COMTREND CORPORATION

CT-820C VoIP Gateway User’s Manual

Version A2.1, August 31, 2010

261053-034

Preface

This manual provides information to network administrators. It covers the installation, operation and application of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications.

Technical support

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, visit Comtrend Corporation at http://www.comtrend.com

⚠ **Warning**

- Before servicing, disconnect power and telephone lines from the device
- Use an appropriate power supply and a UL Listed telephone line cord Power specifications are clearly stated in Appendix C: Specifications

FCC Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which

the receiver is connected

- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cmbetween the radiator & your body.

Copyright

This document is subject to change without notice.

Table of Contents

Chapter 1 Introduction

The CT-820C is a powerful WLAN VoIP Gateway, providing predictable, real-time, toll-quality voice over the Internet. The CT-820C is designed for residential and business users with broadband DSL or cable access, who need to integrate Wi-Fi AP and VoIP technologies. The CT-820C offers users easy access to the Internet via WLAN or Ethernet and provides VoIP via standard analog phones.

1.1 Features

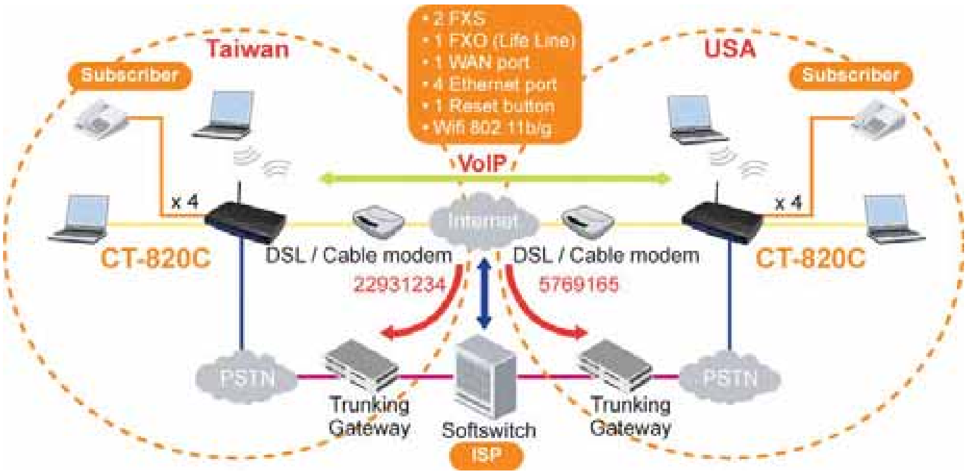
- VoIP and router integrated
- 802.11g/b access point
- VPN passthrough
- QoS for voice
- DNS SRV
- Dial plan
- Call hold
- Call waiting
- Call transfer
- Call forwarding
- 3-way conference
- Direct number dialing
- Supports emergency call
- Day-time parental control
- T.38 fax relay and passthrough
- Caller ID presentation and restriction
- Supports life line: PSTN alive when power off
- Remote administration: automatic firmware upgrade and configuration

Optional

- Centralized configuration and firmware upgrade via APS (Automatic Provision Server)

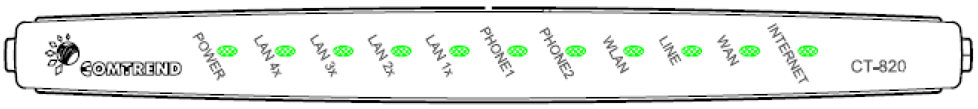
1.2 Application

The following diagram depicts the application of the CT-820C.



1.3 LED Indicators

The front panel LED indicators are shown in this illustration and followed by detailed explanations in the table below.



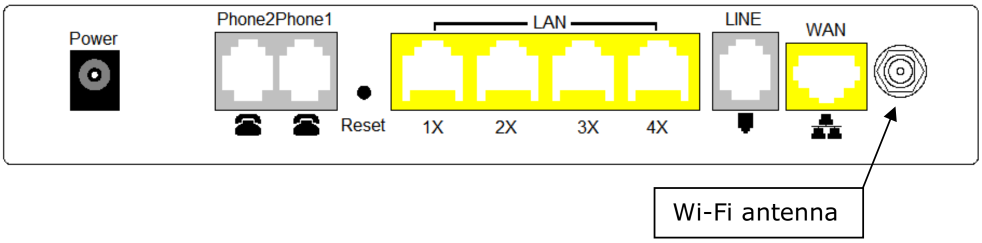
LED	Color	Mode	Function
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
LAN 4x~1x	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
	Green	Blink	Data transmitting or receiving over LAN.
PHONE1	Green	On	The FXS phone 1 is off hook.
		Off	The FXS phone 1 is on hook.
PHONE2	Green	On	The FXS phone 2 is off hook.
		Off	The FXS phone 2 is on hook.
WLAN	Green	On	The wireless module is ready and idle.
		Off	The wireless module is disabled.
	Green	Blink	Data transmitting or receiving over WLAN.
LINE	Green	On	An FXO line is off hook.
		Off	An FXO line is on hook.
WAN	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
INTERNET	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)

註解 [RDP1]: SV tested this device and found that the light did not work as expected. It does not turn on when connected or blink when traffic is passing through the PPPoE connection.

Chapter 2 Hardware Setup

Follow the instructions below to complete the hardware setup.

The diagram below shows the back panel of the device.



Connection to Power
Connect the **Power** jack to the power cord. Attach the power adapter to the wall outlet or other AC source. At startup, the device will perform a self-test. Wait for a few seconds until the test is finished, then the device will be ready to operate.

Caution 1: If the device fails to power up, or it malfunctions, first verify that the power supply is connected correctly. Then power it on again. If the problem persists, contact our technical support engineers.

Caution 2: Before servicing or disassembling this equipment always disconnect all power cords and telephone lines from their outlets.

Connection to Phone1/ Phone2
Connect a telephone to either RJ11 port for VoIP service.

Reset Button
Restore the default parameters of the device by holding down the Reset button until the front panel LED indicators start blinking simultaneously (~ 5 seconds). If held down for more than 12 seconds, the device will go into a firmware update state (CFE boot mode). The user can then update the device from any web browser using the default IP address (http://192.168.1.1) without login.

Connection to LAN/WAN ports
Use a RJ45 cable to connect to a network hub or PC. You can connect the device to up to four LAN devices and one WAN device. The ports are auto-sensing MDI/X and either straight-through cable or crossover cable can be used.

Connection to LINE port
If you wish to connect both the router and a telephone, connect the LINE port to a POTS splitter with a RJ11 connection cable.

Connection to WLAN
Attach the Wi-Fi antenna to enable this feature.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface using an Internet browser such as Microsoft Internet Explorer (version 5.0 and later).

3.1 Default Settings

The following are the default settings for the device.

- Local (LAN access) Username: root , Password: 12345
- Remote (WAN access) Username: support, Password: support
- LAN port IP address: 192.168.1.1
- Remote WAN access: disabled
- NAT and firewall: enabled
- DHCP server on LAN interface: enabled
- WAN IP address: none

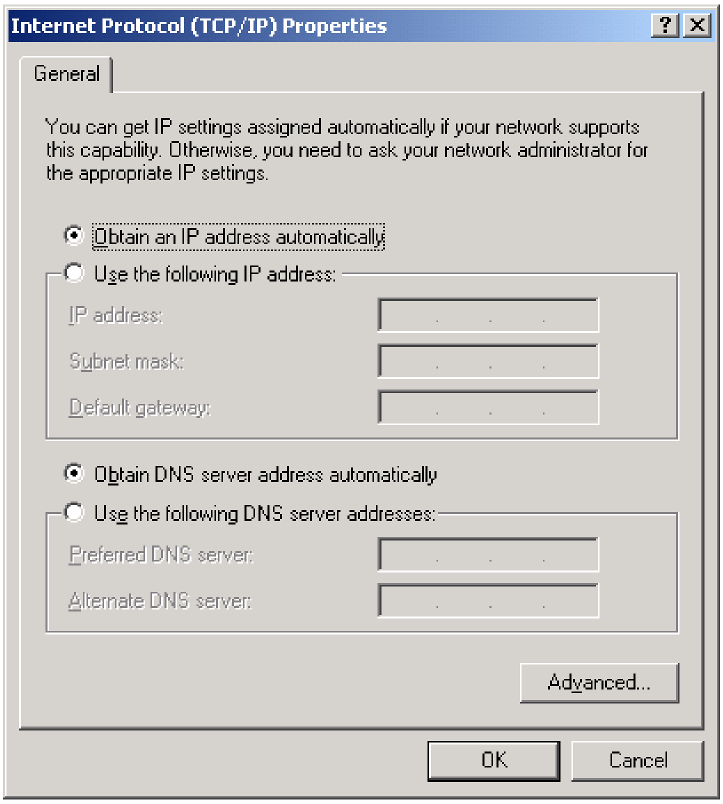
Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 TCP/IP Settings

DHCP Mode

When the device powers up, the DHCP server (on the device) will start automatically. To set your PC for DHCP mode, check the Internet Protocol properties of your Local Area Connection. You can set your PC to DHCP mode by selecting **Obtain an IP address automatically** in the dialog box shown below.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

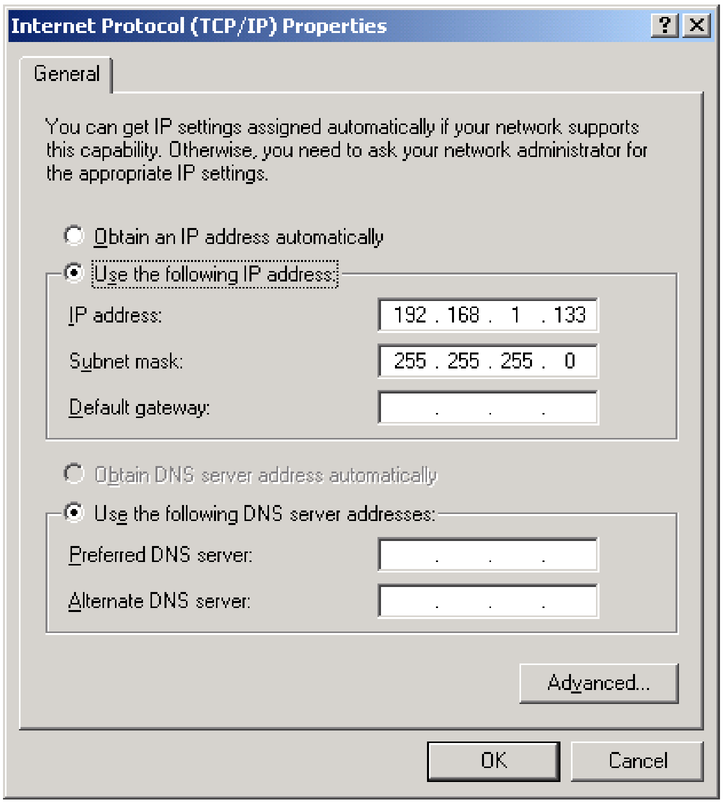
Alternate DNS server: . . .

STATIC IP Mode

To configure the device manually, your PC must have a static IP address within the 192.168.1.x subnet. Follow the steps below to configure your PC IP address to use subnet 192.168.1.x. The following assumes you are running Windows XP.

STEP 1: From the Network Connections window, open the Local Area Connection. (You may also access this screen by double-clicking the Local Area Connection icon on your taskbar.) Click the **Properties** button.

STEP 2: **Select Internet Protocol (TCP/IP) and click the Properties** button. The screen should now display as below. Change the IP address to the domain of 192.168.1.x/24 (i.e. subnet mask=255.255.255.0).



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 133
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

STEP 3: Click OK to submit the settings.

3.3 Login Procedure

Perform the following steps to login to the web user interface.

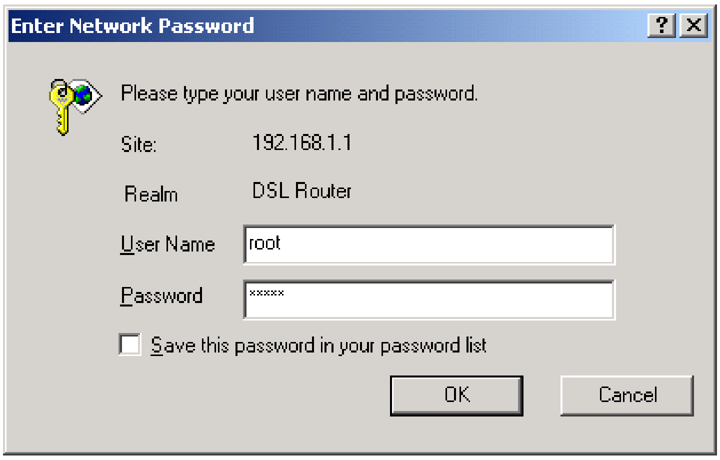
NOTE: The default settings for this device can be found in 3.1 Default Settings.

STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the IP address is 192.168.1.1, type http://192.168.1.1.

NOTE: For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device. For remote access (i.e. WAN), use the remote username and password.

STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.

Click **OK** to continue.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm DSL Router

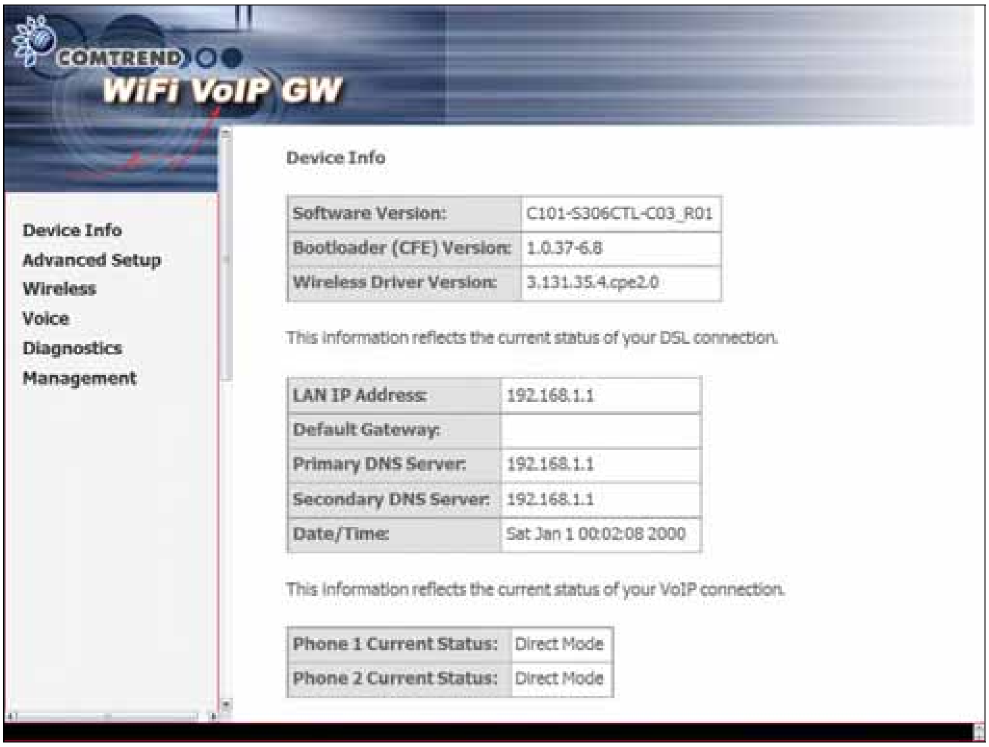
User Name: root

Password: *****

□ Save this password in your password list

NOTE: The login password can be changed later (see 9.5.3 Passwords)

STEP 3: After successfully logging in, you will reach this screen.



Device Info

Software Version:	C101-S306CTL-C03_R01
Bootloader (CFE) Version:	1.0.37-6.8
Wireless Driver Version:	3.131.35.4.cpe2.0

This information reflects the current status of your DSL connection.

LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1
Date/Time:	Sat Jan 1 00:02:08 2000

This information reflects the current status of your VoIP connection.

Phone 1 Current Status:	Direct Mode
Phone 2 Current Status:	Direct Mode

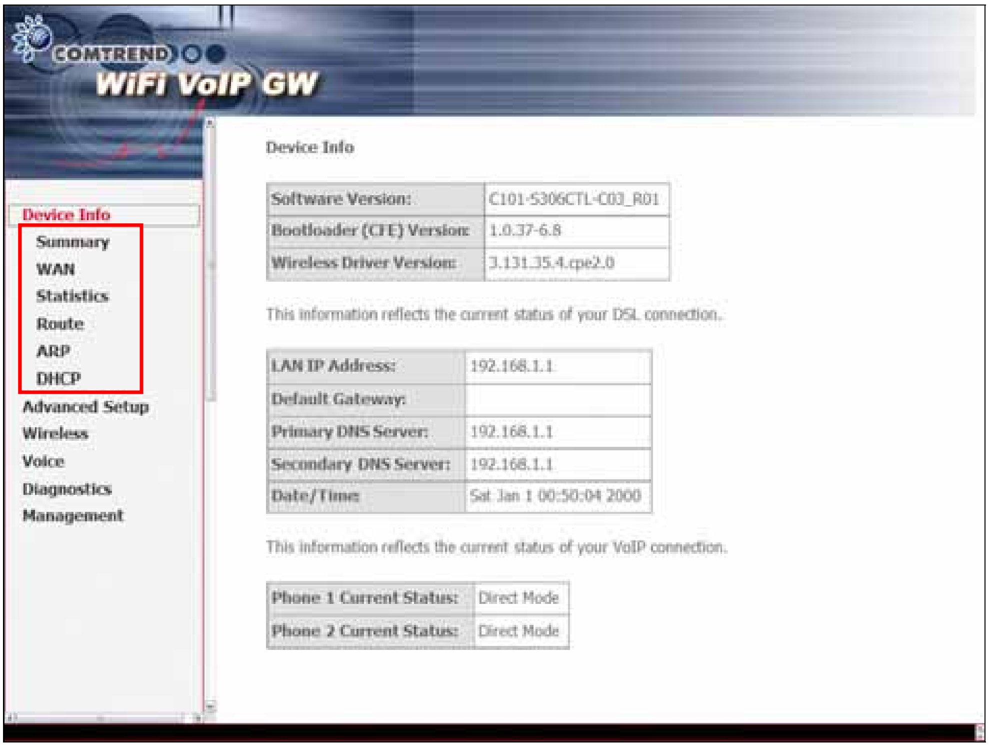
Chapter 4 Device Information

The web user interface is divided into two window panes, the main menu (at left) and the display screen (on the right). The main menu has the following options: **Device Info, Advanced Setup, Wireless, Voice, Diagnostics, Management**. Selecting one of these options will open a submenu with more options.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote). For example, in the Advanced Setup menu, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu will also be disabled.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Device Info submenu (outlined in red in the screenshot below) has the following selections: **Summary, WAN, Statistics, Route, ARP,** and **DHCP**.



Device Info

Software Version:	C101-5306CTL-C03_R01
Bootloader (CFE) Version:	1.0.37-6.8
Wireless Driver Version:	3.131.35.4.cpe2.0

This information reflects the current status of your DSL connection.

LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1
Date/Time:	Sat Jan 1 00:50:04 2000

This information reflects the current status of your VoIP connection.

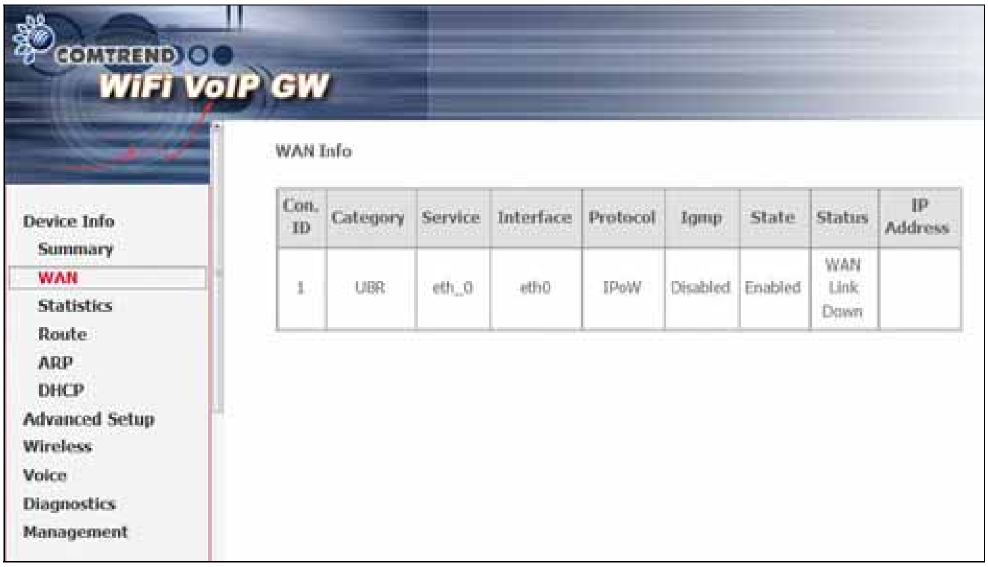
Phone 1 Current Status:	Direct Mode
Phone 2 Current Status:	Direct Mode

The Device Info Summary screen (shown above) is the default startup screen.

It provides summary information regarding the device firmware version, TCP/IP settings, and the status of the two VOIP connections.

4.1 WAN

Select **WAN** from the Device Info submenu to display the configured PVC(s).



WAN Info

Con. ID	Category	Service	Interface	Protocol	Igmp	State	Status	IP Address
1	UBR	eth_0	eth0	IPoW	Disabled	Enabled	WAN Link Down	

The display screen table headings (above) are described in the table below.

Con. ID	Shows the connection ID
Category	Shows the ATM service classes
Service	Shows the name for WAN connection
Interface	Shows connection interfaces
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Igmp	Shows the status of the IGMP Proxy function
State	Shows the connection state of the WAN connection
Status	Lists the WAN or PVC status (ex: Up/Down or Authentication Failure)
IP Address	Shows IP address for WAN interface

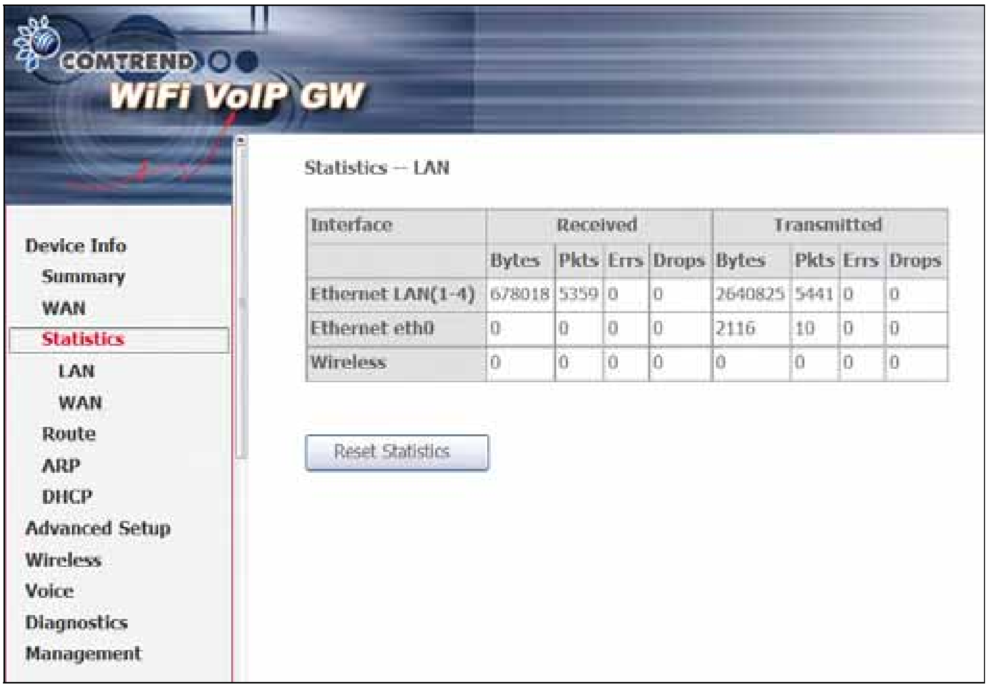
4.2 Statistics

The Statistics screens show detailed information for LAN or WAN Interfaces.

NOTE: These statistics are updated every 15 seconds.

4.2.1 LAN Statistics

This screen shows statistics for Ethernet and Wireless interfaces on the LAN.



