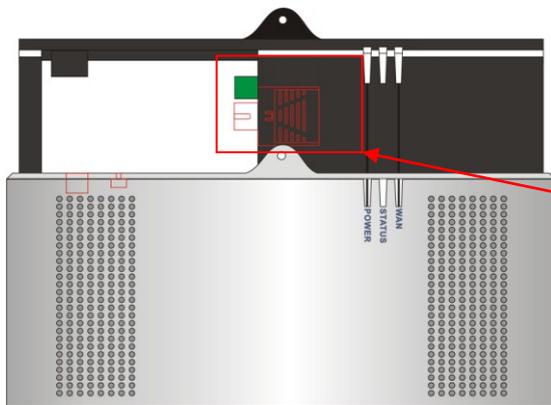


Figure 1-5. Fiber Port Close-up

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.

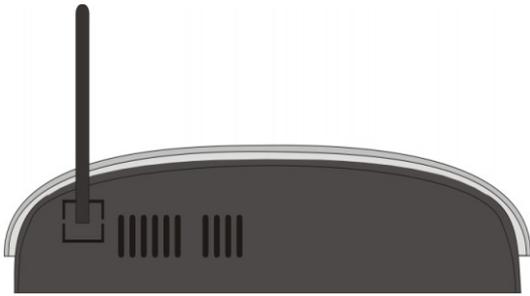


Figure 2-1. Rear Panel for 802.11b/g models

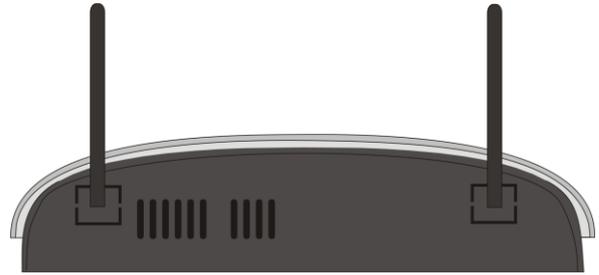


Figure 2-2. Rear Panel for 802.11n models

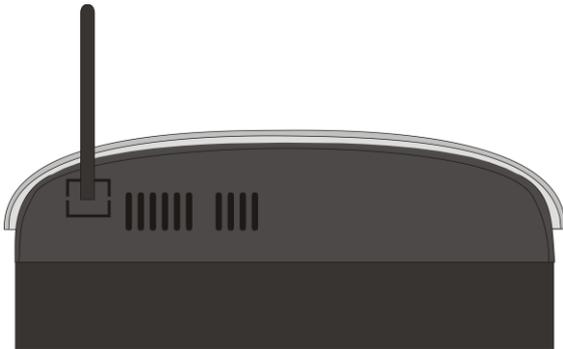


Figure 2-3. Rear Panel for 802.11b/g models with RF module

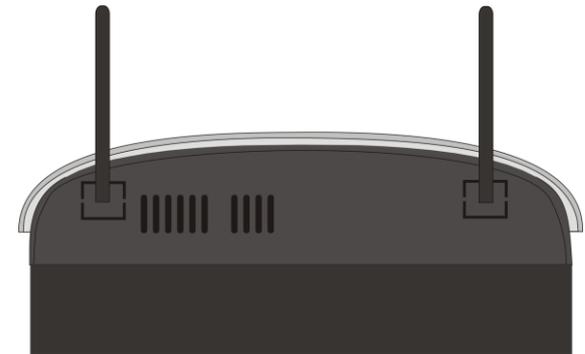


Figure 2-4. Rear Panel for 802.11n models with RF module

1.2 Management Options

Management options available in this Residential Gateway are listed below:

- **Web Management**
Web Management is of course done over the network. Once the Residential Gateway is on the network, you can login and monitor the status remotely or locally by a web browser. Local console-type Web management, especially for the first time use of Residential Gateway to set up the needed IP, can also be done through any of the four 10/100Base-TX 8-pin RJ-45 ports located at the front panel of the Residential Gateway. Direct RJ45 LAN cable connection between a PC and Residential Gateway is required for this.
- **SNMP Management** (See [3. SNMP NETWORK MANAGEMENT](#) for detailed descriptions.)

1.3 Interface Descriptions

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

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

1x100Base-FX Fiber port is located within the upper-left corner of the front top of the Residential Gateway. This port is primarily used for up-link connection and will always operate at 100M/Full Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with other Fast Ethernet Fiber port.

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

4x10/100Base-TX 8-pin RJ-45 ports are located at the front of the Residential Gateway. These RJ-45 ports allow user to connect their traditional copper based Ethernet/Fast Ethernet devices into network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5 cable may be used.

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

1.4 Connecting the Residential Gateway

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

- Connect the power adaptor to the power port of the Residential Gateway on the back, and the other end into a wall outlet. The Power LED should be ON.
- The system starts to initiate. After completing the system test, the Status LED will light up.
- **CAUTION:** For the first-time configuration, connect one end of an Ethernet patch cable (RJ-45) to any ports on the front panel and connect the other end of the patch cable (RJ-45) to the Ethernet port on Administrator computer. LAN LED for the corresponding port will light up.
- Connect one end of an Ethernet patch cable (RJ-45) to other LAN ports of the Router

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

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

1.5 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 WLAN Residential 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 WLAN Residential 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 below for CATV LED descriptions.

1.6 LED Descriptions

LED	Color	Operation
Power	Off	Power is off.
	Green	Power is functioning normally.
WAN	Off	Fiber port link is down or off.
	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.

2. WEB MANAGEMENT

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

2.1 The Concept of IP address

IP addresses have the format n.n.n.n, for example 168.168.8.100.

IP addresses are made up of two parts:

- The first part (168.168 in the example) refers as network address identifies the network on which the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.
- The second part (8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult the allocation organization from which your IP addresses were obtained.

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

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

2.2 Start Configuring

The Residential Gateway can be managed via a Web browser. However, before doing so, you must assign a unique IP address to the Residential Gateway. Use a RJ-45 LAN cable and any of the four 10/100Base-TX RJ-45 ports of Residential Gateway as the temporary RJ-45 Management console port to login to the Residential Gateway and set up the IP address for the first time. (The default IP is “**192.168.0.1**”. You can change the Residential Gateway’s IP to the needed one in the **WAN Settings** under **Network Configuration** menu.)

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

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

1. IP address
 2. Subnet Mask
 3. Default gateway IP address, if required
- Run a Web browser and specify the Residential Gateway's IP address to reach it. (The default IP of Residential Gateway is "192.168.0.1" before any changes.)
 - Login to the Residential Gateway to reach the Main Menu.

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

Login

- Please login

Enter Administrator Name :

Enter Administrator Password :

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

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

NOTE: By default, the remote access to the Residential Gateway is disabled. If you would like to login the Residential Gateway from WAN port or ports assigned in Bridge Mode, you must 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.

VRG-21412-WF-N-RF

- Information
- Network Management
- Switch Management
- Switch Monitor
- SIP Management
- VoIP Management
- CATV Settings
- Management
- Save & Logout

System Information

- System

Company Name	Connection Technology Systems
System Name	VRG-21412-WF-N-RF
System Object ID	.1.3.6.1.4.1.9304.200.21053
System SN.	ABBCDDEF0000000
Firmware Version	1.01.00 (A01)
Host Name	FTTX.Gateway
Date & Time	Thu Jan 1 09:13:33 CST 1970
Up Time	1 hour(s)13 min(s)34 sec(s)
Device Mode	Mode 2
- Fiber Information

Connector	SC
Speed	100
Wave Length	Tx : 1310 Rx : 1310
Distance	30 KM

System Information page for 802.11n models

VRG-21412-WF-G-RF

- Information
- Network Management
- Switch Management
- Switch Monitor
- SIP Management
- VoIP Management
- CATV Settings
- Management
- Save & Logout

System Information

- System

Company Name	Connection Technology Systems
System Name	VRG-21412-WF-G-RF
System Object ID	.1.3.6.1.4.1.9304.200.21053
System SN.	ABBCDDEF0000000
Firmware Version	1.01.00 (A01)
Host Name	FTTX.Gateway
Date & Time	Thu Jan 1 09:10:18 CST 1970
Up Time	10 min(s)26 sec(s)
Device Mode	Mode 2
- Fiber Information

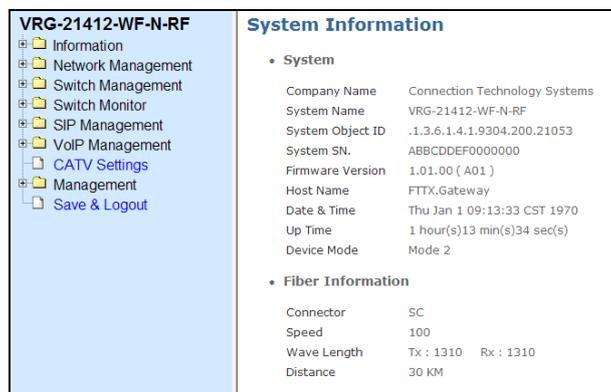
Connector	SC
Speed	100
Wave Length	Tx : 1310 Rx : 1310
Distance	550 M

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.

2.3 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.



- 1. Information:** To display Residential Gateway's system set-up information, including the system information (e.g. location, firmware version, WAN, LAN status, etc.) and the line status (e.g. view-only field that shows the SIP and FXS port status)
- 2. Network Management:** To configure Residential Gateway settings, including WAN and LAN Settings, DHCP, NAT, DDNS, etc.
- 3. Switch Management:** To configure Residential Gateway Ethernet settings, including Port Configuration, Bandwidth Control, VLAN and IGMP settings.
- 4. Switch Monitor:** To show the status of each Residential Gateway port.
- 5. SIP Management:** To configure SIP settings, including SIP Basic/Advanced/Account Settings.
- 6. VoIP Management:** To configure VoIP settings, including Voice, Phone Book, Call server, FAX and FXS port settings, etc.
- 7. CATV Settings:** To enable or disable CATV module (Only available for the WLAN Residential Gateway with RF module installed).
- 8. Management:** The Menu including **Administrator Account**, system **Date/Time** setting, **Ping** test, **Save/Restore** and **Firmware Update**.

9. Save & Logout: To save all configuration changes to the system or logout from the Web Management.

2.4 Information

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

2.4.1 System Information

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

System

• System	
Company Name	Connection Technology Systems
System Name	VRG-21412-WF-N-RF
System Object ID	.1.3.6.1.4.1.9304.200.21053
System SN.	ABBCEDEF0000000
Firmware Version	1.01.00 (A01)
Host Name	FTTX.Gateway
Date & Time	Thu Jan 1 09:13:33 CST 1970
Up Time	1 hour(s)13 min(s)34 sec(s)
Device Mode	Mode 2

Company Name: View-only field that shows the producer or manufacturer of this Residential Gateway.

System Name: View-only field that shows the System name for this Residential Gateway.

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

System S/N.: View-only field that shows the product's serial number.

Firmware Version: View-only field that shows the version of the product's firmware.

Host name: View-only field that shows the Host name of the Residential Gateway.

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

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

Device mode: View-only field that shows the current Residential Gateway operational mode. The device mode can be changed in **WAN Settings**.

Fiber Information

• Fiber Information		
Connector	SC	
Speed	100	
Wave Length	Tx : 1310	Rx : 1310
Distance	30 KM	

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

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

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

Distance: View-only field that shows the maximum distance that this fiber can reach.

WAN

• WAN	
WAN Type	Static IP
MAC Address	00:06:19:03:A0:56
IP Address	192.168.1.198
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
MTU	1500
Packet Info.	RX packets:9750 TX packets:275
DNS 1	192.168.0.1
DNS 2	0.0.0.0

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

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

IP Address: View-only field that shows the unique IP address of WAN interface.

Subnet Mask: View-only field that specifies the subnet mask to be used with the Residential 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 Residential Gateway. This address is required if the Residential 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 Residential Gateway are on the same network.

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

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

DNS1: View-only field that shows the IP address of the primary DNS server which has been either assigned dynamically by your ISP or specified by the user.

DNS2: View-only field that shows the assigned IP address of the secondary DNS server.

LAN

• LAN	
MAC Address	00:06:19:00:00:02
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Packet Info.	RX packets:554 TX packets:311
DHCP Server	Enabled

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

IP Address: View-only field that shows the IP address of LAN interface.

Subnet Mask: View-only field that specifies the subnet mask to be used with the Residential 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 DHCP server is enabled or not.

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.

2.4.2 Line Status

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

Line Status	
• Gateway Status	
TEL Port 1	ONHOOK
TEL Port 2	ONHOOK
• SIP Status	
Port 1 SIP Registered Status	NOT_REGISTERED
Port 2 SIP Registered Status	NOT_REGISTERED
Refresh	

Gateway Status: View-only field that shows the Telephone port (FXS) status of the Residential Gateway.

