DRAFT

User’s Guide

GPT-2541GNAC

Indoor GPON HGU

Default Login Details

http://192.168.1.1

User Name: admin

Password: 1234

Firmware Version 1.00

Edition 1, 9/2015

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Contents

Introduction

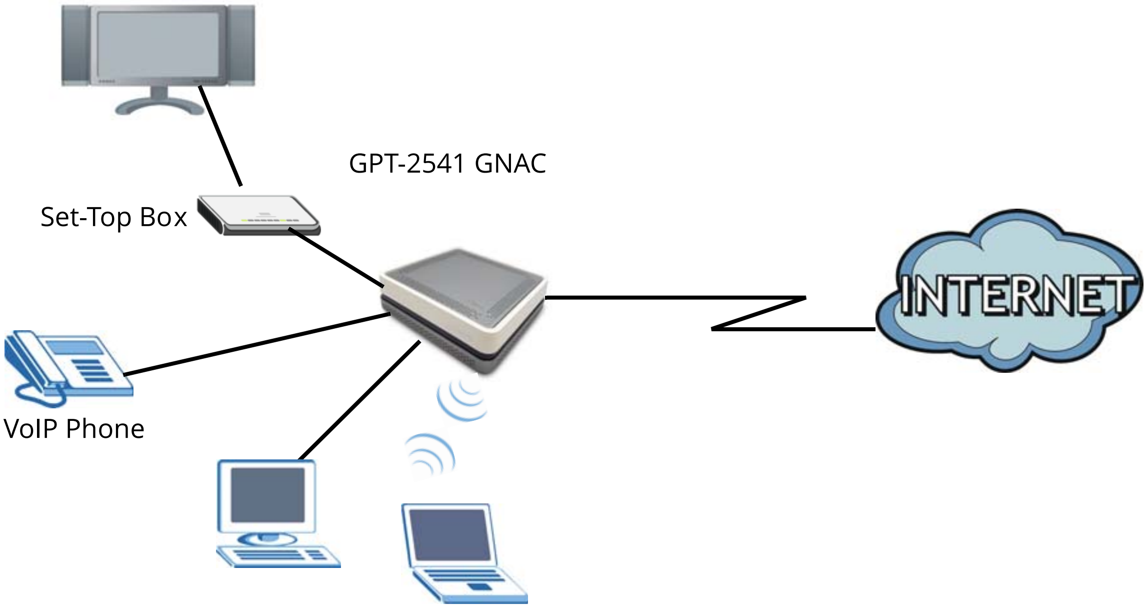
Chapter 1

1.1 Overview

The GPT-2541GNAC GPON ONT combines high-speed Fiber Internet access with a built-in switch, a firewall and high-speed wireless networking capability. It has a phone port for making calls over the Internet (Voice over IP or VoIP). It also supports IPTV service when available from your service provider.

The following figure shows an application example of the Router. The Router is connected to a provides IPTV, VoIP services as well as wired and wireless Internet access to home devices on the LAN.

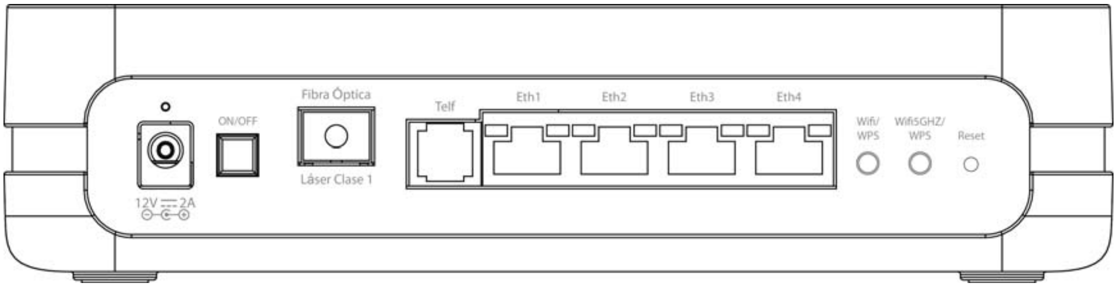
Figure 1 Application Example



1.2 Hardware Connection

Make sure to use the proper cables and power adapter to connect the Router.

Figure 2 Rear Panel



The following table explains the connectors and buttons on the rear panel.

Table 1 Rear Panel

CONECTOR	DESCRIPTION
12V-2A	Connect the provided power adapter to the 12V-1A power connector. Attach the power adapter to a proper power source.
ON/OFF	Use this button to turn the Router on or off.
Fibra Óptica	Connect the service provider's fiber optic cable to this port.
Telf	Use a telephone cable to connect the Router to a VoIP phone for VoIP service.
Eth 1-4	Use an Ethernet cable to connect a computer to one of these ports for initial configuration and/or Internet access.
Wifi/WPS	Use this button to enable or disable the 2.4 GHz WiFi and WPS features on the Router. By default, WiFi is enabled on the Router. Press this button for 1 second to turn it off. To enable the WPS feature, press the button for more than 3 seconds The WPS LED on the front panel will flash green while the Router sets up a WPS Connection with the wireless device. Note: To activate WPS, you must enable WPS in the Router and in another wireless device within two minutes of each other.

Table 1 Rear Panel (continued)

CONECTOR	DESCRIPTION
Wifi5GHz/WPS	Use this button to enable or disable the 5 GHz WiFi and WPS features on the Router. By default, WiFi is enabled on the Router. Press this button for 1 second to turn it off. To enable the WPS feature, press the button for more than 3 seconds The WPS LED on the front panel will flash green while the Router sets up a WPS Connection with the wireless device. Note: To activate WPS, you must enable WPS in the Router and in another wireless device within two minutes of each other.
Reset	Use this button to restore the default settings of the Router. Press this button for 10 seconds to restore default values. Press 1 second or longer to restart it. Note: If you reset the Router, you will lose all configurations that you had previously and the password will be reset to the defaults.

1.3 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 Front Panel LEDs

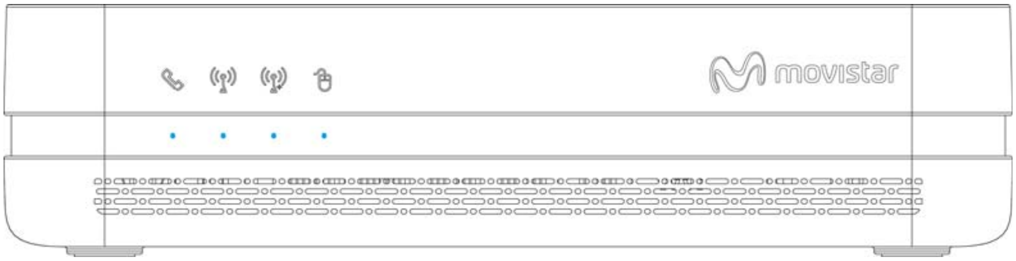


Figure 4 Rear Panel LEDs

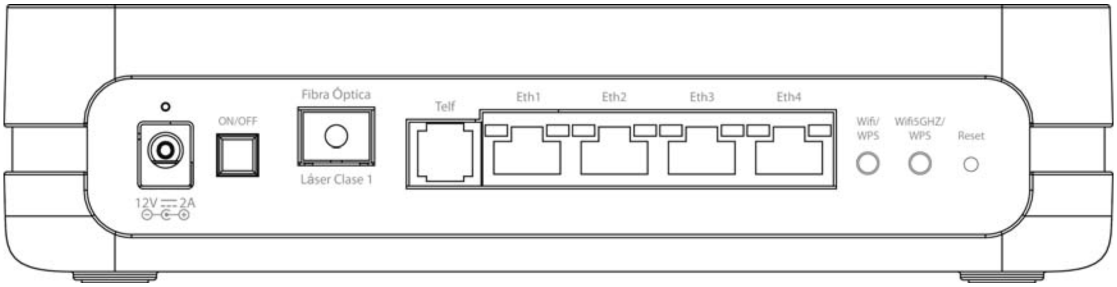


Table 2 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
Power	Blue	On	The Router is receiving power and ready for use.
	Red	On	The Router has hardware failure.
		Blinking	The Router detected an error while self-testing.
		Off	The Router is not receiving power.
Eth 1-4	Blue	On	The Router has a successful Ethernet connection with a device on the LAN.
		Blinking	The Router is sending or receiving data to/from the LAN.
		Off	The Router does not have an Ethernet connection with the LAN.

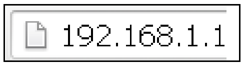
Table 2 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
Telf	Blue	On	The SIP registration is successful.
		Blinking	The Router is negotiating the SIP registration.
	Green	On	There is incoming or outgoing voice traffic.
	Red	Blinking	The Router has failed to register the VoIP service.
		Off	There is no VoIP service.
Wifi/WPS	Blue	On	The 2.4 GHz wireless is on.
		Blinking	The 2.4 GHz WPS is activated. It also blinks when the Router is setting up a WPS connection.
		Off	The 2.4 GHz wireless is not activated.
Wifi5GHz/ WPS	Blue	On	The 5 GHz wireless is on.
		Blinking	The 5 GHz WPS is activated. It also blinks when the Router is setting up a WPS connection.
		Off	The 5 GHz wireless is not activated.
Internet	Blue	On	The Router has a PPP connection but no traffic. It has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		Blinking	Startup process. The Router is running an automatic startup diagnostic process on the GPON port.
		Fast Blinking	The Router is sending or receiving IP traffic. The Router is synchronizing with the PON. Activation phase. The Router is negotiating a PPP connection.
	Red	On	The Router attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed. The GPON port failed during the POST (Power On Self Test) or there is an error due to hardware or firmware failure.
		Blinking	The GPON port’s optical power level is below the threshold.
		Off	There is no Internet connection.

1.4 Advanced Configuration

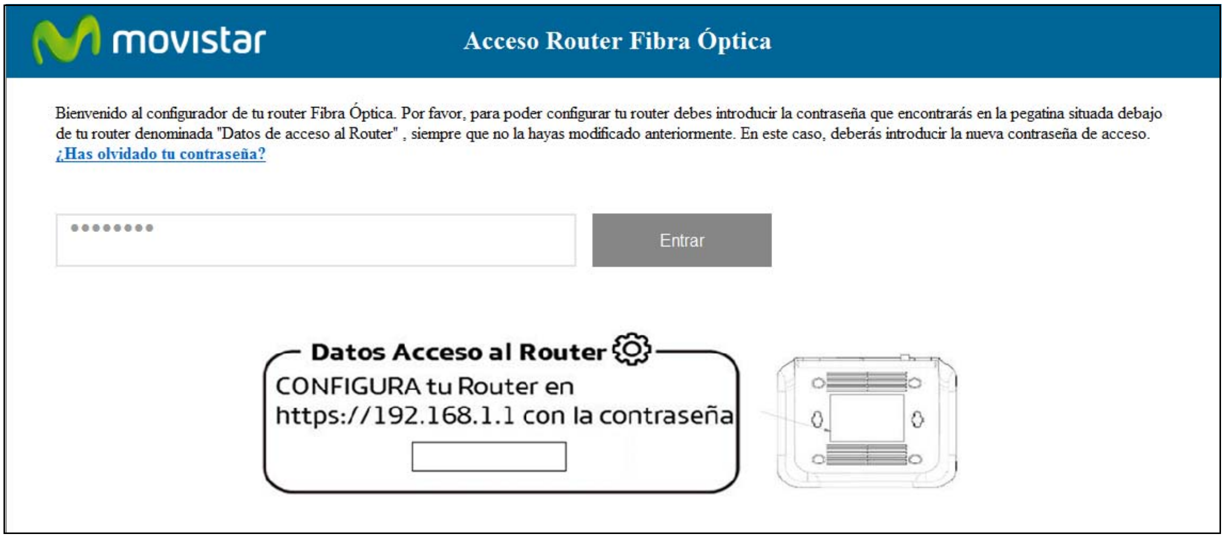
Do the following to access the advanced configuration screens.

1 Access the **Client Wizard** screens. Enter the IP address: http://192.168.1.1.



192.168.1.1

2 The login screen appears. The default password is random. Please refer to the label sticker at the bottom of the device. Enter the password. Click **Entrar** to enter the **Client Wizard**.



movistar Acceso Router Fibra Óptica

Bienvenido al configurador de tu router Fibra Óptica. Por favor, para poder configurar tu router debes introducir la contraseña que encontrarás en la pegatina situada debajo de tu router denominada "Datos de acceso al Router" , siempre que no la hayas modificado anteriormente. En este caso, deberás introducir la nueva contraseña de acceso.

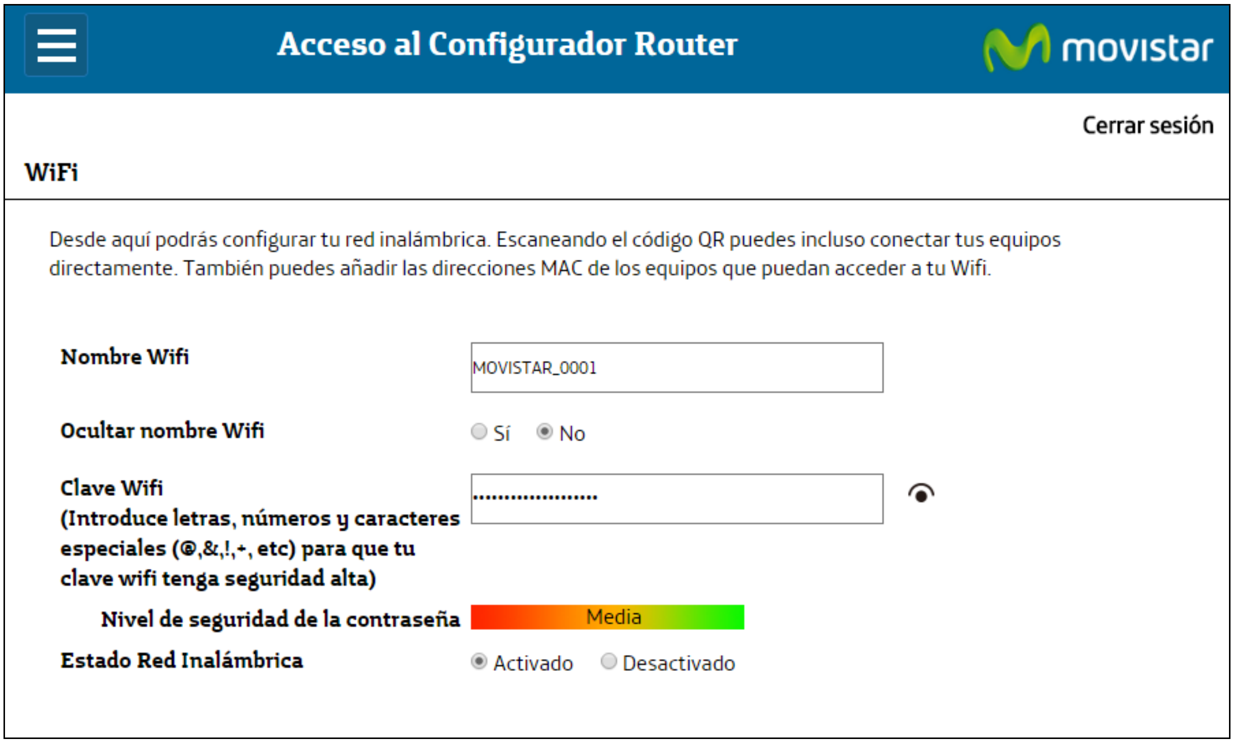
¿Has olvidado tu contraseña?