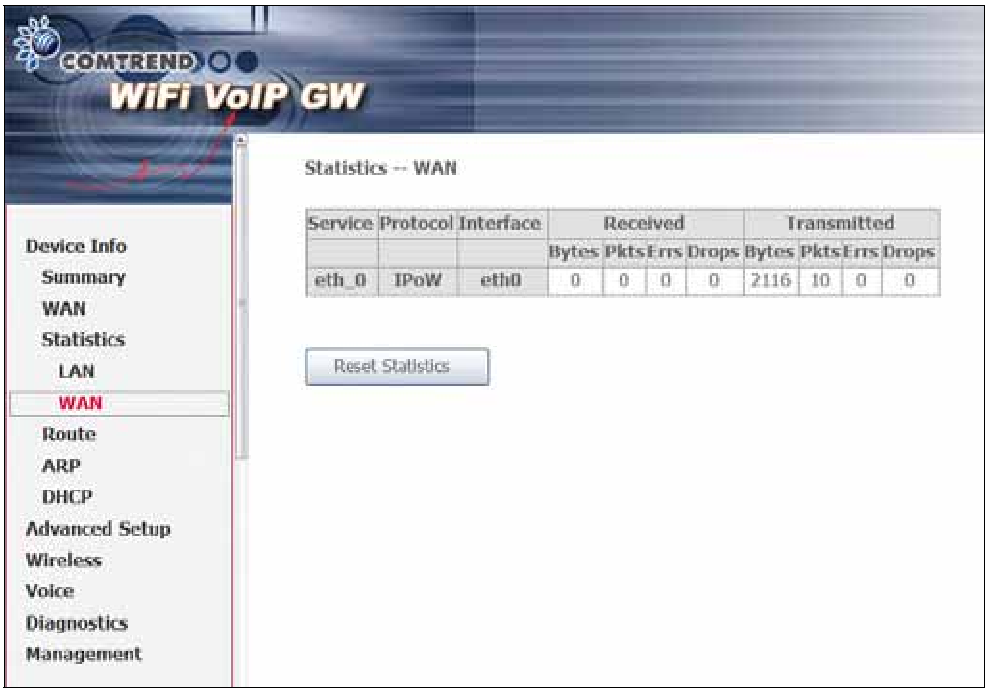
Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet LAN(1-4)	678018	5359	0	0	2640825	5441	0	0
Ethernet eth0	0	0	0	0	2116	10	0	0
Wireless	0	0	0	0	0	0	0	0

Interface	Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.
Received/Transmitted - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in Byte Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) the packets which are errors, Rx/TX (receive/transmit) the packets which are dropped

4.2.2 WAN Statistics

This screen shows statistics for interfaces on the WAN.



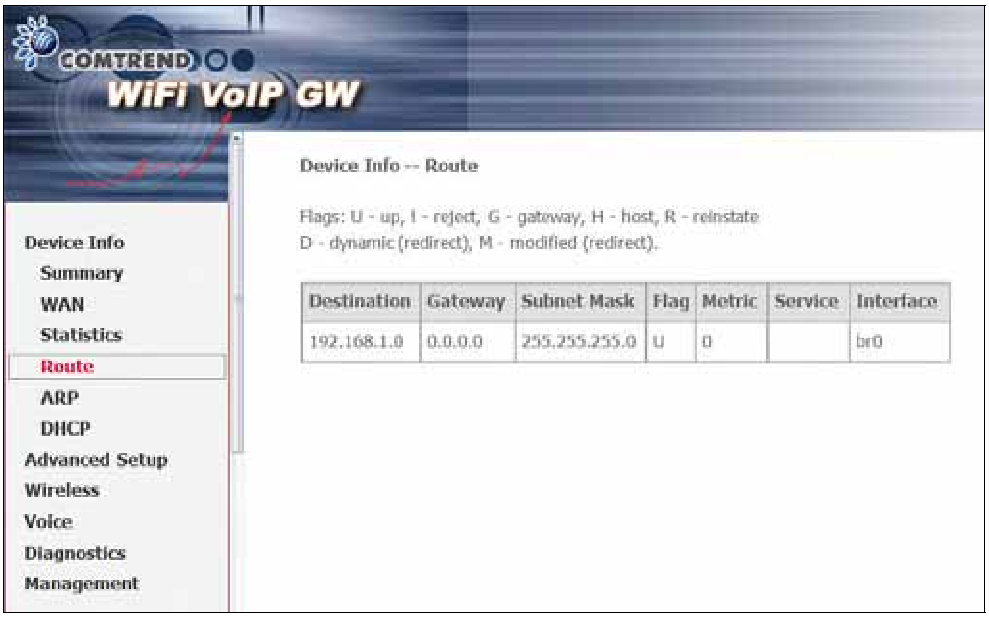
Statistics -- WAN

Service	Protocol	Interface	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth_0	IPoW	eth0	0	0	0	0	2116	10	0	0

Service	Shows the service type, as configured by the administrator
Protocol	Shows the connection type, such as PPPoE, PPPoA, etc.
Interface	Shows connection interfaces in the following format: nas_(VPI number_VCI number). These interfaces are devised by the system and not the user.
Received/Transmitted - Bytes - Pkts - Errs - Drops	Rx/TX (receive/transmit) packet in Byte Rx/TX (receive/transmit) packets Rx/TX (receive/transmit) the packets which are errors, Rx/TX (receive/transmit) the packets which are dropped

4.3 Route

Choose **Route** to display the routes that the route information has learned.



Device Info -- Route

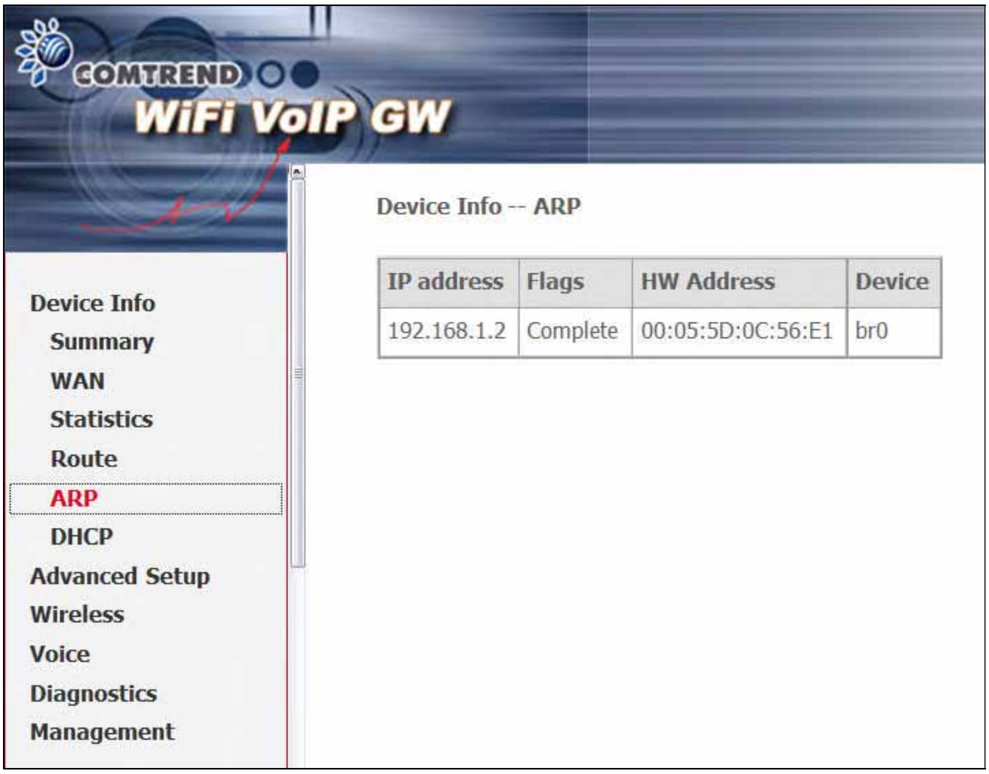
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Field	Description
Destination	Destination network or destination host
Gateway	Next hub IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces

4.4 ARP

Click **ARP** to display the ARP information.

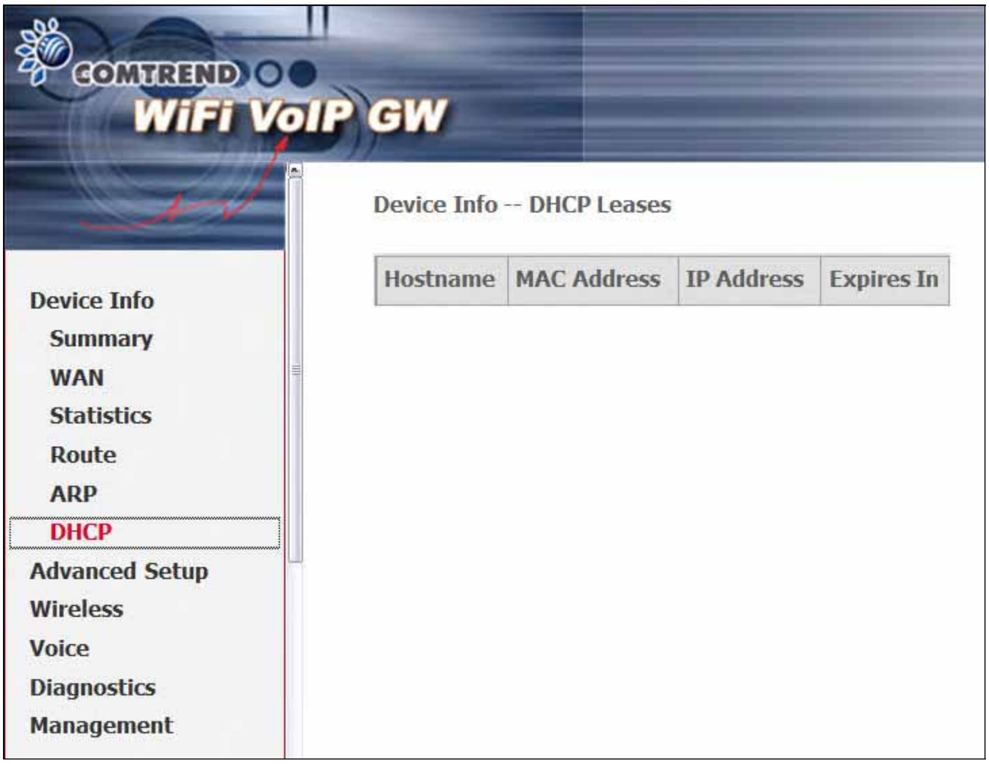


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:05:5D:0C:56:E1	br0

4.5 DHCP

Click **DHCP** to display the DHCP Leases information.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In

Chapter 5 Advanced Setup

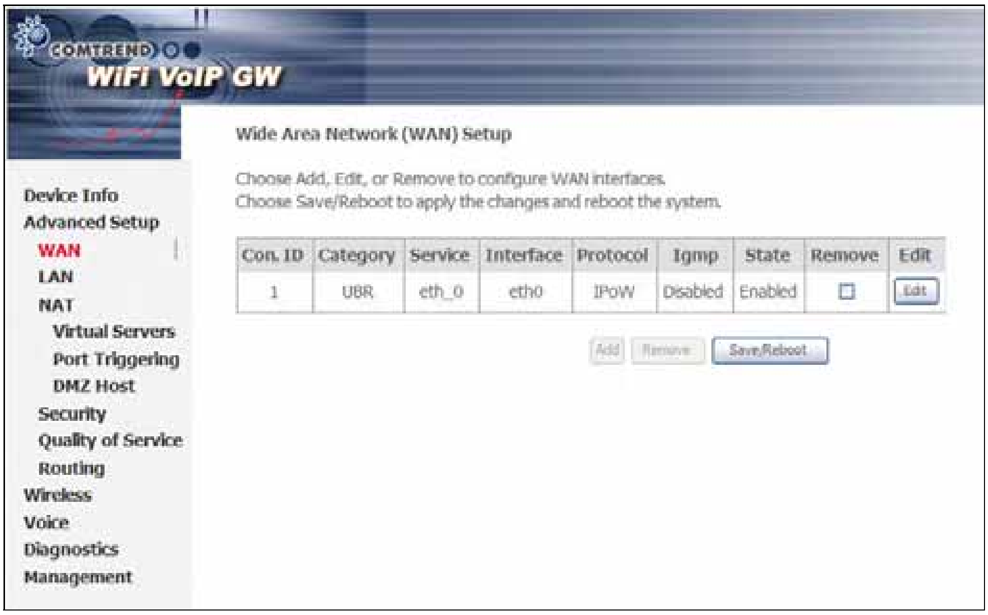
This chapter explains the setup screens for the following services:

- WAN – Wide Area Network
- LAN – Local Area Network
- NAT – Network Address Translation
- SECURITY
- QUALITY OF SERVICE
- ROUTING

5.1 WAN

Follow the steps on the following pages to configure WAN interfaces. The screen below shows all configured WAN connections. The table below gives more details.

STEP 1: Click the **Edit** button next to the WAN connection you wish to configure.



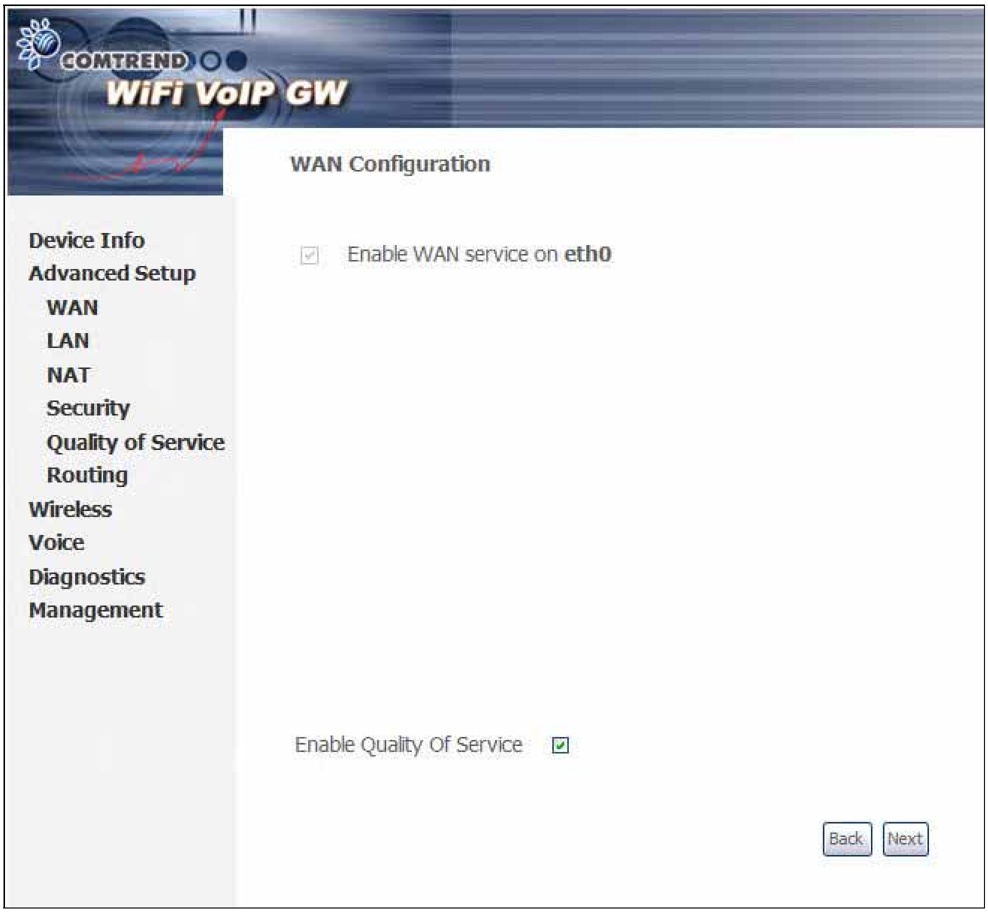
Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Con. ID	Category	Service	Interface	Protocol	Igmp	State	Remove	Edit
1	UBR	eth_0	eth0	IPoW	Disabled	Enabled	□	Edit

Con. ID	ID for WAN connection
Category	ATM service category, e.g. UBR, CBR, …
Service	Name of the WAN connection
Interface	Name of the interface for WAN
Protocol	Shows IPoW or PPPoE modes
Igmp	Shows enable or disable IGMP proxy
State	Shows enable or disable WAN connection

STEP 2: The WAN Configuration screen will display as below. Quality of Service (QoS) is enabled when the box at bottom is checked (☑). Click **Next**.

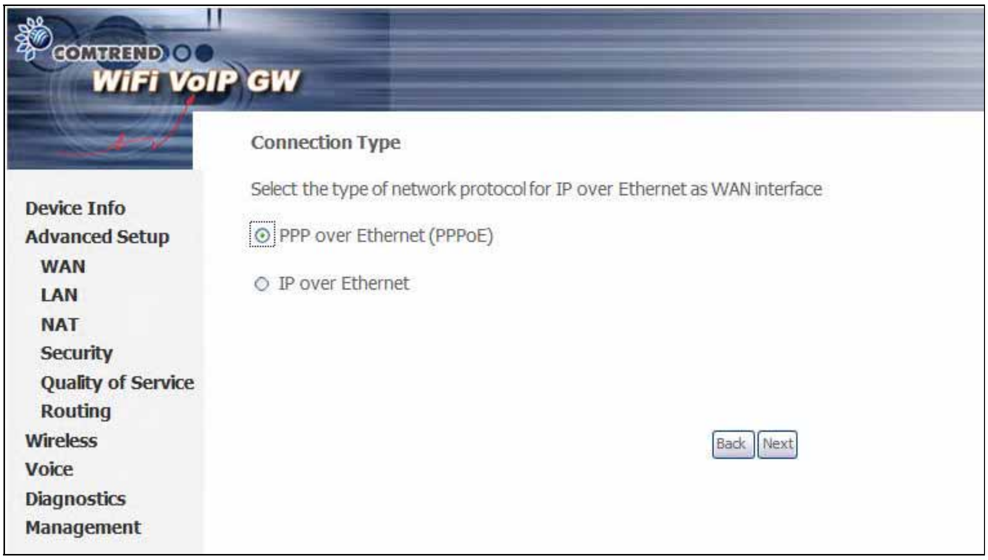


WAN Configuration

☑ Enable WAN service on **eth0**

Enable Quality Of Service ☑

STEP 3: On this screen, you can choose either **PPPoE** or **IPoE** connection types. Once you have chosen, click **Next** to proceed.



Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

● PPP over Ethernet (PPPoE)

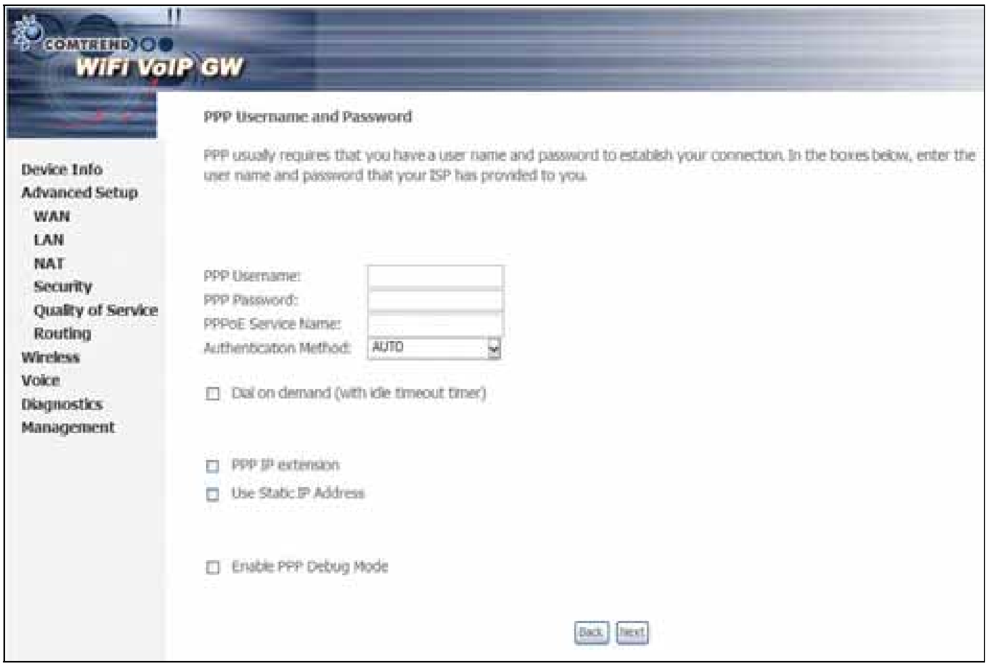
○ IP over Ethernet

Important Note:

For **PPPoE** connections follow **Steps 4-6**
For **IPoE** connections follow **Steps 7-9**

PPPoE –PPP over Ethernet

Step 4: Enter the Username and Password and select the connection options. Review the descriptions below for more details. Click **Next** to continue.



PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO

□ Dial on demand (with idle timeout timer)

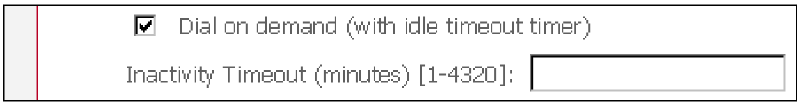
□ PPP IP extension
□ Use Static IP Address

□ Enable PPP Debug Mode

PPP Username/PPP Password
The PPP Username and the PPP password requirement are dependent on the particular requirements of the service provider. A maximum of 256 characters is allowed for the PPP user name and a maximum of 32 characters for PPP password.

PPPoE service name
For PPPoE service, PADI requests contain a service name-tag. Some PPPoE servers (or BRAS) of ISP check this service name-tag for connection.

Dial on Demand
The device can be configured to disconnect if there is no activity for a period of time by selecting this check box. When the checkbox is ticked, you must enter the inactivity timeout period. The timeout period ranges from 1 to 4320 minutes.



☑ Dial on demand (with idle timeout timer)
Inactivity Timeout (minutes) [1-4320]:

PPP IP Extension

The PPP IP Extension is a special feature deployed by some service providers. Unless your service provider specially requires this setup, do not select it.

The PPP IP Extension supports the following conditions:

- Allows only one PC on the LAN
- The public IP address assigned by the remote side using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP. Only one PC on the LAN can be connected to the remote, since the DHCP server within the device has only a single IP address to assign to a LAN device.
- NAT and firewall are disabled when this option is selected.
- The device becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address.
- The device extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet.
- The device bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the device's LAN IP address.

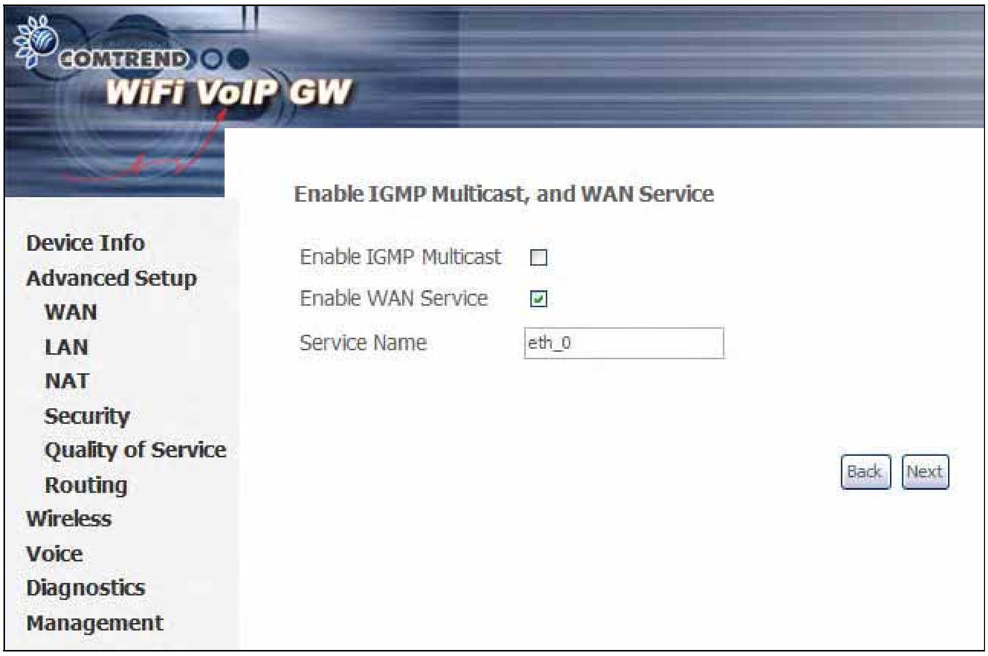
Use Static IP Address

Unless your service provider specially requires this setup, do not select it.
If selected, enter your static IP address in the IP Address field. Also, don't forget to adjust your TCP/IP Settings as described in subsection 3.2 TCP/IP Settings.

Enable PPP Debug Mode

When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

Step 5: On this screen you may enable/disable IGMP Multicast and WAN service. Click **Next** to continue.