SIP Status: View-only field that shows whether the Port 1 and Port 2 have registered with the SIP server.

Click the **“Refresh”** button to update the current line status.

2.4.3 CDR

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

Information																																																																				
• Call Detail Record																																																																				
No	Call/Rcv	Phone No	Call Time	Answer Time	Disconnect Time	Disconnect Reason	Duration	TEL Port																																																												
<p>Disconnect reason code definition</p> <table border="0"> <tr> <td>1000</td> <td>Unknown error</td> <td>1001</td> <td>Can't handle a new call</td> </tr> <tr> <td>1002</td> <td>Normal release by remote end</td> <td>1003</td> <td>User cancelled the call</td> </tr> <tr> <td>1004</td> <td>Forbidden</td> <td>1005</td> <td>User not found/Gone</td> </tr> <tr> <td>1006</td> <td>Request timeout</td> <td>1007</td> <td>Conflict</td> </tr> <tr> <td>1008</td> <td>Request Entity Too Large</td> <td>1009</td> <td>Media type unsupported</td> </tr> <tr> <td>100a</td> <td>User temporarily unavailable</td> <td>100b</td> <td>Address is ambiguous/too long/incomplete</td> </tr> <tr> <td>100c</td> <td>User busy</td> <td>100d</td> <td>Internal Server Error</td> </tr> <tr> <td>100e</td> <td>Service not Implemented</td> <td>100f</td> <td>Bad Gateway</td> </tr> <tr> <td>1010</td> <td>Service Unavailable</td> <td>1011</td> <td>Gateway Timeout</td> </tr> <tr> <td>1012</td> <td>Busy Everywhere</td> <td>1013</td> <td>User declined the call</td> </tr> <tr> <td>1014</td> <td>Does Not Exist Anywhere</td> <td>1015</td> <td>Not Acceptable</td> </tr> <tr> <td>2000</td> <td>No more new calls are acceptable on that endpoint</td> <td>2001</td> <td>Poor media quality</td> </tr> <tr> <td>2002</td> <td>Parsing the remote SDP msg failed</td> <td>2003</td> <td>No codecs matching with remote end</td> </tr> <tr> <td>2004</td> <td>No more processing power available</td> <td>2005</td> <td>Remote SDP is not received</td> </tr> <tr> <td>2006</td> <td>Disconnection after blind transfer</td> <td></td> <td></td> </tr> </table>									1000	Unknown error	1001	Can't handle a new call	1002	Normal release by remote end	1003	User cancelled the call	1004	Forbidden	1005	User not found/Gone	1006	Request timeout	1007	Conflict	1008	Request Entity Too Large	1009	Media type unsupported	100a	User temporarily unavailable	100b	Address is ambiguous/too long/incomplete	100c	User busy	100d	Internal Server Error	100e	Service not Implemented	100f	Bad Gateway	1010	Service Unavailable	1011	Gateway Timeout	1012	Busy Everywhere	1013	User declined the call	1014	Does Not Exist Anywhere	1015	Not Acceptable	2000	No more new calls are acceptable on that endpoint	2001	Poor media quality	2002	Parsing the remote SDP msg failed	2003	No codecs matching with remote end	2004	No more processing power available	2005	Remote SDP is not received	2006	Disconnection after blind transfer		
1000	Unknown error	1001	Can't handle a new call																																																																	
1002	Normal release by remote end	1003	User cancelled the call																																																																	
1004	Forbidden	1005	User not found/Gone																																																																	
1006	Request timeout	1007	Conflict																																																																	
1008	Request Entity Too Large	1009	Media type unsupported																																																																	
100a	User temporarily unavailable	100b	Address is ambiguous/too long/incomplete																																																																	
100c	User busy	100d	Internal Server Error																																																																	
100e	Service not Implemented	100f	Bad Gateway																																																																	
1010	Service Unavailable	1011	Gateway Timeout																																																																	
1012	Busy Everywhere	1013	User declined the call																																																																	
1014	Does Not Exist Anywhere	1015	Not Acceptable																																																																	
2000	No more new calls are acceptable on that endpoint	2001	Poor media quality																																																																	
2002	Parsing the remote SDP msg failed	2003	No codecs matching with remote end																																																																	
2004	No more processing power available	2005	Remote SDP is not received																																																																	
2006	Disconnection after blind transfer																																																																			

Call/Rcv: View-only field that shows whether the user is a caller or a receiver.

Phone NO.: View-only field that shows the phone number of incoming or outgoing calls.

Call Time: View-only field that shows the time when the phone is rang.

Answer Time: View-only field that shows the time when the call is answered.

Disconnect Time: View-only field that shows the time when the call is disconnected.

Disconnect Reason: View-only field that shows the corresponding disconnect reason code.

Duration: View-only field that shows the answering time period of an incoming and outgoing call.

TEL Port: View-only field that shows which telephone port is used.

2.4.4 Syslog Table

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



Syslog Message: The Syslog Table lists the latest 500 system log messages. The user can select what log 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.

2.5 Network Management

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

2.5.1 WAN Setting

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

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: 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

NAT/Bridge Mode: There are 5 modes (Mode 0 ~ Mode 4) in the pull-down menu for selection. According to the application connected to this Residential Gateway, you can select the appropriate mode by referring to the table below:

Mode	Bridge	NAT
0	Pure 5-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**.

- Static IP:** If you choose Static IP, you will need to enter 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: 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: 192.168.0.1

Secondary DNS Server: 0.0.0.0

Ping from WAN: Allowed

Host Name: The Host Name is optional but may be required or defined by the user. The default host name is the device name of the Residential Gateway and may be changed.

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

Subnet Mask: Specify the subnet mask with the Residential 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 Residential Gateway. This address is required if the Residential 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 Residential Gateway are on the same network.

Static IP MTU: Static IP MTU (Maximum Transmission Unit) can be changed for optimal performance. 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 Residential 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 IP address of the DNS server.

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

Ping from WAN: Blocking the Ping may provide some extra security from hackers. Tick this checkbox to allow the WAN port to be pinged.

- DHCP:** Choose DHCP to obtain WAN IP Address information automatically from DHCP server. The **DHCP** 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: FTX - Gateway

DHCP MTU: 1500 bytes

Set DNS server: Manually Automatically

Ping from WAN: Allowed

DHCP MTU: You can change the DHCP MTU for optimal performance. 1500 is the default MTU.

Set DNS server: Choose one of the two options - Manually or Automatically

Primary DNS Server: If you choose **Manually**, you need to specify the IP address of the DNS server.

Secondary DNS Server: Specify the secondary DNS server.

Ping from WAN: Blocking the Ping may provide some extra security from hackers. Tick this checkbox to allow the WAN port to be pinged.

3. **PPPoE:** Choose PPPoE to obtain WAN IP Address information, the **PPPoE** screen page appears as follows:

Network Management

- WAN Setting

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

WAN Port IP Assignment: Static IP DHCP PPPoE

Host Name: FTTX . Gateway

PPPoE Username: PPPOE_USERNAME

PPPoE Password: *****

PPPoE MTU: 1492 bytes

Set DNS server: Manually Automatically

Ping from WAN: Allowed

PPPoE Username: Enter your PPPoE username.

PPPoE Password: Enter your PPPoE password.

PPPoE MTU: You can change the PPPoE MTU for optimal performance. 1492 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 Residential 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 IP address of the DNS server.

Secondary DNS Server: Specify the secondary DNS server.

Ping from WAN: Blocking the Ping may provide some extra security from hackers. Tick this checkbox to allow the WAN port to be pinged.

2.5.2 LAN Setting

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

Network Management

- LAN Settings
 - LAN IP Address: 192.168.0.1
 - Subnet Mask: 255.255.255.0
 - DNS Proxy: Enable
- DHCP Server Settings
 - DHCP Server: Enable
 - Assigned DHCP IP Address
 - Start IP: 192.168.0. 100
 - End IP: 192.168.0. 250
 - DHCP IP Lease Time: 21600 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
2	Will_Kao_NB	00:13:a9:fc:c2:5e	192.168.0.100	Thu Jan 1 08:05:20 1970

LAN Settings

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

Subnet Mask: Specify the subnet mask to be used with the Residential Gateway IP address. The available subnet mask values are listed from the pull-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 Residential 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 Residential 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 Residential 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 will display “Dynamic” only.

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 assigned by the DHCP server.

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

2.5.3 WLAN Setting

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

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 NONE

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.

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: WEP
 - Authentication: Open System
 - WEP Key Length: 64-bit WEP

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).

Key 1 HEX ASCII
 Key 2 HEX ASCII
 Key 3 HEX ASCII
 Key 4 HEX ASCII

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).

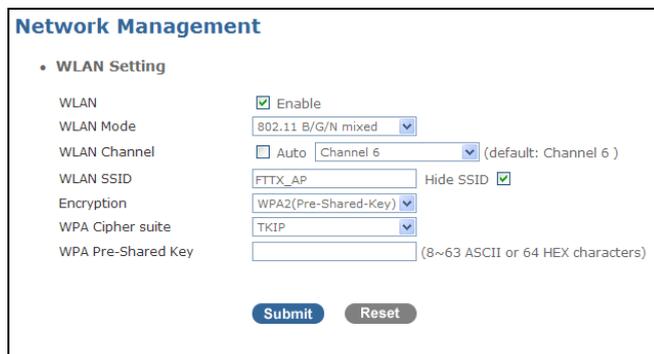
Network Management

- 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)

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.



The screenshot shows the 'Network Management' interface with the 'WLAN Setting' section expanded. The settings are as follows: WLAN is checked 'Enable'; WLAN Mode is set to '802.11 B/G/N mixed'; WLAN Channel has 'Auto' unchecked and 'Channel 6' selected; WLAN SSID is 'FTTX_AP' with 'Hide SSID' checked; Encryption is set to 'WPA2(Pre-Shared-Key)'; WPA Cipher suite is set to 'TKIP'; and the WPA Pre-Shared Key field is empty. At the bottom are 'Submit' and 'Reset' buttons.

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.

2.5.4 WLAN Access Policy

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



The screenshot shows the 'Network Management' interface with the 'Access Policy Setting' section expanded. The 'Access Policy' dropdown is set to 'Allow all'. Below it is an empty 'Access Control List' text area. At the bottom are 'Insert to list', 'Delete from list', 'Submit', and 'Reset' buttons.

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.

2.5.5 Static Route

The Residential 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 Residential Gateway to respond to remote management stations that are not reachable through the default gateway, for example when sending SNMP traps or using ping packets to test IP connectivity.

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



The screenshot shows the 'Network Management' interface with a sub-section for 'Static Route'. It features a table with columns for 'Enable', 'Type', 'Target', 'Netmask', 'Gateway', and 'Action'. The 'Enable' column has a checkbox. The 'Type' column has a dropdown menu with 'Net' selected. The 'Netmask' column has a dropdown menu with '255.255.255.0' selected. The 'Action' column has 'Insert' and 'Change' buttons.

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

Enable: Tick the checkbox to turn on this static route rule.

Type: Specify the Type to be used with the Residential Gateway IP address. The types available are listed in the pull-down menu with 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: Select the subnet mask for this destination from the pull-down menu.

Gateway: Specify the default gateway IP address.

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

2.5.6 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, then the **NAT** screen page appears as follows.

Network Management

- NAT Setting**
 - Network Address Translation Enable
 - DMZ Enable
 - DMZ LAN IP
 - DDOS Protection Enable
 - Detection Frequency
 -
- Virtual Server Mapping**

Enable	WAN Port	Protocol	LAN IP	LAN Port	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
- Port Trigger**

Enable	Trigger Port	Trigger Type	Public Port	Public Type	Action
<input type="checkbox"/>	<input type="text"/>	TCP	<input type="text"/>	TCP	<input type="button" value="Insert"/> <input type="button" value="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 Residential 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 Residential Gateway to detect SYN flooding attacks. By default, this function is disabled which makes your device vulnerable to attacks. To prevent your Residential Gateway from open malicious attacks, you should enable DDoS Protection manually.

Detection Frequency: Specify the frequency of attack requests to Residential Gateway. When Residential 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 Residential 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 Residential 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 Residential 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 Residential Gateway. Change - To modify the current setting.

2.5.7 Packet Filter

This Residential 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, then **Packet Filter** screen page appears.

Network Management

• Packet Filter

WAN Enable

Enable	Public 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.