••••••••

Datos Acceso al Router

CONFIGURA tu Router en https://192.168.1.1 con la contraseña

3 The **main s**creen appears.



Acceso al Configurador Router movistar

WiFi

Desde aquí podrás configurar tu red inalámbrica. Escaneando el código QR puedes incluso conectar tus equipos directamente. También puedes añadir las direcciones MAC de los equipos que puedan acceder a tu Wifi.

Nombre Wifi: MOVISTAR_0001

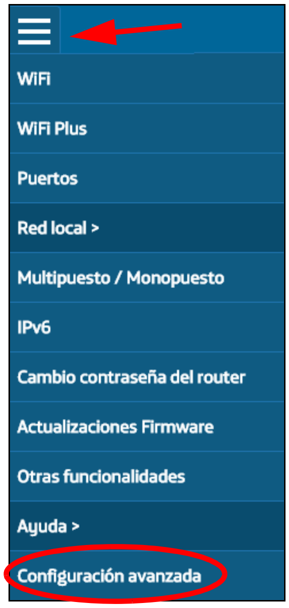
Ocultar nombre Wifi: ○ Sí ● No

Clave Wifi (Introduce letras, números y caracteres especiales (@,&,!,+, etc) para que tu clave wifi tenga seguridad alta): ....

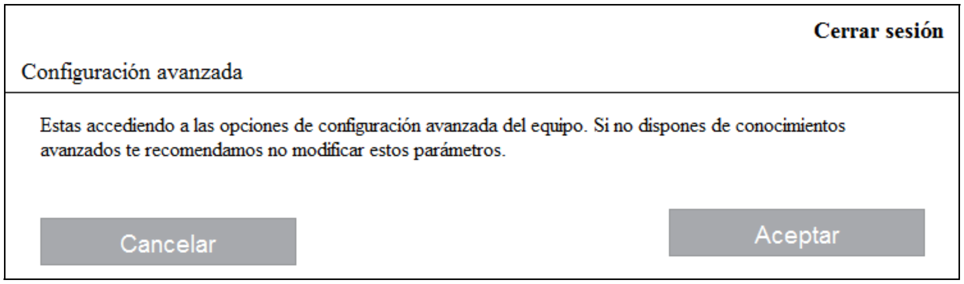
Nivel de seguridad de la contraseña: Media

Estado Red Inalámbrica: ● Activado ○ Desactivado

4 Click the **Menu** button and then **Configuración avanzada**.



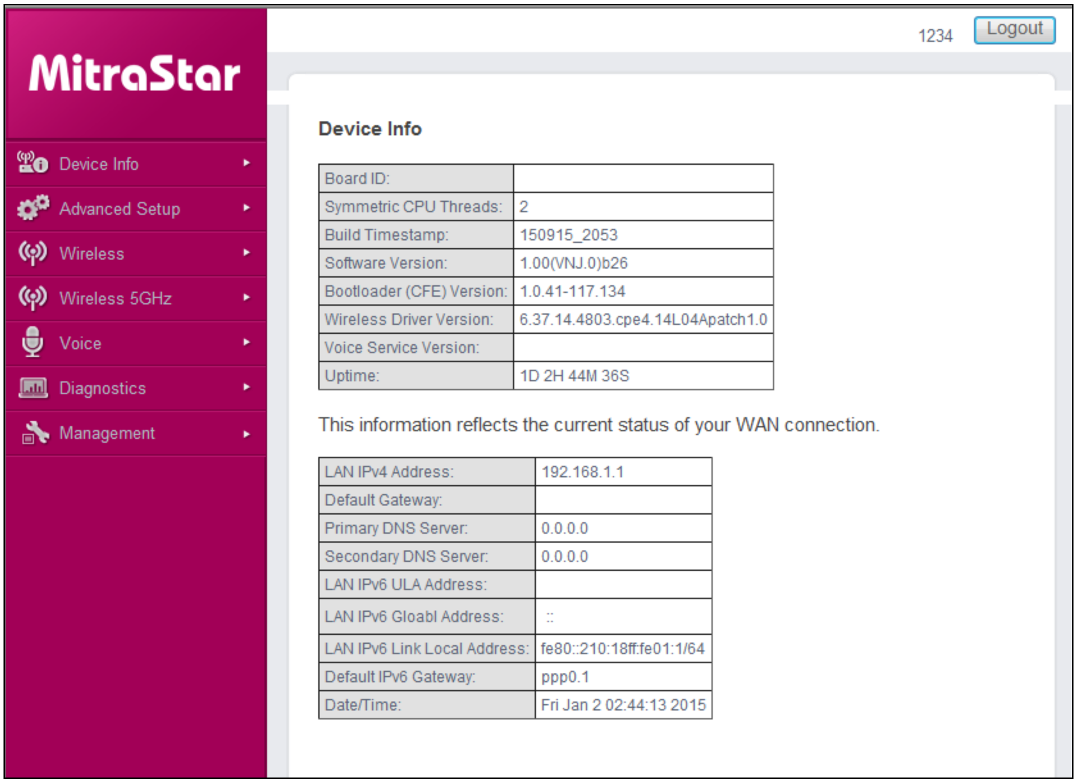
5 Click **Aceptar**.



Configuración avanzada

Estas accediendo a las opciones de configuración avanzada del equipo. Si no dispones de conocimientos avanzados te recomendamos no modificar estos parámetros.

6 The advanced configuration screens display. Use the menu on the left to navigate the screens. Refer to the rest of this guide for details about the screens. Click **Logout** to exit the configuration screens.



Device Info

Board ID:	
Symmetric CPU Threads:	2
Build Timestamp:	150915_2053
Software Version:	1.00(VNJ.0)b26
Bootloader (CFE) Version:	1.0.41-117.134
Wireless Driver Version:	6.37.14.4803.cpe4.14L04Apatch1.0
Voice Service Version:	
Uptime:	1D 2H 44M 36S

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
LAN IPv6 Gloabl Address:	::
LAN IPv6 Link Local Address:	fe80::210:18ff:fe01:1/64
Default IPv6 Gateway:	ppp0.1
Date/Time:	Fri Jan 2 02:44:13 2015

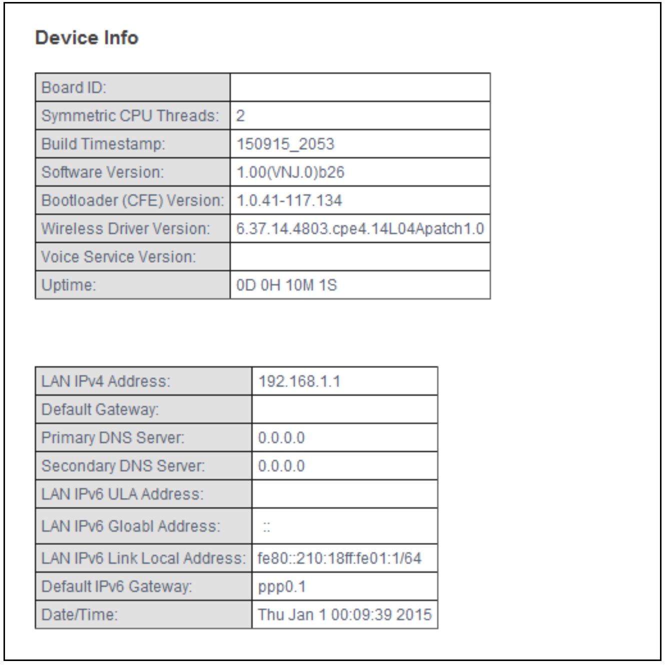
Device Info

Chapter 2

2.1 Device Info Summary

Click **Device Info > Summary** to open this screen with general device and WAN connection status information.

Figure 5 Device Info Summary



Device Info

Board ID:	
Symmetric CPU Threads:	2
Build Timestamp:	150915_2053
Software Version:	1.00(VNJ.0)b26
Bootloader (CFE) Version:	1.0.41-117.134
Wireless Driver Version:	6.37.14.4803.cpe4.14L04Apatch1.0
Voice Service Version:	
Uptime:	0D 0H 10M 1S

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
LAN IPv6 Gloabl Address:	::
LAN IPv6 Link Local Address:	fe80::210:18ff:fe01:1/64
Default IPv6 Gateway:	ppp0.1
Date/Time:	Thu Jan 1 00:09:39 2015

Table 3 Device Info Summary

LABEL	DESCRIPTION
Board ID	This field displays the ID number of the circuit board in the Router.
Symmetric CPU Threads	This field displays the number of threads in the Router’s CPU.
Build Timestamp	This field displays the date (YYMMDD) and time (HHMM) of the firmware in the Router.
Software Version	This field displays the current version of the firmware inside the Router.

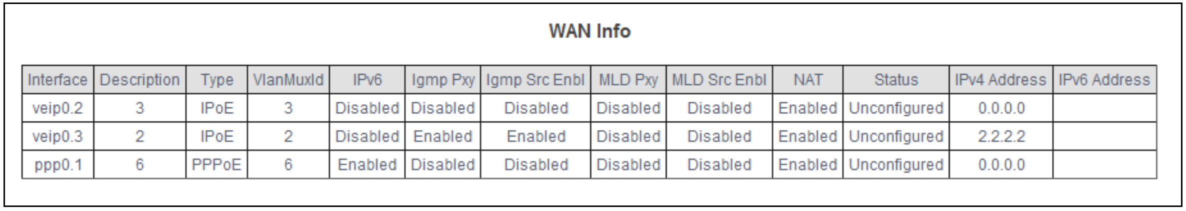
Table 3 Device Info Summary (continued)

LABEL	DESCRIPTION
Bootloader (CFE) Version	This field displays the version of bootloader the Router is using.
Wireless Driver Version	This field displays the version of the driver for the Router’s wireless chipset.
Voice Service Version	This field displays the version of the VoIP software the Router is using.
Uptime	This field displays how long the Router has been running since it last started up.
LAN IPv4 Address	This field displays the current IP address of the Router in the LAN.
Default Gateway	This field displays the IP address of the gateway through which the Router sends traffic unless it matches a static route.
Primary DNS Server	The Router tries this DNS server first when it needs to resolve a domain name into a numeric IP address.
Secondary DNS Server	The Router uses this DNS server first when it needs to resolve a domain name into a numeric IP address if the primary DNS server does not respond.
LAN IPv6 ULA Address	This field displays the current unique local address (ULA). This is a unique IPv6 address for use in private networks but not routable in the global IPv6 Internet.
LAN IPv6 Address (Global)	This field displays the current global IPv6 address of the Router.
LAN IPv6 Link Local Address	This field displays the current IPv6 address of the Router in the LAN.
Default IPv6 Gateway	This field displays the IPv6 address of the gateway through which the Router sends IPv6 traffic unless it matches a static route.
Date/Time	This field displays the Router’s current day of the week, month, hour, minute, second, and year.

2.2 WAN Info

Click **Device Info > WAN** to open this screen which lists the Router's WAN connections and their status.

Figure 6 WAN Info



WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Status	IPv4 Address	IPv6 Address
veip0.2	3	IPoE	3	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Unconfigured	0.0.0.0	
veip0.3	2	IPoE	2	Disabled	Enabled	Enabled	Disabled	Disabled	Enabled	Unconfigured	2.2.2.2	
ppp0.1	6	PPPoE	6	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Unconfigured	0.0.0.0	

Table 4 WAN Info

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line. The **ppp0.*** indicates a PPP connection. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This is the service name of this connection.
Type	This shows the method of encapsulation used by this connection (IP over Ethernet, PPP over Ethernet, or bridging).
VlanMuxID	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IPv6	This displays whether or not IPv6 is enabled on the interface.
Igmp Pxy	This shows whether IGMP (Internet Group Multicast Protocol) proxy is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
Igmp Src Enbl	This shows whether IGMP source enable is activated or not for this connection. IGMP source enable has the Router add routing table entries based on the IGMP traffic.
MLD Pxy	This shows whether Multicast Listener Discovery (MLD) proxy is activated or not for this connection. MLD is not available when the connection uses the bridging service.
MLD Src Enbl	This shows whether MLD source enable is activated or not for this connection. MLD source enable has the Router add routing table entries based on the MLD traffic.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Status	This displays the connection state or **Unconfigured** if the interface has not yet been configured.

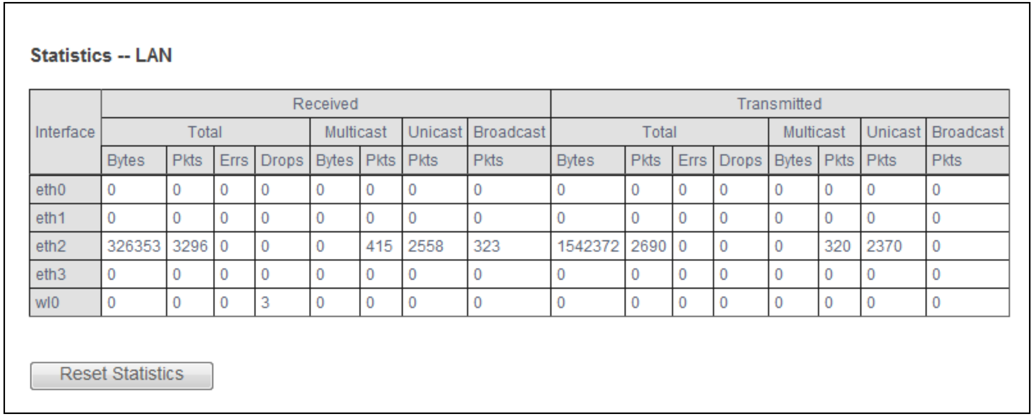
Table 4 WAN Info (continued)

LABEL	DESCRIPTION
IPv4 Address	This displays the interface's current IPv4 address if it has one.
IPv6 Address	This displays the interface's current IPv6 address if it has one.