Enable IGMP Multicast, and WAN Service

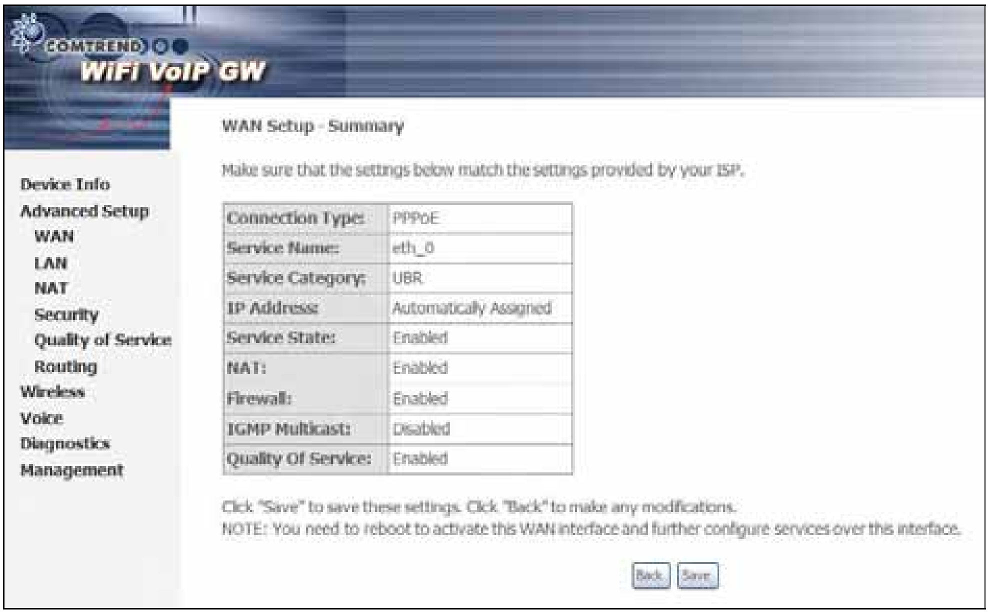
Enable IGMP Multicast □

Enable WAN Service ☑

Service Name eth_0

Enable IGMP Multicast checkbox
Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast device's.

STEP 6: Click **Next** to display the WAN Setup-Summary screen that presents the entire configuration summary review. Click **Back** to modify the settings.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

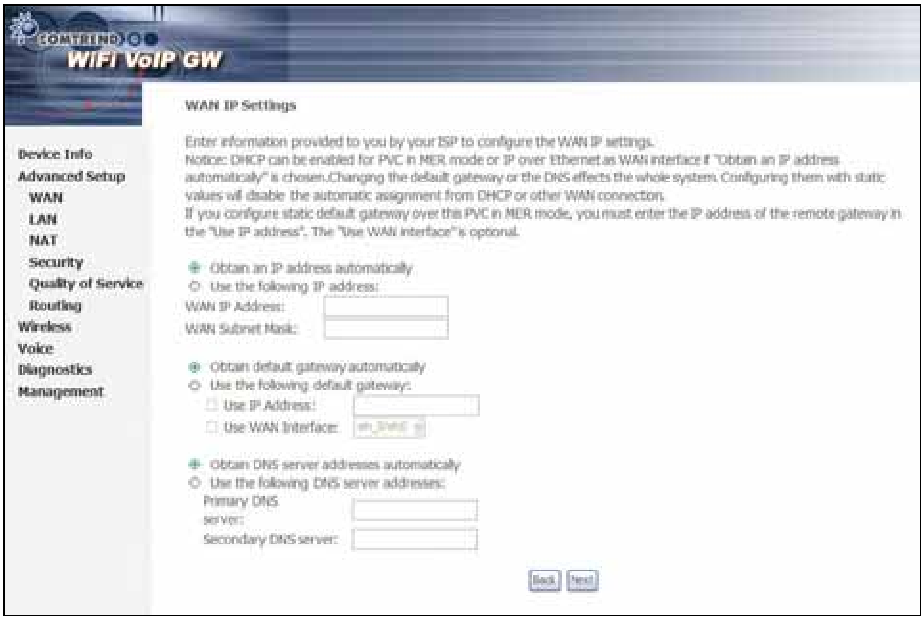
Connection Type:	PPPoE
Service Name:	eth_0
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

Click Save/Reboot and skip to Step 10.

IPoE – Internet Protocol over Ethernet

STEP 7: The WAN IP Settings screen below allows for configuration of the connection in DHCP (automatic) or Static IP (manual) modes.



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen.Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.
If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

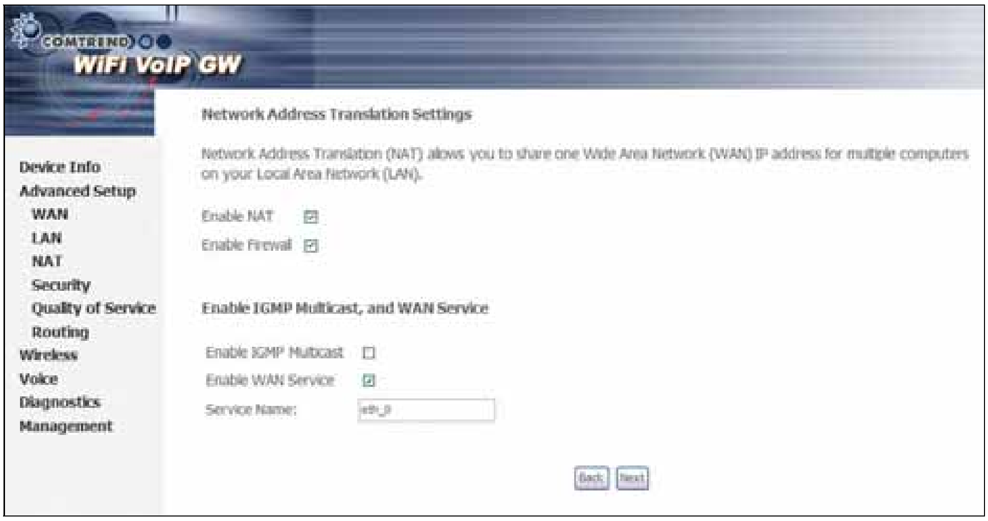
● Obtain an IP address automatically
○ Use the following IP address:
WAN IP Address:
WAN Subnet Mask:

● Obtain default gateway automatically
○ Use the following default gateway:
□ Use IP Address:
□ Use WAN Interface: eth_3/eth0

● Obtain DNS server addresses automatically
○ Use the following DNS server addresses:
Primary DNS server:
Secondary DNS server:

Enter information provided to you by your ISP to configure the WAN IP settings. DHCP mode must be enabled when **Obtain an IP address automatically** is chosen. Changing the default gateway or the DNS affects the whole system. Where Static mode is selected, the IP address and subnet mask must be entered, however, the **Use WAN interface** field does not need to be selected.

STEP 8: The next screen combines NAT, IGMP and WAN service selection options.



Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT ☑
Enable Firewall ☑

Enable IGMP Multicast, and WAN Service

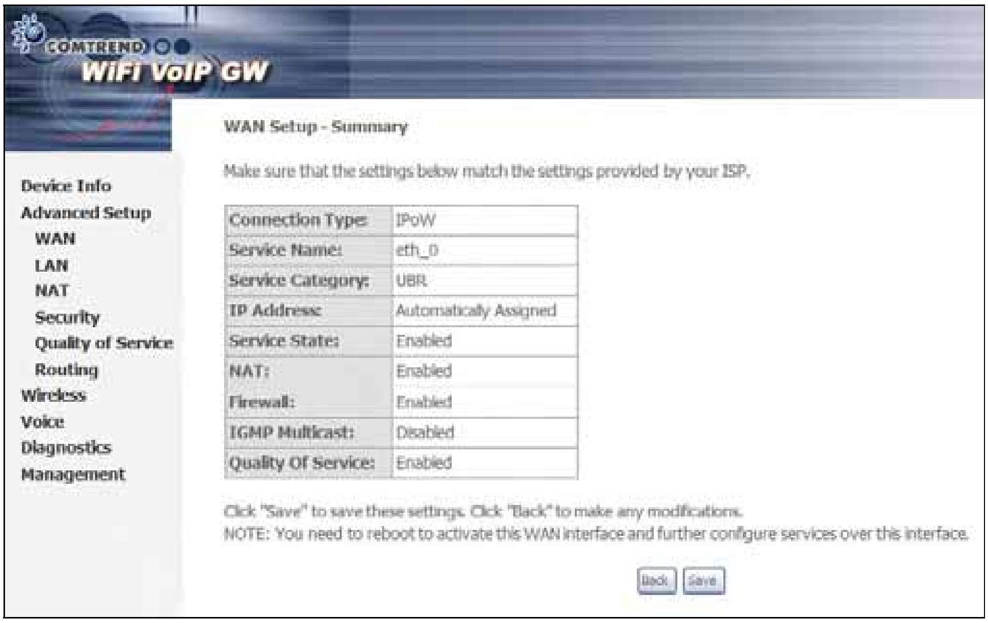
Enable IGMP Multicast □
Enable WAN Service ☑
Service Name: eth_0

Enable NAT
If the LAN is configured with a private IP address, the user should select this checkbox. The user can then configure NAT-related features. If a private IP address is not used on the LAN side, this checkbox should not be selected, so as to free up system resources for improved performance.

Enable Firewall
If the firewall checkbox is selected, the user can configure the device firewall.

Enable IGMP Multicast checkbox
Tick the checkbox to enable IGMP multicast (proxy). IGMP (Internet Group Membership Protocol) is a protocol used by IP hosts to report their multicast group memberships to any immediately neighboring multicast device's.

STEP 9: Click Next to display the WAN Setup-Summary screen that presents the entire configuration summary review. Click Back to modify the settings.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoW
Service Name:	eth_0
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

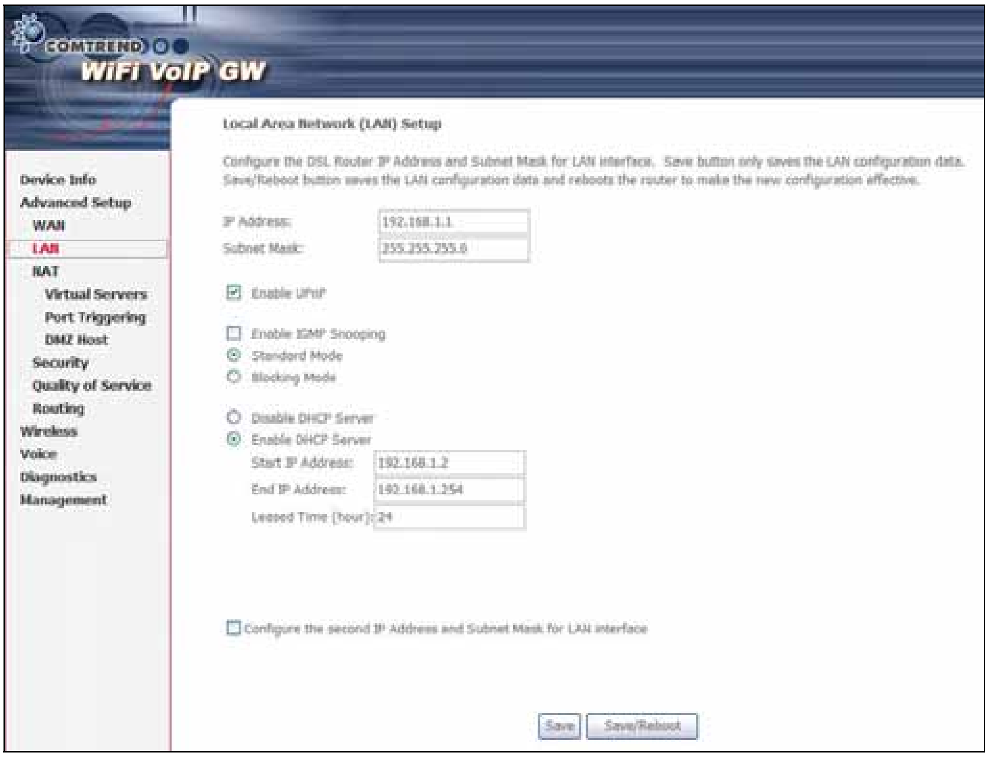
Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

STEP 10: At this point, the device will save the configuration to flash memory and reboot. The Web UI will not respond until the device is ready. The Web UI should refresh to the default page automatically.

If not, restart the browser and login again, following the steps in subsection 3.3 Login Procedure**.**

5.2 LAN

Configure the device IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the device to apply the new configuration.



Local Area Network (LAN) Setup

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

☑ Enable UPnP

□ Enable IGMP Snooping
● Standard Mode
○ Blocking Mode

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.1.2
End IP Address: 192.168.1.254
Leased Time (hour): 24

□ Configure the second IP Address and Subnet Mask for LAN interface

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

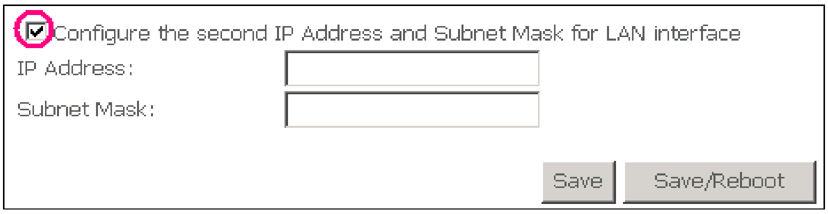
Enable UPnP: Tick the box to enable.

Enable IGMP Snooping: Enable by ticking the box.

Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group – even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

To configure a secondary IP address tick the checkbox shown below.



☑ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:	
Subnet Mask:	

IP Address: Enter the secondary IP address for the LAN port.

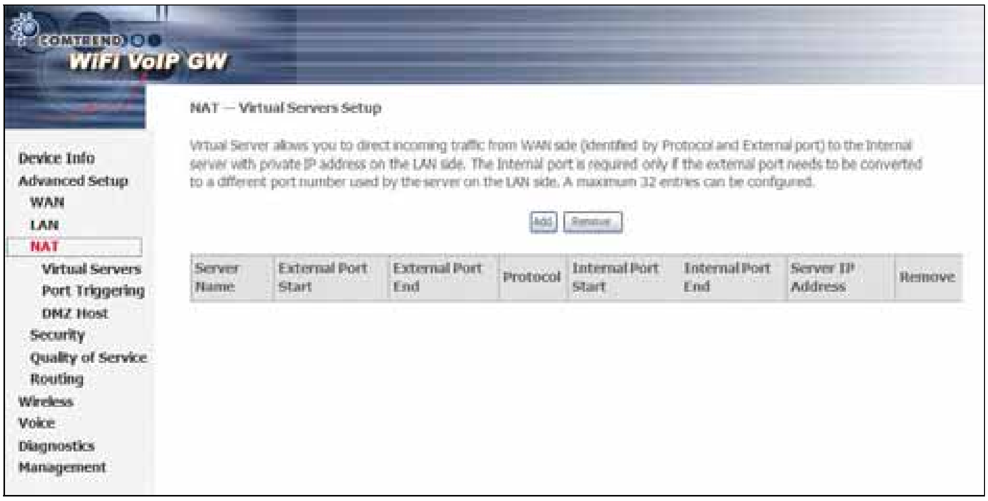
Subnet Mask: Enter the secondary subnet mask for the LAN port.

5.3 NAT

NOTE: To display the NAT function, you must enable NAT in WAN Setup.

5.3.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the Internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.

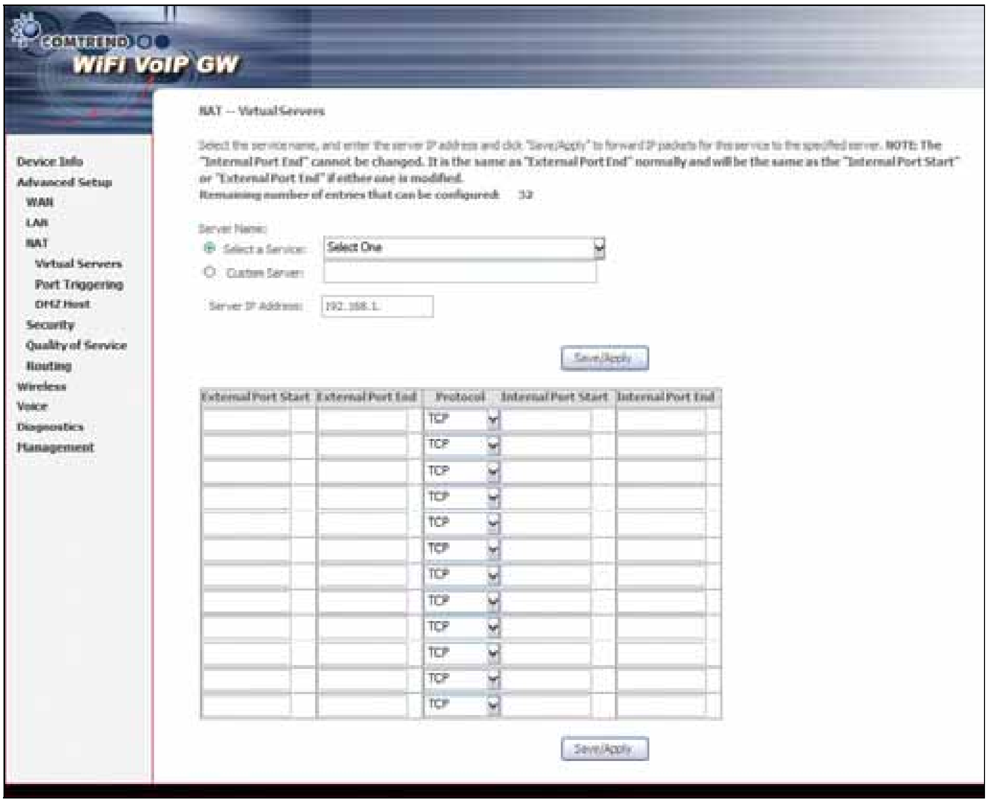


NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove

To add a Virtual Server, click the **Add** button. The following screen will display.



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**
Remaining number of entries that can be configured: 32

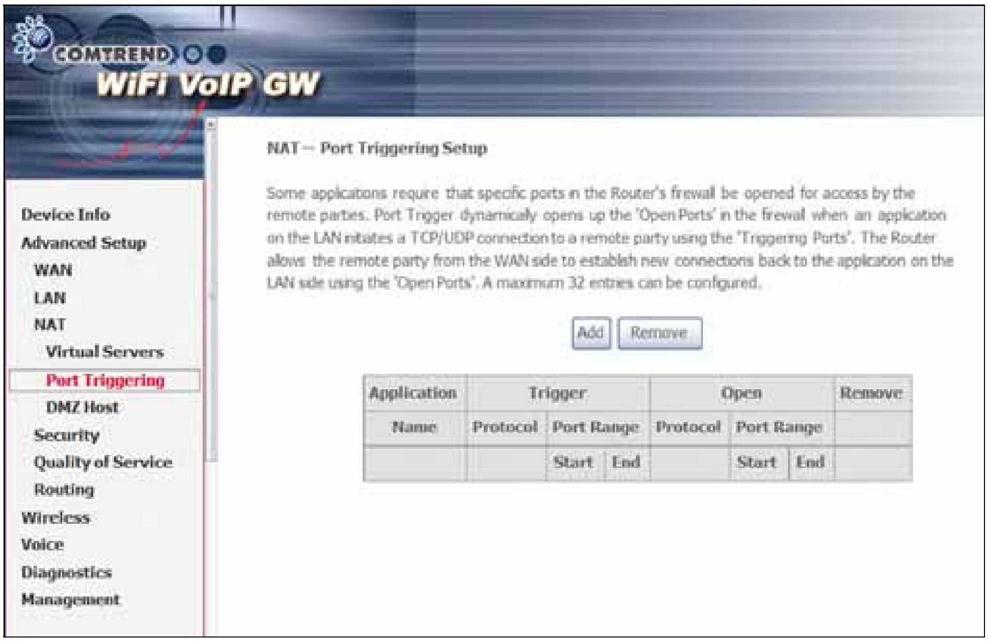
Server Name:
● Select a Service: Select One
○ Custom Server:
Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

Select a Service Or Custom Server	User should select the service from the list. Or User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

5.3.2 Port Triggering

Some applications require that specific ports in the device's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The device allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum of 32 entries can be configured.

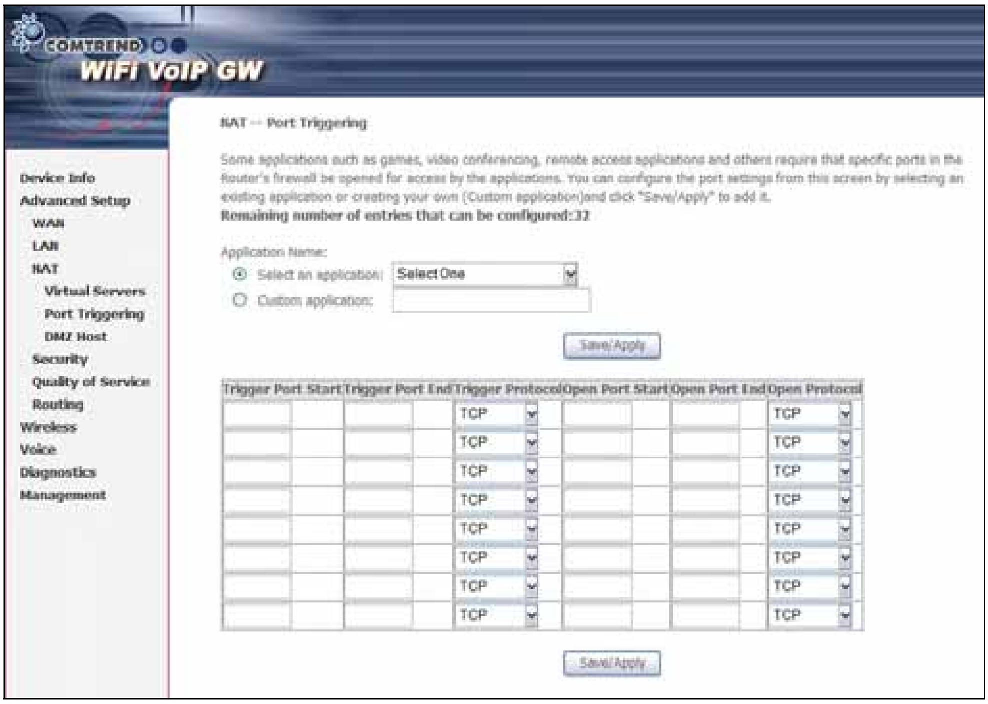


NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application	Trigger			Open			Remove
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	

To add a Trigger Port, click the **Add** button. The following screen will display.



NAT -- Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Application Name:

◉ Select an application: Select One

○ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

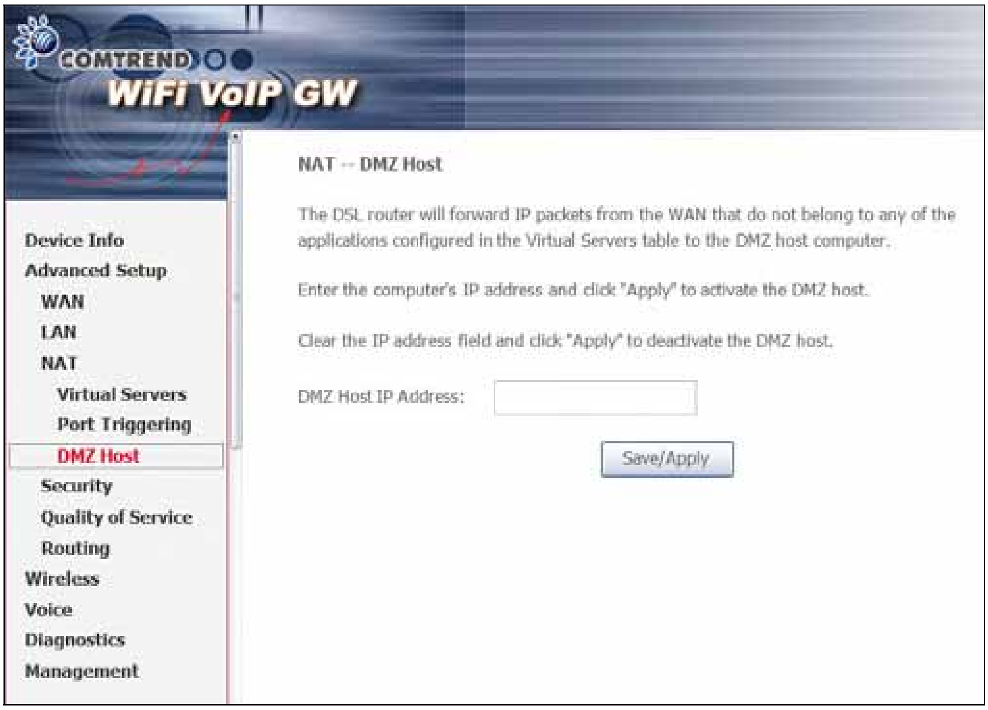
Select an Application Or Custom Application	User should select the application from the list. Or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Trigger Protocol	User can select from: TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected the port ranges are automatically configured.
Open Protocol	User can select from: TCP, TCP/UDP or UDP.