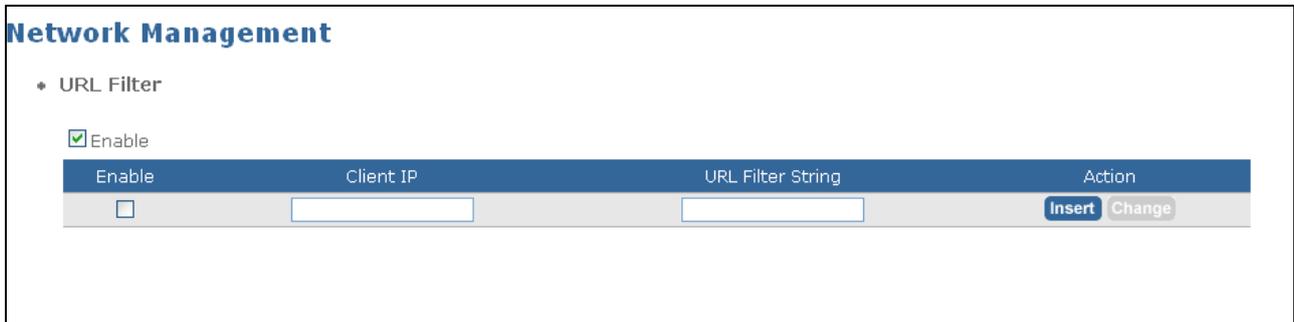
- Always (always block which means that access to the requested service will be denied)
- By schedule (follow “Day” and “time” field setting)

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

2.5.8 URL Filter

This feature allows users to create a list of websites or client IP address that you want to either allow or deny users' access.

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



The screenshot shows the 'Network Management' interface with the 'URL Filter' section expanded. It features a table with columns for 'Enable', 'Client IP', 'URL Filter String', and 'Action'. The 'Enable' column has a checked checkbox. The 'Client IP' and 'URL Filter String' columns have empty text input fields. The 'Action' column contains 'Insert' and 'Change' buttons.

Enable	Client IP	URL Filter String	Action
<input checked="" 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 from accessing 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.

2.5.9 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. In turn, a device can leave a network smoothly and automatically.

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

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

UPnP Setting

UPnP Internet Gate Device: Tick this checkbox then click Submit button to enable UPnP feature. UPnP provides compatibility with networking equipment, 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 Residential 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.

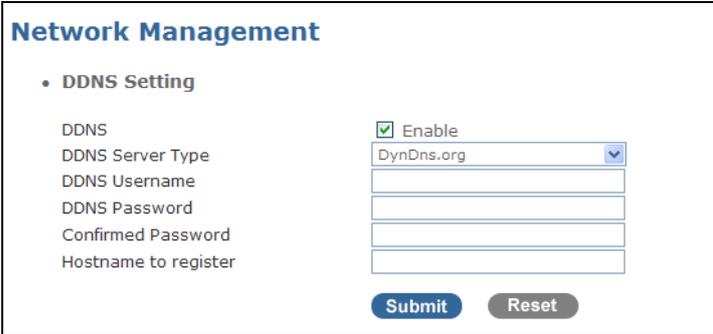
Duration: View-only field. This rule will be disabled when the duration is timeout.

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

2.5.10 DDNS

The WLAN Gateway supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any domains, allowing 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 that makes it 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 setup with one of the supported DDNS providers.

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



The screenshot shows the 'Network Management' interface with a sub-section for 'DDNS Setting'. It includes a checkbox for 'Enable' (checked), a dropdown menu for 'DDNS Server Type' (set to 'DynDns.org'), and input fields for 'DDNS Username', 'DDNS Password', 'Confirmed Password', and 'Hostname to register'. There are 'Submit' and 'Reset' buttons at the bottom.

DDNS: Enable DDNS global setting, if checked.

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

DDNS User name: Enter the username given to you by your DDNS server.

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

Confirmed password: Re-enter DDNS password.

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

2.5.11 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 WLAN Residential Gateway through the network via SNMP version one (SNMPv1), SNMP version 2c.



The screenshot shows a configuration page titled "Network Management" with a sub-section "SNMP Setting". The settings are as follows:

Setting	Value	Default
SNMP	<input checked="" type="checkbox"/> Enable	
SNMP Read Community	public	(default:public)
SNMP Write Community	private	(default:private)
SNMP Trap Host		
SNMP Trap Community	public	(default:public)
SNMP Power Down Trap	<input type="checkbox"/> Enable	

At the bottom of the form are two buttons: "Submit" and "Reset".

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.

2.6 Switch Management

In this section, users can setup several advanced features. Select **Switch Management** from the **Main Menu**, the sub-items – **Port Configuration**, **Bandwidth Control**, **Configure VLAN** and **IGMP Snooping** – will show up.

2.6.1 Port Configuration

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

Switch Management							
• Port Configuration							
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 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 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 pull-down menu.

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

2.6.2 Bandwidth Configuration

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

• 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)				
<input type="button" value="Submit"/> <input type="button" value="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.

2.6.2.1 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.

2.6.2.1.1 By Port Only

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

The screenshot shows the 'Switch Management' configuration page. Under 'Egress QoS Control', the 'Bandwidth Mode' is set to 'By Port Only'. Below this, a table shows bandwidth settings for various ports:

Port	Port.1	Port.2	Port.3	Port.4	NAT Download stream	NAT Upload stream	WAN
Bandwidth	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.

2.6.2.1.2 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.

The screenshot shows the 'Switch Management' configuration page. Under 'Egress QoS Control', the 'Bandwidth Mode' is set to 'By Port with Queue'. Below this, a table shows queue mapping for various ports:

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

Below the table, there is a section for '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).

2.6.2.1.3 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.

The screenshot shows the 'Switch Management' configuration page. Under 'Egress QoS Control', the 'Bandwidth Mode' is set to 'By DSCP'. The 'By DSCP' section shows a 'DSCP Map' dropdown set to 'DSCP(0)' and a 'Queue' dropdown set to 'Q0'. Below this is a table for mapping DSCP values to queues:

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

At the bottom, the 'Reserve Min. Egress Bandwidth of Queue' table is shown:

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).

2.6.2.1.4 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							

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).

2.6.2.1.5 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	0	0	Q0
2	Doesn't Compare	0	0	Q0
3	Doesn't Compare	0	0	Q0
4	Doesn't Compare	0	0	Q0
5	Doesn't Compare	0	0	Q0
6	Doesn't Compare	0	0	Q0
7	Doesn't Compare	0	0	Q0
8	Doesn't Compare	0	0	Q0

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)

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).

2.6.2.2 Ingress Bandwidth Setting

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

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

Submit Reset

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).

2.6.3 Configure VLAN

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

Switch Management

Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID	1	1	1	1
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
3	0	U	T	U	U	Edit

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 VLAN 2 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.

2.6.4 Traffic Flow for Bridge & NAT Mode

The Residential 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.

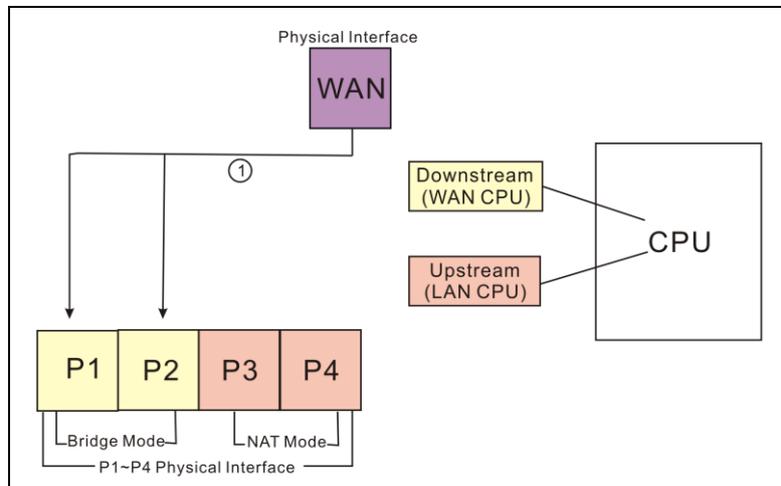


Figure 1: Traffic Flow for Bridge Mode

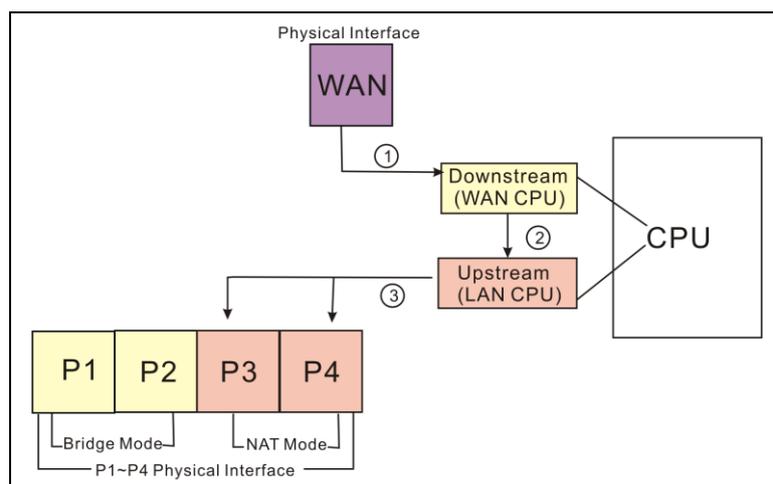


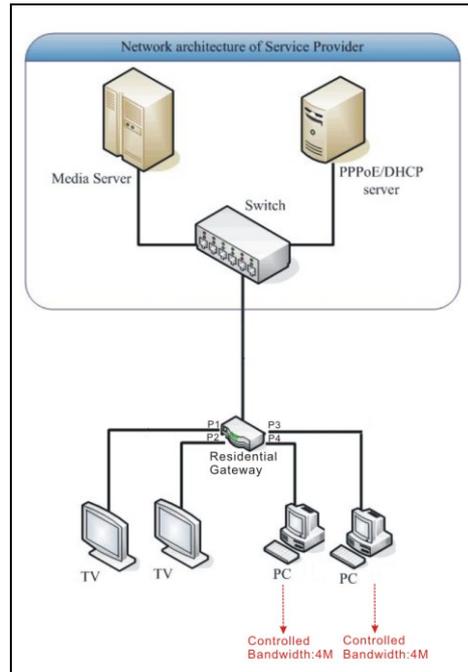
Figure 2: Traffic Flow for NAT Mode

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.

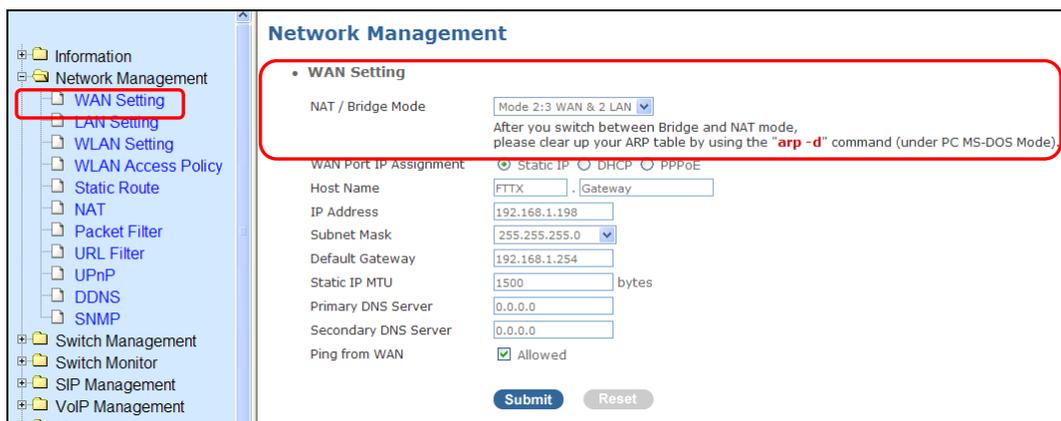
2.6.5 Bandwidth Control Setup Examples

Scenario I:

In this scenario, the WLAN 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 WLAN 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



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

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

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

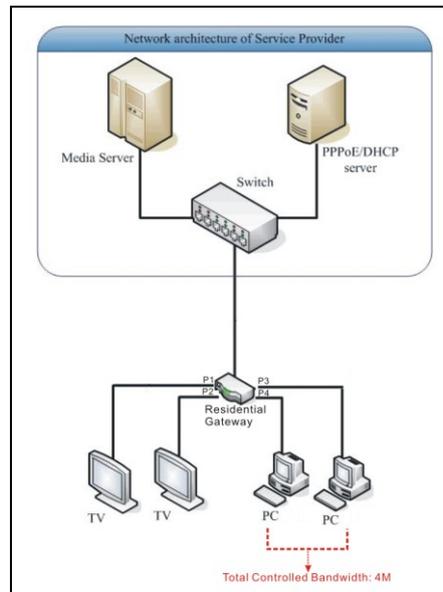
In this scenario, "Bandwidth Control" can be configured to control the outbound (egress) bandwidth to PC devices. To limit the bandwidth to 4Mbps for both Port 3 and Port 4, "By Port Only" Bandwidth Mode can be used to achieve this goal.