2.3 LAN Statistics

Click **Device Info > Statistics > LAN** to open this screen of traffic statistics counters for the Router's wired and wireless LAN interfaces. Use the button to clear the counters.

Figure 7 LAN Statistics



Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
eth0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	326353	3296	0	0	0	415	2558	323	1542372	2690	0	0	0	320	2370	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0

Table 5 LAN Statistics

LABEL	DESCRIPTION
Interface	These fields identify the LAN interfaces. **eth0** ~ **eth3** represent the ethernet LAN ports 1 ~ 4. **wlo** represents the wireless LAN interface.
Received / Transmitted	These fields display the number of bytes, packets, error packets, and dropped packets for each interface.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of packets received on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.

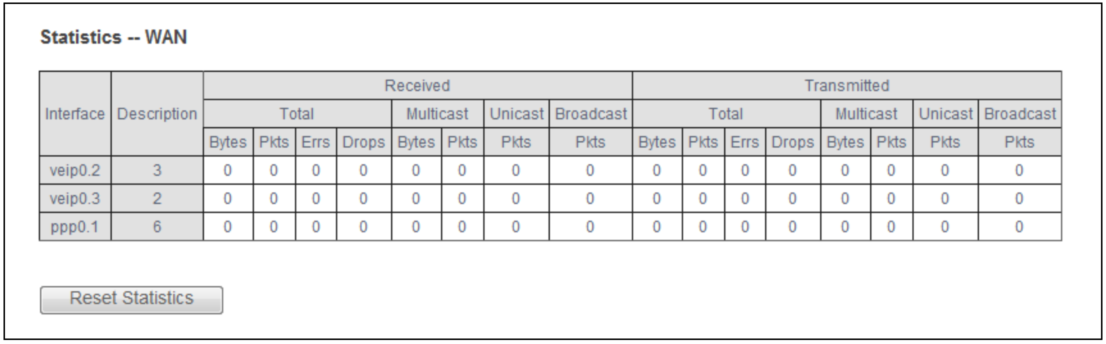
Table 5 LAN Statistics (continued)

LABEL	DESCRIPTION
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.
Drops	This indicates the number of outgoing packets dropped on this interface.
Reset Statistics	Click this to clear the screen’s statistics counters.

2.4 WAN Statistics

Click **Device Info > Statistics > WAN Service** to display the total, multicast, unicast, and broadcast traffic statistics counters for the Router’s WAN interfaces. Use the button to clear the counters.

Figure 8 WAN Statistics



Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
veip0.2	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
veip0.3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ppp0.1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 6 WAN Statistics

LABEL	DESCRIPTION
Interface	This shows the name of the WAN interface used by this connection. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line. The **ppp0.*** indicates a PPP connection. **eth0** ~ **eth3** represent the Ethernet LAN ports 1 ~ 4 and are the foundation for eth0/* which are virtual WAN interfaces of the physical Gigabit Ethernet line. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This is the service name of this connection.
Received	
Bytes	This indicates the number of bytes received on this interface.
Pkts	This indicates the number of packets received on this interface.
Errs	This indicates the number of frames with errors received on this interface.
Drops	This indicates the number of received packets dropped on this interface.
Transmitted	
Bytes	This indicates the number of bytes transmitted on this interface.
Pkts	This indicates the number of transmitted packets on this interface.
Errs	This indicates the number of frames with errors transmitted on this interface.

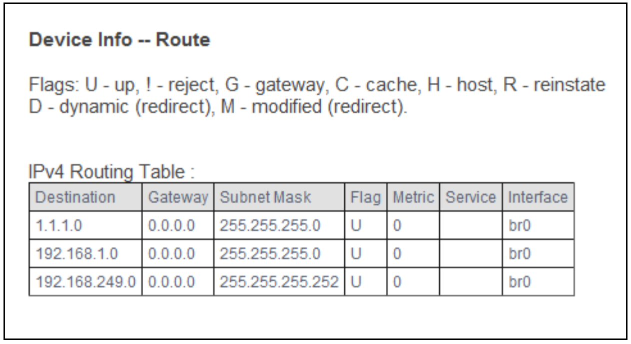
Table 6 WAN Statistics (continued)

LABEL	DESCRIPTION
Drops	This indicates the number of outgoing packets dropped on this interface.
Reset	Click this to clear the screen's statistics counters.

2.5 Route Info

Click **Device Info > Route** to display the Router's IPv4 and IPv6 routing tables.

Figure 9 Route Info



Device Info -- Route

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

IPv4 Routing Table :

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
1.1.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
192.168.249.0	0.0.0.0	255.255.255.252	U	0		br0

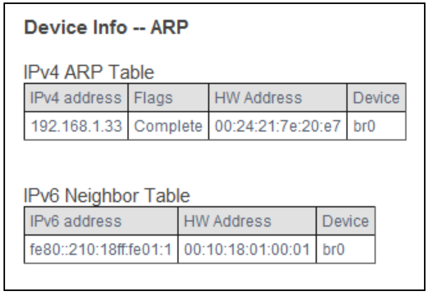
Table 7 Route Info

LABEL	DESCRIPTION
Destination	This displays the IP address to which this entry applies.
Gateway	This displays the gateway the Router uses to send traffic to the entry's destination address.
Subnet Mask	This displays the subnet mask of the destination net.
Flag	This displays whether the route is up (**U**), the Router drops packets for this destination (**!**), the route uses a gateway (**G**), the target is in the neighbor cache (**C**), the target is a host (**H**), reinstate route for dynamic routing (**R**), the route was dynamically installed by redirect (**D**), or modified from redirect (**M**).
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly-connected networks.
Service	The name of a specific service to which the route applies if one is specified.
Interface	The interface through which this route sends traffic.

2.6 ARP Info

Click **Device Info > ARP** to display the Router’s IPv4 Address Resolution Protocol and IPv6 neighbor tables. This screen lists the IP addresses the Router has mapped to MAC addresses.

Figure 10 ARP Info



Device Info -- ARP

IPv4 ARP Table

IPv4 address	Flags	HW Address	Device
192.168.1.33	Complete	00:24:21:7e:20:e7	br0

IPv6 Neighbor Table

IPv6 address	HW Address	Device
fe80::210:18ff:fe01:1	00:10:18:01:00:01	br0

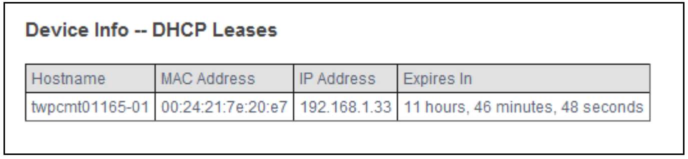
Table 8 ARP Info

LABEL	DESCRIPTION
IPv4 / IPv6 address	The learned IP address of a device connected to one of the system’s ports.
Flags	**Static** - static entry, **Dynamic** - dynamic entry that is not yet complete, **Complete** - dynamic entry that is complete.
HW Address	The MAC address of the device with the listed IP address.
Device	The interface through which the Router sends traffic to the device listed in the entry.

2.7 DHCP Leases

Click **Device Info > DHCP** to display the Router's list of IP address currently leased to DHCP clients.

Figure 11 DHCP Leases



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
twpcmt01165-01	00:24:21:7e:20:e7	192.168.1.33	11 hours, 46 minutes, 48 seconds

Table 9 DHCP Leases

LABEL	DESCRIPTION
Hostname	This field displays the name used to identify this device on the network (the computer name). The Router learns these from the DHCP client requests. “None” shows here for a static DHCP entry.
MAC Address	This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order.
IP Address	This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order.
Expires In	This field displays how much longer the IP address is leased to the DHCP client.

WAN

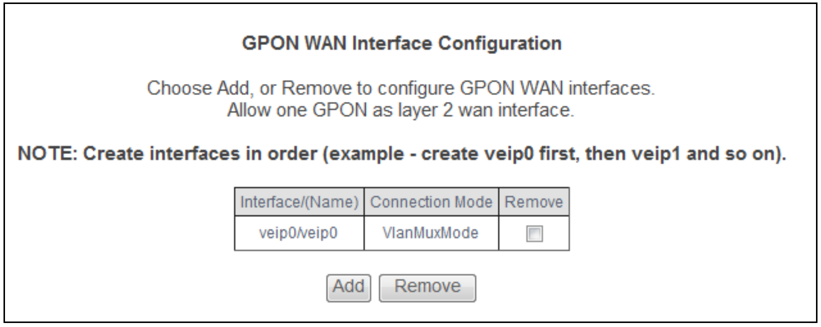
3 Chapter

3.1 GPON Layer2 Interface

The Router must have a layer-2 interface to allow users to use the GPON port to access the Internet. Log into the Router’s Web Configurator and click **Advanced Setup > Layer2 Interface > GPON Interface** to manage the GPON layer-2 interface.

ⓘ The GPON and ETH layer-2 interfaces cannot work at the same time.

Figure 12 GPON Interface



GPON WAN Interface Configuration

Choose Add, or Remove to configure GPON WAN interfaces.
Allow one GPON as layer 2 wan interface.

NOTE: Create interfaces in order (example - create veip0 first, then veip1 and so on).

Interface/(Name)	Connection Mode	Remove
veip0/veip0	VlanMuxMode	□

The following table describes the fields in this screen.

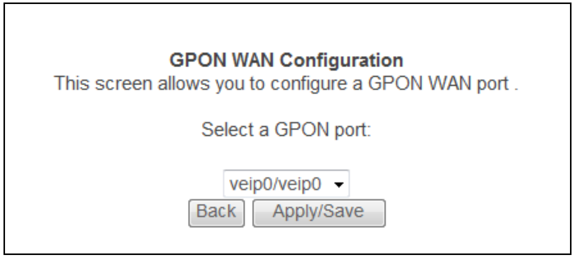
Table 10 GPON Interface

LABEL	DESCRIPTION
Interface/(Name)	The name of a configured layer-2 interface. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface.
Connection Mode	This shows the connection mode of the layer-2 interface.
Remove	Select an interface and click the **Remove** button to delete it. You cannot remove a layer-2 interface when a WAN service is associated with it.
Add	Click this button to create a new layer-2 interface. You can only have one GPON layer 2 interface at a time.

3.1.1 Layer-2 GPON Interface Configuration

Click the **Add** button in the **Layer2 Interface: GPON Interface** screen to open the following screen. Use this screen to create a new layer-2 interface.

Figure 13 GPON Interface Configuration



GPON WAN Configuration

This screen allows you to configure a GPON WAN port .

Select a GPON port:

veip0/veip0

Select the GPON port and click **Apply/Save**.

The following table describes the fields in this screen.

Table 11 GPON Interface Configuration

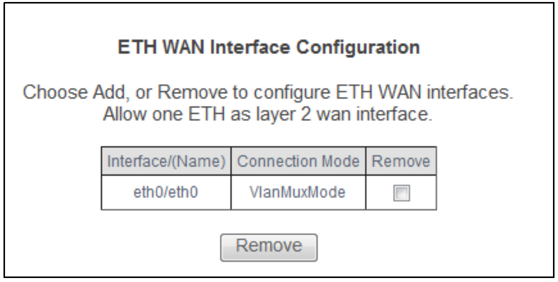
LABEL	DESCRIPTION
Select a GPON port	Select a GPON port. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

3.2 Ethernet Layer2 Interface

The Router must have a layer-2 interface to allow users to use the Gigabit Ethernet port to access the Internet. Log into the Router’s Web Configurator and click **Advanced Setup > Layer2 Interface > ETH Interface** to manage the Ethernet layer-2 interface.

ⓘ The GPON and ETH layer-2 interfaces cannot work at the same time.

Figure 14 ETH Interface



ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth0/eth0	VlanMuxMode	□

The following table describes the fields in this screen.

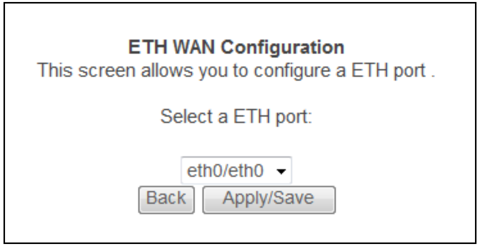
Table 12 ETH Interface

LABEL	DESCRIPTION
Interface/(Name)	The name of a configured layer-2 interface. **eth0** ~ **eth3** represent the ethernet LAN ports 1 ~ 4.
Connection Mode	This shows the connection mode of the layer-2 interface.
Remove	Select an interface and click the **Remove** button to delete it. You cannot remove a layer-2 interface when a WAN service is associated with it.
Add	Click this button to create a new layer-2 interface. You can only have one ETH layer 2 interface at a time.

3.2.1 Ethernet Layer-2 Interface Configuration

Click the **Add** button in the **Layer2 Interface: ETH Interface** screen to open the following screen. Use this screen to create a new layer-2 interface.

Figure 15 ETH Interface Configuration



ETH WAN Configuration

This screen allows you to configure a ETH port .

Select a ETH port:

The following table describes the fields in this screen.

Table 13 ETH Interface Configuration

LABEL	DESCRIPTION
Select a ETH port	Select an Ethernet port. **eth0** ~ **eth3** represent the ethernet LAN ports 1 ~ 4.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

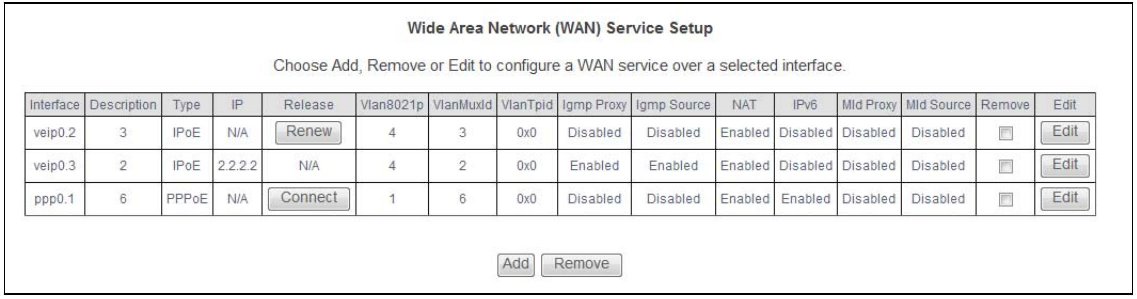
3.3 WAN Service

Use this screen to change your Router’s WAN settings. Click **Advanced Setup > WAN Service**. The summary table shows you the configured WAN services (connections) on the Router.