5.3.3 DMZ Host

The device will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click **Apply** to activate the DMZ host.

Clear the IP address field and click **Apply** to deactivate the DMZ host.



NAT -- DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

5.4 Security

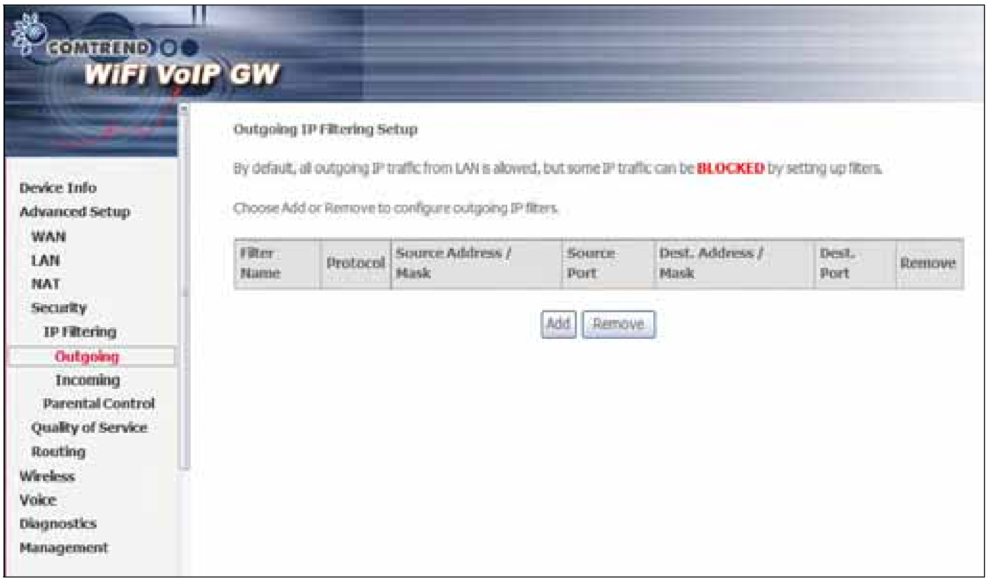
NOTE: The Firewall must be enabled to access this option

5.4.1 IP Filtering

IP filtering allows you to create a filter rule to identify outgoing/incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click **Save/Apply** to save and activate the filter.

Outgoing IP Filter

NOTE: The default setting for all Outgoing traffic is **ACCEPTED**.



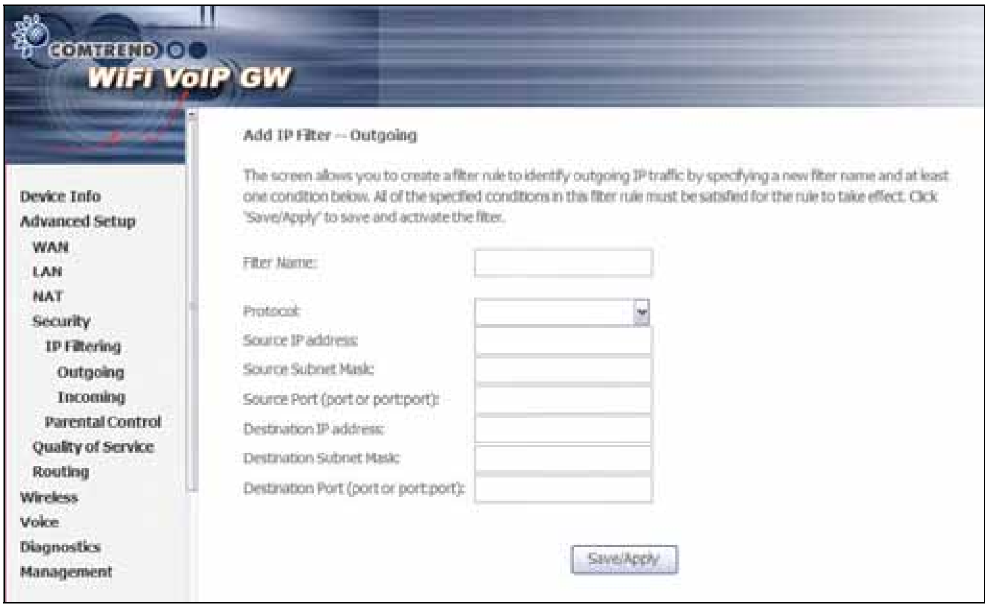
Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Choose Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, click the **Add** button. The following screen will display.



Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

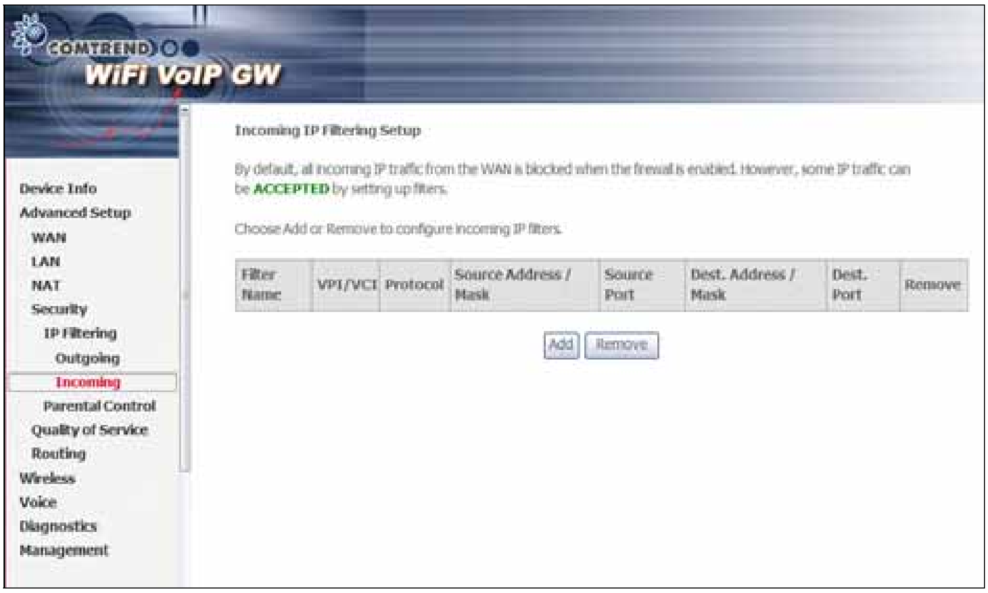
Destination Subnet Mask:

Destination Port (port or port:port):

Filter Name	Type a name for the filter rule.
Protocol	TCP, TCP/UDP, UDP or ICMP.
Source IP address	Enter source IP address.
Source Subnet Mask	Enter source subnet mask.
Source Port (port or port:port)	Enter source port number or port range.
Destination IP address	Enter destination IP address.
Destination Subnet Mask	Enter destination subnet mask.
Destination port (port or port:port)	Enter destination port number or port range.

Incoming

NOTE: The default setting for all Incoming traffic is **BLOCKED**.



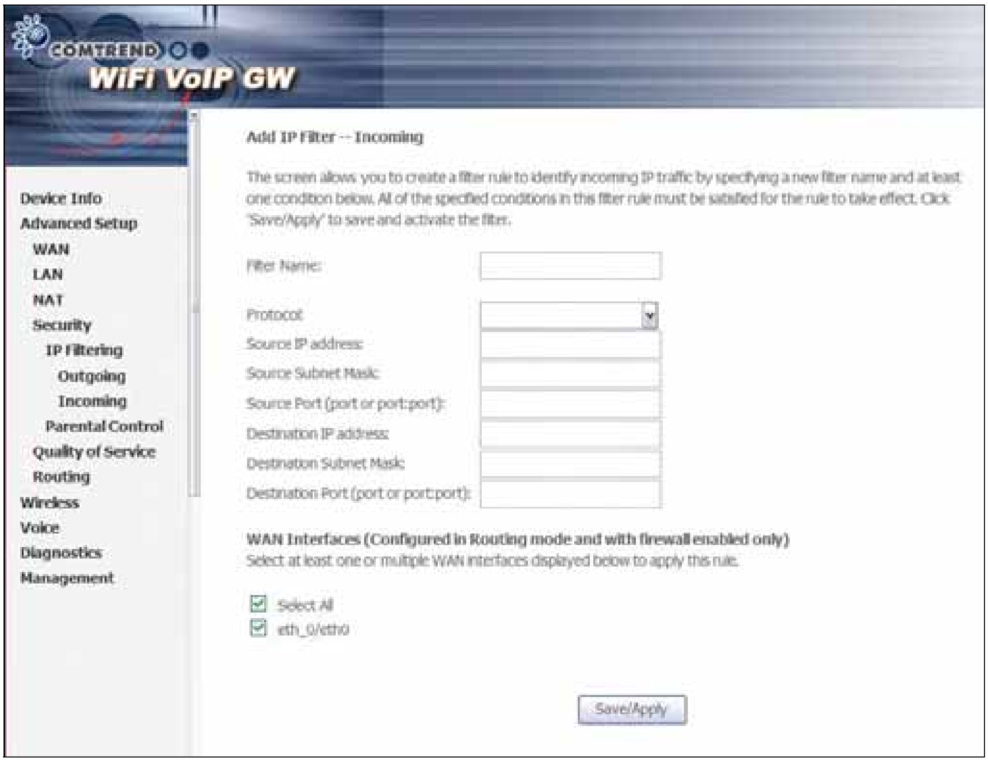
Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name	VPI/VCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove

To add a filtering rule, click the **Add** button. The following screen will display.



Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

Select at least one or multiple WAN interfaces displayed below to apply this rule.

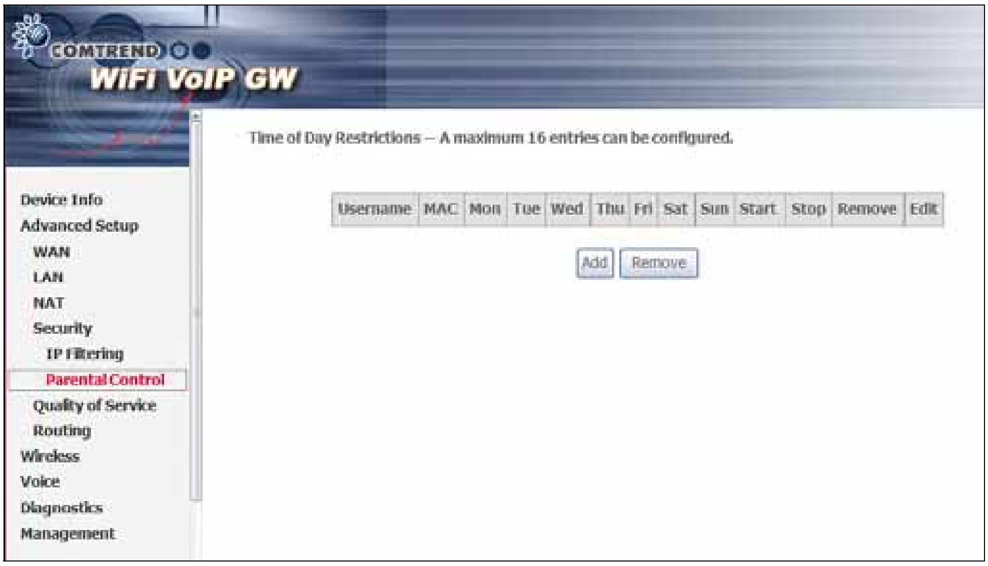
☑ Select All

☑ eth_0/eth0

To configure the parameters, please reference the **Outgoing IP Filter** table.

5.4.2 Parental Control

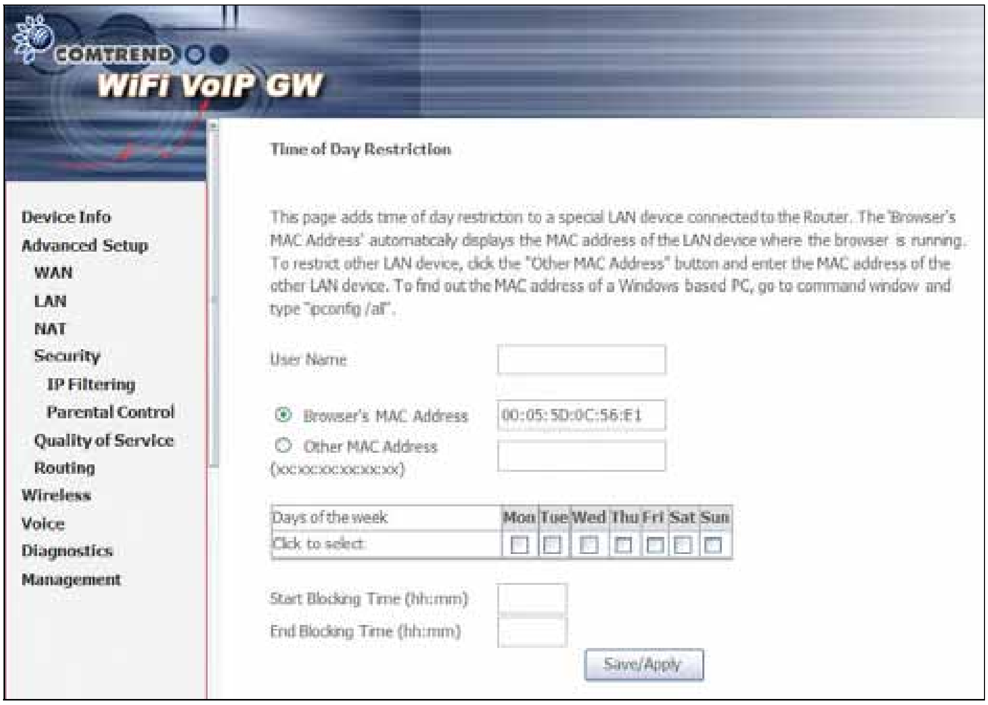
Daytime Parental Control
This feature restricts access of a selected LAN device to an outside network through the router, as per chosen days of the week and the chosen times.



Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove	Edit

Click **Add** to display the following screen.



Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

User Name

● Browser's MAC Address 00:05:5D:0C:56:E1

○ Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	□	□	□	□	□	□	□

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

See below for instructions. Click **Save/Apply** to apply the settings.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

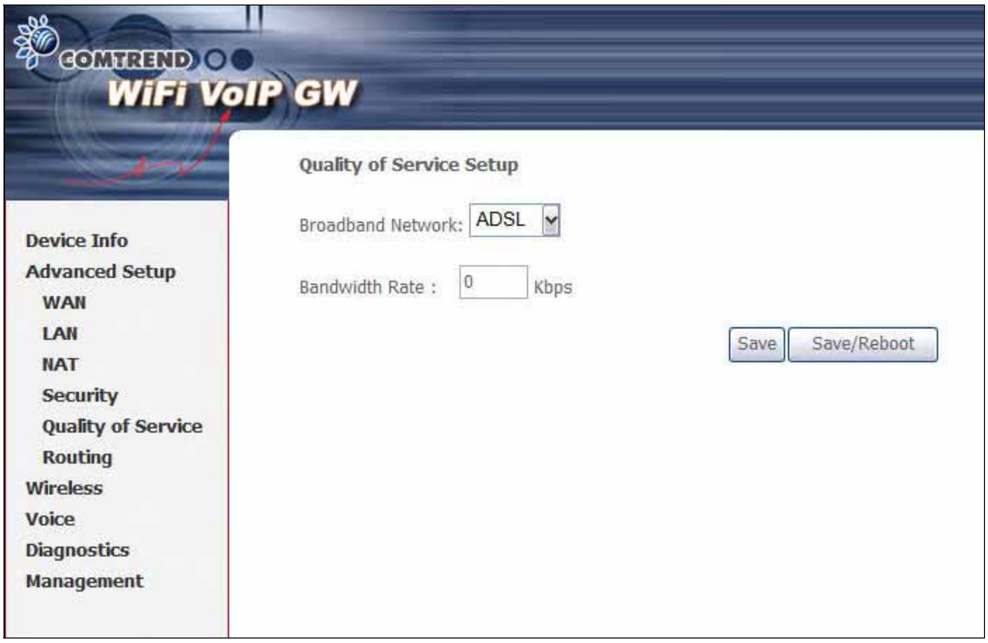
Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

5.5 Quality of Service

Choose the broadband network environment: **Cable** or **ADSL**. Then set the maximum upstream bandwidth rate in Kbps. Click **Save** or **Save/Reboot**.



Quality of Service Setup

Broadband Network: ADSL

Bandwidth Rate : 0 Kbps

NOTE: To display this function, QoS must be enabled in WAN Setup.

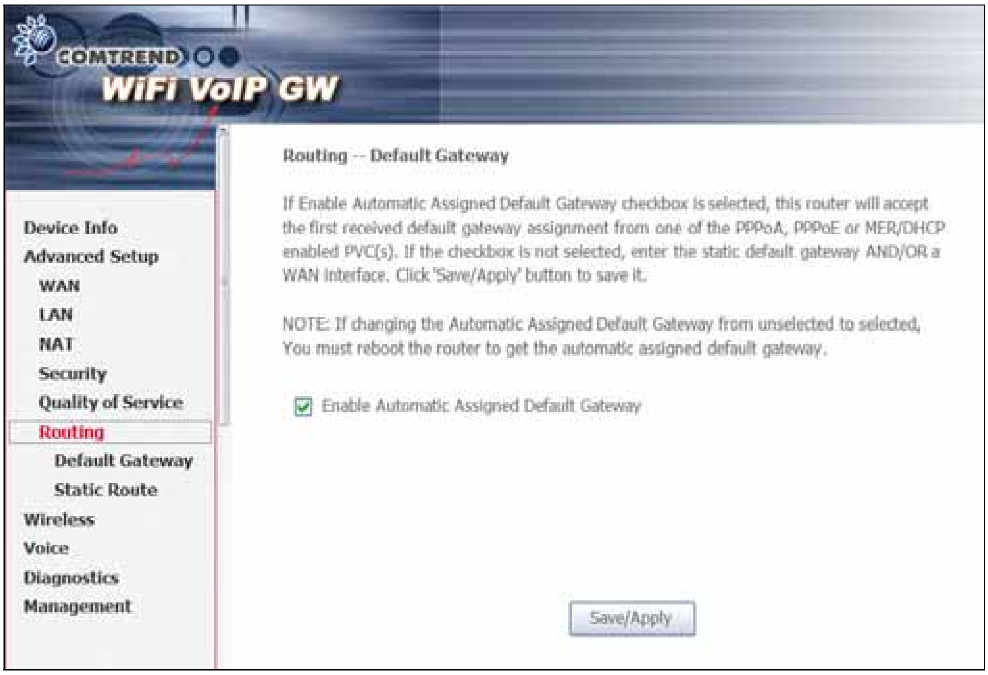
5.6 Routing

This option allows for **Default Gateway** and **Static Route** configuration.

5.6.1 Default Gateway

If **Enable Automatic Assigned Default Gateway** checkbox is selected, this device will accept the first received default gateway assignment from one of the enabled PVC(s). If the checkbox is not selected, enter the static default gateway and/or WAN interface. Click **Save/Apply** button to save it.

NOTE:	After enabling the Automatic Assigned Default Gateway, the device must be rebooted to activate the assigned default gateway.



Routing -- Default Gateway

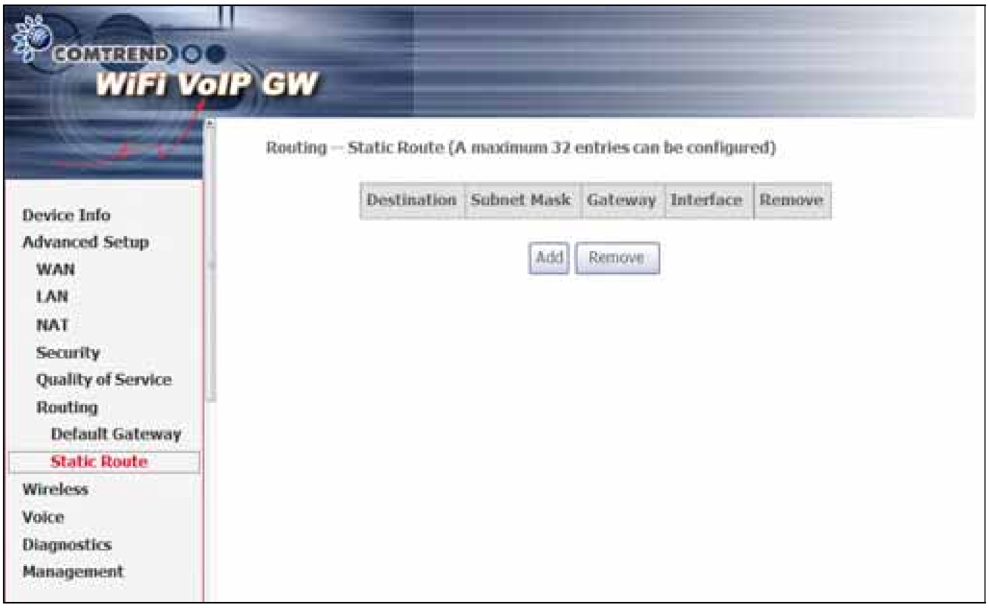
If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway AND/OR a WAN interface. Click 'Save/Apply' button to save it.

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☑ Enable Automatic Assigned Default Gateway

5.6.2 Static Route

The Static Route screen lists the configured static routes.
Choose **Add** or **Remove** to configure the static routes.

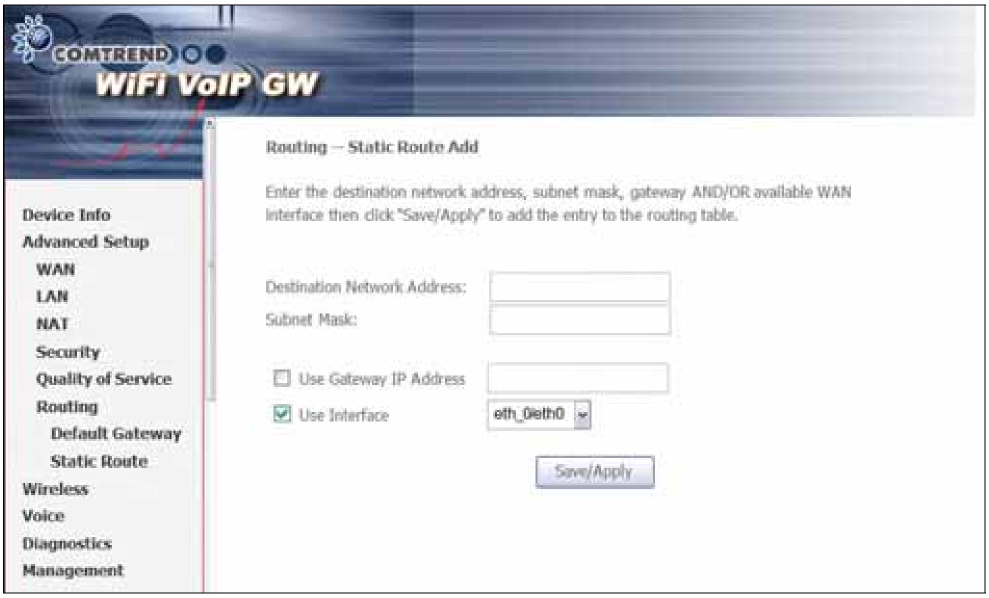


Routing -- Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove

Click the **Add** button and the following screen will display.

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click **Save/Apply** to add the entry to the routing table.



Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.