Select “By Port Only”:

- 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 WLAN 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 WLAN 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

The screenshot shows the 'Network Management' interface. On the left is a tree view with 'WAN Setting' highlighted. The main panel is titled 'WAN Setting' and contains the following configuration options:

- NAT / Bridge Mode:** Mode 2:3 WAN & 2 LAN (selected)
- WAN Port IP Assignment:** Static IP (selected), 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

Buttons for 'Submit' and 'Reset' are located at the bottom of the configuration panel.

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

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

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	0	U	T	-	-	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
1100	0	-	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.
- 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 Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: OFF
- **Ingress Bandwidth**

Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	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

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)				

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

Port	Port.1	Port.2	Port.3	Port.4	WAN
Map to Q	Q0	Q0	Q0	Q0	Q1
 - Reserve Min. Egress Bandwidth of Queue

Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	4096 (K)	102400 (K)	102400 (K)	102400 (K)
- Ingress Bandwidth Control

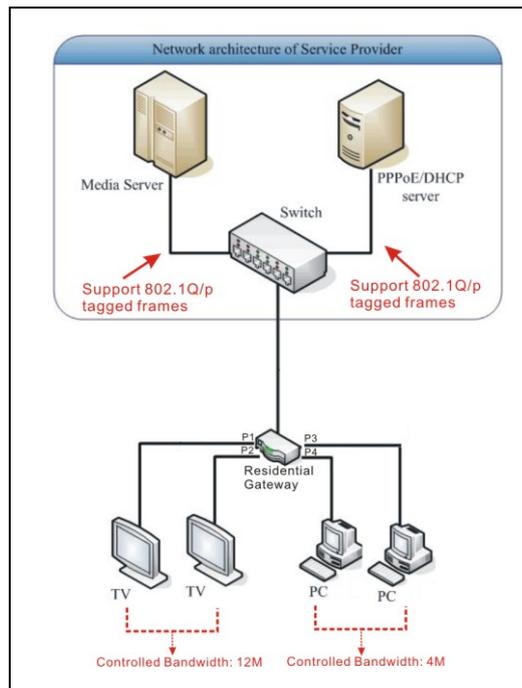
Port	Port.1	Port.2	Port.3	Port.4	WAN
Enabler	Disable	Disable	Disable	Disable	Disable
Bandwidth	102400 (K)				

Settings changed, still not saved.

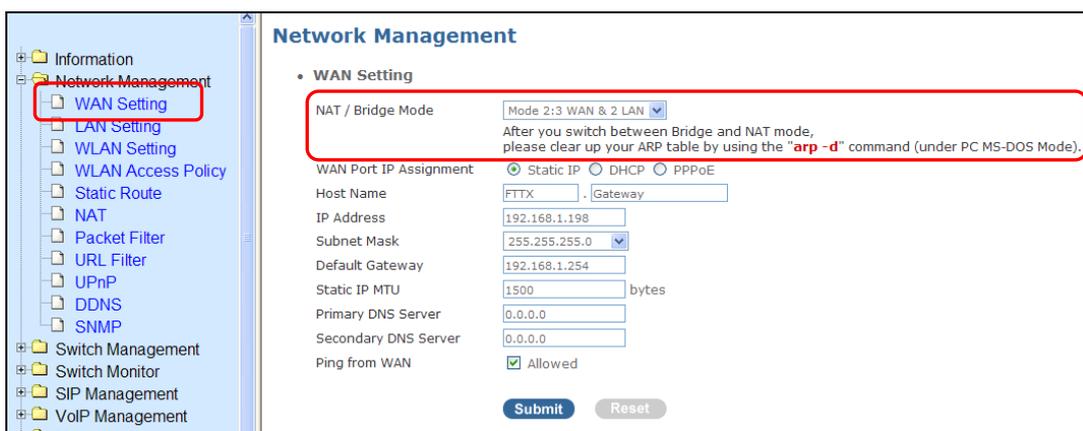
- Select each port’s corresponding queue. Set Port 1, 2, 3, and 4’s queue to Q0 and WAN’s queue to Q1. **By default, when “By Port with Queue” bandwidth mode is selected, (Upstream & Downstream) CPU belongs to Q0 and this queue setting for CPU can not be modified. For LAN and WAN traffic flow, please 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 WLAN 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 WLAN 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



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

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

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	4	U	T	-	-	Edit Delete
1100	5	-	T	U	U	Edit 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 Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: OFF
- **Ingress Bandwidth Control**

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

Submit Reset

Select “By 802.1p”:

Switch Management

- **Bandwidth Range**
Min. Bandwidth Unit: 1024K~100M (Min. unit size 1024k)
- **Egress QoS Control**
Bandwidth Mode: By 802.1p
- **Map to Q**
- **Reserve Min. Egress Bandwidth of Queue**
- **Ingress Bandwidth Control**

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	Q0	Q1	Q3	Q3

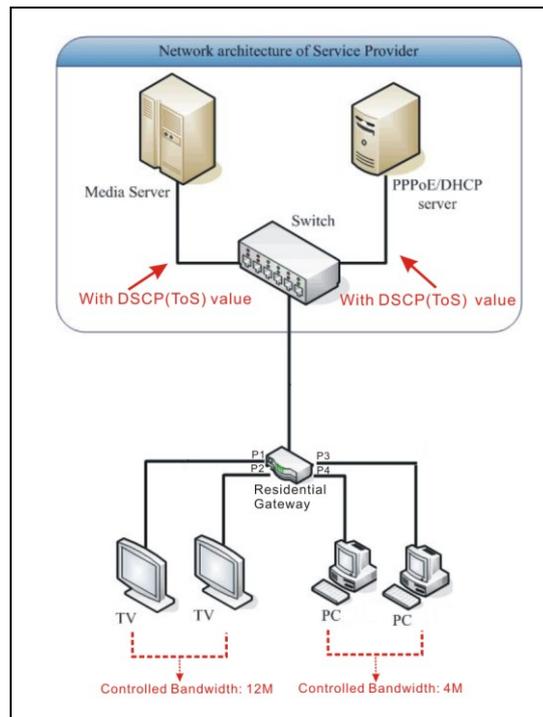
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	4096 (K)	12288 (K)	102400 (K)	102400 (K)

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

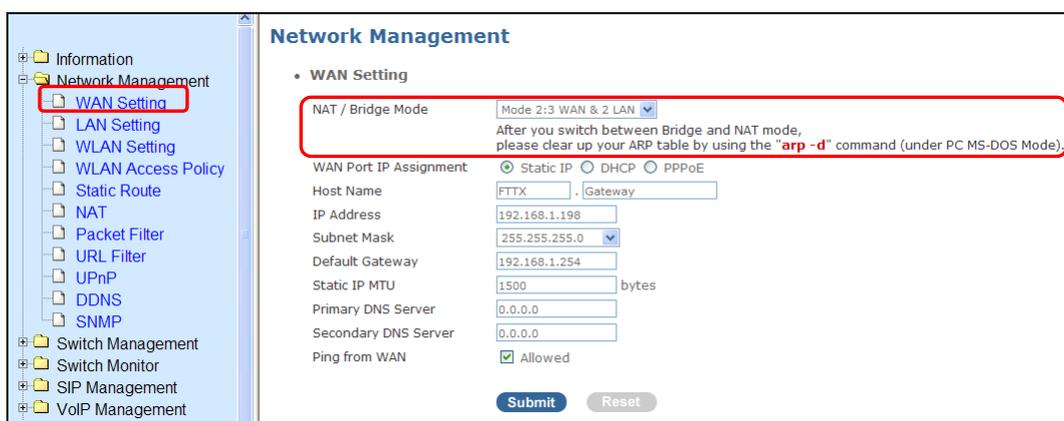
- Map P-bit 4 to Q0 and P-bit 5 to Q1.
- Set Queue 0's reserved bandwidth to 4096K and Queue 1's reserved bandwidth to 12288K.

Scenario IV:

In this scenario, the WLAN 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 WLAN 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



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

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

Buttons: 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

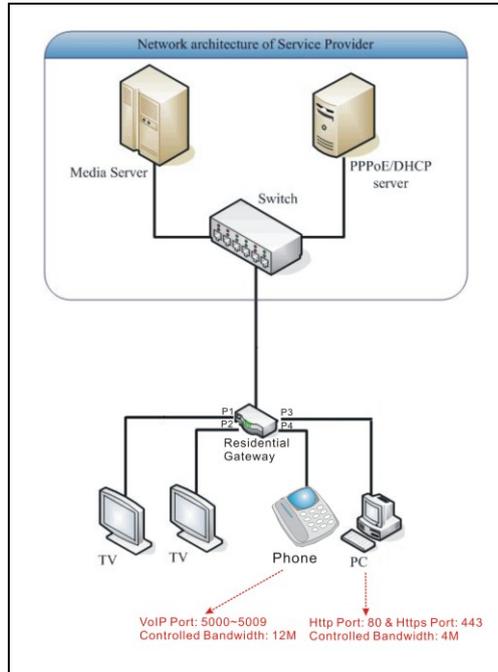
DSCP	Queue
Q0-DSCP	0~39, 48~63
Q1-DSCP	40~47
Q2-DSCP	
Q3-DSCP	

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.

Scenario V:

In this scenario, the WLAN Residential Gateway supports VoIP, IPTV application and internet access. As illustrated in Figure 6, IPTV applications are connected to Port 1 (P1) and Port 2 (P2); VoIP application is connected to Port 3 (P3) and one PC device is connected to Port 4 (P4) to access the internet. If you would like the WLAN Residential Gateway to control how much traffic gets forwarded for VoIP application (Port 5060) and Internet access (Port 80) as wished (12Mbps for VoIP, 4Mbps for Internet), you can follow the suggested setup steps below.



Step 1. Set Up NAT/Bridge Mode

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 Application” can be used to prioritize the egress bandwidth to 12Mbps for VoIP application and 4Mbps for Internet access.

Switch Management

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

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

Submit Reset

Select “By Application”:

Egress QoS Control

Bandwidth Mode: By Application

By Application

No.	Compare	Port Start	Port End	Queue
1	Destination or Source	5000	5009	Q3
2	Destination or Source	80	80	Q2
3	Destination or Source	443	443	Q2
4	Doesn't Compare	0	0	Q0
5	Doesn't Compare	0	0	Q0
6	Doesn't Compare	0	0	Q0
7	Doesn't Compare	0	0	Q0
8	Doesn't Compare	0	0	Q0

Reserve Min. Egress Bandwidth of Queue

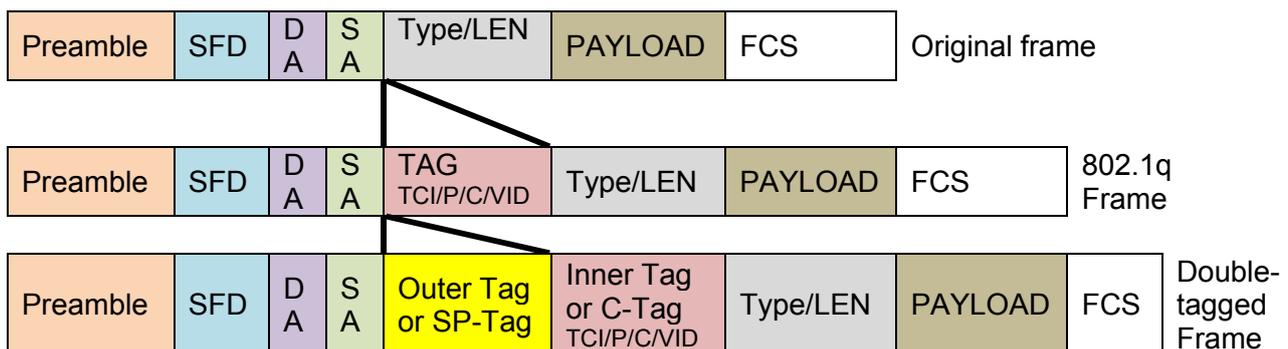
Queue	Queue-0	Queue-1	Queue-2	Queue-3
Reserve BW	102400 (K)	102400 (K)	4096 (K)	12288 (K)

- Set up rule No.1 for limiting VoIP Port 5000~5009 bandwidth.
 - Select “Destination or Source”. This means that both Destination Address and Source Address with the specified port number will follow the bandwidth setting.
 - Set Port Start to 5000 and Port End to 5009.
 - Select Q3 (highest priority).
- Set up rule No.2 for limiting Http Port 80 bandwidth.
 - Select “Destination or Source”. This means that both Destination Address and Source Address with the specified port number will follow the bandwidth setting.
 - Set Port Start and Port End to 80.
 - Select Q2.