To use NAT, firewall or IGMP proxy in the Router, you need to configure a WAN connection with PPPoE or IPoE.

When a layer-2 interface is in **VLAN MUX Mode**, you can configure up to five WAN services on the Router.

Figure 16 WAN Service



Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	IP	Release	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	IPv6	Mld Proxy	Mld Source	Remove	Edit
veip0.2	3	IPoE	N/A	Renew	4	3	0x0	Disabled	Disabled	Enabled	Disabled	Disabled	Disabled	☐	Edit
veip0.3	2	IPoE	2.2.2.2	N/A	4	2	0x0	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled	☐	Edit
ppp0.1	6	PPPoE	N/A	Connect	1	6	0x0	Disabled	Disabled	Enabled	Enabled	Disabled	Disabled	☐	Edit

Table 14 WAN Service

LABEL	DESCRIPTION
Interface	This shows the name of the interface used by this connection. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line. The **ppp0.*** indicates a PPP connection. The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection. The number after the underscore (_) represents the index number of connections through the same interface. **(null)** means the entry is not valid.
Description	This is the service name of this connection.
Type	This shows the method of encapsulation used by this connection (IP over Ethernet, PPP over Ethernet, or bridging).
IP	This displays the IP address the connection uses. This displays **N/A** when the connection does not have an IP address.
Release	Use the buttons in this column to renew, release, or connect a WAN connection. This displays **N/A** for a connection with a static IP address.
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
VlanTpid	This field displays the VLAN Tag Protocol Identifier (TPID), a four-digit hexadecimal number from 0000 to FFFF that the OLT adds to the matched packets.
Igmp Proxy	This shows whether IGMP (Internet Group Multicast Protocol) proxy is activated or not for this connection. IGMP is not available when the connection uses the bridging service.

Table 14 WAN Service (continued)

LABEL	DESCRIPTION
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
IPv6	This shows whether IPv6 is activated or not for this connection. IPv6 is not available when the connection uses the bridging service.
Mld Proxy	This shows whether Multicast Listener Discovery (MLD) proxy is activated or not for this connection. MLD is not available when the connection uses the bridging service.
MLD Source	This shows whether MLD source is activated or not for this connection.
Remove	Select an interface and click the **Remove** button to delete it. You cannot remove a layer-2 interface when a WAN service is associated with it.
Edit	Click the **Edit** button to configure the WAN connection. Click the **Remove** icon to delete the WAN connection.
Add	Click **Add** to create a new connection.

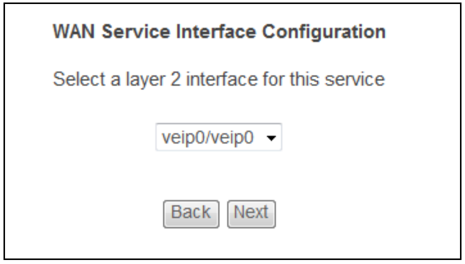
3.3.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **WAN Service** screen to configure a WAN connection.

3.3.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 17 WAN Configuration: WAN Interface



WAN Service Interface Configuration

Select a layer 2 interface for this service

veip0/veip0

Table 15 WAN Configuration: WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select the port this WAN service uses for data transmission. **veip0/veip0** is the GPON port. **eth0** ~ **eth3** represent the ethernet LAN ports 1 ~ 4.

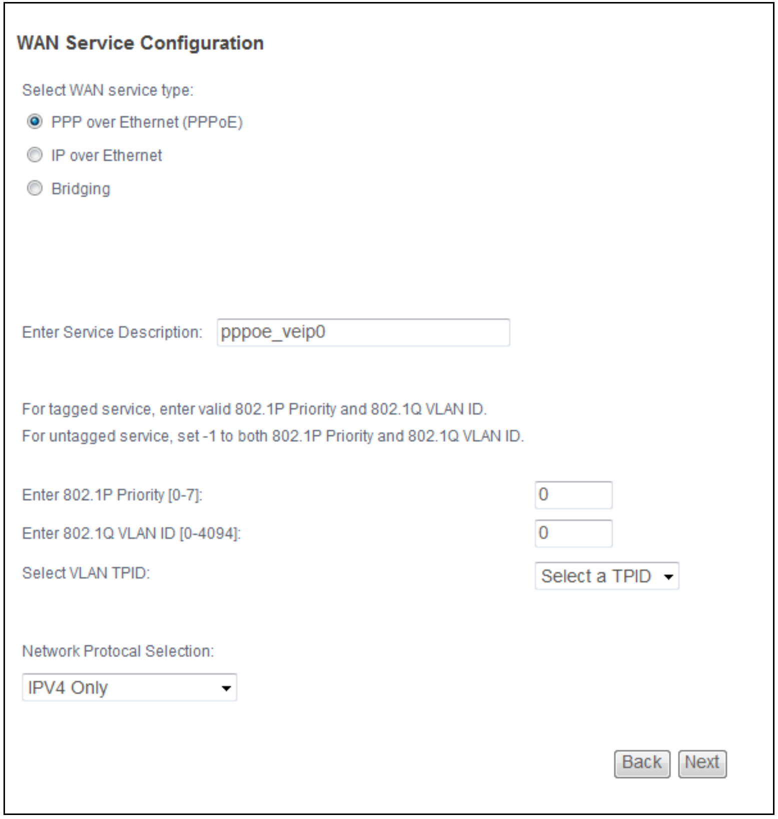
Table 15 WAN Configuration: WAN Interface (continued)

LABEL	DESCRIPTION
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

3.3.1.2 WAN Service Configuration

This screen displays after you select the WAN interface for a new WAN connection.

Figure 18 WAN Configuration: WAN Service Configuration



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)

○ IP over Ethernet

○ Bridging

Enter Service Description: pppoe_veip0

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]: 0

Enter 802.1Q VLAN ID [0-4094]: 0

Select VLAN TPID: Select a TPID

Network Protocal Selection: IPV4 Only

Table 16 WAN Configuration: WAN Service Configuration

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are **PPP over Ethernet (PPPoE)**, **IP over Ethernet** and **Bridging**.
Allow as IGMP Multicast Source	This displays when you select the **Bridging** service type. Select this to have the Router add routing table entries based on the IGMP traffic.

Table 16 WAN Configuration: WAN Service Configuration

LABEL	DESCRIPTION
Allow as MLD Multicast Source	This displays when you select the **Bridging** service type. Select this to have the Router add routing table entries based on the MLD traffic.
Enter Service Description	Specify a name to identify the service. **veip0** stands for a virtual Ethernet card and is the foundation for veip0/* which are virtual WAN interfaces of the physical GPON line. **eth0** ~ **eth3** represent the ethernet LAN ports 1 ~ 4.
Enter 802.1P Priority [0-7]	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Type the IEEE 802.1p priority level (from 0 to 7) to add to traffic through this connection. The greater the number, the higher the priority level.
Enter 802.1Q VLAN ID [0-4094]	Type the VLAN ID number (from 1 to 4094) for traffic through this connection.
Select VLAN TPID	Select a Tag Protocol Identifier (TPID) the Router to add it to the service's packets.
Network Protocol Selection	Select **IPv4 Only** to have the Router use only IPv4. Select **IPv4&IPv6(Dual Stack)** to let the Router connect to IPv4 and IPv6 networks an choose the protocol for applications according to the address type. This lets the Router use an IPv6 address when sending traffic through this connection. You can only select this for a WAN service that uses the PPPoE or IPoE encapsulation method over the layer 2 interface. Select **IPv6 Only** to have the Router use only IPv6.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

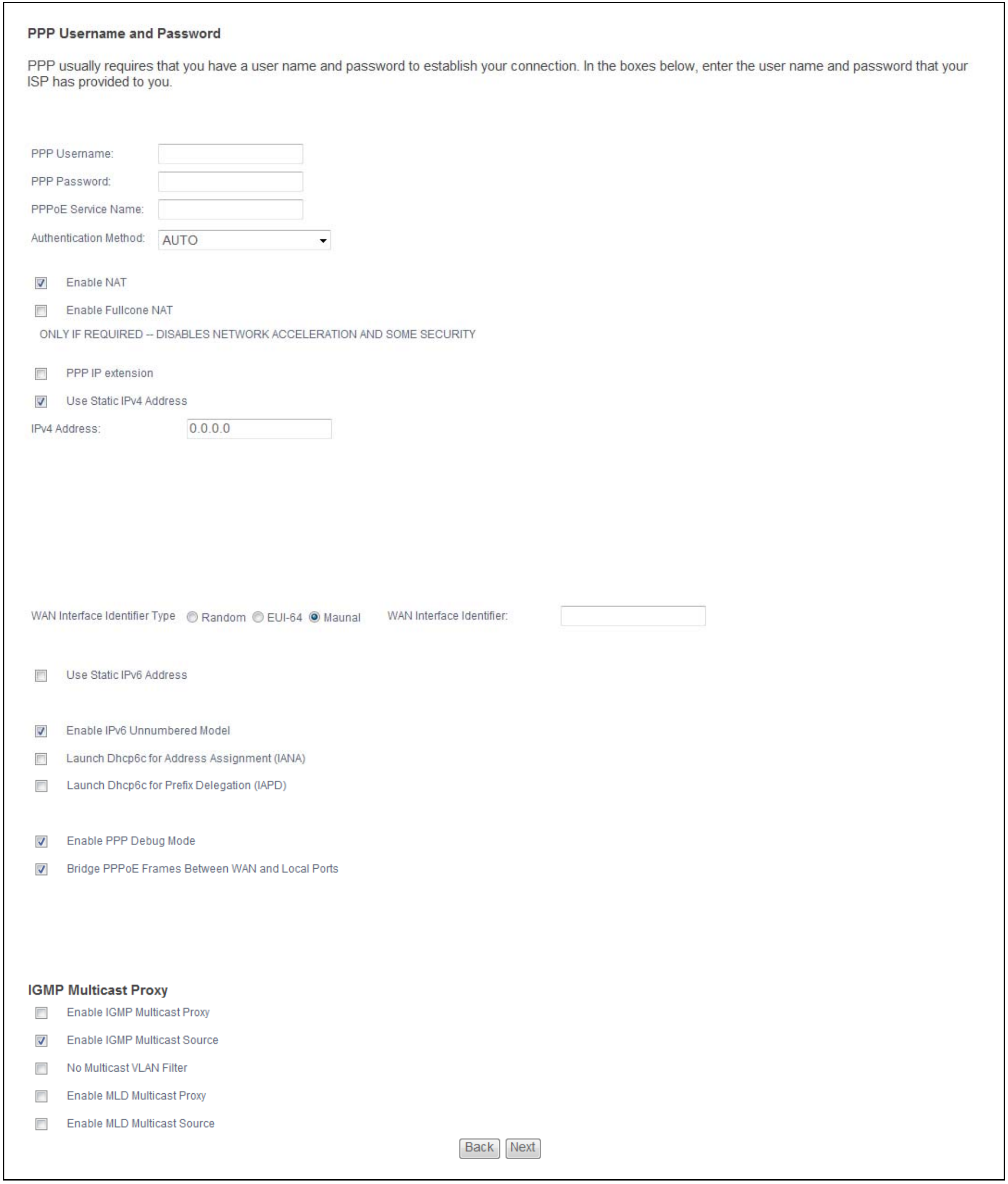
3.3.1.3 WAN IP Address and DNS Server

The screen differs by the encapsulation you selected in the previous screen.

PPPoE

This screen displays when you select **PPP over Ethernet (PPPoE)** in the **WAN Service Configuration** screen.

Figure 19 WAN Configuration: PPPoE



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

☑ Enable NAT

□ Enable Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

□ PPP IP extension

☑ Use Static IPv4 Address

IPv4 Address: 0.0.0.0

WAN Interface Identifier Type ○ Random ○ EUI-64 ● Maunal WAN Interface Identifier:

□ Use Static IPv6 Address

☑ Enable IPv6 Unnumbered Model

□ Launch Dhcp6c for Address Assignment (IANA)

□ Launch Dhcp6c for Prefix Delegation (IAPD)

☑ Enable PPP Debug Mode

☑ Bridge PPPoE Frames Between WAN and Local Ports

IGMP Multicast Proxy

□ Enable IGMP Multicast Proxy

☑ Enable IGMP Multicast Source

□ No Multicast VLAN Filter

□ Enable MLD Multicast Proxy

□ Enable MLD Multicast Source

Table 17 WAN Configuration: PPPoE

LABEL	DESCRIPTION
PPP Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.
Authentication Method	The Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your Router accepts either CHAP or PAP when requested by this remote node. **PAP** - Your Router accepts PAP only. **CHAP** - Your Router accepts CHAP only. **MSCHAP** - Your Router accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	This field is available only when you select **Enable NAT**. Select this check box to activate full cone NAT on this connection.
PPP IP extension	Select this only if your service provider requires it. PPP IP extension extends the service provider's IP subnet to a single LAN computer. • It lets only one computer on the LAN connect to the WAN. • The public IP address from the ISP is forwarded through DHCP to the LAN computer instead of being used on the WAN PPP interface. • It disables NAT and the firewall. • DHCP tells the LAN computer to use the gateway as the default gateway and DNS server. • The Router bridges IP packets between the WAN and LAN ports except packets destined for the Router's LAN IP address.
Use Static IPv4 Address	Select this option if you have a fixed IPv4 address assigned by your ISP.
IPv4 Address	Enter the IPv4 address assigned by your ISP.
WAN Interface Identifier Type	Select **Random** to have the Device randomly configure a WAN Identifier, which is shown in the WAN Interface Identifier field. Select **EUI-64** to use the EUI-64 format to generate an interface ID from the MAC address of the WAN interface. Select **Manual** to manually enter a WAN Identifier as the interface ID to identify the WAN interface. The WAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address.