Destination Network Address:

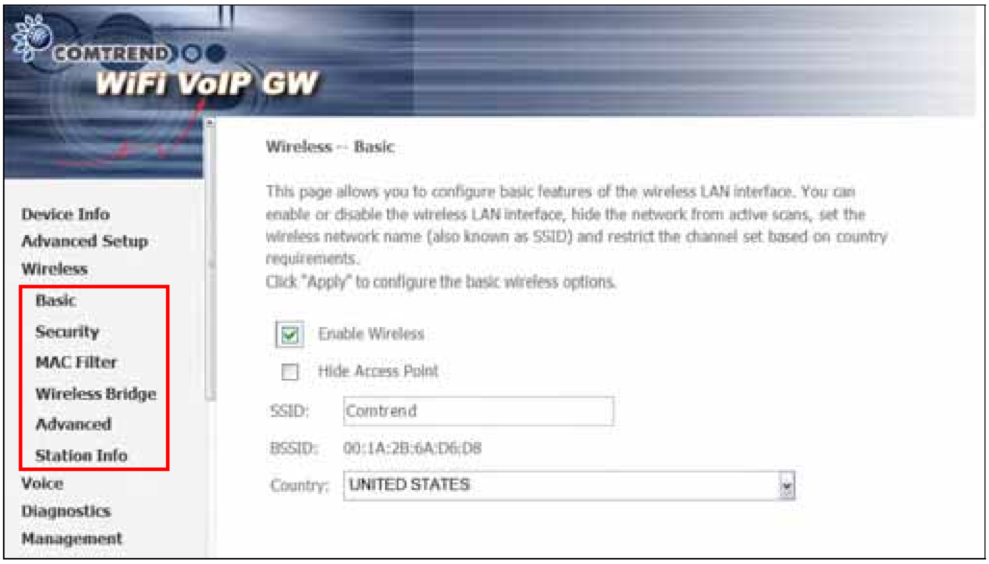
Subnet Mask:

☐ Use Gateway IP Address

☑ Use Interface eth_0/eth0

Chapter 6 Wireless

The Wireless menu allow you to enable the wireless capability, hide the access point, set the wireless network name and restrict the channel set.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

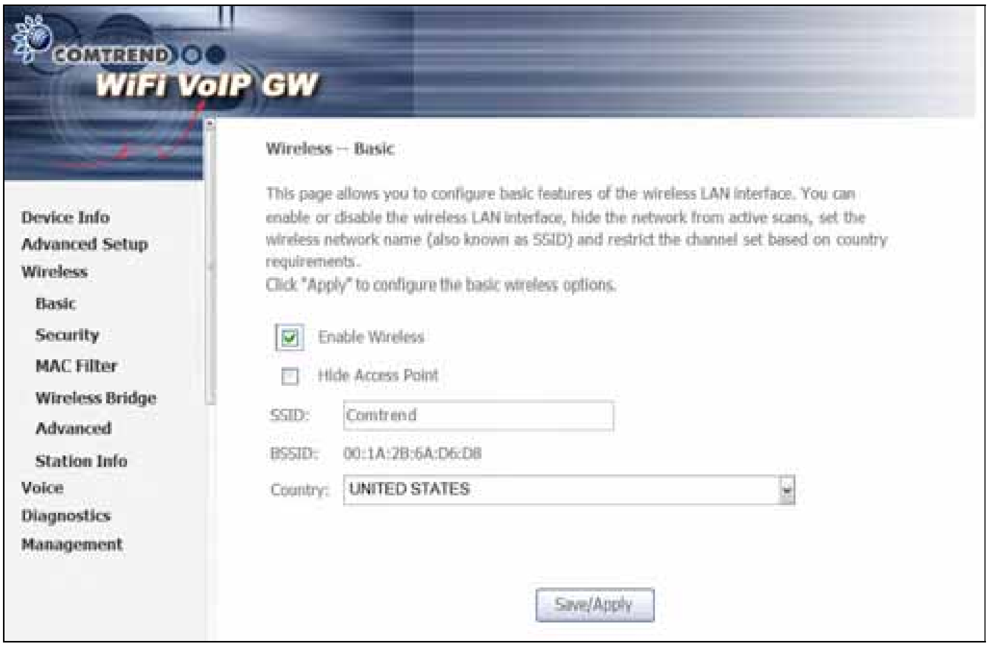
SSID: Comtrend

BSSID: 00:1A:2B:6A:D6:D8

Country: UNITED STATES

6.1 Basic

This screen allows you to enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.



Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Click "Apply" to configure the basic wireless options.

☑ Enable Wireless

□ Hide Access Point

SSID: Comtrend

BSSID: 00:1A:2B:6A:D6:D8

Country: UNITED STATES

Option	**Description**
Enable Wireless	A checkbox that enables or disables the wireless LAN interface. When selected, the Web UI displays Hide Access point, SSID, and County settings. The default is Enable Wireless.
Hide Access Point	Select Hide Access Point to protect device access point from detection by wireless active scans. If you do not want the access point to be automatically detected by a wireless station, this checkbox should be de-selected. The station will not discover this access point. To connect a station to the available access points, the station must manually add this access point name in its wireless configuration. In Windows XP, go to the Network>Programs function to view all of the available access points. You can also use other software programs such as NetStumbler to view available access points.
SSID	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access. The naming conventions are: Minimum is one character and maximum number of characters: 32 bytes.
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each county listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan=10-13, Israel=TBD

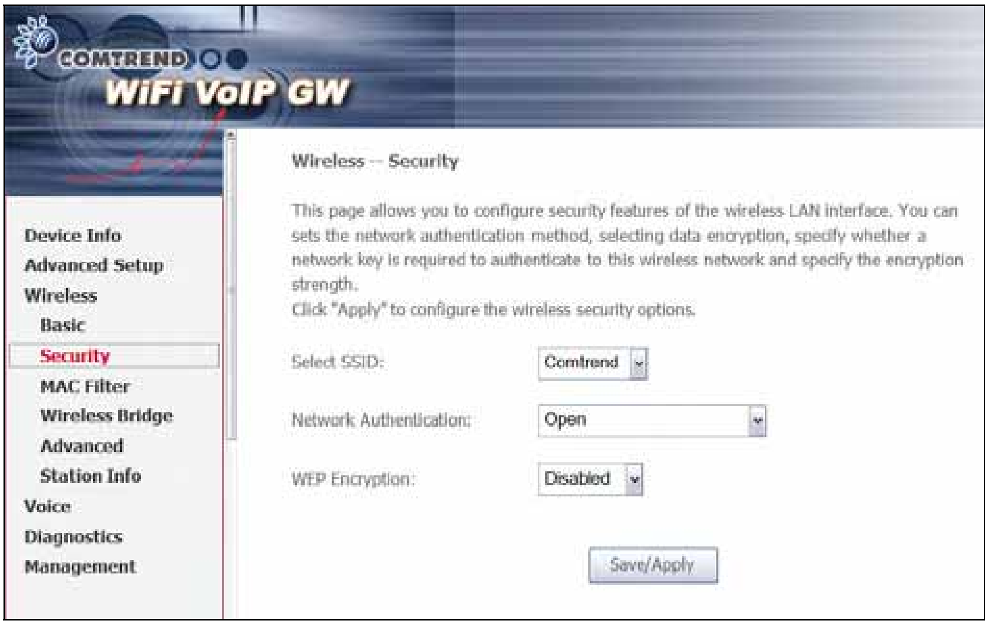
6.2 Security

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

802.11 supports two subtypes of network authentication services: open system and shared key. Under open system authentication, any wireless station can request authentication. The system that needs to authenticate with another wireless station sends an authentication management frame that contains the identity of the sending station. The receiving station then sends back a frame that indicates whether it recognizes the identity of the sending station.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from 802.11 wireless network communications channel.

The following screen appears when Security is selected. The Security page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.



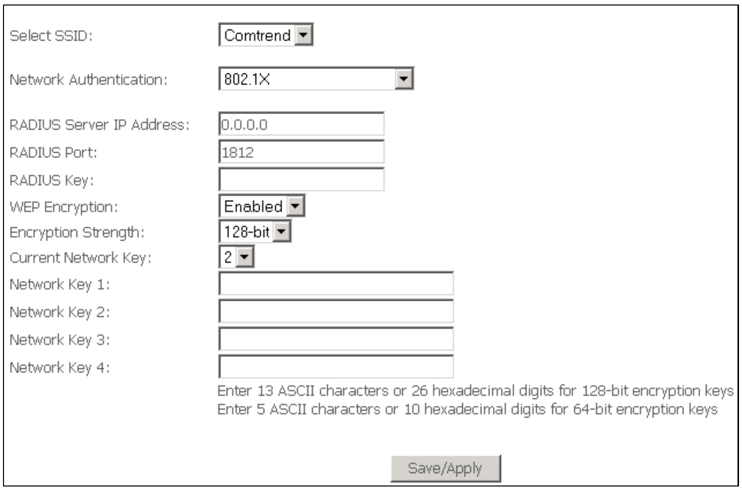
Wireless -- Security

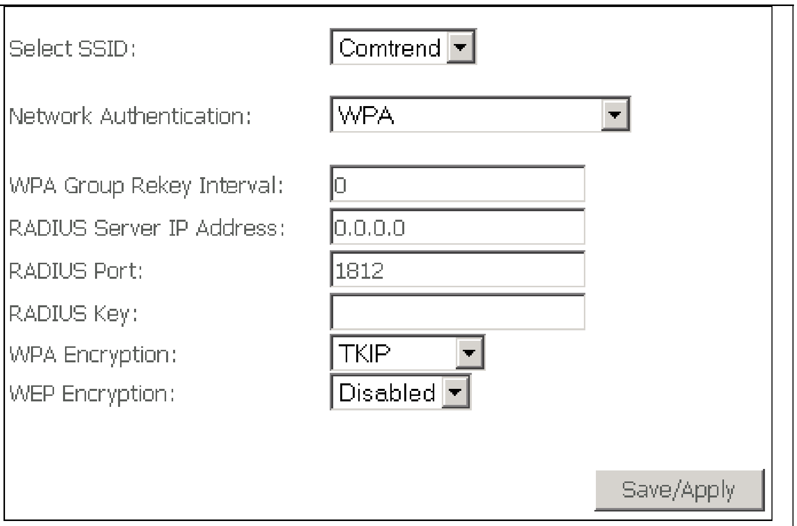
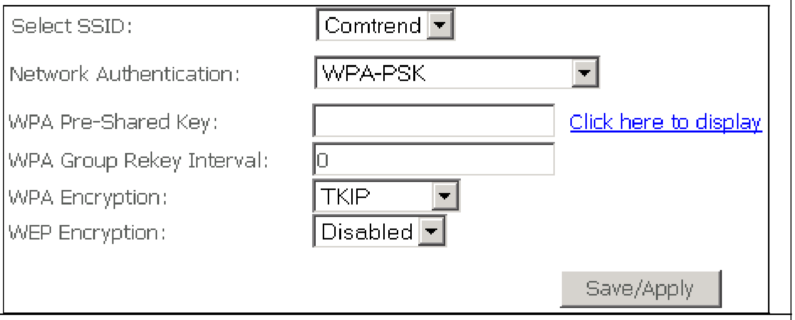
This page allows you to configure security features of the wireless LAN interface. You can sets the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

Select SSID: Comtrend

Network Authentication: Open

WEP Encryption: Disabled

Option	Description
Network Authentication	It specifies the network authentication. When this checkbox is selected, it specifies that a network key be used for authentication to the wireless network. If the Network Authentication (Shared mode) checkbox is not shared (that is, if open system authentication is used), no authentication is provided. Open system authentication only performs identity verifications. Different authentication type pops up different settings requests. Choosing **802.1X**, enter RADIUS Server IP address, RADIUS Port, RADIUS key and Current Network Key. Also, enable WEP Encryption and select Encryption Strength.  Select SSID: Comtrend Network Authentication: 802.1X RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WEP Encryption: Enabled Encryption Strength: 128-bit Current Network Key: 2 Network Key 1: Network Key 2: Network Key 3: Network Key 4: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys Select the Current Network Key and enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys and enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys. Choosing **WPA**, you must enter WPA Group Rekey Interval.

	 Select SSID: Comtrend Network Authentication: WPA WPA Group Rekey Interval: 0 RADIUS Server IP Address: 0.0.0.0 RADIUS Port: 1812 RADIUS Key: WPA Encryption: TKIP WEP Encryption: Disabled Save/Apply Choosing **WPA-PSK**, you must enter WPA Pre-Shared Key and Group Rekey Interval.  Select SSID: Comtrend Network Authentication: WPA-PSK WPA Pre-Shared Key: Click here to display WPA Group Rekey Interval: 0 WPA Encryption: TKIP WEP Encryption: Disabled Save/Apply
WEP Encryption	It specifies that a network key is used to encrypt the data is sent over the network. When this checkbox is selected, it enables data encryption and prompts the Encryption Strength drop-down menu. Data Encryption (WEP Enabled) and Network Authentication use the same key.
Encryption strength	A session's key strength is proportional to the number of binary bits comprising the session key file. This means that session keys with a greater number of bits have a greater degree of security, and are considerably more difficult to forcibly decode. This drop-down menu sets either a 64 8-bit (5-character or 10-character hexadecimal or 128 8-bit (13-character or 10-character) key. If you set a minimum 128-bit key strength, users attempting to establish a secure communications channel with your server must use a browser capable of communicating with a 128-bit session key. The Encryption Strength settings do not display unless the network Authentication (shared Mode) check box is selected.

6.3 MAC Filter

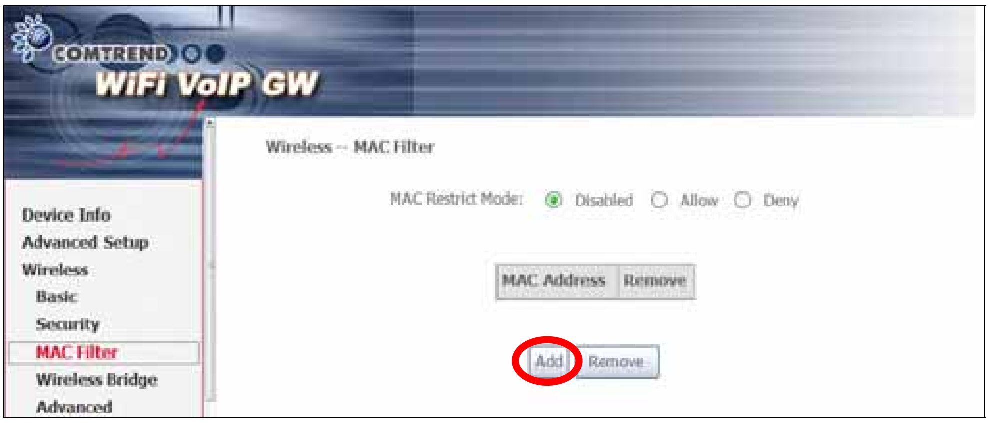
This MAC Filter page allows access to be restricted/allowed based on a MAC address. All NICs have a unique 48-bit MAC address burned into the ROM chip on the card. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. Therefore, an access point will grant access to any computer that is using a NIC whose MAC address is on its "allows" list.

Wi-Fi device's and access points that support MAC filtering let you specify a list of MAC addresses that may connect to the access point, and thus dictate what devices are authorized to access the wireless network. When a device is using MAC filtering, any address not explicitly defined will be denied access.

MAC Restrict mode: **Off** - disables MAC filtering; **Allow** – permits **access** for the specified MAC address; deny; reject access of the specified MAC address, then click the **SET** button.

To delete an entry**,** select the entry at the bottom of the screen and then click the **Remove** button, located on the right hand side of the screen.

To add a MAC entry, click **Add** and enter MAC address

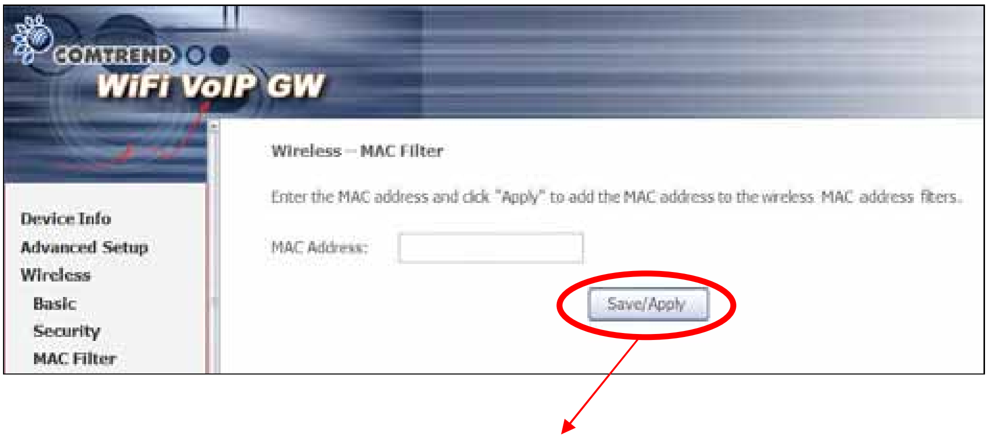


Wireless -- MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

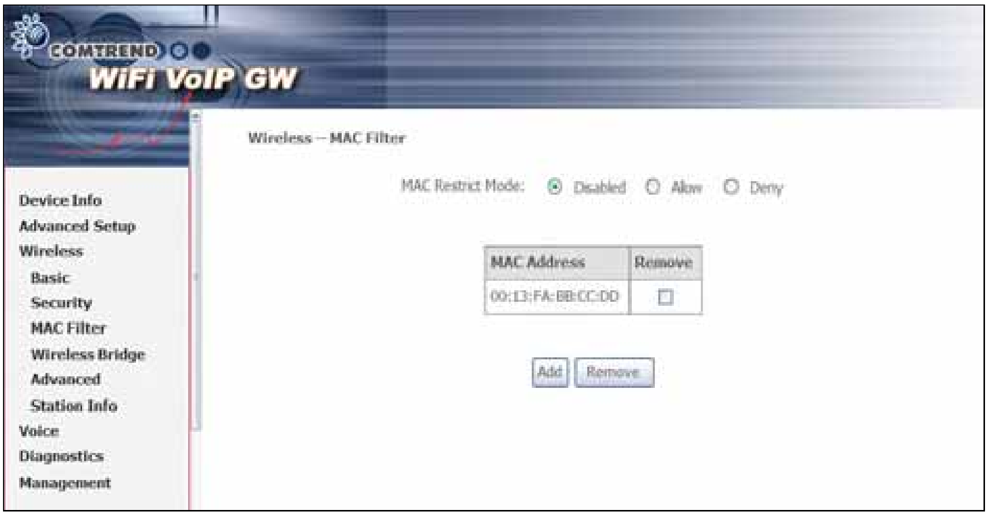
The following screen will appear. Enter the MAC address and click **Save/Apply** to add the MAC address to the wireless MAC address filters.



Wireless -- MAC Filter

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

MAC Address:



Wireless -- MAC Filter

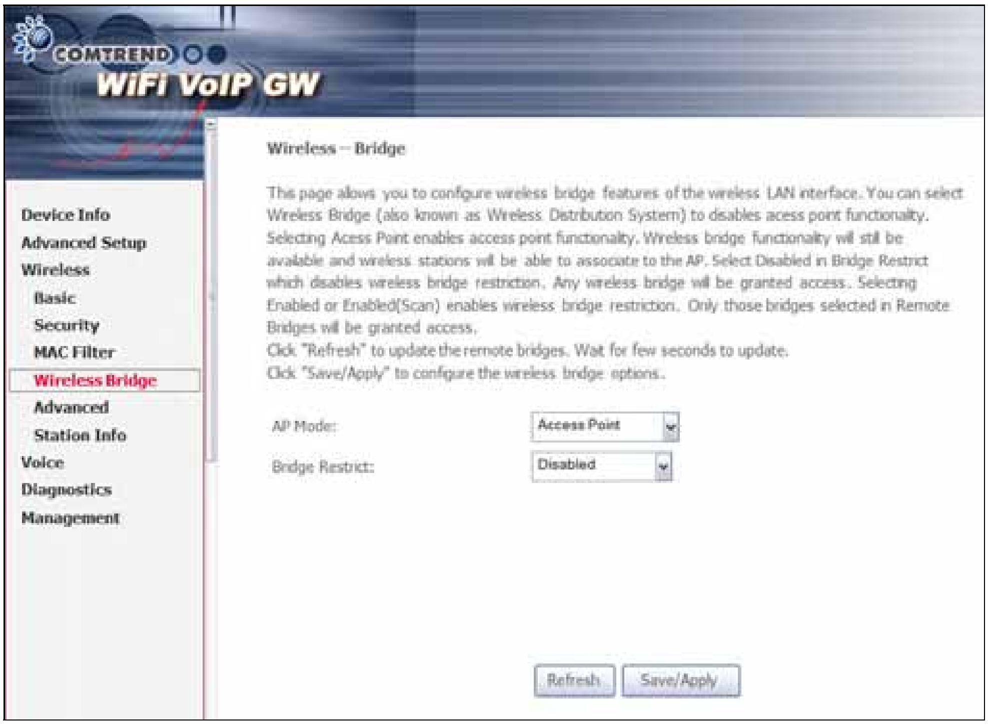
MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove
00:13:FA:BB:CC:DD	□

Option	Description
MAC Restrict Mode	Radio buttons that allow settings of; Off: MAC filtering function is disabled. Allow: Permits PCs with listed MAC addresses to connect to the access point. Deny: Prevents PCs with listed MAC from connecting to the access point.
MAC Address	Lists the MAC addresses subject to the Off, Allow, or Deny instruction. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. The maximum number of MAC addresses that can be added is 60.

6.4 Wireless Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select **Wireless Bridge** (also known as Wireless Distribution System) to disable access point functionality. Selecting **Access Point** enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select **Disabled** in **Bridge Restrict** to disable wireless bridge restriction. Any wireless bridge will then be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.



Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disables acess point functionality. Selecting Acess Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Save/Apply" to configure the wireless bridge options.

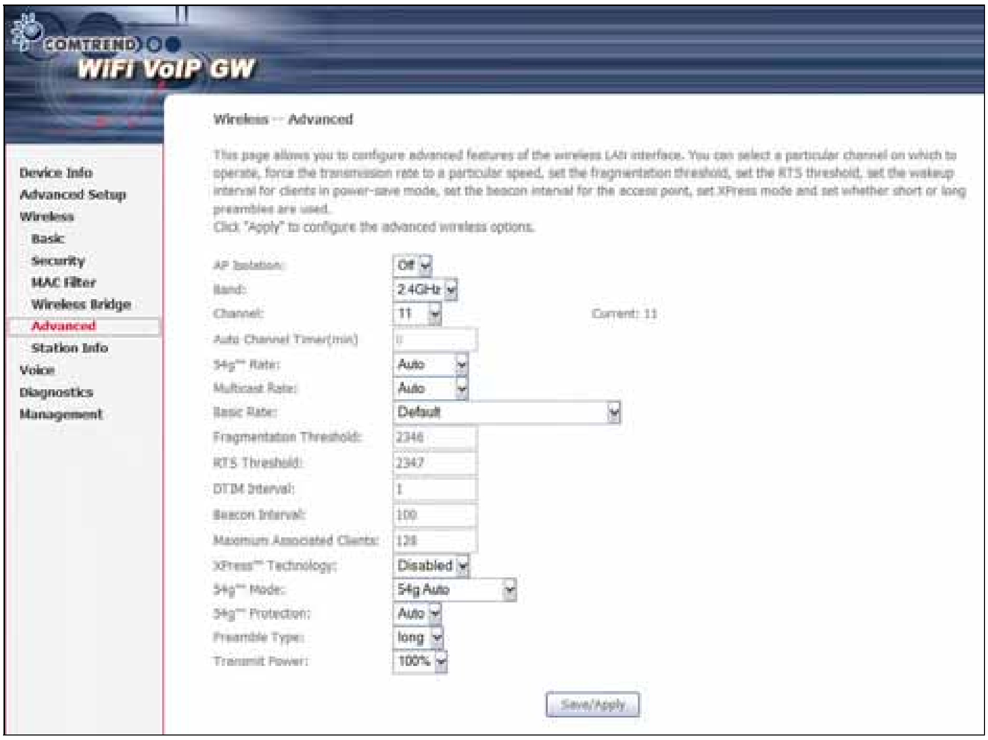
AP Mode: Access Point

Bridge Restrict: Disabled

Mode	Options
AP Mode	Access Point Wireless Bridge
Bridge Restrict	Enabled Enabled (Scan) Disabled

6.5 Advanced

The Advanced page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point and set whether short or long preambles are used. Click **Apply** to configure the advanced wireless options.



Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.
Click "Apply" to configure the advanced wireless options.

AP Isolation: Off
Band: 2.4GHz
Channel: 11   Current: 11
Auto Channel Timer(min): 0
54g™ Rate: Auto
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Maximum Associated Clients: 128
XPress™ Technology: Disabled
54g™ Mode: 54g Auto
54g™ Protection: Auto
Preamble Type: long
Transmit Power: 100%

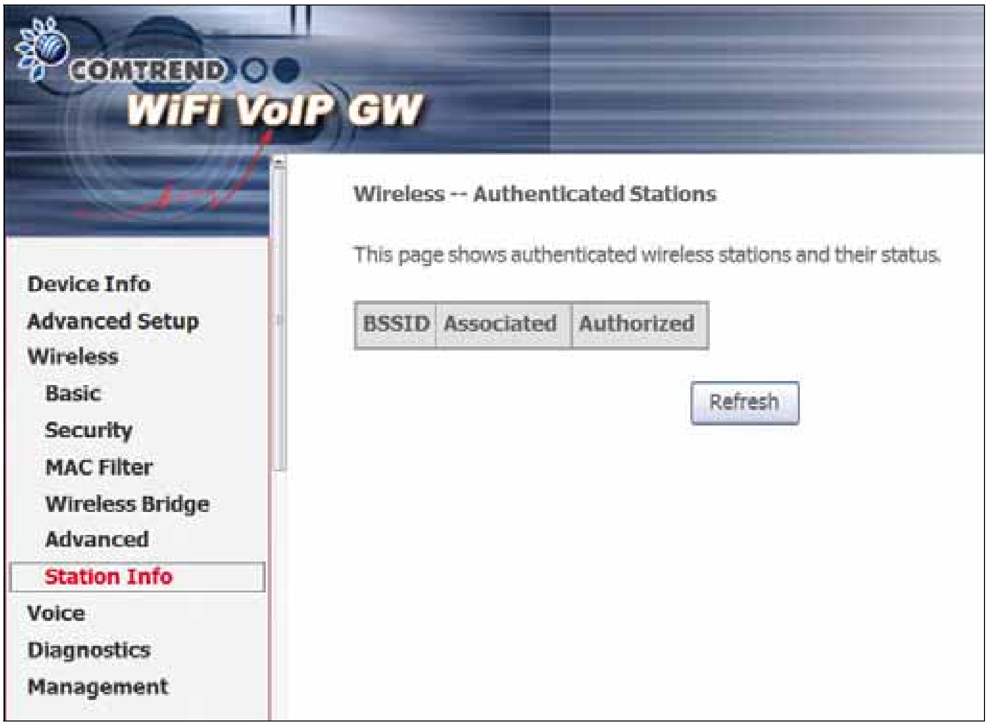
Option	**Description**
AP Isolation	Select On or Off. By enabling this feature, wireless clients associated with the Access Point will be able to connect to each other.
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band.
Channel	Drop-down menu that allows selection of specific channel
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
54g™ Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary.