- Set up rule No.3 for limiting Https Port 443 bandwidth.
 - Select “Destination or Source”. This means that both Destination Address and Source Address with the specified port number will follow the bandwidth setting.
 - Set Port Start and Port End to 443.
 - Select Q2.
- Set Queue 2’s reserved bandwidth to 4096K.
- Set Queue 3’s reserved bandwidth to 12288K.

2.6.6 Configure Q-in-Q

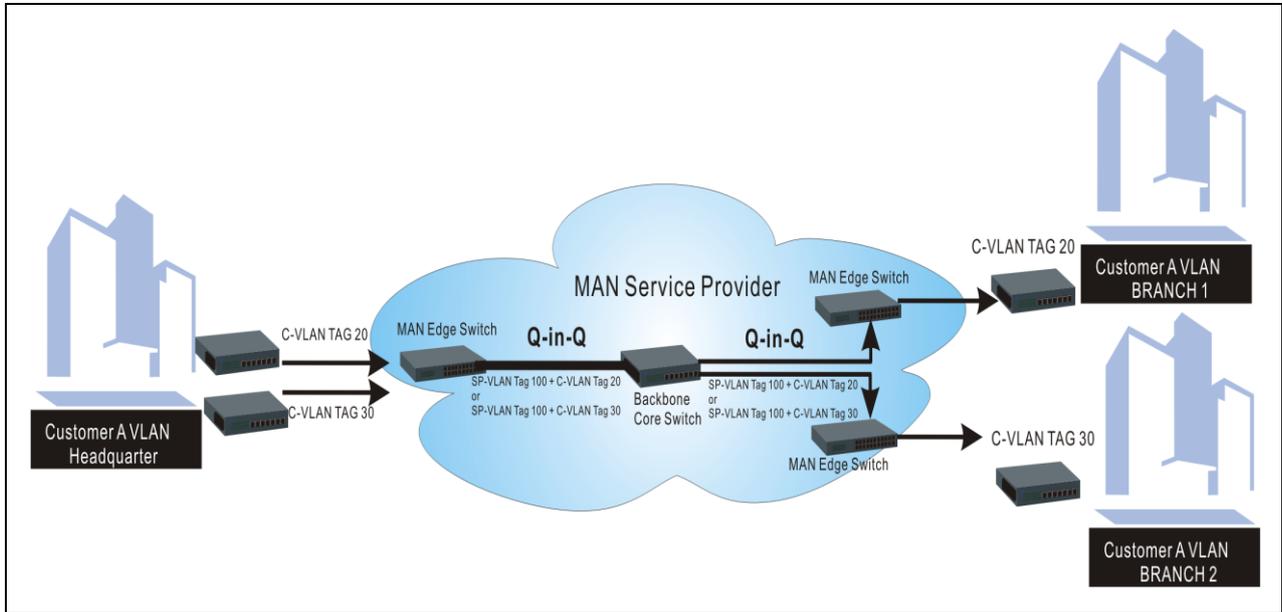
The IEEE 802.1Q double tagging VLAN is also referred to Q-in-Q or VLAN stacking (IEEE 802.1ad). Its purpose is to expand the 802.1q VLAN space by tagging the inner tagged packets. In this way, a “double-tagged” frame is created so as to separate customer traffic within a service provider network. As 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

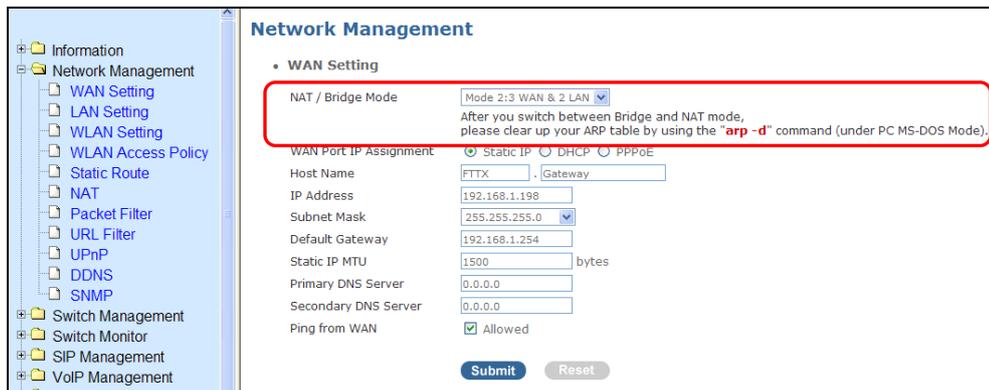
to customers is to encapsulate the original VLAN with a second VLAN ID of 100. This second VLAN ID is known as SP-VLAN (Service Provider VLAN) that is added as data enters the service provider's network and then removed as data exits. Eventually, with the help of SP-Tag, the information sent from Headquarter 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



- 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

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"/>

Submit Reset

VID 2 is reserved for internal use.

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

Submit Reset

VID 2 is reserved for internal use.

VID	P-Bit	NAT Interface	WAN	Port .1	Port .2	Action
	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	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

Switch Management

- Configure VLAN

Port Number	NAT Interface	WAN	Port .1	Port .2
Default VLAN ID				
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
	0	-	-	-	-	Insert Change
1	0	U	U	U	U	Edit
2	0	-	-	-	-	Edit
100	0	-	T	T	-	Edit Delete

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.

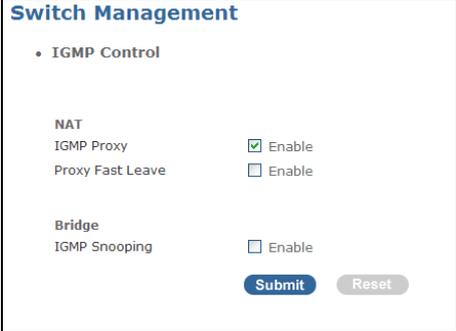
2.6.7 IGMP Control

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 Residential 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. And, 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 gateway using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the gateway and also reduces the workload at the end hosts.

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



The screenshot shows a web interface titled "Switch Management" with a sub-section "IGMP Control". Under the "NAT" section, there are two options: "IGMP Proxy" which is checked and labeled "Enable", and "Proxy Fast Leave" which is unchecked and labeled "Enable". Under the "Bridge" section, there is one option: "IGMP Snooping" which is unchecked and labeled "Enable". At the bottom of the form are two buttons: "Submit" and "Reset".

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.

2.7 Switch Monitor

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

The screenshot shows the 'Switch Monitor' interface. It has two main sections: 'Port State Settings' and 'Switch Port State'.

Port State Settings:

- Port State Polling: Enable
- Polling Time: seconds
- Buttons: Submit, Reset

Switch Port State:

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

Buttons: Refresh

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 in full or half duplex mode.

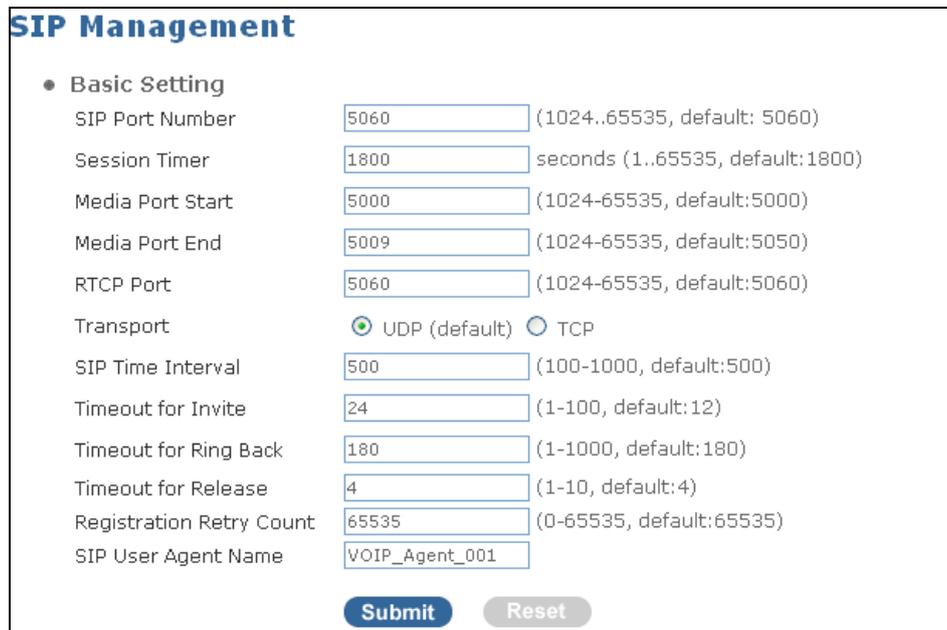
Flow Control: View-only field that shows whether each port's flow control function is enabled or disabled.

2.8 SIP Management

Select **SIP Management** from the **Main Menu**, the sub-item – **Basic setting**, **Account setting**, and **Server setting** – will show up.

2.8.1 Basic Setting

Select **Basic Setting** from the **SIP Management** menu, then **Basic Setting** screen page appears.



The screenshot shows the 'SIP Management' configuration page with the 'Basic Setting' tab selected. The page contains several configuration fields, each with a text input box and a range/default value in parentheses. The fields are: SIP Port Number (5060), Session Timer (1800 seconds), Media Port Start (5000), Media Port End (5009), RTCP Port (5060), Transport (radio buttons for UDP (selected) and TCP), SIP Time Interval (500), Timeout for Invite (24), Timeout for Ring Back (180), Timeout for Release (4), Registration Retry Count (65535), and SIP User Agent Name (VOIP_Agent_001). At the bottom, there are 'Submit' and 'Reset' buttons.

Field	Value	Range/Default
SIP Port Number	5060	(1024..65535, default: 5060)
Session Timer	1800	seconds (1..65535, default:1800)
Media Port Start	5000	(1024-65535, default:5000)
Media Port End	5009	(1024-65535, default:5050)
RTCP Port	5060	(1024-65535, default:5060)
Transport	UDP (default)	UDP (default) / TCP
SIP Time Interval	500	(100-1000, default:500)
Timeout for Invite	24	(1-100, default:12)
Timeout for Ring Back	180	(1-1000, default:180)
Timeout for Release	4	(1-10, default:4)
Registration Retry Count	65535	(0-65535, default:65535)
SIP User Agent Name	VOIP_Agent_001	

SIP Port Number: Specify the IP phone number. The number ranges from 1024 to 65535. The default setting is 5060.

Session Timer: Specify the time interval in seconds to refresh SIP. The default setting is 1800 seconds.

Media Port Start: Specify the media port Start number for RTP.

Media Port End: Specify the media port End number for RTP.

RTCP: Specify the RTCP port number.

Transport: Choose either UDP or TCP. The default SIP transport type is UDP.

SIP Time Interval: Specify SIP time interval in milliseconds. The default setting is 500 msec.

Time out for Invite: Specify the time interval for Invite message timeout. The Invite message will be dropped if a response is not received within the designated time.

Time out for Ring back: Specify the timeout time for ring back.

Time out for Release: Specify the Release time.

Registration Retry Count: Specify the time interval for registration retry time.

SIP User Agent Name: Specify SIP User Agent Name.

2.8.2 Account Setting

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

The screenshot shows the 'SIP Management' interface with a sub-section for 'Account Setting'. Under 'Port 1', there is a list of configuration fields:

Field Name	Value
User Name	100
Display Name	100
Authentication User Name	100
Authentication Password	•••
Confirmed Password	•••
MWI	<input checked="" type="checkbox"/> Enable(default:Disabled)
P-Asserted	<input checked="" type="checkbox"/> Enable (default:Disabled)
Asserted Identity URI	100
Asserted Identity Displayname	100

User name: Specify a user name for Port 1 or Port 2.

Display Name: Specify a display name for Port 1 or Port 2.

Authentication User Name: Specify an authentication name for Port 1 or Port 2.

Authentication Password: Specify an authentication password for Port 1 or Port 2.

Confirmed Password: Re-type the authentication password to confirm.

MWI: MWI stands for Message Waiting Indication. To enable your phone to give you a message–waiting (beeping) dial tone when you have one or more voice messages, your VoIP service provider must have a messaging system that sends message-waiting-status SIP packets as defined in RFC 3842.

P-Asserted: To enable P-Asserted identity. If enabled, this allows the network to assert a public user identity for a calling user.

Asserted Identity URI: Specify the P-asserted identity number.

Asserted Identity Display Name: Specify the display name for P-asserted identity.

2.8.3 Server Setting

Select **Server Setting** from the **SIP Management** menu, then **Server Setting** screen page appears.