Table 17 WAN Configuration: PPPoE (continued)

LABEL	DESCRIPTION
WAN Interface Identifier	If you selected **Random**, this field is automatically configured. If you selected **Manual**, enter the WAN Identifier in this field. The WAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
Use Static IPv6 Address	Select this option if you have a fixed IPv6 address assigned by your ISP.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Enable IPv6 Unnumbered Model	Select this to enable IPv6 processing on the interface without assigning an explicit IPv6 address to the interface.
Launch Dhcp6c for Address Assignment (IANA)	Select this check box to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Router using the IPv6 prefix from an RA.
Launch Dhcp6c for Prefix Delegation (IAPD)	Select this to use DHCP PD (Prefix Delegation) that enables the Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.
Bridge PPPoE Frames Between WAN and Local Ports	Select this option to forward PPPoE packets from the WAN port to the LAN ports and from the LAN ports to the WAN port. In addition to the Router's built-in PPPoE client, you can select this to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Router. Each host can have a separate account and a public WAN IP address. This is an alternative to NAT for application where NAT is not appropriate. Clear this if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Enable IGMP Multicast Proxy	Select this check box to have the Router act as an IGMP proxy on this connection. This allows the Router to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable IGMP Multicast Source	Select this check box to have the Router add routing table entries based on the IGMP traffic.
No Multicast VLAN Filter	Select this check box to have the Router not filter multicast traffic based on its VLAN.
Enable MLD Multicast Proxy	Select this check box to have the Router act as an MLD proxy on this connection. This allows the Router to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.

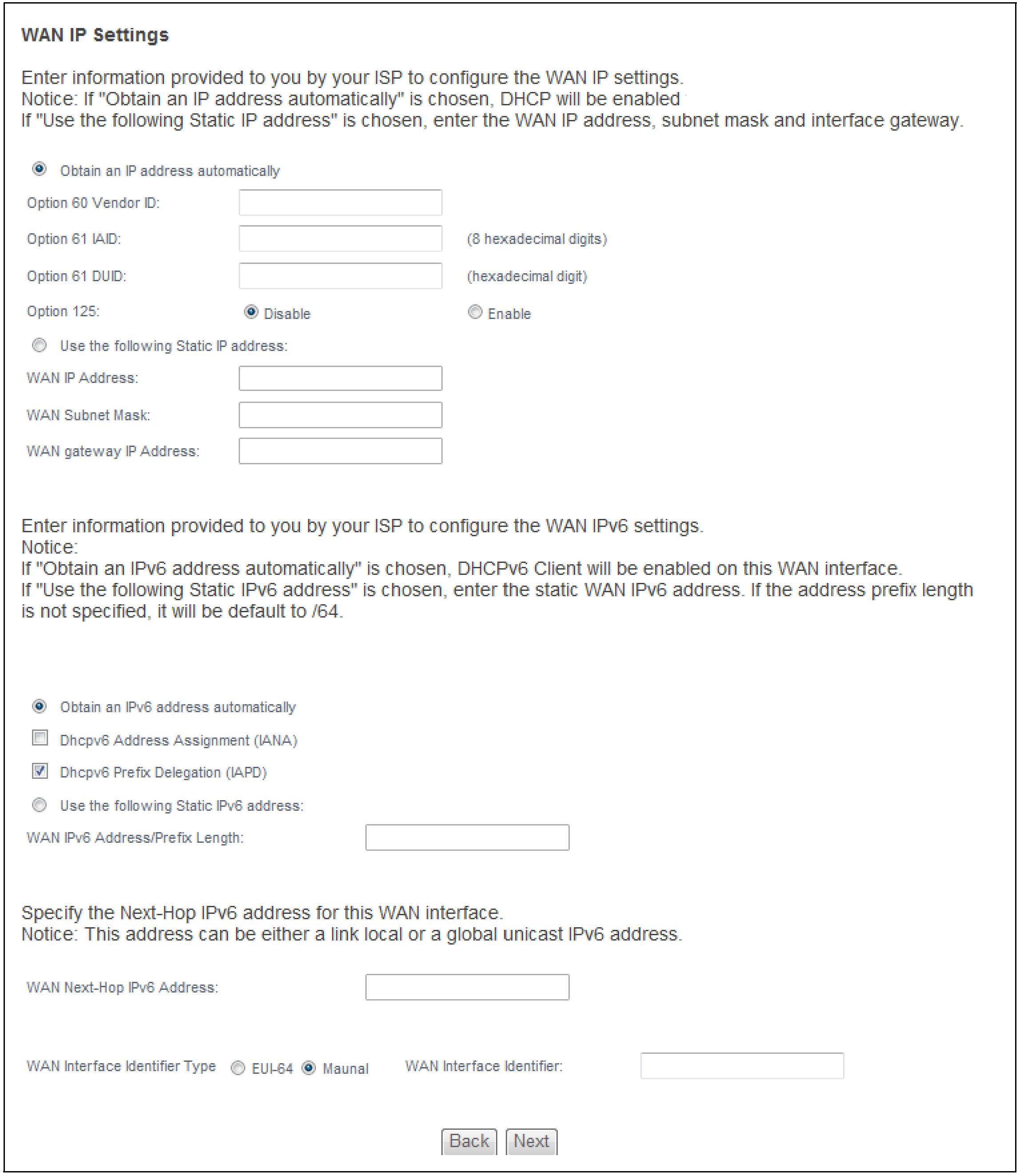
Table 17 WAN Configuration: PPPoE (continued)

LABEL	DESCRIPTION
Enable MLD Multicast Source	Select this check box to have the Router add routing table entries based on the MLD traffic.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 20 WAN Configuration: IPoE



WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.

● Obtain an IP address automatically

Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(hexadecimal digit)
Option 125:	● Disable	○ Enable

○ Use the following Static IP address:

WAN IP Address:	
WAN Subnet Mask:	
WAN gateway IP Address:	

Enter information provided to you by your ISP to configure the WAN IPv6 settings.
Notice:
If "Obtain an IPv6 address automatically" is chosen, DHCPv6 Client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.

● Obtain an IPv6 address automatically

□ Dhcpv6 Address Assignment (IANA)

☑ Dhcpv6 Prefix Delegation (IAPD)

○ Use the following Static IPv6 address:

WAN IPv6 Address/Prefix Length:

Specify the Next-Hop IPv6 address for this WAN interface.
Notice: This address can be either a link local or a global unicast IPv6 address.

WAN Next-Hop IPv6 Address:

WAN Interface Identifier Type ○ EUI-64 ● Maunal WAN Interface Identifier:

Table 18 WAN Configuration: IPoE

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Option 60 Vendor ID	DHCP Option 60 identifies the vendor and functionality of the Router in DHCP requests that the Router sends to a DHCP server when getting a WAN IP address. Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Option 61 IAID	DHCP Option 61 identifies the Router in DHCP requests the Router sends to a DHCP server when getting a WAN IP address. Enter the Identity Association Identifier (IAID) of the Router. For example, the WAN connection index number.
Option 61 DUID	Enter the DHCP Unique Identifier (DUID) of the Router.
Option 125	Enable this to add vendor specific information to DHCP requests that the Router sends to a DHCP server when getting a WAN IP address.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Obtain an IPv6 address automatically	Select this option to have the Router use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.
Dhcpv6 Address Assignment	Select this check box to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Router using the IPv6 prefix from an RA.
Dhcp6c Prefix Delegation (IAPD)	Select this to use DHCP PD (Prefix Delegation) that enables the Device to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.
Use the following Static IPv6 address	Select this option if you have a fixed IPv6 address assigned by your ISP.
WAN IPv6 Address/Prefix Length	Enter the static IPv6 address and bit number of the IPv6 subnet mask provided by your ISP.
WAN Next-Hop IPv6 Address	Enter the gateway IPv6 address provided by your ISP.

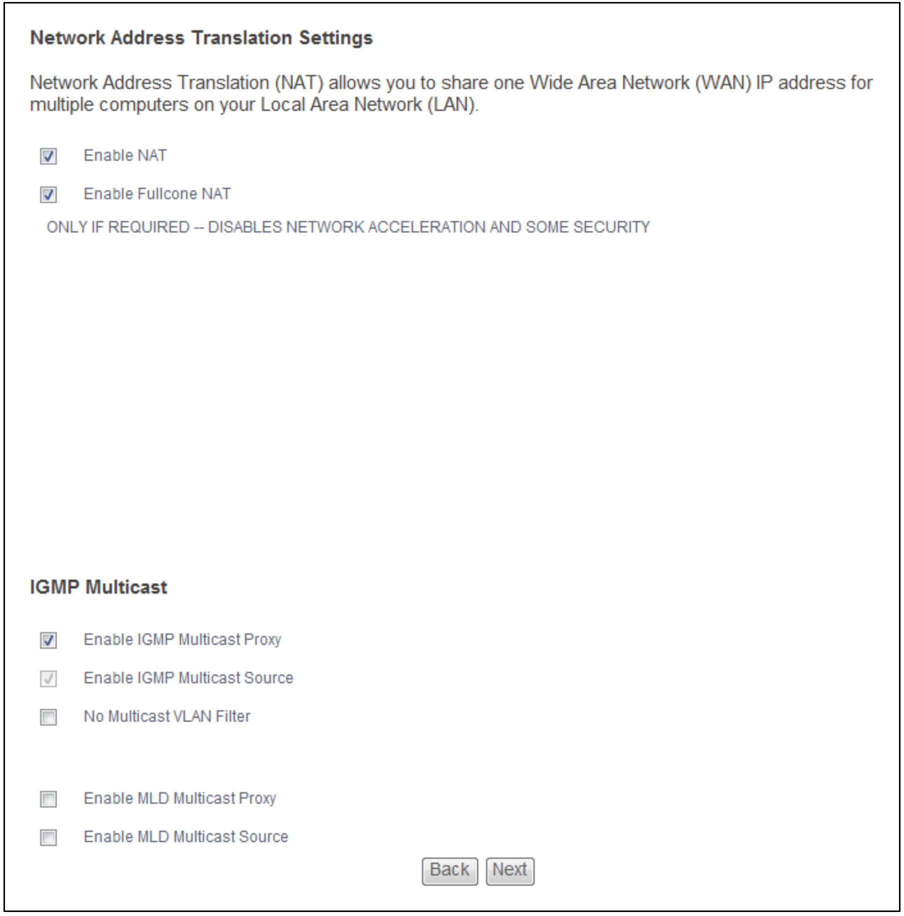
Table 18 WAN Configuration: IPoE (continued)

LABEL	DESCRIPTION
WAN Interface Identifier Type	Select **Random** to have the Device randomly configure a WAN Identifier, which is shown in the WAN Interface Identifier field. Select **EUI-64** to use the EUI-64 format to generate an interface ID from the MAC address of the WAN interface. Select **Manual** to manually enter a WAN Identifier as the interface ID to identify the WAN interface. The WAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address.
WAN Interface Identifier	If you selected **Random**, this field is automatically configured. If you selected **Manual**, enter the WAN Identifier in this field. The WAN identifier should be unique and 64 bits in hexadecimal form. Every 16 bit block should be separated by a colon as in XXXX:XXXX:XXXX:XXXX where X is a hexadecimal character. Blocks of zeros can be represented with double colons as in XXXX:XXXX::XXXX.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

3.3.1.4 NAT and IGMP Multicast

This screen is available only when you select **IP over Ethernet** in the **WAN Service Configuration** screen.

Figure 21 WAN Configuration: NAT and IGMP Multicast: IPoE



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 Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

IGMP Multicast

☑ Enable IGMP Multicast Proxy

☑ Enable IGMP Multicast Source

□ No Multicast VLAN Filter

□ Enable MLD Multicast Proxy

□ Enable MLD Multicast Source

Table 19 WAN Configuration: NAT and IGMP Multicast: IPoE

LABEL	DESCRIPTION
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	Select this check box to activate full cone NAT on this connection. This field is available only when you select **Enable NAT**.
Enable IGMP Multicast Proxy	Select this check box to have the Router act as an IGMP proxy on this connection. This allows the Router to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable IGMP Multicast Source	Select this check box to have the Router add routing table entries based on the IGMP traffic.

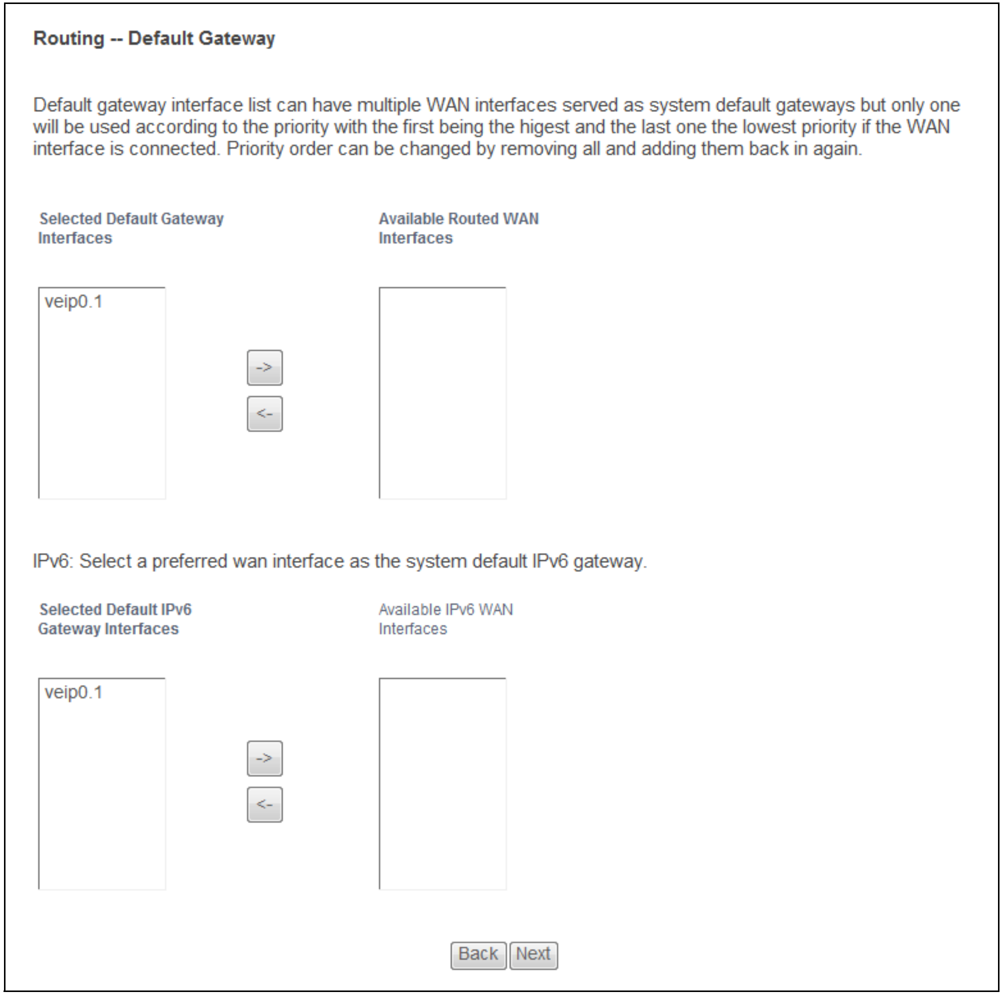
Table 19 WAN Configuration: NAT and IGMP Multicast: IPoE (continued)

LABEL	DESCRIPTION
No Multicast VLAN Filter	Select this check box to have the Router not filter multicast traffic based on its VLAN.
Enable MLD Multicast Proxy	Select this check box to have the Router act as an MLD proxy on this connection. This allows the Router to get subscription information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable MLD Multicast Source	Select this check box to have the Router add routing table entries based on the MLD traffic.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

3.3.1.5 Default Gateway (PPPoE or IPoE)

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

Figure 22 WAN Configuration: Default Gateway



Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces: veip0.1

Available Routed WAN Interfaces:

IPv6: Select a preferred wan interface as the system default IPv6 gateway.