	1 Mbps, 2Mbps, 5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate
Basic Rate	Setting basic transmit rate
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into, smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate, try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, when set in bytes, specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.
DTIM Interval	Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.
Beacon Interval	The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point. Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)
Maximum Associated Clients	The maximum number of clients that may connect to the access point. The device supports up to 128.
Xpress ^{TM} Technology	Xpress Technology is compliant with draft

	specifications of two planned wireless industry standards.
54g ^{TM} Mode	Select the mode to 54g Auto for the widest compatibility. Select the mode to 54g Performance for the fastest performance among 54g certified equipment. Set the mode to 54g LRS if you are experiencing difficulty with legacy 802.11b equipment.
54g Protection	In Auto mode the device will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
Preamble Type	Short preamble is intended for application where maximum throughput is desired but it doesn't cooperate with the legacy. Long preamble interoperates with the current 1 and 2 Mbit/s DSSS specification as described in IEEE Std 802.11-1999
Transmit Power	The router will set different power output (by percentage) according to this selection.

6.6 Station Info

This page shows authenticated wireless stations and their status.



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

BSSID	Associated	Authorized

BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

Chapter 7   Voice

This chapter first describes the **SIP** and **Dial Plan** configuration screens. The last section (**7.3 Telephone Calls**) describes how to use the VoIP (Voice over IP) and PSTN (Public Switched Telephone Network) voice services.

7.1 SIP

Session Initiation Protocol (SIP) is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. It is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP.

It is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

Session Initiation Protocol is a peer-to-peer protocol.

There are four components in the SIP standard:

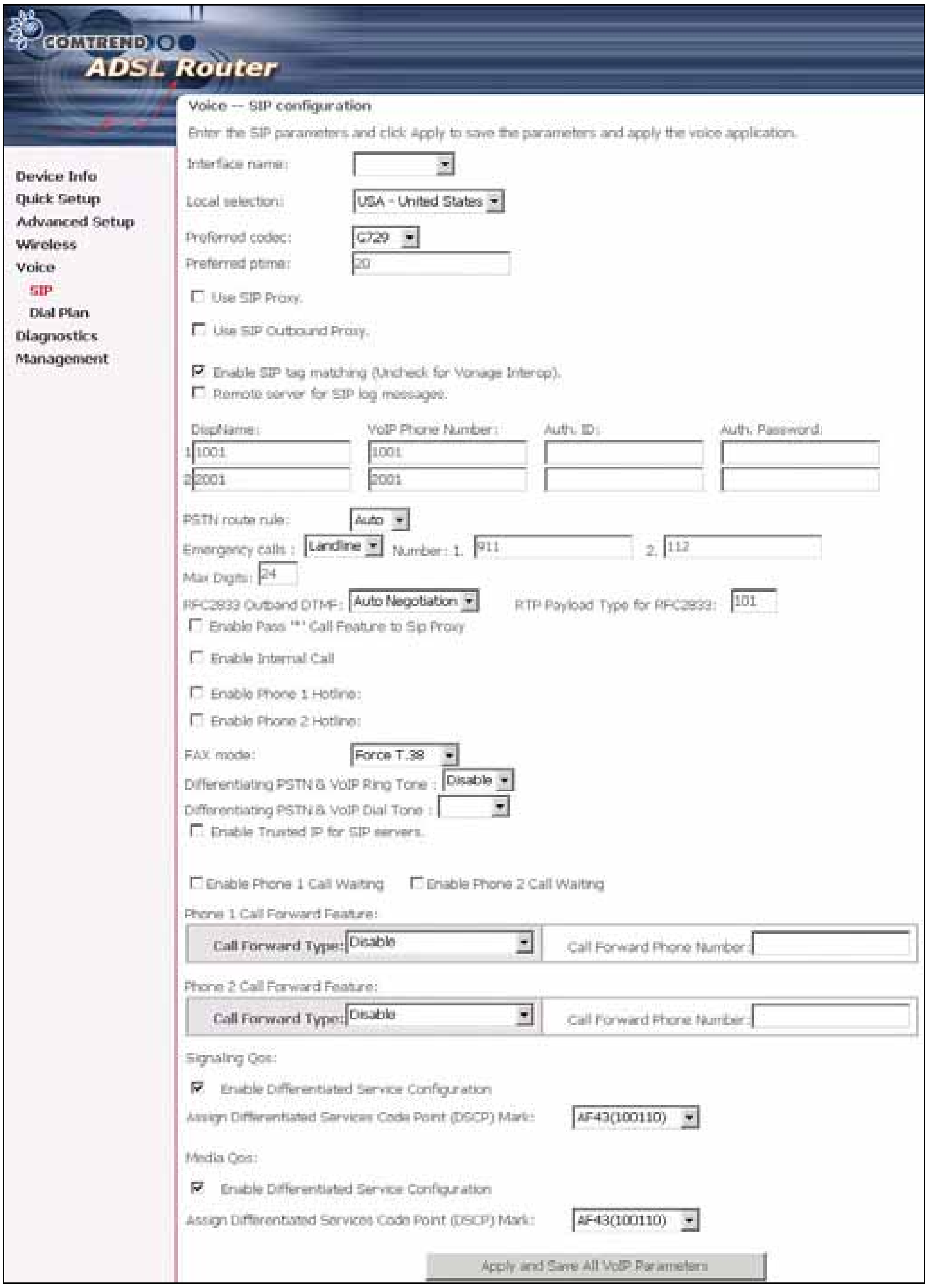
(a) User Agents (**UA**) - SIP phone clients (hardware or software)

(b) Proxy Server – relays data between **UA** and external servers

(c) Registrar Server - a server that accepts register requests from **UA**

(d) Redirect Server – provides an address lookup service to **UA**

To access the SIP configuration screen, click **SIP** from the **Voice** submenu.



Voice -- SIP configuration

Enter the SIP parameters and click Apply to save the parameters and apply the voice application.

Interface name:

Local selection: USA - United States

Preferred codec: G729

Preferred ptime: 20

□ Use SIP Proxy.

□ Use SIP Outbound Proxy.

☑ Enable SIP tag matching (Uncheck for Vonage Interop).

□ Remote server for SIP log messages:

	DispName:	VoIP Phone Number:	Auth. ID:	Auth. Password:
1	1001	1001		
2	2001	2001		

PSTN route rule: Auto

Emergency calls : Landline Number: 1. 911 2. 112

Max Digits: 24

RFC2833 Outband DTMF: Auto Negotiation RTP Payload Type for RFC2833: 101

□ Enable Pass "*" Call Feature to Sip Proxy

□ Enable Internal Call

□ Enable Phone 1 Hotline:

□ Enable Phone 2 Hotline:

FAX mode: Force T.38

Differentiating PSTN & VoIP Ring Tone : Disable

Differentiating PSTN & VoIP Dial Tone :

□ Enable Trusted IP for SIP servers.

□ Enable Phone 1 Call Waiting □ Enable Phone 2 Call Waiting

Phone 1 Call Forward Feature:

Call Forward Type: Disable Call Forward Phone Number :

Phone 2 Call Forward Feature:

Call Forward Type: Disable Call Forward Phone Number :

Signaling Qos:

☑ Enable Differentiated Service Configuration

Assign Differentiated Services Code Point (DSCP) Mark: AF43(100110)

Media Qos:

☑ Enable Differentiated Service Configuration

Assign Differentiated Services Code Point (DSCP) Mark: AF43(100110)

Once the settings are configured click **Apply and Save All VoIP Parameters** to reset the VoIP service to use the new settings.

This table describes the SIP configuration options shown on the previous page.

Interface name	WAN interface name
Local Selection	Set tone, ring type and physical characteristics for each specific country.
Preferred codec	The default is G.711U.
Preferred ptime	The default is 20.
Use SIP proxy	A proxy is an intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or transferred to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it. Input IP address or domain name of the SIP proxy server, used for VOIP service. 5060 is the default (change based on your VoIP service provider).
Register Expire Time	The time period that the user would like the registration to be valid with the Registrar/ Proxy Server. The default is 300 seconds.
SIP domain name	Provided by your VoIP service provider.
Use SIP outbound proxy	Select if required by your VoIP provider.
Enable SIP tag matching (Uncheck for Vonage Interop).	Select if required by your VoIP provider.
Remote server for SIP log messages	Enable or disable remote server SIP log messages.
DispName	The caller ID display name.
VoIP Phone Number	As the modem has two FXS, two phone numbers can be listed.
Auth. ID	The authentication username for the Registrar/Proxy, as assigned by the VOIP service provider.
Auth. Password	The authentication password for the Registrar/proxy, as assigned by the VOIP service provider.
PSTN route rule	If PSTN route rule is **Auto**, an incoming PSTN call will ring an idle phone, either Phone1 or Phone2 (if Phone1 is busy). If PSTN route rule is **Fixed**, an incoming PSTN call will attempt to ring only the assigned phone line (Phone1 or Phone2).
Emergency calls Number 1 & 2	Emergency phone numbers. **Landline** or **VoIP** can be selected. **Please Note:** These numbers must be changed to correspond to the emergency numbers that are used in your location.
Max Digits	Sets the maximum number of digits for the phone number.
RFC2833 Outband DTMF	Enable the special use of RTP packets to transmit digit events.
RTP Payload Type for RFC2833	Payload types are defined in RFC 2833, RTP

	Payload for DTMF Digits, Telephony Tones and Telephony Signals. A payload type is a number from 96 to 127 that identifies the type of payload carried in the packet. The payload type should be identical on the GW and call agent.
Enable Pass '*' Call Feature to Sip Proxy	Only Tick if your VoIP Service Provider requires this.
Enable Internal Call	Tick if you would like to intercom your 2nd VoIP phone.
Enable Phone 1/2 Hotline	This setting is used if you require a certain phone number to always be dialled when you pickup your VoIP phone on Line 1 or Line 2. Setting this would mean that you can not make calls to any other number except the one programmed in here.
FAX mode	Choose Force T.38 or Pass through (G711u). You can plug a fax machine into either phone port and send or receive faxes. **Note:** This depends upon fax compatibility with your VoIP service provider.
Differentiating PSTN & VoIP Ring Tone	When there is an incoming call, you can set the ring tone you hear to let you know this call is coming from PSTN or VoIP.
Differentiating PSTN & VoIP Dial Tone	When you take your VoIP phone off hook, you can set the tone sound you hear to let you know you have selected a VoIP line. It is advised to have different sounding tone with the normal PSTN tone as you then know your VoIP account is active and connected and you will not make expensive calls on your normal PSTN account if your VoIP account is inactive for whatever reason.
Enable Trusted IP for SIP servers	Default is disabled.
Enable Phone 1/2 Call Waiting	Allows you to hear another incoming call whilst you are on the phone, if call waiting is enabled on a line, and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.
Phone 1/2 Call Forward Feature	Allows for the creation of a simple line rotary phone system equivalent. If you have 2 x VoIP lines and you only want to publish 1 phone number then you should set the main VOIP number to Phone 1 and create a Call Forward Type rule to When Busy or No Answer and type in the 2nd VoIP number into the Call Forward Phone Number field (include the STD code). You would normally disable Call Waiting at least on Phone 1 so that all your incoming calls to Phone 1 Forward to Phone 2, when

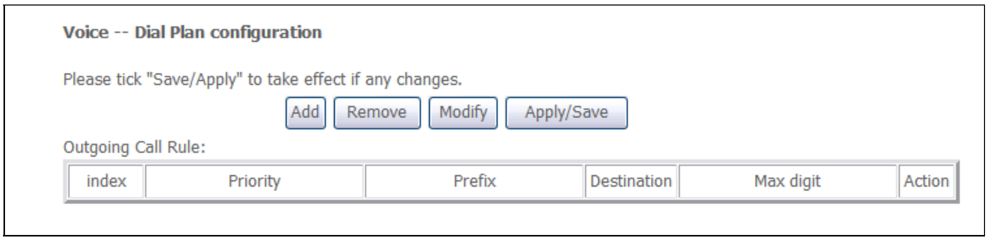
	you are on Phone 1. Please note that you may not be able to Call Forward from Line 1 to Line 2 and then if Line 2 is also busy to Call Forward to a 3rd party number even if you have correctly setup a rule for Call Forward on Line 2. Success of this operation depends on your VoIP Service Provider's network ability.
Signaling QoS	The function set creates a traffic class rule to classify the VoIP SIP upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte.
Enable Differentiated Service Configuration	When enabled Assign Differentiated Service Code Point (DSCP) Mark will be displayed. When disabled, mark the priority and type of IP service for all SIP upstream traffic.
Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.
Media Qos	The function set creates a traffic class rule to classify the VoIP RTP upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte.
Enable Differentiated Service Configuration	When enabled Assign Differentiated Service Code Point (DSCP) Mark will be displayed. When disabled, mark the priority and type of IP service for all RTP upstream traffic.
Assign Differentiated Services Code Point (DSCP) Mark	The selected Code Point gives the corresponding priority to the packets that satisfies the rules set below.

7.2 Dial Plan

With this function you can modify the translation rules for phone numbers. This is can be done by establishing **Incoming** and **Outgoing** rules, while the **Advance** screen provides for even greater customization.

All three screens are similar in design as can be seen in the figures below.

Outgoing



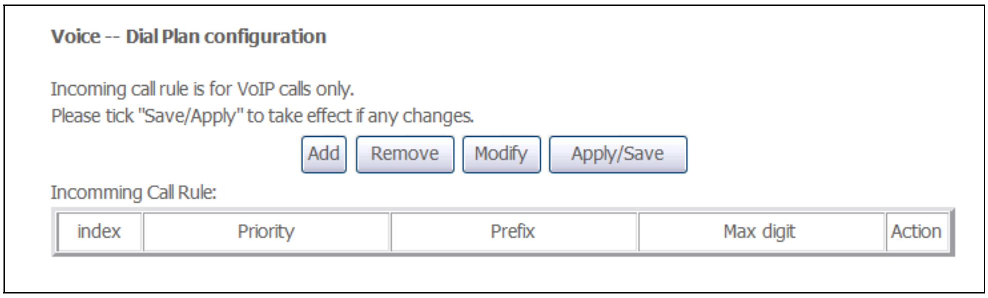
Voice -- Dial Plan configuration

Please tick "Save/Apply" to take effect if any changes.

Outgoing Call Rule:

index	Priority	Prefix	Destination	Max digit	Action

Incoming



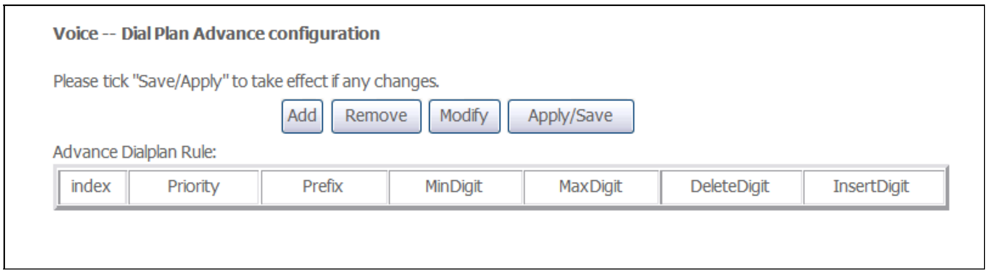
Voice -- Dial Plan configuration

Incoming call rule is for VoIP calls only.
Please tick "Save/Apply" to take effect if any changes.

Incomming Call Rule:

index	Priority	Prefix	Max digit	Action

Advance



Voice -- Dial Plan Advance configuration

Please tick "Save/Apply" to take effect if any changes.

Advance Dialplan Rule:

index	Priority	Prefix	MinDigit	MaxDigit	DeleteDigit	InsertDigit

Each screen has the same four buttons at top:

Add
Click this button to go to the add rule screen. Follow the detailed instructions given there. After completing the form click **Apply** to add a new dial plan rule.

Remove
Select the dial plan rule you wish to delete and click the **Remove** button.

Modify
Select a dial plan rule and click this button to go to the modify rule screen. Follow the detailed instructions given there. After adjusting the values in the form, click **Apply** to change the dial plan rule.

Apply/Save
Use this button to save and apply a new Dial Plan configuration.

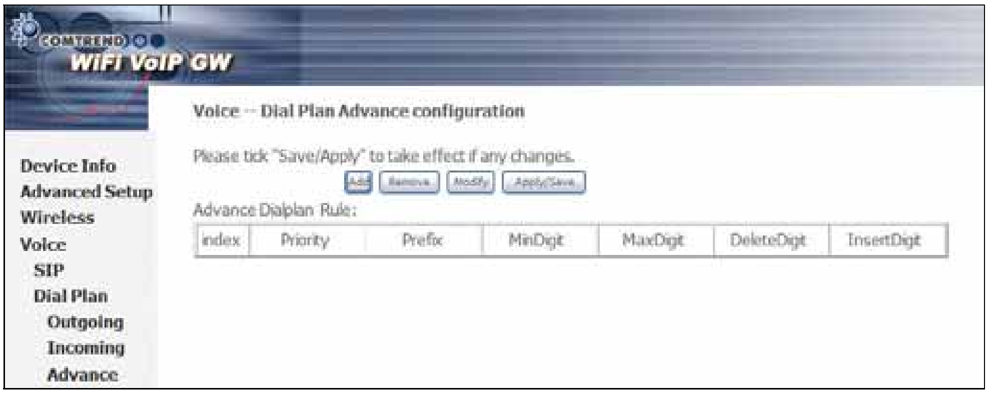
CONFIGURATION PARAMETERS

The following table of parameters is included for your reference. For more detailed instructions consult the **Add**/**Modify** rules configuration screens.

Index	Use this radio button to select a rule for modification or removal
Priority	All the rules will be applied in order according to their priority. This field can be set to any number between 0 and 32767 with lower values indicating higher priority
Prefix	Prefix digit sequence syntax
Destination	VoIP or PSTN
Mini digit	The minimum number of prefix digits
Max digit	The maximum number of digits
Delete digit	The number of prefix digits to delete
Insert digit	The prefix digits to insert
Action	Allow or Deny the action

EXAMPLE

We will use the **Advanced** configuration option for our example. To begin, select **Advanced** from the **Dial Plan** menu. The user interface should display as below.



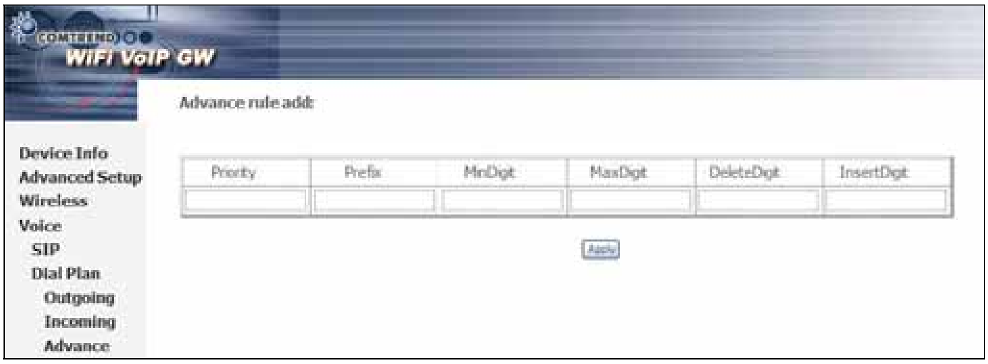
Voice -- Dial Plan Advance configuration

Please tick "Save/Apply" to take effect if any changes.

Advance Dialplan Rule:

index	Priority	Prefix	MinDigit	MaxDigit	DeleteDigit	InsertDigit

Click the **Add** button to go to the **Advance rule add** screen, shown below.



Advance rule add:

Priority	Prefix	MinDigit	MaxDigit	DeleteDigit	InsertDigit

For this example, assume that the device needs to convert the following 11 digit dial sequence "123-xxx-xxxxx" into "002-xxx-xxxxx", where "x" is any number.

Here are the steps involved.

Step 1: Enter any number between 0 and 32767 in the **Priority** field.

Step 2: In the **prefix** field enter "123".

Step 3: Enter "3" in the **Mindigit** field to limit the prefix minimum to 3 digits.

Step 4: Enter "11" or greater as the **MaxDigit** value to accept all 11 digits of the dial sequence.

Step 5: In the **DeleteDigit** field, enter "3" to delete the "123" prefix

Step 6: Enter "002" in the **InsertDigit** field to add "002" as the prefix.

Step 7: Click the **Apply** button to return to the **Advance** configuration screen.

Step 8: Click **Apply/Save** to apply this rule to all outgoing calls.

NOTE: This prefix swap example is especially helpful for corporate environments where the device is dialing through a PBX system.

The **Dial Plan** function is designed for maximum flexibility for your particular environment. If you have a question contact your ISP for detailed instructions.

7.3 Telephone Calls

To make a call, simply dial the number. The dial plan (i.e. the dialed digits) is normally customized for each installation. The default dial plan delivered by Comtrend allows dialing of 4-digit extensions or direct IP addresses. Shorter extension numbers (e.g. 3-digits) can be dialed by completing the dial string with a final #.

When a Call Server (SIP Proxy Server) is configured into the system, the dialed digits are translated and routed by the Call Server to the correct destination as registered with the Call Server.

If no Call Server is configured, calls can still be made using 4-digit extensions, rather than using full IP addresses. The originator translates the dialed-digits to a destination device as follows:

First Digit:	Line identifier (for multi-line gateways)
Remaining digits:	Host number part of an IP address. The Network number part is considered to be the same as the caller's IP address.

For example, if a caller at address 10.136.64.33/24 dials "2023", the call will be placed to the second line at address 10.136.64.23. All devices have to be on the same Class C subnet (24 bit subnet mask).

To dial an IP address directly, dial the IP address digits, using keypad * as the dot. Complete the address with a final * or #. When using IP address dialing it is not possible to specify which line at a gateway is called, so the gateway always routes IP-address dialed calls to the first line.

Network busy tone (fast busy) will be played for unknown or unreachable destinations. To answer a call, pick up the phone or press the handsfree button.

Caller ID
The Call Manager delivers Calling Number when placing calls. The calling number is transmitted to the analog line for CLASS recognition.

Call Hold
To put a call on hold, press flash then hang up (optional). To return to the original call, press flash or pick up the phone. The phone will issue a short ring burst every 30 seconds or so while on-hook to remind you that a call is on hold.

Call Transfer

- To transfer a call, press flash then dial the new number.
- To transfer immediately, hang up (blind transfer).
- To transfer with consultation, wait for the party to answer, consult, and hang up.
- To abort the transfer (if the third party does not answer), press flash to return to the original call.

Conference Calling
To turn a two-party call into a three-party conference call, press flash and dial the third party. Wait for the party to answer, then press flash.

To drop the third party and return to a two-party call, press flash again. To drop yourself out of the conference, hang up. The call will be transferred (so that the other two parties remain connected to each other). In conference mode, the conference initiator performs the audio bridge/mixing function – there are only two voice streams established.

Call Waiting
If call waiting is enabled on a line, and you hear the call waiting tone during a call, press flash to answer the second call. The first call is automatically placed on hold. To switch between calls, press flash again.

- To disable the call waiting feature, dial *60.
- To enable the call waiting feature, dial *61.

Call forward feature settings (Busy or All) takes priority over the call waiting feature. The call waiting feature is ignored on new incoming calls if there is already a call on hold or in conference.

Call Forward Number
- To set the call forward number, dial *74 then the number. Note that this does not actually enable forwarding; to do so, select the call forward action as described below.
- To disable all call forwarding features, dial *70

Call Forward No Answer
- To enable call forward on no answer, dial *71. Incoming calls will be forward if unanswered for 18 seconds.