The screenshot shows the 'SIP Management' interface with a 'Server Setting' section. It includes fields for 'Authentication Expired Time' (3600 seconds), 'Use Outbound Proxy for All Messages' (checked), and two sections: 'Port 1' and 'Port 2'. 'Port 1' contains settings for 'Register' (checked), 'Registrar Server Address' (61.218.109.83), 'Registrar Server Port' (5060), 'Proxy Address' (61.218.109.83), 'Proxy Port' (5060), 'Use Outbound Proxy' (checked), 'Outbound Proxy Address' (61.218.109.83), 'Outbound Proxy Port' (5060), and 'DNS SRV support' (checked). 'Port 2' has a 'Register' checkbox that is unchecked. 'Submit' and 'Reset' buttons are at the bottom right.

Authentication Expired Time: Specify SIP authentication expired time in seconds. The default setting is 3600 seconds.

Use Outbound Proxy for all messages: Tick the checkbox to enable outbound proxy.

Register: Tick the checkbox to enable registration.

Register Server Address: Specify the registration server address.

Register Server Port: Specify the registration server port.

Proxy Address: Specify the proxy address of the SIP server.

Proxy Port: Specify the proxy port of the SIP server.

Use Outbound Proxy: Tick the checkbox to use outbound proxy.

Outbound Proxy Address: When outbound proxy is enabled, you need to further specify the IP address of SIP outbound proxy server.

Outbound Proxy Port: When outbound proxy is enabled, you need to further specify the port number of outbound proxy server.

DNS SRV Support: Tick the checkbox to enable DNS SRV support. When enabled, calls will be routed to the proxy address specified.

2.9 VoIP Management

Select **VoIP Management** from the **Main Menu**, the sub-item – **Voice setting**, **Call service**, and **FXS setting**, etc – will show up.

2.9.1 Voice Setting

Select **Voice Setting** from the **VoIP Management** menu, then **Voice Setting** screen page appears.

• Voice Setting	
Codec Priority 1	G.723
Codec Priority 2	G.729
Codec Priority 3	G.711/Ulaw
Codec Priority 4	G.711/Alaw
Codec Priority 5	G.726(16Kbps)
Codec Priority 6	G.726(24Kbps)
Codec Priority 7	G.726(32Kbps)
Codec Priority 8	G.726(40Kbps)
Codec Priority 9	iLBC

Codec Priority 1~9: Select codec from the drop-down menu for each priority. Code priority 1 will allow the value selected to have the highest priority. On the other hand, code priority 9 will give the value selected the lowest priority.

G.723 Rate	6.3 Kbps	(default:6.3KBps)
iLBC mode	30 msec.	(default:30)
Packet Length	20 msec.	(default:20)
DTMF Method	Out-band 2833 relay	(default:Out-band 2833 relay)
Outband 2833 Payload Type Value	100	(default:100)
RTP Timeout	25	second (1..100, default:25)
RTP Packet Lost Percentage	30	% (0..100, default:30)
Maximum ICMP Unreachable	10	(0..1000, default:10)

G.723 Rate: Choose G.723 Rate from the drop-down menu – 6.3Kbps or 5.3Kbps.

iLBC mode: Choose iLBC mode from the drop-down menu. The default setting is 30 msec.

Packet Length: Choose Packet Length from the drop-down menu. The default setting is 20 msec.

DTMF Method: Choose DTMF Method from the drop-down menu. There are two categories of sending the DTMF tone, these are In-band and Out-band. Select “In-band” options will send the DTMF tone in voice packet. Choose “Out-band” will send the DTMF tone as a RTP payload signal. Sending DTMF tone as a signal could tolerate more packet loss caused by the network. If this selection is enabled, the DTMF tone will be sent as a signal.

Outband 2833 Payload type value: Choose a value from the drop-down menu.

RTP Timeout: Specify a value for RTP timeout.

RTP packet lost Percentage: Specify the packet lost percentage.

Maximum ICMP Unreachable: Specify the maximum ICMP unreachable value.

Outband 2833 Payload type value: Choose a value from the drop-down menu.

The screenshot shows a configuration panel for two ports, Port 1 and Port 2. Each port has a set of five settings, all of which are currently set to 'Disabled' or '24 msec'. The settings are: Voice Active Detector, Line Echo Canceller Tail Length, Acoustic Echo Canceller Tail Length, Automatic Gain Control Tx Level, and Automatic Gain Control Rx Level. At the bottom of the panel, there are two buttons: 'Submit' and 'Reset'.

Voice Active Detector: Select a mode from the drop-down menu. The default setting of this function is disabled.

Line Echo Canceller Tail Length: Select Tail Length for line echo cancellation from the drop-down menu. The echo canceller removes your echo from the returning audio stream without removing responder’s voice.

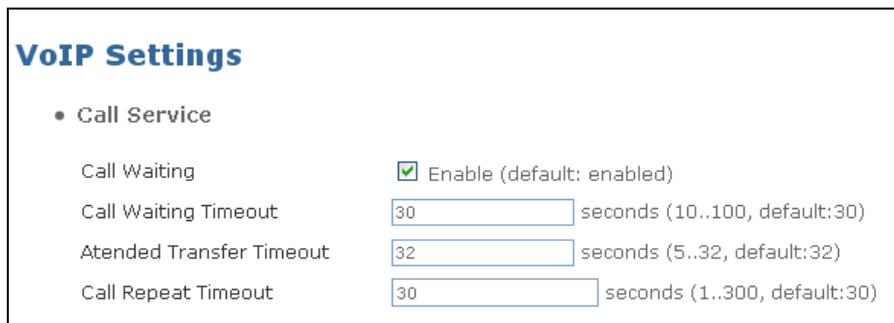
Acoustic Echo Canceller Tail Length: Select Tail Length for acoustic echo cancellation from the drop-down menu.

Automatic Gain Control Tx Level: The transmitting AGC level can be selected is from 0 (0db) to 30 (30db). The default setting is disabled.

Automatic Gain Control Rx Level: The receiving AGC level can be selected is from 0 (0db) to 30 (30db). The default setting is disabled.

2.9.2 Call Service

Select **Call Service** from the **VoIP Management** menu, then **Call Service** screen page appears.



The screenshot shows the 'VoIP Settings' page with a sub-section for 'Call Service'. It includes four settings: 'Call Waiting' (checked), 'Call Waiting Timeout' (30 seconds), 'Attended Transfer Timeout' (32 seconds), and 'Call Repeat Timeout' (30 seconds).

Setting	Value	Unit / Range
Call Waiting	<input checked="" type="checkbox"/>	Enable (default: enabled)
Call Waiting Timeout	30	seconds (10..100, default:30)
Attended Transfer Timeout	32	seconds (5..32, default:32)
Call Repeat Timeout	30	seconds (1..300, default:30)

Call Waiting: The Call Waiting function allows you to answer the second incoming call while you are already on a phone call. When the other caller tries to reach you when you are on the phone, the call waiting feature will send a special tone to notify you of the incoming call. To answer the second incoming call or switch back and forth between two calls, please press Flash button or FlashHook once.

Call Waiting Timeout: Specify Call Waiting timeout in seconds. If you would like to continue with your first call and ignore a waiting call, this is the time that the second caller will wait before disconnecting the waiting call.

NOTE: When Call Waiting function is enabled, Call Forward function will be deactivated. In other words, if you enable Call Waiting function and set up "Call Forward on Busy URI" and "Call Forward on NoAnswer URI" at the same time, the waiting call will be disconnected instead of forwarding to the specified number when time is out.

Attended Transfer Timeout: Specify the time value for Attended Transfer timeout. When time is out and the second called party does not answer the phone, the call will be disconnected.

Call Repeat Timeout: Specify the time value for Call Repeat timeout. If the number you are calling is busy and has no Call Waiting feature enabled, the Call Repeat function allows you to connect to the busy number when the line becomes free.

Port 1	
Call Transfer Option	Allowed
Call Forward Option	Allowed
Call Forward on Busy URI	
Call Forward on NoAnswer URI	
Call Forward Always URI	
Call Forward on NoAnswer Timeout	30 seconds (1..300, default:30)
Do Not Disturb	<input type="checkbox"/> Enable (default: disabled)
Auto Answer	<input type="checkbox"/> Enable (default: disabled)
Auto Answer Timeout	180 seconds (10..300, default:180)
Hot Line	<input checked="" type="checkbox"/> Enable (default: disabled)
Hot Line Number	

Call Transfer Option: Select “Allowed” or “Restricted” for call transfer function. When call transfer is allowed, the user can transfer the incoming and outgoing calls to another SIP number.

Call Forward Option: Select “Allowed” or “Restricted” for call forward function. When call forward is allowed, all calls will be forwarded to the specified phone number depending on different situations (busy, no answer, always forwarding).

Call Forward on Busy URI: Specify the account user name. When the line is busy, incoming calls will be forwarded to the designated number.

Call Forward on NoAnswer URI: Specify the account user name. When the call is not answered, it will be forwarded to the designated number.

Call Forward Always URI: Specify the account user name. All incoming calls are always forwarded.

Call Forward on NoAnswer Timeout: Specify No Answer timeout. When time is out, the call will be forwarded to the specified number.

Do Not Disturb: When enabled, all incoming calls will be rejected (the phone will not ring).

Hot Line: Tick the checkbox to enable Hot Line function. A call will be automatically dialed to the designated number once the handset of the telephone is picked up.

Hot Line Number: Enter the hot line number. A call will be automatically dialed to the designated number once the handset of the telephone is picked up.

2.9.3 FXS Port Setting

Select **FXS port setting** from the **VoIP Management** menu, then **FXS port setting** screen page appears.



VoIP Settings

- FXS Port Setting
 - Dial Pulse Type: 10PPS 20PPS
 - FXS Reverse: Enable (default: disabled)
 - Tone Setting: Taiwan
 - Caller ID Type: DTMF
 - Caller ID Power Level: 20 db. (0..20, default:20)
 - Caller ID Display: Before Ring

Dial Pulse Type: Choose one of the options – 10PPS or 20PPS.

FXS Reverse: Tick the checkbox to enable FXS Reverse function

Tone Setting: Select Tone setting from the drop-down menu.

Caller ID Type: Select the appropriate Caller ID type from the drop-down menu. Seven options are available, these are: Disabled, DTMF, FSK Bellcore, FSK ETSI, Japan CLIP, Japan JCLIP, BT.

Caller ID Power Level: Specify the caller ID Power Level from 0 to 20. The default setting is 20 db.

Caller ID Display: When “Before Ring”/”After Ring” is selected, information of caller ID is shown before/after ringing.

When you select a certain “Caller ID Type” option, “Caller ID Display” available for selection will be shown in the drop-down menu.

Caller ID Type	“Caller ID Display” options available
DTMF	After Ring
FSK Bellcore	Before Ring
FSK ETSI	Before Ring
JAPAN CLIP	After Ring & Before Ring
JAPAN JCLIP	After Ring & Before Ring
BT	After Ring & Before Ring

Port 1	
Ring Impedance	600ohm (default:600ohm)
Hook Flash Detect Upper Bound	300 msec. (100..2000, default:300)
Hook Flash Detect Lower Bound	100 msec. (100..2000, default:100)
Voice Tx Level	3 (default:3)
Voice Rx Level	3 (default:3)

Ring Impedance: Eight Ring Impedance types are available from the drop-down menu.

Hook Flash Detect Upper Bound: Specify the maximum time to detect hook flash.

Hook Flash Detect Lower Bound: Specify the minimum time to detect hook flash.

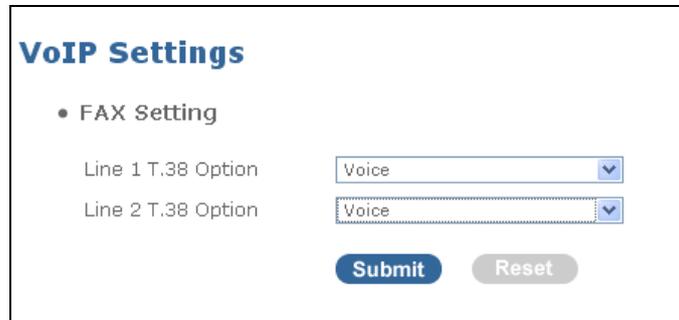
Voice Tx Level: Select the transmitting sound level from the drop-down menu. The corresponding value for each level can be found in the table below.

Voice Rx Level: Select the receiving sound level from the drop-down menu. The corresponding value for each level can be found in the table below.

Tx/Rx Voice Gain Value	
Level	Decibel (dB)
1	-24 dB
2	-18 dB
3	-12 dB
4	-6 dB
5	-2.5 dB

2.9.4 FAX Setting

Select **FAX Setting** from the **VoIP Management** menu, then **FAX Setting** screen page appears.