Selected Default IPv6 Gateway Interfaces: veip0.1

Available IPv6 WAN Interfaces:

Table 20 WAN Configuration: Default Gateway

LABEL	DESCRIPTION
Selected Default Gateway Interfaces	Select a WAN interface through which to forward the service’s traffic. You can select multiple WAN interfaces for the device to try. The Router tries the WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.
Available Routed WAN Interfaces	Select from these WAN interfaces.

Table 20 WAN Configuration: Default Gateway (continued)

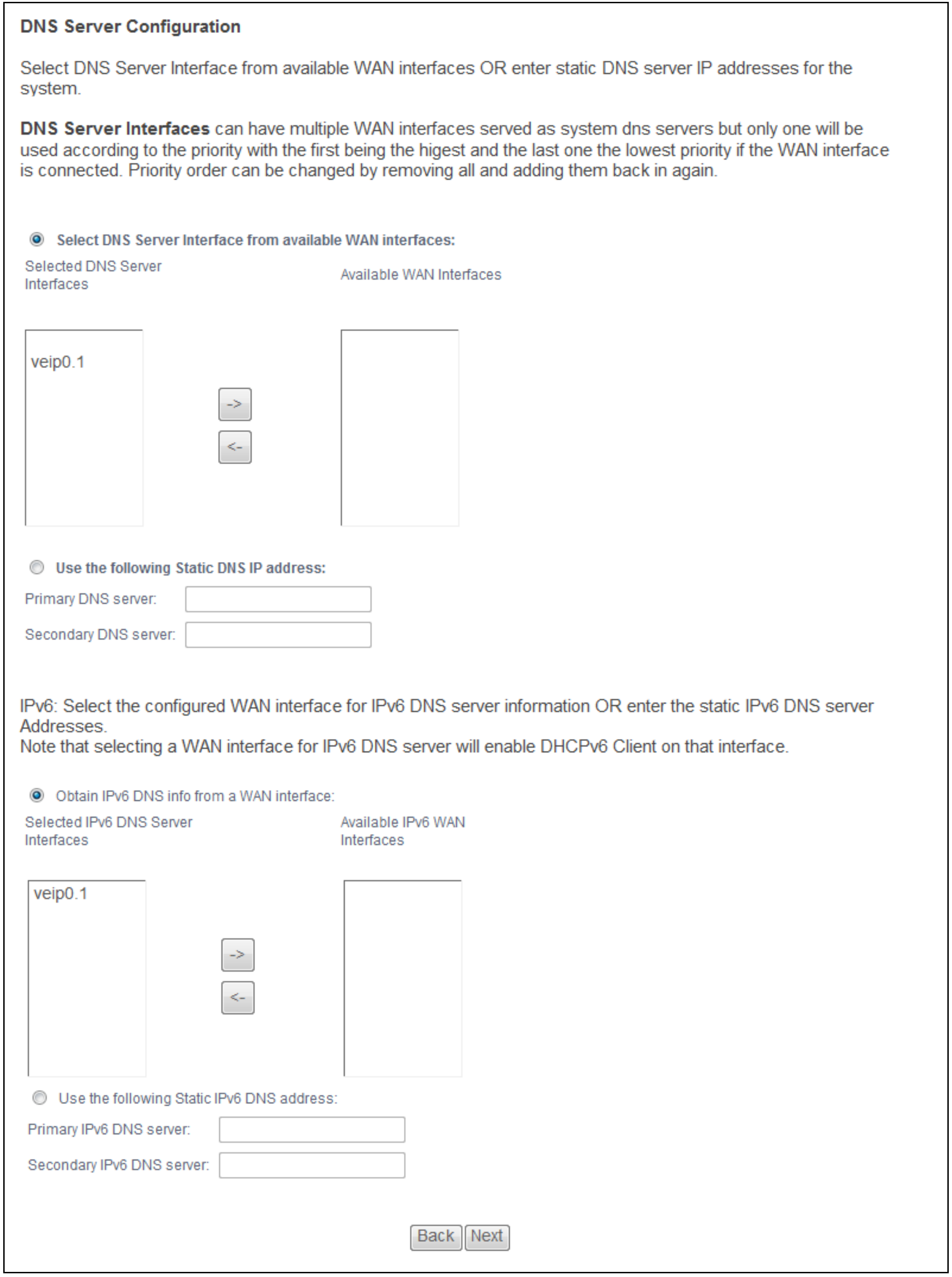
LABEL	DESCRIPTION
Selected WAN Interface	Select a WAN interface through which to forward IPv6 traffic.
Selected Default IPv6 Gateway Interfaces	Select an IPv6 WAN interface through which to forward the service's IPv6 traffic. You can select multiple WAN interfaces for the device to try. The Router tries the WAN interfaces in the order listed and uses only the default gateway of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.
Available IPv6 WAN Interfaces	Select from these IPv6 WAN interfaces.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

3.3.1.6 DNS Server

The screen is not available when you select **Bridging** in the **WAN Service Configuration** screen.

ⓘ If you configure only one IPoE connection, you must enter the static DNS server address.

Figure 23 WAN Configuration: DNS Server: PPPoE or IPoE



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: veip0.1

Available WAN Interfaces:

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

IPv6: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface:

Selected IPv6 DNS Server Interfaces: veip0.1

Available IPv6 WAN Interfaces:

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

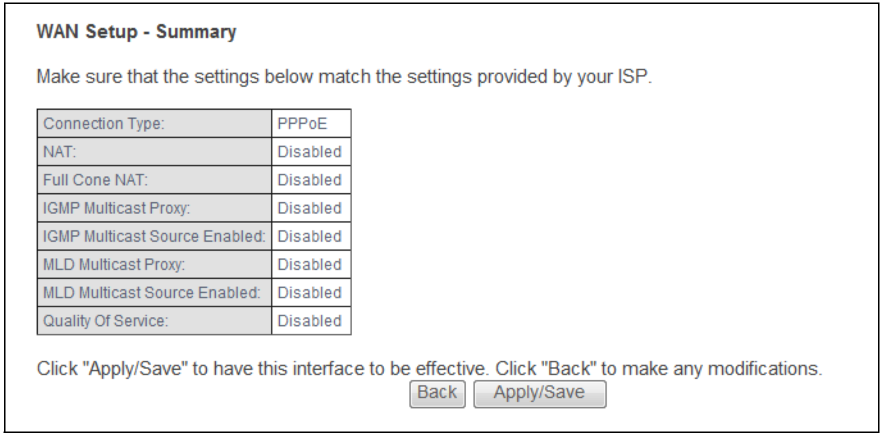
Table 21 WAN Configuration: DNS Server: PPPoE or IPoE

LABEL	DESCRIPTION
Select DNS Server Interface from available WAN interfaces	Select this to have the Router get the DNS server addresses from one of the Router's WAN interfaces.
Selected DNS Server Interfaces	Select a WAN interface through which to get DNS server addresses. You can select multiple WAN interfaces for the device to try. The Router tries the WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.
Available WAN Interfaces	These are the WAN interfaces you can select from.
Use the following Static DNS IP address	Select this to have the Router use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Obtain IPv6 DNS info from a WAN interface	Select this to have the Router get the IPv6 DNS server addresses from the ISP automatically.
WAN Interface selected	Select a WAN interface through which you want to obtain the IPv6 DNS related information.
Use the following Static IPv6 DNS address	Select this to have the Router use the IPv6 DNS server addresses you configure manually.
Primary IPv6 DNS server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS server	Enter the second IPv6 DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

3.3.1.7 Configuration Summary

This read-only screen shows the current WAN connection settings.

Figure 24 WAN Configuration: Configuration Summary



WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Disabled
Full Cone NAT:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Table 22 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
NAT	This shows whether NAT is active or not for this connection.
Full Cone NAT	This shows whether full cone NAT is active or not for this connection.
IGMP Multicast Proxy	This shows whether IGMP proxy is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
IGMP Multicast Source Enabled	This shows whether IGMP source enable is activated or not for this connection. IGMP source enable has the Router add routing table entries based on the IGMP traffic.
MLD Multicast Proxy	This shows whether MLD proxy is activated or not for this connection. MLD is not available when the connection uses the bridging service.
MLD Multicast Source Enabled	This shows whether MLD source enable is activated or not for this connection. MLD source enable has the Router add routing table entries based on the MLD traffic.
Quality Of Service	This shows whether QoS is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

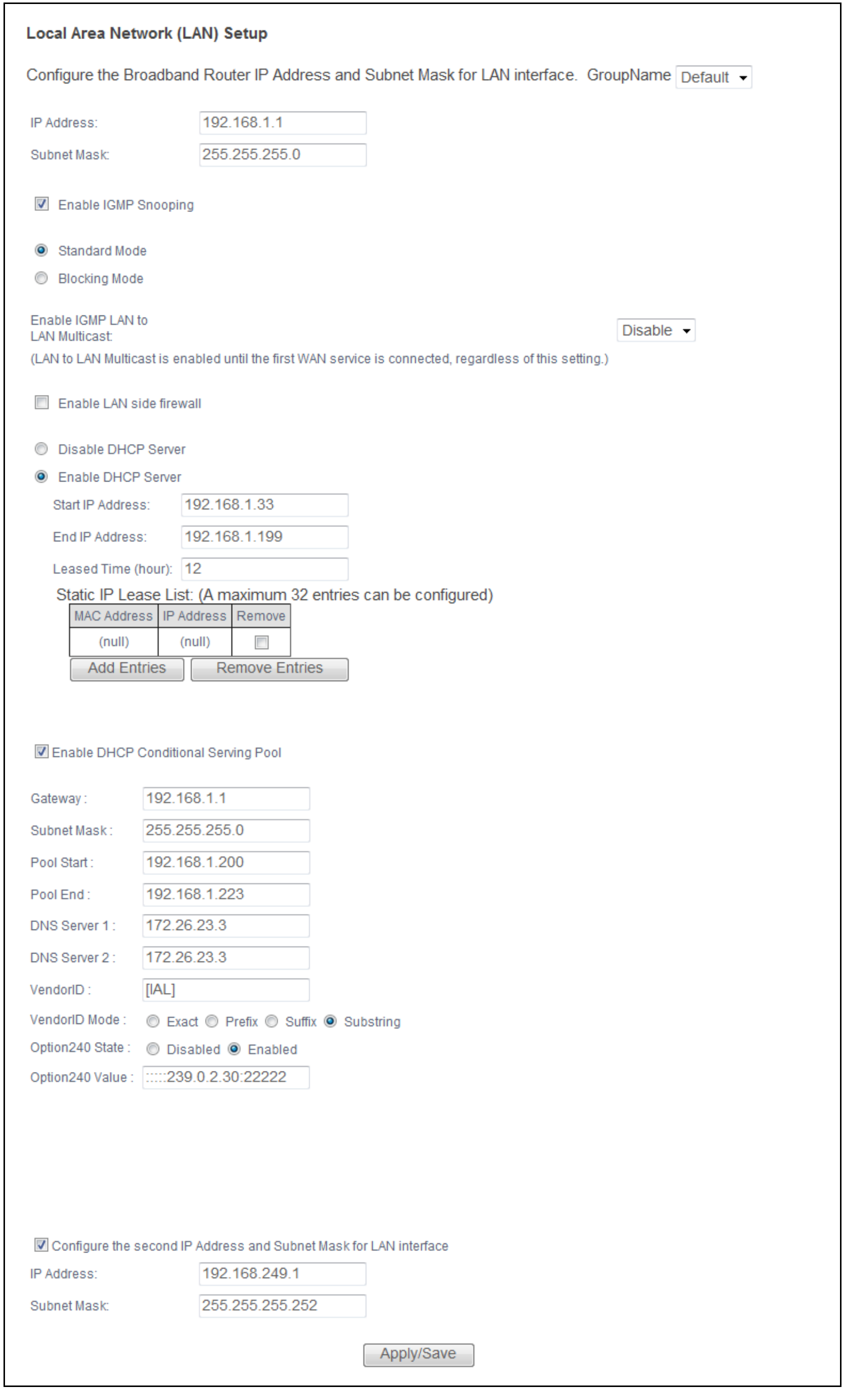
LAN

4 Chapter

4.1 LAN Setup

Click **Advanced Setup > LAN** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your Router and configure the DNS server information that the Router sends to the DHCP client devices on the LAN.

Figure 25 LAN Setup



Local Area Network (LAN) Setup

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

● Standard Mode

○ Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.1.33

End IP Address: 192.168.1.199

Leased Time (hour): 12

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
(null)	(null)	□

☑ Enable DHCP Conditional Serving Pool

Gateway : 192.168.1.1

Subnet Mask : 255.255.255.0

Pool Start : 192.168.1.200

Pool End : 192.168.1.223

DNS Server 1 : 172.26.23.3

DNS Server 2 : 172.26.23.3

VendorID : [IAL]

VendorID Mode : ○ Exact ○ Prefix ○ Suffix ● Substring

Option240 State : ○ Disabled ● Enabled

Option240 Value : :::::239.0.2.30:22222

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

IP Address: 192.168.249.1

Subnet Mask: 255.255.255.252

Table 23 LAN Setup

LABEL	DESCRIPTION
Group Name	Select the LAN interface for which to configure the IP address and subnet mask.
IP Address	Enter the LAN IP address you want to assign to your Router. The factory default is 192.168.1.1.
Subnet Mask	Type the subnet mask of your network. The factory default is 255.255.255.0. Your Router automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
Enable IGMP Snooping	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. Select this to activate IGMP Snooping. This allows the Router to passively learn memberships in multicast groups. Otherwise, clear the option to deactivate it. Select **Standard Mode** to have the Router forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports. Select **Blocking Mode** to have the Router block all unknown multicast packets from the WAN.
Enable IGMP LAN to LAN Multicast	Select this to allow IGMP multicast traffic to travel between the LAN ports.
Disable DHCP Server	Select this to have the Router not provide DHCP services. Users must configure LAN devices with manual network settings if you do not have another DHCP server on the network.
Enable DHCP Server	Select this to have the Router serve as the DHCP server for the network to assign IP addresses and provide subnet mask, gateway, and DNS server information to LAN devices.
Start IP Address	This field specifies the first of the contiguous addresses in the IP address pool.
End IP Address	This field specifies the last of the contiguous addresses in the IP address pool.
Leased Time (hour)	Specify for how many hours to assign an IP address to a LAN device before making it available for reassignment to other systems.
Static IP Lease List	Use this table to assign IP addresses on the LAN to specific computers based on their MAC Addresses.
MAC Address	The MAC (Media Access Control) of a LAN device to which the entry’s IP address is assigned.
IP Address	This field displays the IP address reserved for the LAN device with the entry’s MAC.
Remove	Select entries and click the **Remove Entries** button to delete them.
Add Entries	Click this button to create a new static IP lease entry.
Enable DHCP Conditional Serving Pool	Select this to enable the DHCP conditional serving pool for IPTV set-top boxes. DHCP server will offer IP address from the conditional pool if the DHCP request sent from a set-top box contains the specific Vendor ID.