Call Forward Busy
- To enable call forward if busy, dial *72. Incoming calls will be immediately forwarded if the phone is off-hook.

Call Forward All
- To enable call forward for all calls, dial *73.
- To disable the "forward all calls" feature, dial *75.

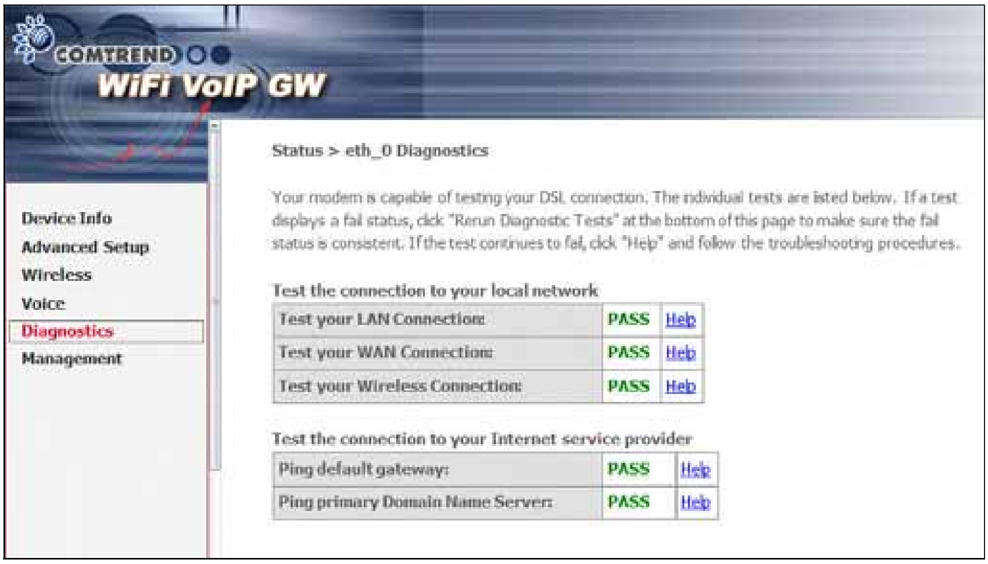
Previous settings for Call Forward Busy or No Answer are not modified.

Call Return
To place a call to the last known incoming caller (unanswered or not), dial *69.

Redial
- To redial the last outgoing number, dial *68.

Chapter 8 Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status, click **Rerun Diagnostic Tests** at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click **Help** and follow the troubleshooting procedures.



Status > eth_0 Diagnostics

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN Connection:	PASS	Help
Test your WAN Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider

Ping default gateway:	PASS	Help
Ping primary Domain Name Server:	PASS	Help

Test	**Description**
LAN Connection	**Pass:** Indicates that the Ethernet interface from your computer is connected to the LAN port of this device. **Fail:** Indicates that the device does not detect the Ethernet interface from your computer.
WAN connection	**Pass: :** Indicates that the WAN interface from the modem (ADSL/cable) is connected to the WAN port of this device. **Fail:** Indicates that the device does not detect the WAN interface from the modem (ADSL/cable).
Wireless connection	**Pass:** Indicates that the Wireless interface from your computer is connected to the wireless network. **Down:** Indicates that the device does not detect the wireless network.
Ping Default Gateway	**Pass:** Indicates that the device can communicate with the first entry point to the network. It is usually the IP address of the ISP local router. **Fail:** Indicates that the device was unable to communicate with the first entry point on the network. It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue**.**

Test	Description
Ping Primary Domain Name Server	**Pass:** Indicates that the device can communicate with the primary Domain Name Server (DNS). **Fail:** Indicates that the device was unable to communicate with the primary Domain Name Server (DNS). It may not have an effect on your Internet connectivity. Therefore if this test fails but you are still able to access the Internet, there is no need to troubleshoot this issue.

Chapter 9 Management

The Management section of the device supports the following maintenance functions and processes:

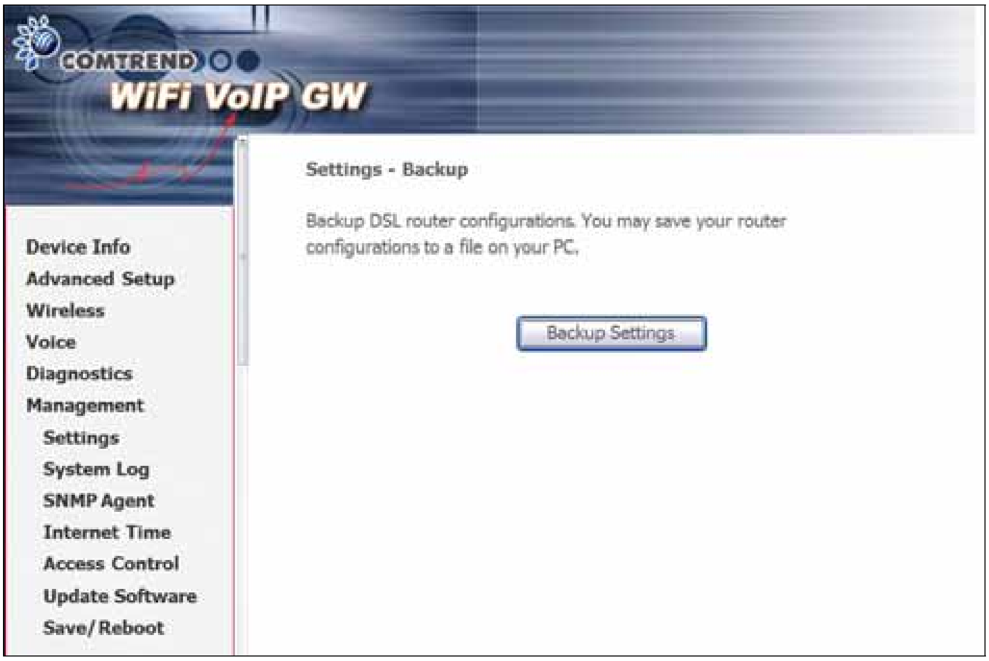
- Settings
- System log
- SNMP Agent
- Internet Time
- Access Control
- Update software
- Save/Reboot

9.1 Settings

The Settings screen allows for the backup, retrieval and restoration of settings. Each of these functions is accessed from the Settings submenu and described in more detail in the following discussion.

9.1.1 Backup Settings

Select **Backup** from the **Settings** submenu to access the screen shown below. Click the **Backup Settings** button to save the current configuration settings. You will be prompted to define the location of a backup file to save to your PC.

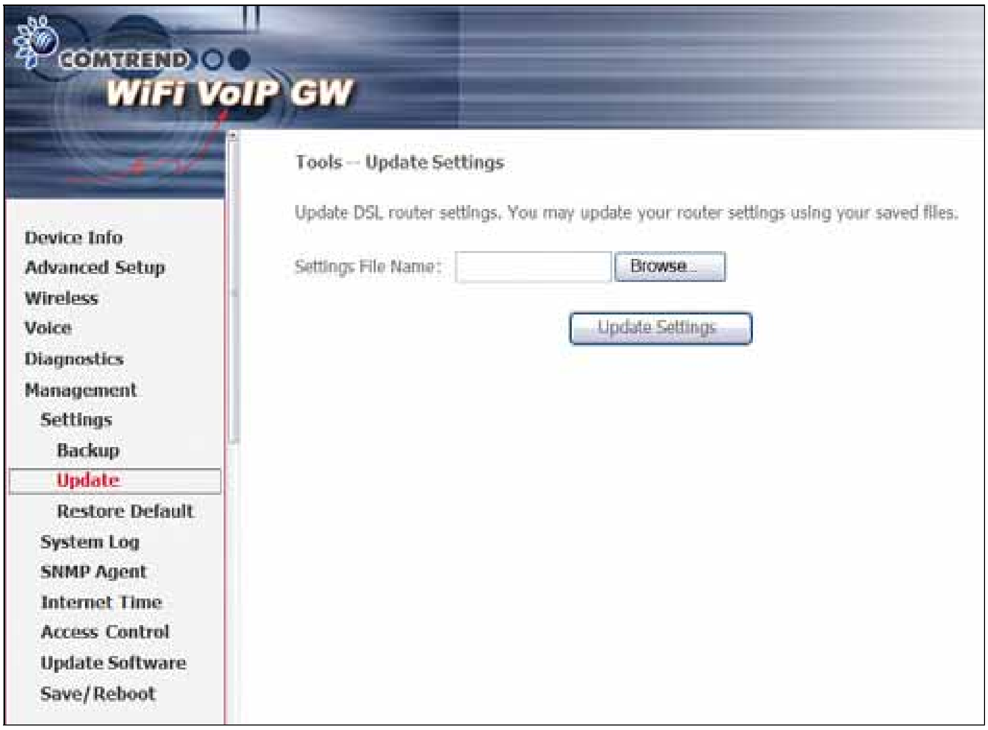


Settings - Backup

Backup DSL router configurations. You may save your router configurations to a file on your PC.

9.1.2 Update Settings

Select **Update** from the **Settings** submenu to access the screen shown below. Enter a previously saved configuration backup file in the **Settings File Name** field and click the **Update Settings** button to load it. If you forget the filename and path you can search your PC by clicking on the **Browse** button.



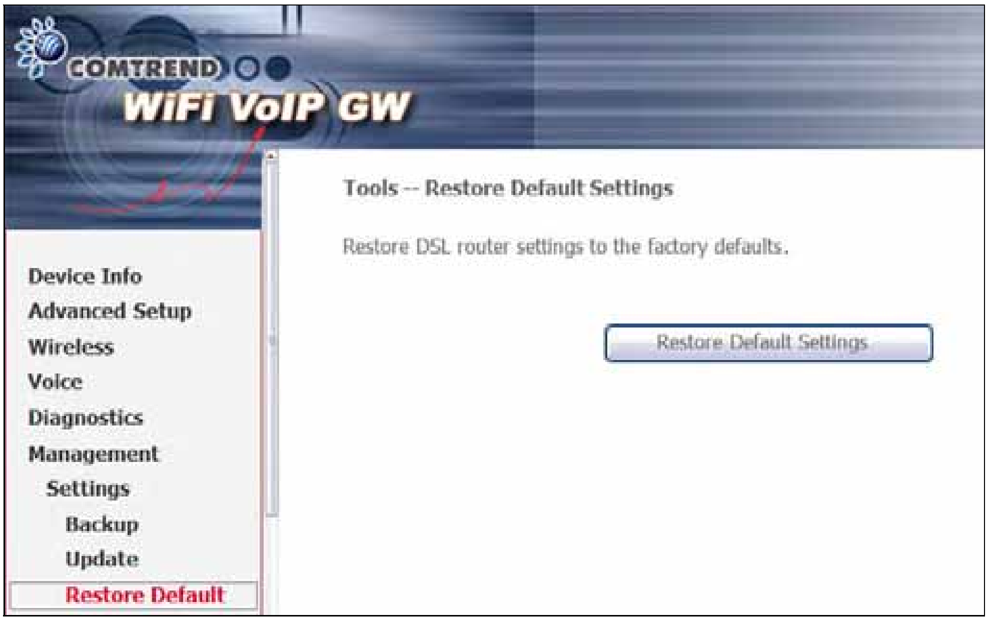
Tools -- Update Settings

Update DSL router settings. You may update your router settings using your saved files.

Settings File Name:

9.1.3 Restore Default

Select **Restore Default** from the **Settings** submenu to access the screen shown below. Click the **Restore Default Settings** button to restore the device to the default firmware settings. Restoring system settings require a device reboot.

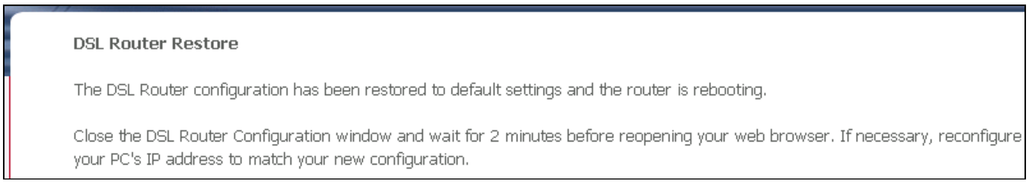


Tools -- Restore Default Settings

Restore DSL router settings to the factory defaults.

The default settings can be found in section 3.1 Default Settings.

After the Restore Default Configuration button is selected, the following screen appears. Close the device Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.



DSL Router Restore

The DSL Router configuration has been restored to default settings and the router is rebooting.

Close the DSL Router Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

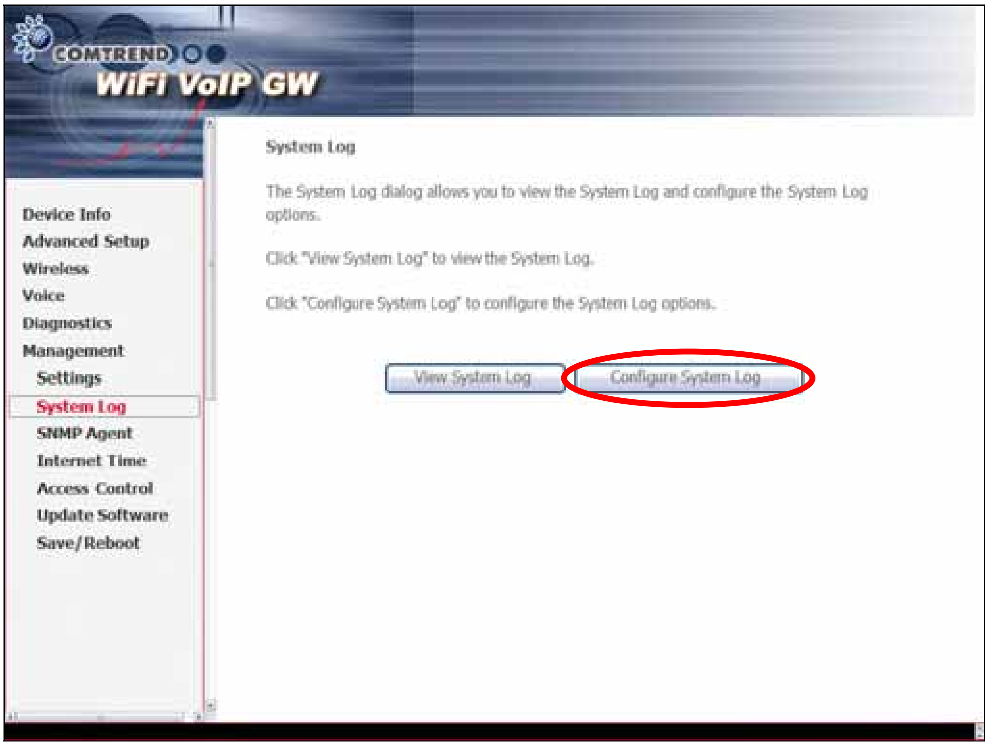
After a successful reboot, the browser will return to the **Device Info** screen. If the browser does not refresh to the default page, close and restart the browser.

NOTE:	The Restore Default function has the same effect as the reset button. The device board hardware and the boot loader support the **reset to default** button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

9.2 System Log

The **System Log** option under **Management** allows for the viewing of system events and configuration of related options. The default setting for the System Log is enabled. Follow the steps below to enable and view the System Log.

STEP 1: Click **Configure System Log** to continue.



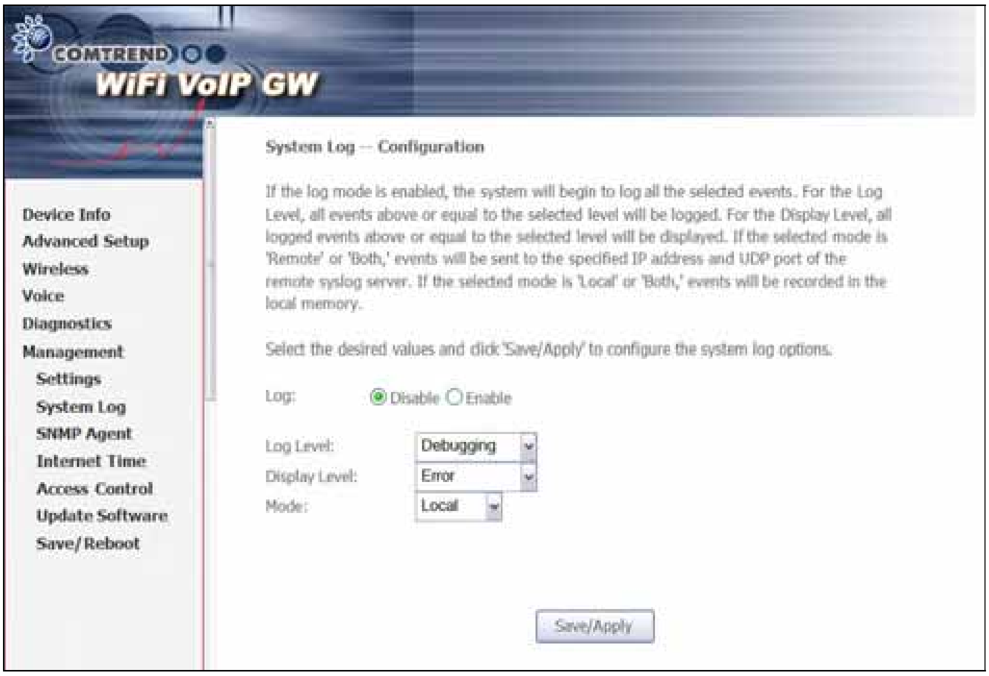
System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

Step 2: Select from the desired system log options (see table below) and then click **Save/Apply**.



System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ● Disable ○ Enable

Log Level: Debugging

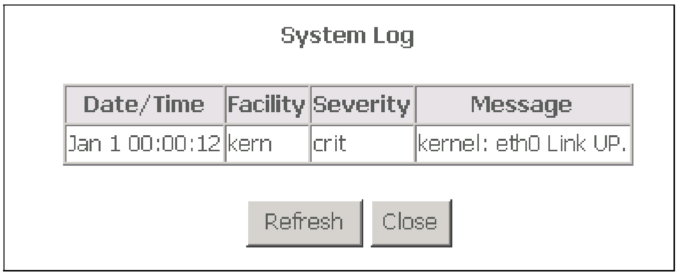
Display Level: Error

Mode: Local

Option	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, click Enable and then Apply button.
Log level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the CT-820C SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging," which is the lowest critical level. The following log levels are • Emergency = system is unstable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice • Informational • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** page for events of this level and above to the highest Emergency level.

Option	Description
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote syslog server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote syslog server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

3. Click **View System Log**. The results are displayed in as follows.



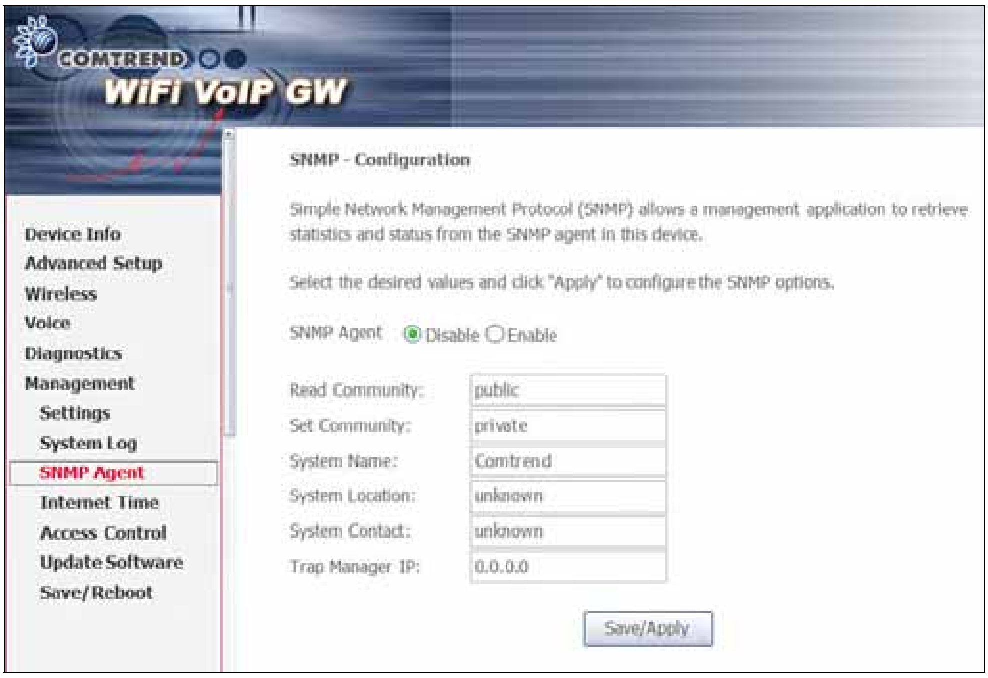
System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:12	kern	crit	kernel: eth0 Link UP.

9.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click **Save/Apply** to configure the SNMP options.



SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

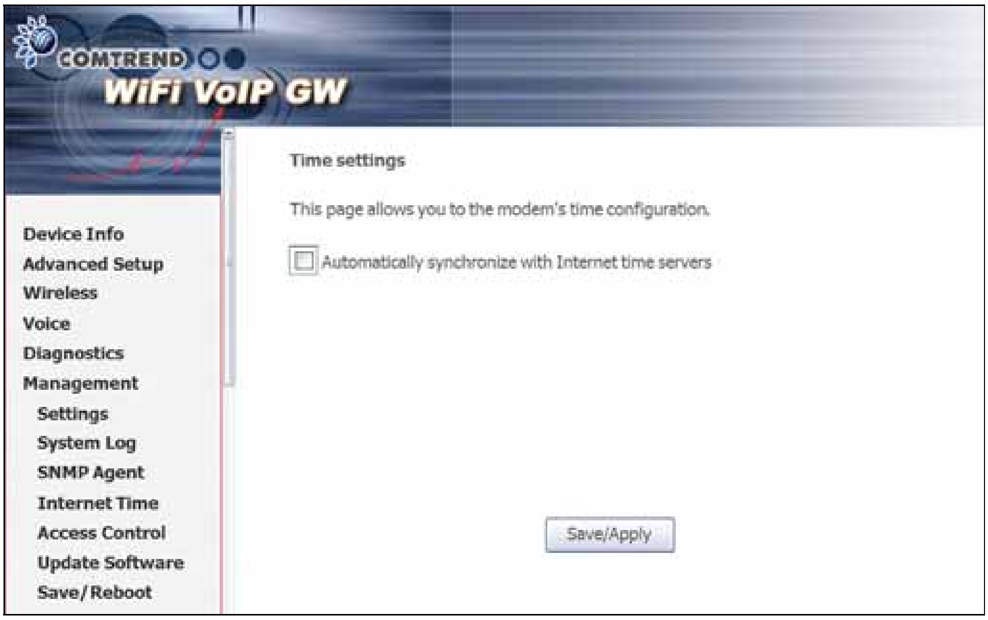
SNMP Agent ● Disable ○ Enable

Read Community:	public
Set Community:	private
System Name:	Comtrend
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

9.4 Internet Time

NOTE: Internet Time must be activated to use Parental Control (section 5.4.2)

The Internet Time option under the Management submenu configures the time settings of the device. To automatically synchronize with Internet timeservers, tick the corresponding box displayed on this screen, then click **Save/Apply**.

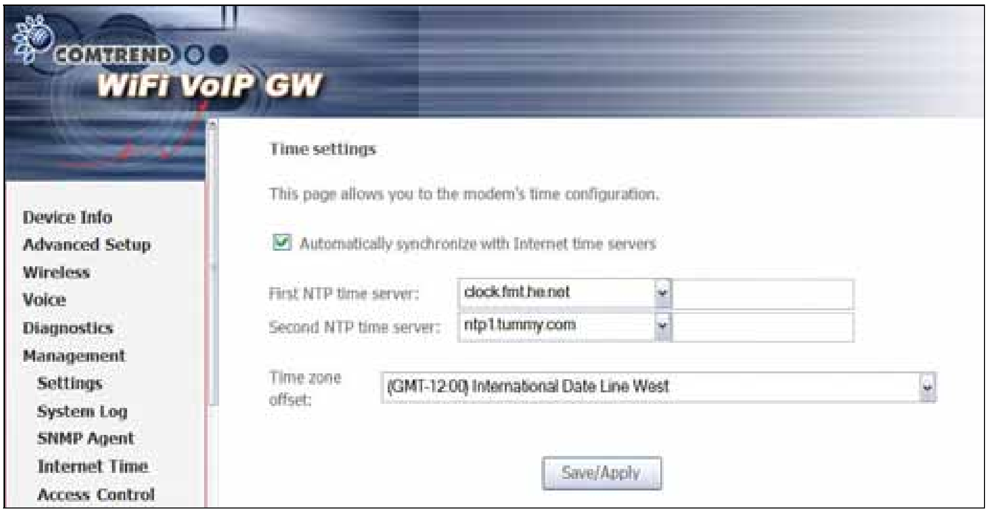


Time settings

This page allows you to the modem's time configuration.