The screenshot shows the 'VoIP Settings' page with the 'FAX Setting' section selected. It contains two dropdown menus for 'Line 1 T.38 Option' and 'Line 2 T.38 Option', both currently set to 'Voice'. Below the dropdowns are 'Submit' and 'Reset' buttons.

Line 1 & 2 T.38 Option: Select the T.38 FAX option from the drop-down menu.

Voice: When “Voice” is selected, voice data will be transmitted in accordance with CODEC priority defined in **Voice Setting**.

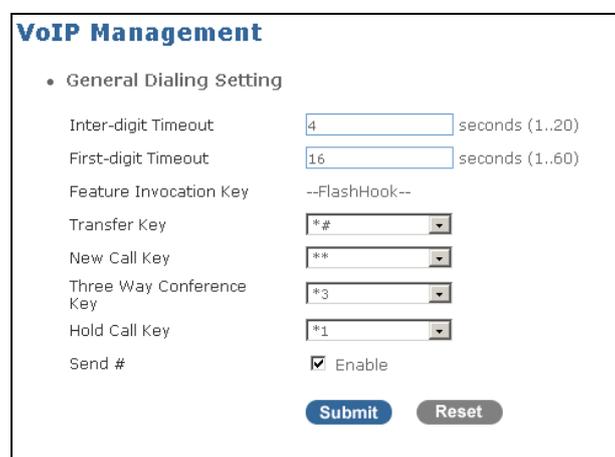
T.38 FAX Relay: Select “T.38 FAX Relay” option, if you would like to send fax messages as UDP or TCP/IP packets. This provides better quality; however, the peer device must use T.38 as well.

Voice and T.38 Relay: When this option is selected, voice will be transmitted with the defined CODEC priority and fax messages will be sent with T.38.

Voice and Fax Pass Through: When this option is selected, voice will be transmitted with the defined CODEC priority and fax messages will be sent with G.711/Ulaw.

2.9.5 General Dialing Setting

Select **General Dialing Setting** from the **VoIP Management** menu, then **General Dialing Setting** screen page appears.



The screenshot shows the 'VoIP Management' page with the 'General Dialing Setting' section selected. It contains several input fields and dropdown menus: 'Inter-digit Timeout' (4 seconds), 'First-digit Timeout' (16 seconds), 'Feature Invocation Key' (--FlashHook--), 'Transfer Key' (*#), 'New Call Key' (**), 'Three Way Conference Key' (*3), and 'Hold Call Key' (*1). There is also a checkbox for 'Send #' which is checked. Below the fields are 'Submit' and 'Reset' buttons.

Inter-digit Timeout: Specify Inter-digit timeout in seconds. This is the time value allowed between two digits that are entered.

First-digit Timeout: Specify time for First-digit timeout in seconds. When the user picks up the handset without dialing a call within the specified time, then the dialing tone will be changed to busy tone.

Transfer Key: Select the key from the drop-down menu. When hook flash is pressed on a call, the transfer key will be activated and a call will be transferred by pressing the selected key(s). You can follow the procedures below to transfer a call.

- Press FlashHook
- Dial the transfer key “*#”
- Dial the phone number of the called party and then press “#”

For example:

Press FlashHook	Dial the transfer key “*#”	Dial the no. of the called party	Dial “#”
-----------------	----------------------------	----------------------------------	----------

New Call key: Select the key from the drop-down menu. When hook flash is pressed on a call, the new call key will be activated and a new call will be dialed by pressing the selected key(s).

Three Way Conference key: Select the key from the drop-down menu. When hook flash is pressed on a call, the three-way conference key will be activated and a three way conference call will be initiated by pressing the selected key(s). You can follow the procedures below to begin a three-way conversation.

- Dial the number of the first conferee. After the connection is established, ask the first conferee to hold.
- Press FlashHook and then dial “* *” followed by the phone number of the second conferee.
- After the connection is established with the second conferee, press “*3” to initiate a three-way conversation.

For example:

Dial the no. of the first conferee	Press FlashHook	Dial “* *”	Dial the no. of the second conferee	Dial “* 3”
------------------------------------	-----------------	------------	-------------------------------------	------------

Hold Call Key: Select the key from the drop-down menu. When the selected keys are pressed, a call will be put on hold. To resume a call, please press FlashHook.

There are two ways to put a call on hold, please see the table below for detailed descriptions.

To put a call on hold, press~	To resume a call on hold, press~
Method 1. “* 1” (Hold Call Key combination)	“FlashHook”
Method 2. “FlashHook”	“FlashHook”

Send #: When enabled, users have to dial “#” after every phone number.

2.9.6 Phone Book

The Residential Gateway supports 2-digit speed dial for the local lines and the SIP phone numbers that are used frequently.

Select **Phone Book** from the **VoIP Management** menu, then **Phone Book** screen page appears.

VoIP Settings

- URI Phone Book

SpeedDial	Phone Number	Note	Action
-None-	<input type="text"/>	<input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>
#0	29090001	Office 1	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
#1	29090002	Office 2	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Speed Dial: This function allows you to dial the frequently called number by entering pre-programmed codes. The maximum of 10 speed-dial entries can be assigned.

Phone Number: Enter the SIP number for an associated speed dial.

Note: Enter the contact description.

Click the **“Insert”** button to add the new rule to the URI Phone book below.

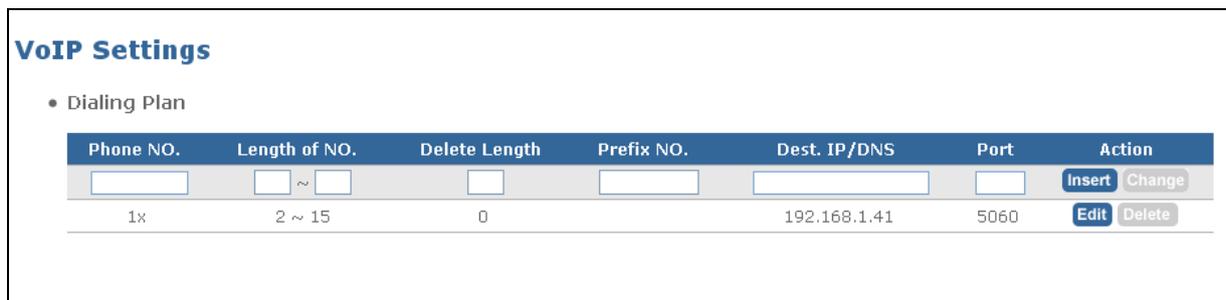
Click the **“Edit”** button on the entry that you would like to make some changes. When the selected entry is highlighted in blue, users can make some changes by selecting from the drop-down menu or enter the new phone number or notes.

Click the **“Change”** button to apply the changes. The modified changes will apply to the URI Phone Book immediately.

2.9.7 Dialing Plan

The Residential Gateway supports Dialing Plan. A dialing plan establishes the expected number and pattern of digits for a telephone number. This includes country codes, access codes, area codes and all combinations of digits dialed. For instance, the North American public switched telephone network (PSTN) uses a 10-digit dial plan that includes a 3-digit area code and a 7-digit telephone number. Most PBXs support variable-length dial plans that use 3 to 11 digits. Dial plans must comply with the telephone networks to which they connect.

Select **Phone Book** from the **VoIP Management** menu, then **Phone Book** screen page appears.



The screenshot shows the 'VoIP Settings' page with a section for 'Dialing Plan'. It contains a table with the following columns: Phone NO., Length of NO., Delete Length, Prefix NO., Dest. IP/DNS, Port, and Action. The table has one row with the following values: Phone NO. (1x), Length of NO. (2 ~ 15), Delete Length (0), Prefix NO. (empty), Dest. IP/DNS (192.168.1.41), Port (5060), and Action (Edit, Delete). The 'Action' column contains two buttons: 'Edit' and 'Delete'.

Phone NO.	Length of NO.	Delete Length	Prefix NO.	Dest. IP/DNS	Port	Action
<input type="text"/>	<input type="text"/> ~ <input type="text"/>	<input type="button" value="Insert"/> <input type="button" value="Change"/>				
1x	2 ~ 15	0		192.168.1.41	5060	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Phone NO.: Identify a specific digit (do not use #).

Length of NO.: Specify the minimum and maximum digits.

Delete Length: Specify the number of digits that can be entered. If digits you enter are more than specified, the extra digits will be ignored.

Prefix No.: Match any single digit that is dialed.

Dest. IP / DNS: Specify Destination IP / DNS address.

Port: Specify the port number.

Click the **“Insert”** button to add this new rule to the Dialing Plan below after you enter the new settings.

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

Click the **“Change”** button to apply the changes. The modified changes will apply to the Dialing Plan immediately.

2.10 CATV Setting (Only available for RF module)

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



CATV Setting (default:Enable)

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

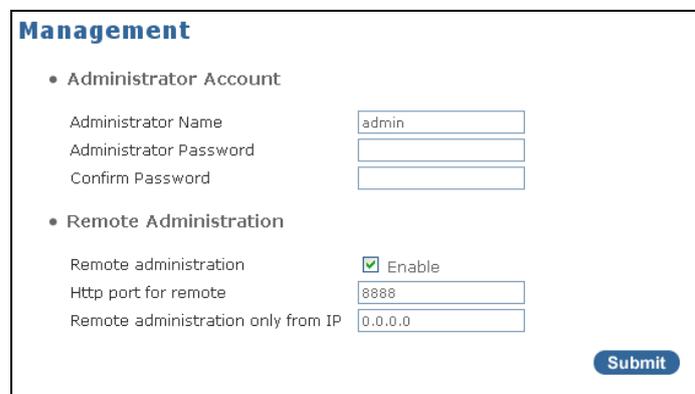
2.11 Management

In this session you’ll be able to setup 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.

2.11.1 Administrator Account

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



Management

- Administrator Account
 - Administrator Name
 - Administrator Password
 - Confirm Password
- Remote Administration
 - Remote administration Enable
 - Http port for remote
 - Remote administration only from IP

Administrator Account

Administrator Name: Specify the authorized user login name, up to 31 alphanumeric characters. The default value is “admin”.

Administrator Password: Enter the desired user password.

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

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.*

2.11.2 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 as follows:

System Log	<input checked="" type="checkbox"/> Enable
Log Service	<input checked="" type="checkbox"/> WAN <input type="checkbox"/> LAN <input type="checkbox"/> VoIP <input type="checkbox"/> DDNS <input type="checkbox"/> HTTPD <input type="checkbox"/> IGMP <input type="checkbox"/> NAT <input type="checkbox"/> NTP <input type="checkbox"/> SNMP <input type="checkbox"/> UPnP <input type="checkbox"/> PPPoE <input type="checkbox"/> DHCP
Remote	<input checked="" type="checkbox"/> Enable
Syslog Level	Warning
Remote Server	your.syslog.server
Remote Port	514

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.

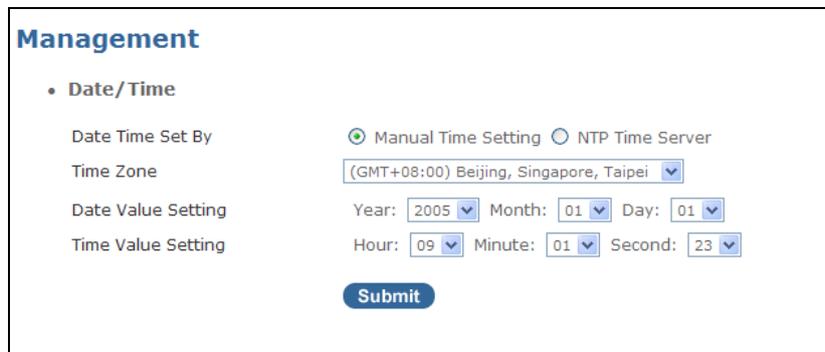
Remote: Enable the remote server, if checked.

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.

2.11.3 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 configuration options are:

- Date Time Set By:** Manual Time Setting NTP Time Server
- Time Zone:** (GMT+08:00) Beijing, Singapore, Taipei
- Date Value Setting:** Year: 2005, Month: 01, Day: 01
- Time Value Setting:** Hour: 09, Minute: 01, Second: 23

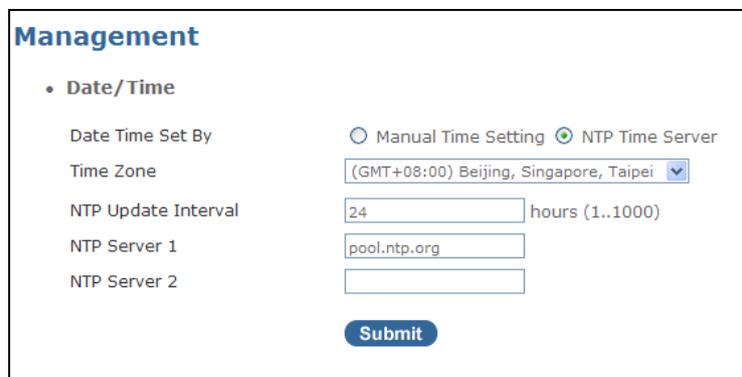
A 'Submit' button is located at the bottom of the form.