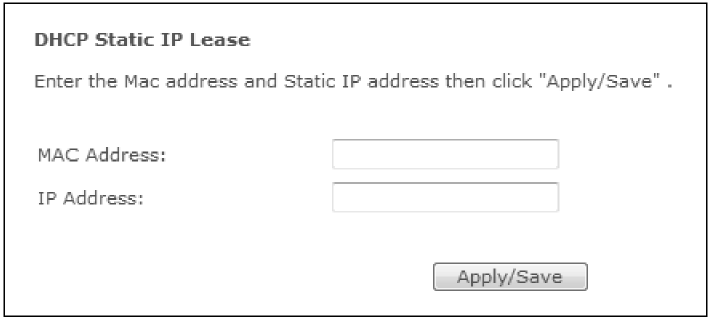
Table 23 LAN Setup (continued)

LABEL	DESCRIPTION
Gateway	Enter the IPTV server’s IP address.
Subnet Mask	Enter the IPTV server’s subnet mask.
Pool Start/End	Specify the first and last of the contiguous addresses in the IPTV server’s IP address pool.
DNS Server 1/2	Enter the IPTV server’s first/second DNS server IP address.
VendorID	Specify the IPTV’s vendor ID.
VendorID Mode	Specify the IPTV’s vendor ID mode type.
VendorID Exclude	Specify if you want to enable vendor ID exclude.
Option240 State	Select **Enabled** to have the Router assign DHCP option 240 to the LAN set top box.
Option240 Value	Enter the option 240 value.
Configure the second IP Address and Subnet Mask for LAN interface	Select the check box to use IP alias to configure another LAN network for the Router. IP alias partitions a physical network into different logical networks over the same Ethernet interface. The Router supports multiple logical LAN interfaces via its physical Ethernet interface with the Router itself as the gateway for the LAN network. You can also configure firewall rules to control access to the LAN's logical network (subnet).
IP Address	Enter the second LAN IP address of your Router in dotted decimal notation.
Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default).

4.1.1 Add DHCP Static IP Lease

Click **Add Entries** in the **LAN Setup** screen to display the following screen.

Figure 26 Add DHCP Static IP Lease



DHCP Static IP Lease

Enter the Mac address and Static IP address then click "Apply/Save" .

MAC Address:

IP Address:

Table 24 Add DHCP Static IP Lease

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Apply/Save	Click this button to save your changes and go back to the previous screen.

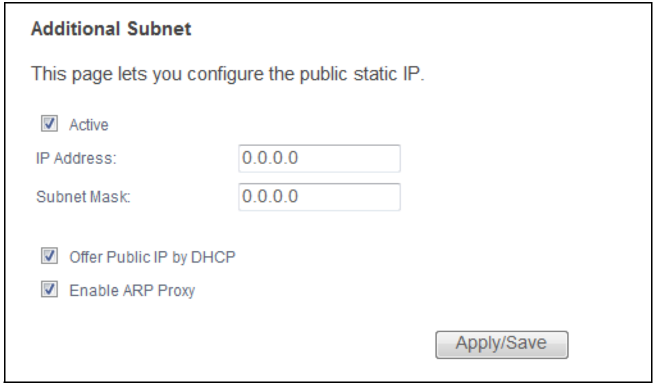
4.2 LAN Additional Subnet

Click **Advanced Setup > LAN > Additional Subnet** to open the **Additional Subnet** screen. Use this screen to configure IP alias and public static IP.

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Router supports multiple logical LAN interfaces via its physical Ethernet interface with the Router itself as the gateway for the LAN network. When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

If your ISP provides the Public LAN service, the Router may use an LAN IP address that can be accessed from the WAN.

Figure 27 LAN Additional Subnet



Additional Subnet

This page lets you configure the public static IP.

☑ Active

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

☑ Offer Public IP by DHCP

☑ Enable ARP Proxy

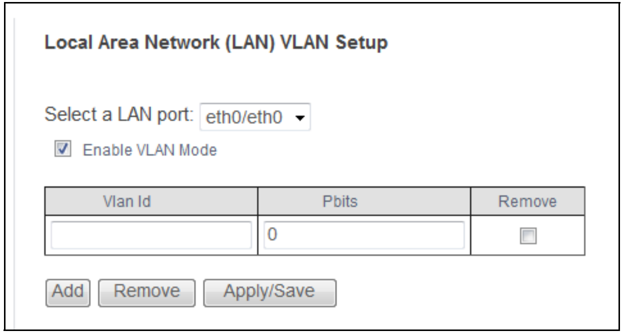
Table 25 LAN Additional Subnet

LABEL	DESCRIPTION
Active	Select the check box to configure a LAN network for the Router.
IP Address	Enter the IP address of your Router in dotted decimal notation.
IP Subnet Mask	Your Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Router.
Offer Public IP by DHCP	Select the check box to enable the Router to provide public IP addresses by DHCP server.
Enable ARP Proxy	Select the check box to enable the ARP (Address Resolution Protocol) proxy.
Apply/Save	Click this button to save your changes and go back to the previous screen.

4.3 LAN VLAN

Click **Advanced Setup > LAN > LAN VLAN** to open this screen. Use this screen to control the VLAN ID and IEEE 802.1p priority tags of traffic sent out through individual LAN ports.

Figure 28 LAN VLAN



Local Area Network (LAN) VLAN Setup

Select a LAN port: eth0/eth0

☑ Enable VLAN Mode

Vlan Id	Pbits	Remove
	0	□

Table 26 LAN VLAN

LABEL	DESCRIPTION
Select a LAN port	**eth0** ~ **eth3** represent the Ethernet LAN ports 1 ~ 4. Select a port.
Enable VLAN Mode	Select this to use VLAN on the LAN port you selected.
VLAN ID	Specify the VLAN ID (from 0 to 4094) to use for this LAN port’s downstream traffic.

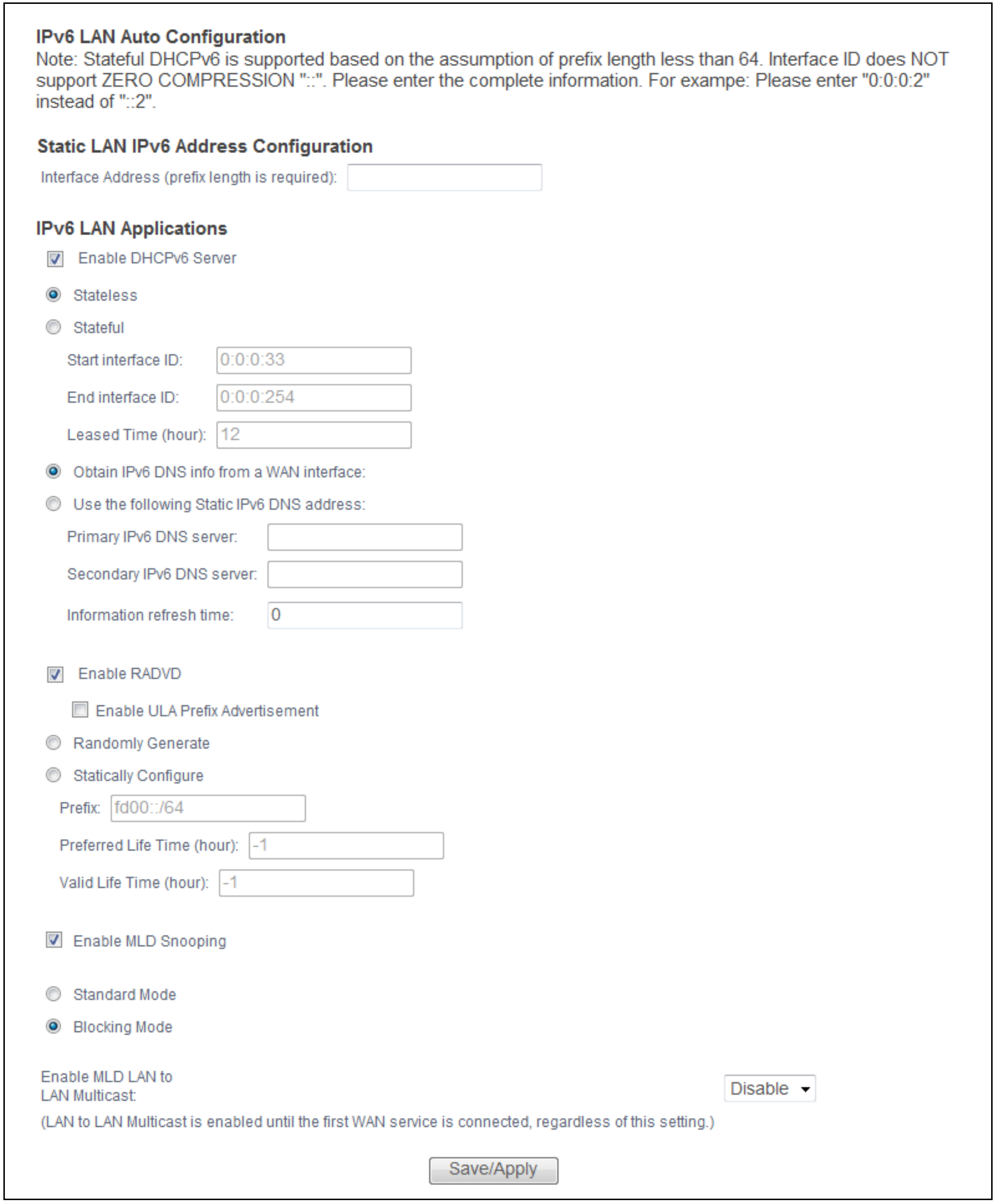
Table 26 LAN VLAN (continued)

LABEL	DESCRIPTION
Pbits	Set the IEEE 802.1p priority tag value (o to 7) to use for the LAN port’s downstream traffic. The larger the number, the higher the priority.
Remove	Select an entry and click the **Remove** button to delete it.
Add	Click this button to create a new LAN VLAN setting entry.
Apply/Save	Click this button to save your changes and go back to the previous screen.

4.4 IPv6 LAN Auto Configuration

Click **Advanced Setup > LAN > IPv6 Autoconfig** to open the **IPv6 LAN Auto Configuration** screen. Use this screen to set the Local Area Network interface IPv6 settings.

Figure 29 IPv6 LAN Auto Configuration



IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For exampe: Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☑ Enable DHCPv6 Server

● Stateless

○ Stateful

Start interface ID: 0:0:0:33

End interface ID: 0:0:0:254

Leased Time (hour): 12

● Obtain IPv6 DNS info from a WAN interface:

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

Information refresh time: 0

☑ Enable RADVD

□ Enable ULA Prefix Advertisement

○ Randomly Generate

○ Statically Configure

Prefix: fd00::/64

Preferred Life Time (hour): -1

Valid Life Time (hour): -1

☑ Enable MLD Snooping

○ Standard Mode

● Blocking Mode

Enable MLD LAN to LAN Multicast: Disable

(LAN to LAN Multicast is enabled until the first WAN service is connected, regardless of this setting.)

The following table describes the fields in this screen.

Table 27 IPv6 LAN Auto Configuration

LABEL	DESCRIPTION
Interface Address	To use a static IPv6 address, enter the IPv6 address prefix and prefix length that the Router uses for the LAN IPv6 address. The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Enable DHCPv6 Server	Select this to have the Router act as a DHCPv6 server and pass IPv6 addresses, DNS server and domain name information to DHCPv6 clients.
Stateless	Select this to have the Router use IPv6 stateless autoconfiguration.
Stateful	Select this to have the Router use IPv6 stateful autoconfiguration. **Start interface ID**: specify the first IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients. **End interface ID**: specify the last IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients. **Leased Time (hour)**: Specify for how many hours to assign an IPv6 address to a DHCPv6 client before making it available for reassignment to other systems.
Obtain IPv6 DNS info from a WAN interface	Select this to have the Router get the IPv6 DNS server addresses from the ISP automatically.
Use the following Static IPv6 DNS address	Select this to have the Router use the IPv6 DNS server addresses you configure manually.
Primary IPv6 DNS server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS server	Enter the second IPv6 DNS server address assigned by the ISP.
Enable RADVD	Select this to have the Router send router advertisement messages to the LAN hosts. Router advertisement is a response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters, such as IPv6 prefix and DNS information. Router solicitation is a request from a host to locate a router that can act as the default router and forward packets. Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.
Enable ULA Prefix Advertisement	Select this to send Unique Local IPv6 Unicast Addresses (ULA) advertisement messages to the LAN hosts.
Randomly Generate	Select this to automatically create a LAN IPv6 address prefix.

Table 27 IPv6 LAN Auto Configuration (continued)

LABEL	DESCRIPTION
Statically Configure	Select this to send a fixed LAN IPv6 address prefix. **Prefix**: enter the IPv6 prefix and length the Router uses to generate the LAN IPv6 address. The prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask. **Preferred Life Time (hour)**: enter the preferred lifetime for the prefix. -1 means no time limit. **Valid Life Time (hour)**: enter the valid lifetime for the prefix. Set this greater than or equal to the preferred life time. -1 means no time limit.
Enable MLD Snooping	Select this to have the Router check Multicast Listener Discovery (MLD) packets to learn the multicast group membership. This helps reduce multicast traffic.
Standard Mode	Select this to have the Router forward multicast packets to a port that joins the multicast group and broadcast unknown multicast packets from the WAN to all LAN ports.
Blocking Mode	Select this to have the Router block all unknown multicast packets from the WAN.
Enable MLD LAN to LAN Multicast	Select this to allow MLD multicast traffic to travel between the LAN ports.
Save/Apply	Click this button to save your changes.