□ Automatically synchronize with Internet time servers

On the screen below, choose your Time Zone and click **Save/Apply** to continue.



Time settings

This page allows you to the modem's time configuration.

☑ Automatically synchronize with Internet time servers

First NTP time server: clock.fmt.he.net

Second NTP time server: ntp1.tummy.com

Time zone offset: (GMT-12:00) International Date Line West

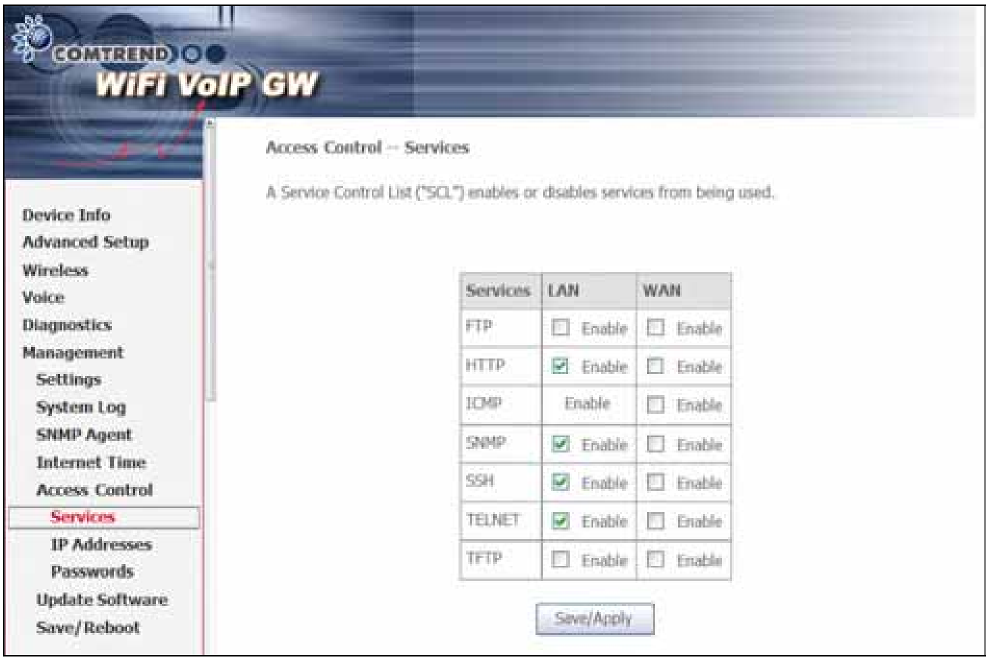
Field Descriptions
First NTP time server: Select your required server.
Second NTP time server: Select second time server if required.
Time zone offset: Select your local time zone.

9.5 Access Control

The Access Control option under Management menu bar configures access related parameters in three areas: Services, IP Addresses, and Passwords. Use Access Control to control local and remote management settings for the device.

9.5.1 Services

The Services option limits or opens the access services over the LAN or WAN. These access services are available: FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Enable a service by ticking its checkbox. Click **Save/Apply** to continue.



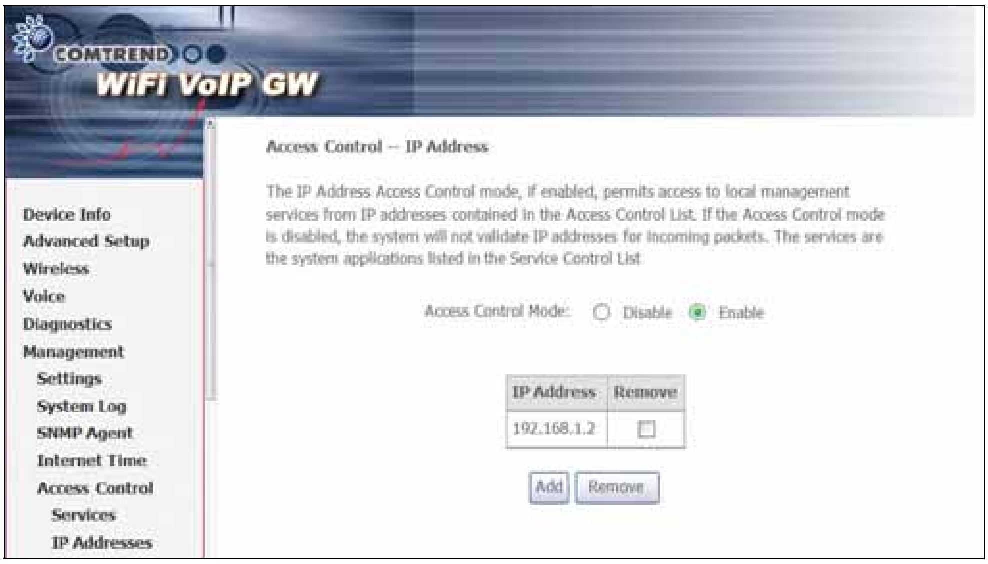
Access Control -- Services

A Service Control List ("SCL") enables or disables services from being used.

Services	LAN	WAN
FTP	☐ Enable	☐ Enable
HTTP	☑ Enable	☐ Enable
ICMP	Enable	☐ Enable
SNMP	☑ Enable	☐ Enable
SSH	☑ Enable	☐ Enable
TELNET	☑ Enable	☐ Enable
TFTP	☐ Enable	☐ Enable

9.5.2 IP Addresses

The IP Addresses option limits local access by IP address. When the **Access Control Mode** is enabled, only the IP addresses listed here can access the device. Before enabling **Access Control Mode**, add IP addresses with the **Add** button.



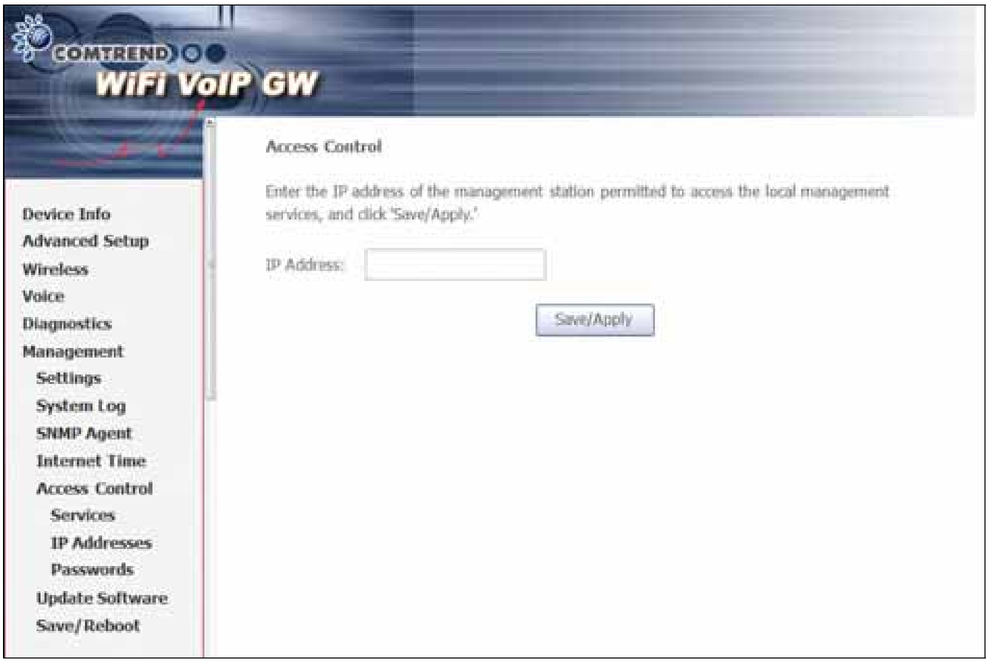
Access Control -- IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List

Access Control Mode: ○ Disable ● Enable

IP Address	Remove
192.168.1.2	□

On this screen, enter the IP address of a local PC which you wish to give management permissions. Click **Save/Apply to continue.**



Access Control

Enter the IP address of the management station permitted to access the local management services, and click 'Save/Apply.'

IP Address:

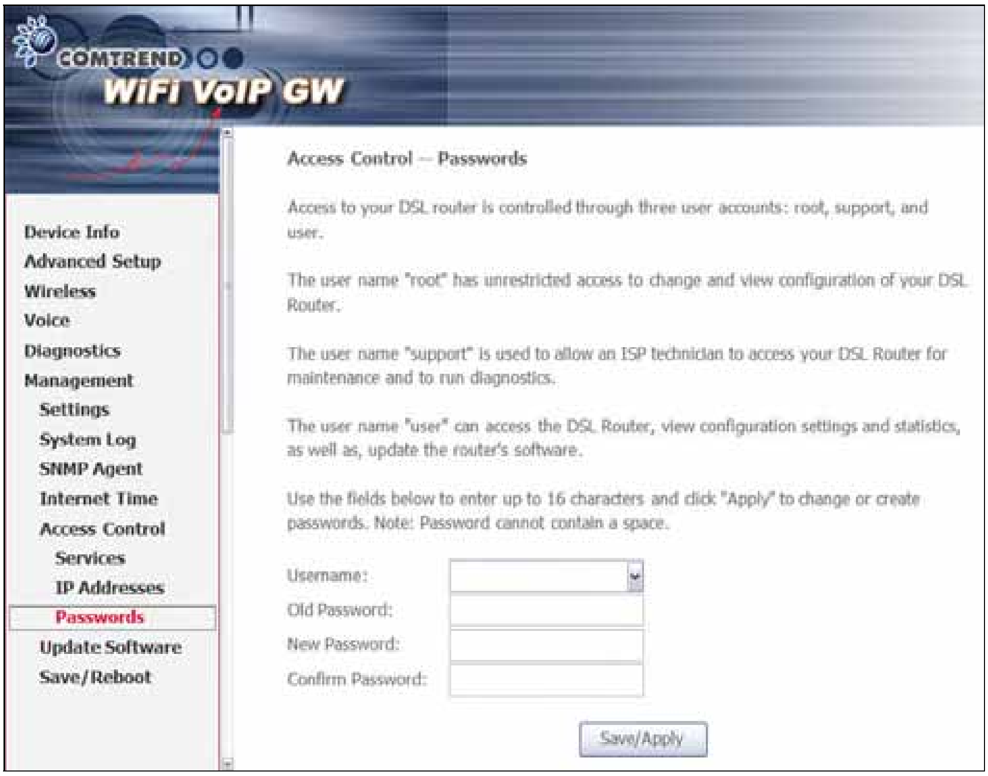
9.5.3 Passwords

The Passwords option configures the user account access passwords for the device. Access to the device is limited to the following three user accounts:

- **root** is to be used for local unrestricted access control.
- **support** is to be used for remote maintenance of the device
- **user** is to be used to view information and update device firmware.

NOTE: Default account passwords can be found in section 3.1 Default Settings

Use the fields in the screen below to select a username and change its password. Passwords must be 16 characters or less. Click **Save/Apply** to continue.



Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: root, support, and user.

The user name "root" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

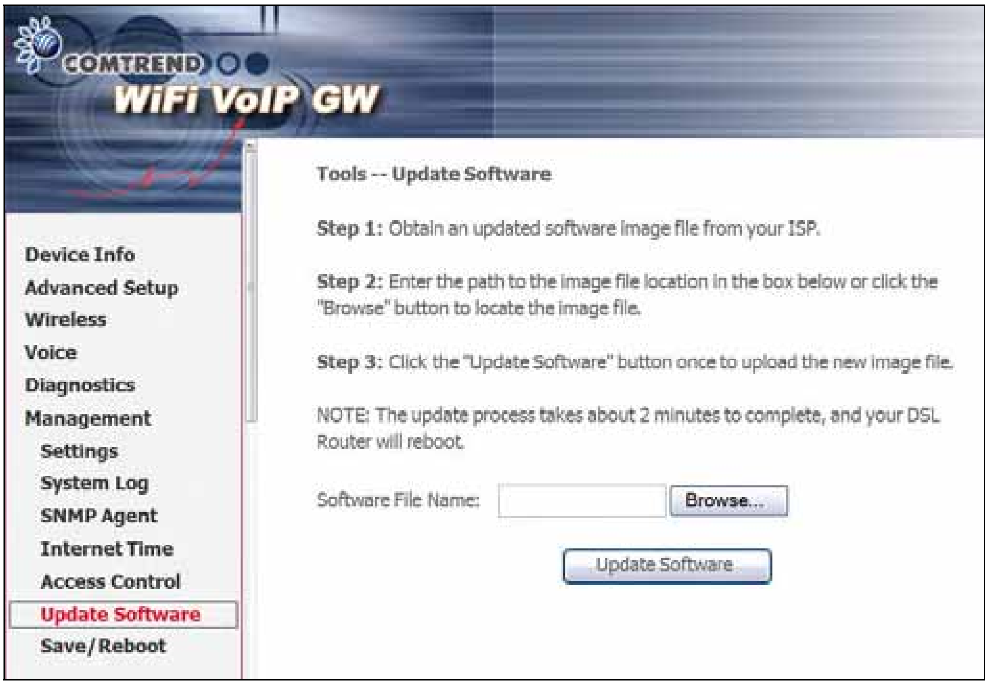
The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:
Old Password:
New Password:
Confirm Password:

9.6 Update Software

The **Update Software** screen allows for firmware updates. Manual device upgrades from a locally stored file can be performed using the following screen.



Tools -- Update Software

Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Software" button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.

Software File Name:

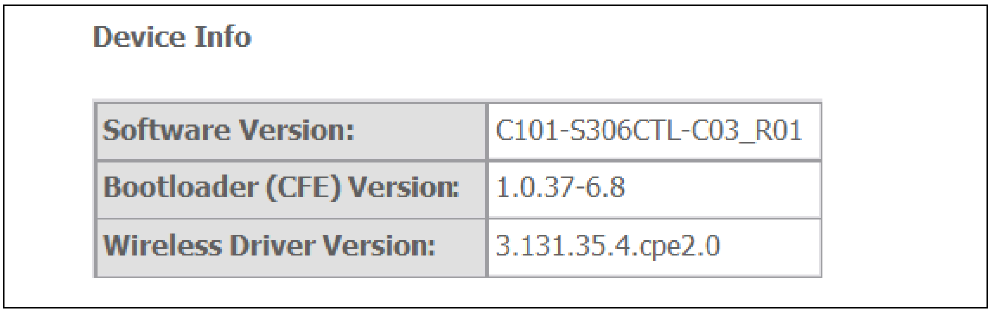
Step 1: Obtain an updated software image file from your ISP.

Step 2: Enter the path and filename of the firmware image file in the **Software File Name** field or click the **Browse** button to locate the image file.

Step 3: Click the **Update Software** button once to upload and install the file.

NOTE 1: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation.

It is recommended that you compare the **Software Version** at the top of the **Device Info** Summary screen (see screenshot below) with the firmware version installed, to confirm the installation was successful.

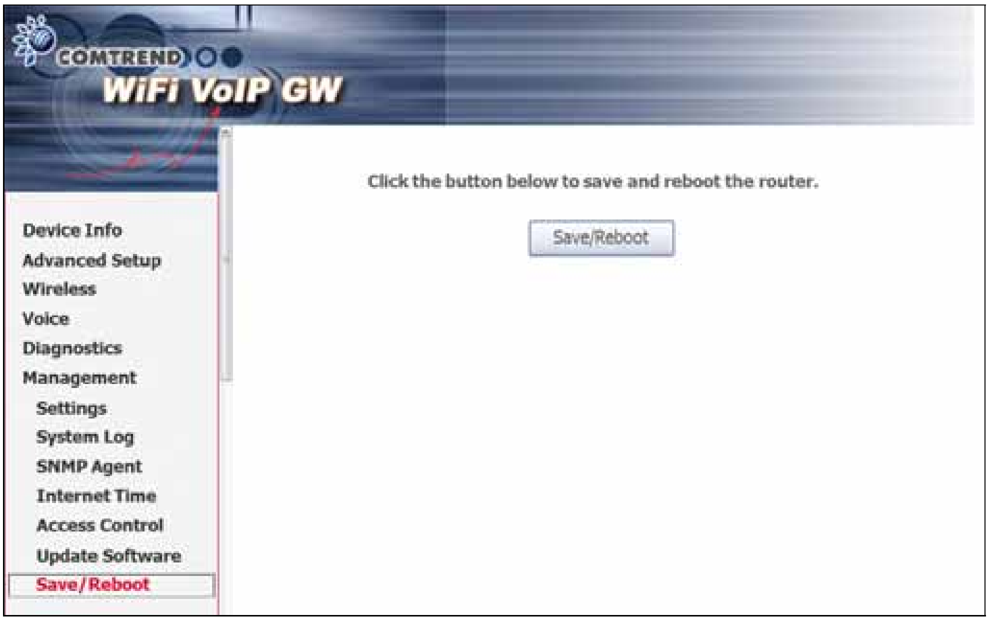


Device Info

Software Version:	C101-S306CTL-C03_R01
Bootloader (CFE) Version:	1.0.37-6.8
Wireless Driver Version:	3.131.35.4.cpe2.0

9.7 Save and Reboot

The Save/Reboot option saves the current configuration and reboots the device. Close your browser, wait about 2 minutes and then restart the web user interface.



Click the button below to save and reboot the router.

NOTE: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the DHCP server you will need to apply Static IP settings. In this case, see section 3.2 TCP/IP Settings for detailed instructions.

NOTE: If you lose all access to the web user interface, simply press the reset button on the rear panel for 5-7 seconds to restore to default settings.

Appendix A: Firewall

Stateful Packet Inspection
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

Denial of Service attack
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have.

Various DoS attacks the device can withstand are: ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack and Tear Drop.

TCP/IP/Port/Interface Filter
These rules help in the filtering of traffic at the Network layer i.e. Layer 3.
When a Routing interface is created "Enable Firewall" must be checked.
Navigate to Advanced Setup -> Security -> IP Filtering.

Outgoing IP Filter
Helps in setting rules to DROP packets from the LAN interface. By default if Firewall is Enabled all IP traffic from LAN is allowed. By setting up one or more filters, particular packet types coming from the LAN can be dropped.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from: TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be dropped.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be dropped.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be dropped.

Examples:

1.	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Destination Address	: NA
	Destination Subnet Mask	: NA
	Destination Port	: NA

This filter will Drop all TCP packets coming from LAN with IP Address/Sub. Mask 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

2. Filter Name : Out_Filter2
Protocol : UDP
Source Address : 192.168.1.45
Source Subnet Mask : 255.255.255.0
Source Port : 5060:6060
Destination Address : 172.16.13.4
Destination Subnet Mask : 255.255.255.0
Destination Port : 6060:7070

This filter will drop all UDP packets coming from LAN with IP Address/ Subnet Mask 192.168.1.45/24 and a source port in the range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port in the range of 6060 to 7070.

Incoming IP Filtering:

Helps in setting rules to ACCEPT packets from the WAN interface. By default all incoming IP traffic from WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, particular packet types coming from the WAN can be Accepted.

Filter Name: User defined Filter Name.

Protocol: Can take on any values from TCP/UDP, TCP, UDP or ICMP

Source IP Address/Source Subnet Mask: Packets with the particular "Source IP Address/Source Subnet Mask" combination will be accepted.

Source Port: This can take on either a single port number or a range of port numbers. Packets having a source port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

Destination IP Address/Destination Subnet Mask: Packets with the particular "Destination IP Address/Destination Subnet Mask" combination will be accepted.

Destination Port: This can take on either a single port number or a range of port numbers. Packets having a destination port equal to this value or falling within the range of port numbers(portX : portY) will be accepted.

The WAN interface on which these rules apply needs to be selected by user.

Examples:

1. Filter Name : In_Filter1
Protocol : TCP
Source Address : 210.168.219.45
Source Subnet Mask : 255.255.0.0
Source Port : 80
Destination Address : NA
Destination Sub. Mask : NA
Destination Port : NA

Selected WAN interface: mer_0_35/nas_0_35

This filter will ACCEPT all TCP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Sub. Mask 210.168.219.45/16 having a source port of 80 irrespective of the destination. All other incoming packets on this interface are DROPPED.

2. Filter Name : In_Filter2
Protocol : UDP
Source Address : 210.168.219.45
Source Subnet Mask : 255.255.0.0
Source Port : 5060:6060
Destination Address : 192.168.1.45
Destination Subnet Mask : 255.255.255.0
Destination Port : 6060:7070

This rule will ACCEPT all UDP packets coming from WAN interface mer_0_35/nas_0_35 with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

Parental Control
This feature restricts access of a selected LAN device to an outside Network through the router, as per chosen days of the week and the chosen times.

User Name: Name of the Filter.

Browser's MAC Address: Displays MAC address of the LAN device on which the browser is running.

Other MAC Address: If restrictions are to be applied to a device other than the one on which the browser is running, the MAC address of that LAN device is entered.

Days of the Week: Days of the week, when the restrictions are applied.

Start Blocking Time: The time when restrictions on the LAN device are put into effect.

End Blocking Time: The time when restrictions on the LAN device are lifted.

Example:
User Name: FilterJohn
Browser's MAC Address: 00:25:46:78:63:21
Days of the Week: Mon, Wed, Fri
Start Blocking Time: 14:00
End Blocking Time: 18:00

When this rule i.e. FilterJohn is entered, a LAN device with MAC Address of 00:25:46:78:63:21 will be restricted access to the outside network on Mondays, Wednesdays and Fridays, from 2pm to 6pm. On all other days and time this device will have access to the outside Network.

Appendix B: Pin Assignments

Pin Assignments of the RJ11 Port

Line port (RJ11)

Pin	Definition	Pin	Definition
1	-	4	ADSL_TIP
2	-	5	-
3	ADSL_RING	6	-

Pin assignments of the LAN Port

LAN Port (RJ45)

Pin	Definition	Pin	Definition
1	Transmit data+	5	NC
2	Transmit data-	6	Receive data-
3	Receive data+	7	NC
4	NC	8	NC

Appendix C: Specifications

WAN Interface

Ethernet x 1

LAN Interface

Ethernet x 4

WLAN

Standard	IEEE802.11g, backward compatible with 802.11b
Encryption	64, 128-bit Wired Equivalent Privacy (WEP)
Channels	11 (US, Canada)/ 13 (Europe)/ 14 (Japan)
Data Rate	Up to 54Mbps

MAC Address Filtering, WEP, WPA, IEEE 802.1x

10, 25, 50, 100mW @ 22MHz channel bandwidth Output power level can be selected according to the environment

Analog Interface

FXS x 2, FXO x 1 (Life Line)

WAN Connection

PPPoE (RFC 2516), DHCP Client, Static IP

Management

SNMP, SNTP, Telnet, Web-based management, Configuration backup and restoration. Software upgrade via HTTP, TFTP client and server or FTP server.

Centralized configuration and firmware upgrade via APS (optional)

Bridge Functions

Transparent bridging and learning	IEEE 802.1d
IGMP Proxy	Yes
IGMP Snooping	Yes

Routing Functions

Static route, RIP v1/v2, NAT/PAT, DMZ, DHCP Client/Server/Relay, DNS Proxy, DDNS, IGMP proxy, ARP

Security Functions

Authentication protocols	PAP, CHAP
VPN	PPTP/L2TP/IpSec pass-through

Stateful Packet Inspection, Packet filtering, Denial Of Service protection, Traffic Conditioning, WFQ-based Bandwidth Management, HTTP proxy

QoS

L3 policy-based QoS, IP QoS, ToS

Voice Functions

SIP	RFC 3261
Codec	G.711a/u, G.729, ILBC
RTP	RFC 1889
SDP	RFC 2327
Caller ID	ETSI based
Life line/Emergency call	Yes
Echo cancellation	G.168
Silence suppression	Yes
T.38/Fax passthrough	Yes
DTMF	RFC2833/in-band
QoS	Yes
ToS/DSCP bit tagging	Yes
Dial Plan	Yes

Power External power adapter	Input: AC100-240V Output: DC12V/1.5A

Environmental Conditions

Operating temperature	0 ~ 50 degrees Celsius
Relative humidity	5 ~ 90% (non-condensing)

Dimensions

205 mm (W) x 47 mm (H) x 145 mm (D)

NOTE: Specifications are subject to change without notice

Appendix D: SSH Client

Linux OS comes with an ssh client. Microsoft Windows does not have ssh client but there is a public domain one called “putty” that you can download here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the device using Linux ssh client:
From LAN: Use the device WEB UI to enable SSH access from LAN.
(default is enabled)
type: ssh -l root 192.168.1.1

From WAN: In the device, use WEB UI to enable SSH access from WAN.
type: ssh -l support device-WAN-ip-address

To access the device using the Windows “putty” ssh client:
From LAN: Use the device WEB UI to enable SSH access from LAN
(default is enabled)
type: putty -ssh -l admin 192.168.1.1

From WAN: In the device, use WEB UI to enable SSH access from WAN.
type: putty -ssh -l support device-WAN-ip-address