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 configuration options are:

- Date Time Set By:** Manual Time Setting NTP Time Server
- Time Zone:** (GMT+08:00) Beijing, Singapore, Taipei
- NTP Update Interval:** 24 hours (1..1000)
- NTP Server 1:** pool.ntp.org
- NTP Server 2:** (empty field)

A 'Submit' button is located at the bottom of the form.

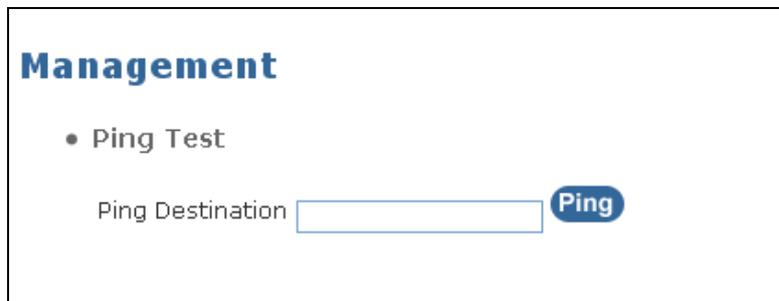
NTP Update Interval: Specify how frequent to update system clock. The default setting is 24 hours.

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

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

2.11.4 Ping Test

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



The screenshot shows a web interface titled "Management". Underneath, there is a sub-menu item "Ping Test" which is selected. Below this, there is a text input field labeled "Ping Destination" and a blue button labeled "Ping".

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.

2.11.5 Save/Restore

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



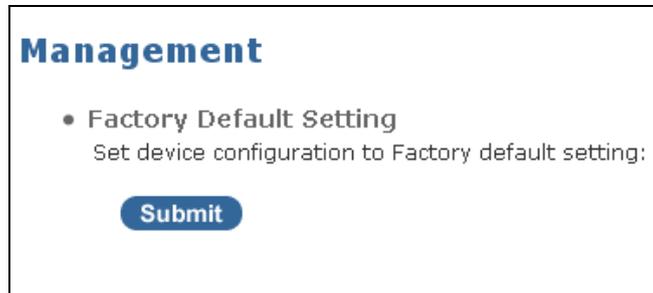
The screenshot shows a web interface titled "Management". Underneath, there is a sub-menu item "Save/Restore Setting" which is selected. Below this, there are two sections: "Save" with the text "Save device running configuration to local file" and a "Save" button; and "Restore" with the text "Upload a local file to restore as device configuration:", 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 Residential Gateway configurations. When the restore process is completed, a pop-up window will appear to notify the user.

2.11.6 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 section for "Factory Default Setting" with the instruction "Set device configuration to Factory default setting:". Below this instruction is a blue "Submit" button.

If you want to set the Residential Gateway to Factory default settings, click the **“Submit”** button.

2.11.7 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: "Manual Firmware Upgrade" and "Ftp Firmware Upgrade".

- Manual Firmware Upgrade:** Includes a "Firmware File" label, a text input field, a "Browse" button, and an "Upload" button.
- Ftp Firmware Upgrade:** Includes four labels with corresponding text input fields: "Absolute Path File Name", "IP or URL", "Ftp User Name", and "Ftp User Password".

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.

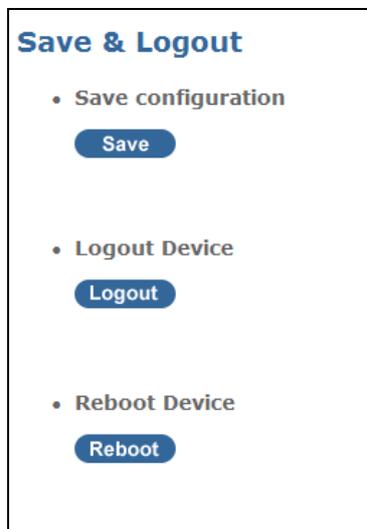
FTP User Name: Specify the FTP login user name.

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.

2.12 Save & Logout

Select **Save & Logout** from the **Main Menu**, then **Save & Logout** screen page appears.



Click the **“Save”** button to save current configuration settings. Please note that all unsaved configurations will be lost when the power is off.

Click the **“Logout”** button to logout from the web management.

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

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.

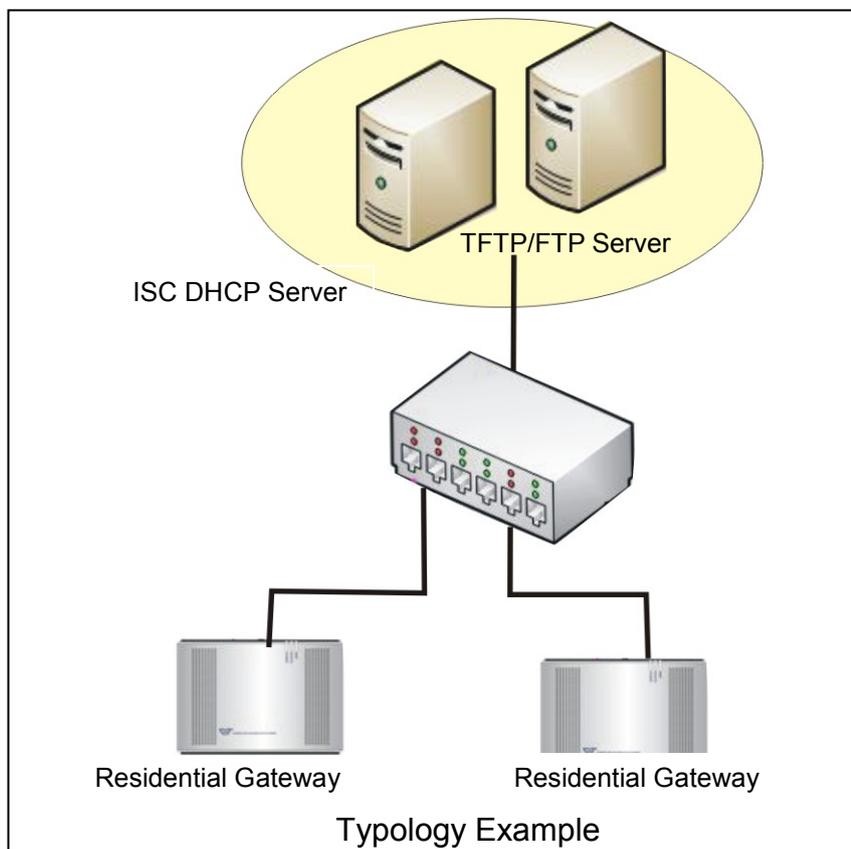
APPENDIX A: Set Up DHCP Auto-Provisioning

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.



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 "metafile"; 10
option SAMPLE configuration-md5 95:d6:5c:39:4d:83:76:30:61:16:9b:de:37:ba:12:84;
option SAMPLE option 1;
}
```

Modify the marked area with your own settings.

1. This value is configurable and can be defined by users.
2. Specify the protocol used (Protocol 1: FTP; Protocol 0: TFTP).
3. Specify the FTP or TFTP IP address.
4. Login FTP server anonymously.
5. Specify FTP Server login name.
6. Specify FTP Server login password.
7. Specify the product model name.
8. Specify the firmware filename.
9. Specify the MD5 for firmware image. The format of MD5 might be the same as the one in the sample text.
10. Specify the configuration image filename.

Step 5. Generate a Configuration File

Before preparing the configuration image in TFTP/FTP Server, please make sure the device generating the configuration image is set to “Get IP address from DHCP” assignment. This is because that DHCP Auto-provisioning is running under DHCP mode, so if the configuration image is uploaded by the network type other than DHCP mode, the downloaded configuration image has no chance to be equal to DHCP when provisioning, and it results in MD5 never match and causes the device to reboot endlessly.

In order for your Residential Gateway to retrieve the correct configuration image in TFTP/FTP Server, please use the following rule to define the configuration image’s filename. The filename should contain the configuration image filename specified in **dhcpd.conf** followed by the last three octets of your device’s MAC address. For example, if the configuration image’s filename specified in dhcpd.conf is “metafile” and the MAC address of your device is “00:06:19:03:21:80”, the configuration image filename should be named to “metafile032180.dat”.

Step 6. Place a copy of Firmware and Configuration File in TFTP/FTP Server

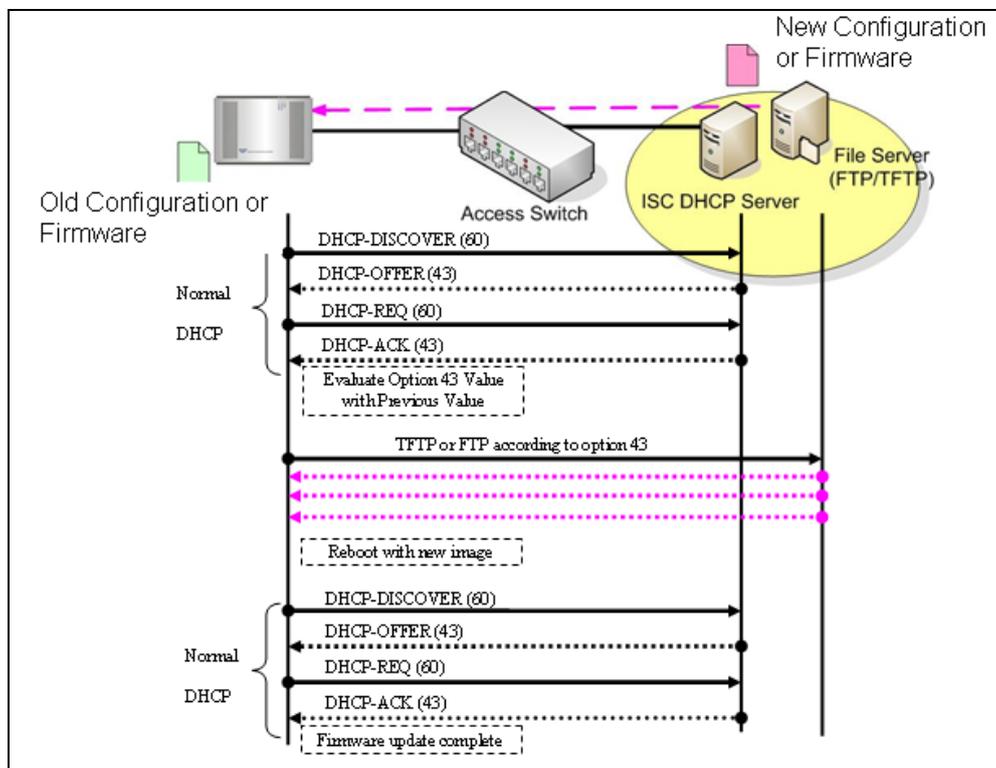
The TFTP/FTP File server should include the following items:

1. Firmware image
2. Configuration image
3. User account for your device (For FTP server only)

B. Auto-Provisioning Process

This Residential Gateway is setting-free (through auto-upgrade and configuration) and its upgrade procedures are as follows:

1. The ISC DHCP server will recognize the device whenever it sends an IP address request to it. And ISC DHCP server will tell the device how to get a new firmware or configuration.
2. The device will compare the firmware and configuration MD5 code form of DHCP option every time when it communicates with DHCP server.
3. If MD5 code is different, the device will then upgrade the firmware or configuration. However, it will not be activated right after.
4. If the Urgency Bit is set, the device will be reset to activate the new firmware or configuration immediately.
5. The device will retry for 3 times if the file is incorrect, then it gives up until getting another DHCP ACK packet again.



APPENDIX B: DHCP Text Sample

```
default-lease-time 90;
max-lease-time 7200;
```

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

```
subnet 192.168.2.0 netmask 255.255.255.0 {
    range 192.168.2.1 192.168.2.99;
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.2.255;
    option routers 192.168.2.2;
    option domain-name-servers 168.95.1.1, 168.95.192.1, 192.168.2.2;
```

```
host CTS-FAE {
    hardware ethernet 00:14:85:06:5A:06;
    fixed-address 192.168.2.99;
}
```

```
}
```

#Please copy the text below to your dhcpd.conf file#

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

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

```
option SAMPLE.protocol 1;
option SAMPLE.server-ip 192.168.2.1;
# option SAMPLE.server-login-name "anonymous";
option SAMPLE.server-login-name "sqa";
option SAMPLE.server-login-password "a12345A";
```

```
subclass "vendor-classes" "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.