VPN

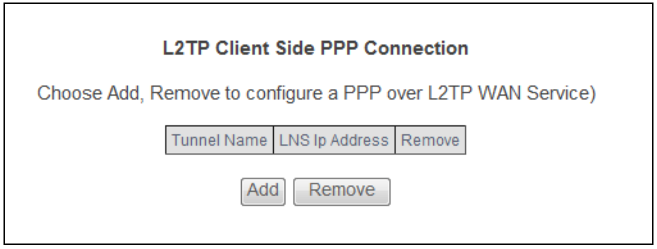
5 Chapter

5.1 L2TP VPN Client

Use this screen to manage WAN service Layer 2 Tunneling Protocol (L2TP) client settings for connecting to L2TP servers.

Click **Advanced Setup > VPN > L2TP Client** to open this screen as shown next.

Figure 30 L2TP Client



L2TP Client Side PPP Connection

Choose Add, Remove to configure a PPP over L2TP WAN Service)

Tunnel Name	LNS Ip Address	Remove

This screen contains the following fields:

Table 28 L2TP Client

LABEL	DESCRIPTION
Tunnel Name	This is the name of this client connection.
LNS Ip Address	This is the IP address of the L2TP VPN server.
Remove	Select entries and click the **Remove** button to delete them.
Status	This is the connection status.
Add	Click this to add a VPN client profile.

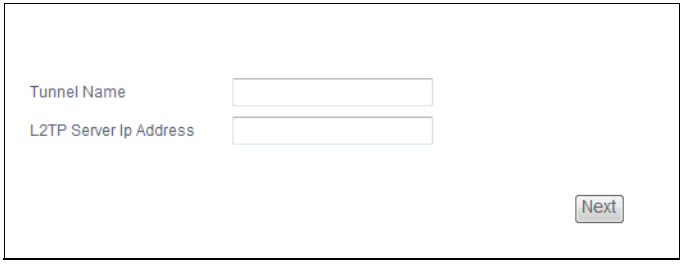
5.1.1 L2TP VPN Client: Add

Click **Advanced Setup > VPN > L2TP Client > Add** to configure L2TP WAN service settings for connecting to L2TP servers.

5.1.1.1 Name and Server IP Address

This screen displays when you add a new L2TP client WAN service.

Figure 31 L2TP Client: Add



Tunnel Name

L2TP Server Ip Address

This screen contains the following fields:

Table 29 L2TP Client: Add

LABEL	DESCRIPTION
Tunnel Name	Enter the name for this client connection.
L2TP Server Ip Address	Enter the IP address of the L2TP server.
L2TP Protocol Version	Select the L2TP Protocol Version **2** or **3**. L2TPv2 is a standard method for tunneling Point-to-Point Protocol (PPP) while L2TPv3 provides improved support for other types of networks including frame relay and ATM.
NAT Mode?	Select **Yes** if the client will be located behind a NAT enabled router. This will allow multiple clients using NAT to connect with L2TP at the same time.
Auth Protocol	Select the Authentication Protocol allowed for the connection. Options are: **PAP** - Password Authentication Protocol (PAP) authentication occurs in clear text and does not use encryption. It's probably not a good idea to rely on this for security. **CHAP** - Challenge Handshake Authentication Protocol (CHAP) provides authentication through a shared secret key and uses a three way handshake. **MSCHAPv1** - Microsoft CHAP v1 (MSCHAPv1) provides authentication through a shared secret key and uses a three way handshake. It provides improved usability with Microsoft products. **MSCHAPv2** - Microsoft CHAP v2 (MSCHAPv2) provides encryption through a shared secret key and uses a three way handshake. It provides additional security over **MSCHAPv1**, including two-way authentication.
MPPE Encryption	If **MSCHAPv1** or **MSCHAPv2** is selected as an **Auth Protocol**, use the drop-down list box to select the type of Microsoft Point-to-Point Encryption (MPPE). Options are: **MPPE 40 -** MPPE with 40 bit session key length **MPPE 128 -** MPPE with 128 bit session key length **Auto -** Automatically select either **MPPE 40** or **MPPE 128**

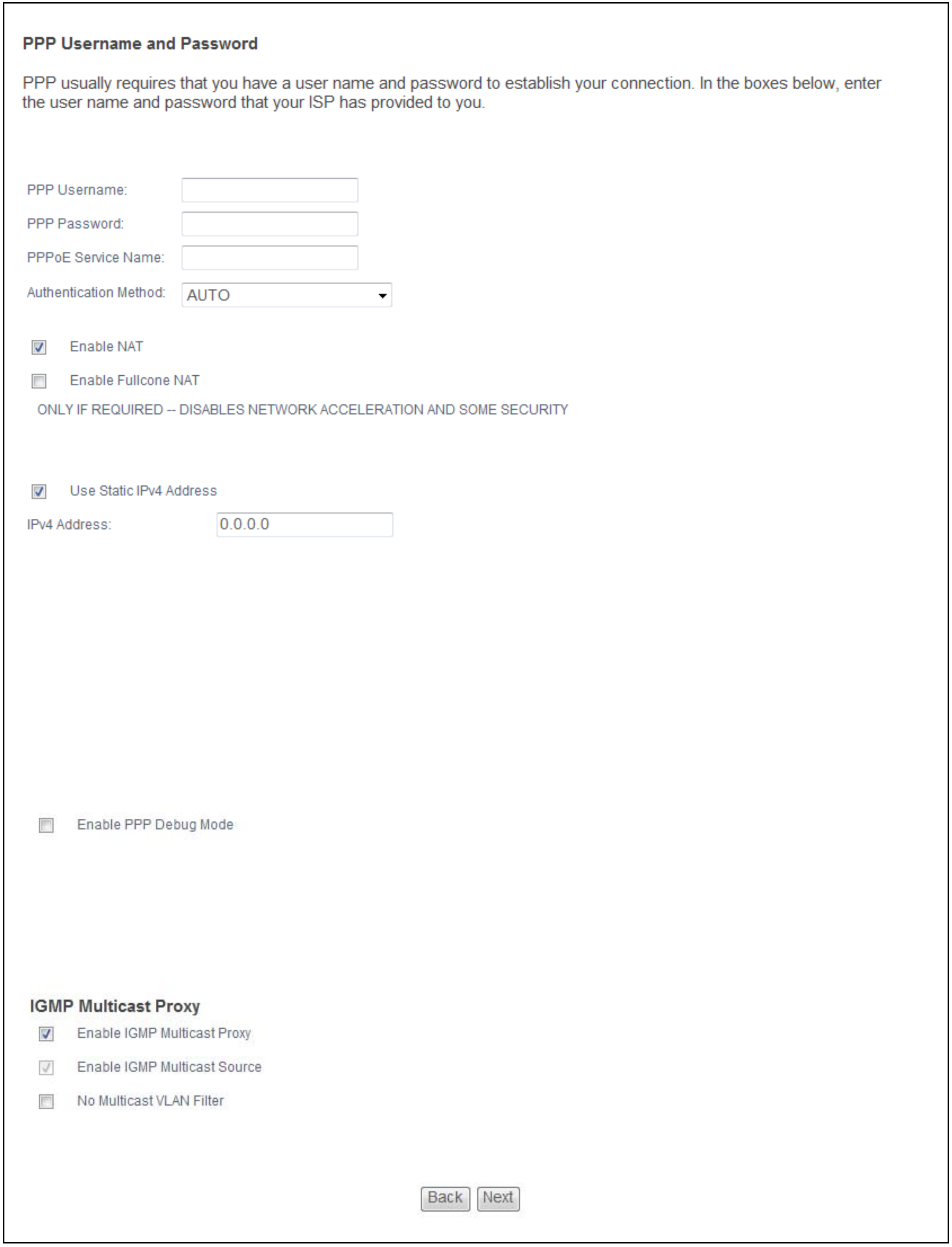
Table 29 L2TP Client: Add (continued)

LABEL	DESCRIPTION
MPPE Stateful?	Select **Yes** to enable stateful MPPE encryption. This can increase performance over stateless MPPE, but should not be used in lossy network environments like layer two tunnels over the Internet.
User Name	Enter the user name for connecting to the L2TP server.
Password	Enter the password for connecting to the L2TP server.
Retype	Retype the password for connecting to the L2TP server.
Get IP automatically	Select **Yes** to have the L2TP server assign a local IP address to the client.
Assign IP Address	Enter the IP address for the client. Ensure that the IP address is configured to be allowed on the L2TP server.
Idle Timeout	Enter the time in minutes to timeout L2TP connections.

5.1.1.2 PPP

This screen displays second when you add a new L2TP client WAN service.

Figure 32 L2TP Client Add: PPP



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

☑ Enable NAT

□ Enable Fullcone NAT

ONLY IF REQUIRED -- DISABLES NETWORK ACCELERATION AND SOME SECURITY

☑ Use Static IPv4 Address

IPv4 Address: 0.0.0.0

□ Enable PPP Debug Mode

IGMP Multicast Proxy

☑ Enable IGMP Multicast Proxy

☑ Enable IGMP Multicast Source

□ No Multicast VLAN Filter

This screen contains the following fields:

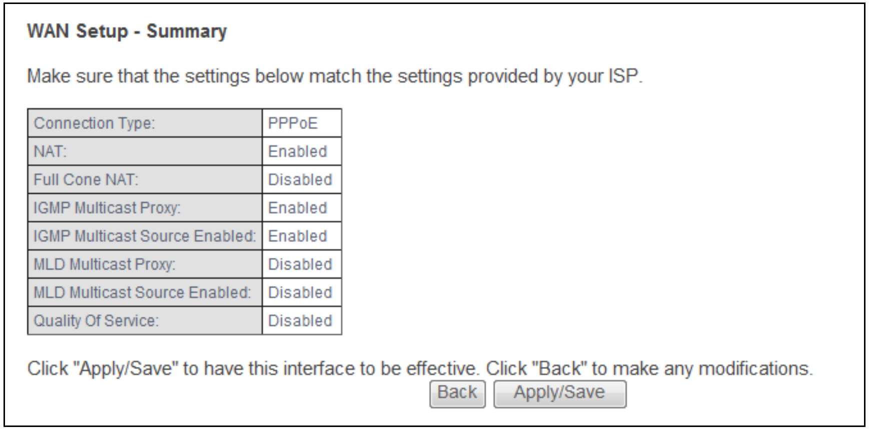
Table 30 L2TP Client Add: PPP

LABEL	DESCRIPTION
PPP Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection.
Authentication Method	The Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your Router accepts either CHAP or PAP when requested by this remote node. **PAP** - Your Router accepts PAP only. **CHAP** - Your Router accepts CHAP only. **MSCHAP** - Your Router accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Enable NAT	Select this check box to activate NAT on this connection.
Enable Fullcone NAT	This field is available only when you select **Enable NAT**. Select this check box to activate full cone NAT on this connection.
Tunnel Name	Enter the name for this client connection.
Use Static IPv4 Address	Select this option if you have a fixed IPv4 address assigned by your ISP.
IPv4 Address	Enter the IPv4 address assigned by your ISP.
Enable PPP Debug Mode	Select this option to display PPP debugging messages on the console.
Enable IGMP Multicast Proxy	Select this check box to have the Router act as an IGMP proxy on this connection. This allows the Router to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Enable IGMP Multicast Source	Select this check box to have the Router add routing table entries based on the IGMP traffic.
No Multicast VLAN Filter	Select this check box to have the Router not filter multicast traffic based on its VLAN.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.1.1.3 L2TP Client Add: Configuration Summary

This read-only screen shows the current L2TP WAN connection settings.

Figure 33 L2TP Client Add: Configuration Summary



WAN Setup - Summary

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

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
IGMP Multicast Proxy:	Enabled
IGMP Multicast Source Enabled:	Enabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Table 31 L2TP Client Add: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
NAT	This shows whether NAT is active or not for this connection.
Full Cone NAT	This shows whether full cone NAT is active or not for this connection.
IGMP Multicast Proxy	This shows whether IGMP proxy is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
IGMP Multicast Source Enabled	This shows whether IGMP source enable is activated or not for this connection. IGMP source enable has the Router add routing table entries based on the IGMP traffic.
MLD Multicast Proxy	This shows whether MLD proxy is activated or not for this connection.
MLD Multicast Source Enabled	This shows whether MLD source enable is activated or not for this connection. MLD source enable has the Router add routing table entries based on the MLD traffic.
Quality Of Service	This shows whether QoS is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

Network Address Translation (NAT)

6 Chapter

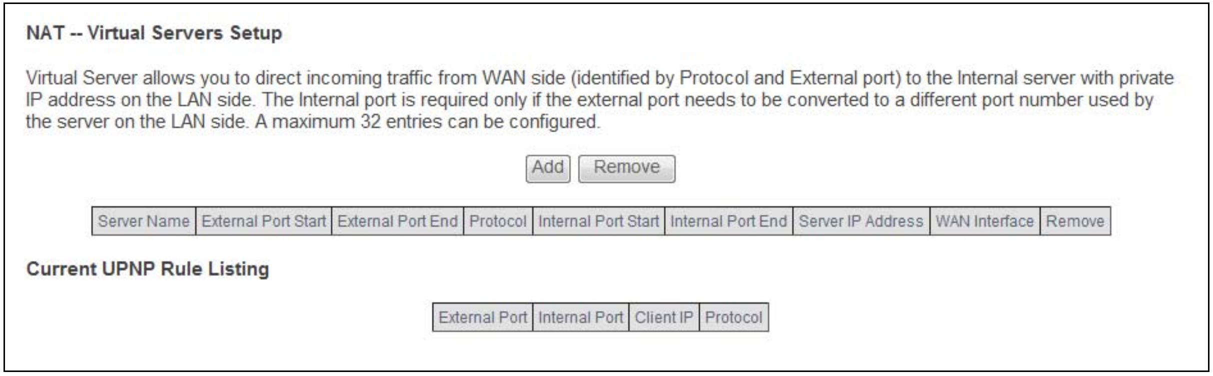
6.1 Virtual Servers

Click **Advanced Setup > NAT > Virtual Servers** to open the screen where you manage the list of virtual server rules.

A virtual server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Figure 34 Virtual Servers



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	WAN Interface	Remove

Current UPNP Rule Listing

External Port	Internal Port	Client IP	Protocol

Table 32 Virtual Servers

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
Remove	Select entries and click the **Remove** button to delete them.

Table 32 Virtual Servers (continued)

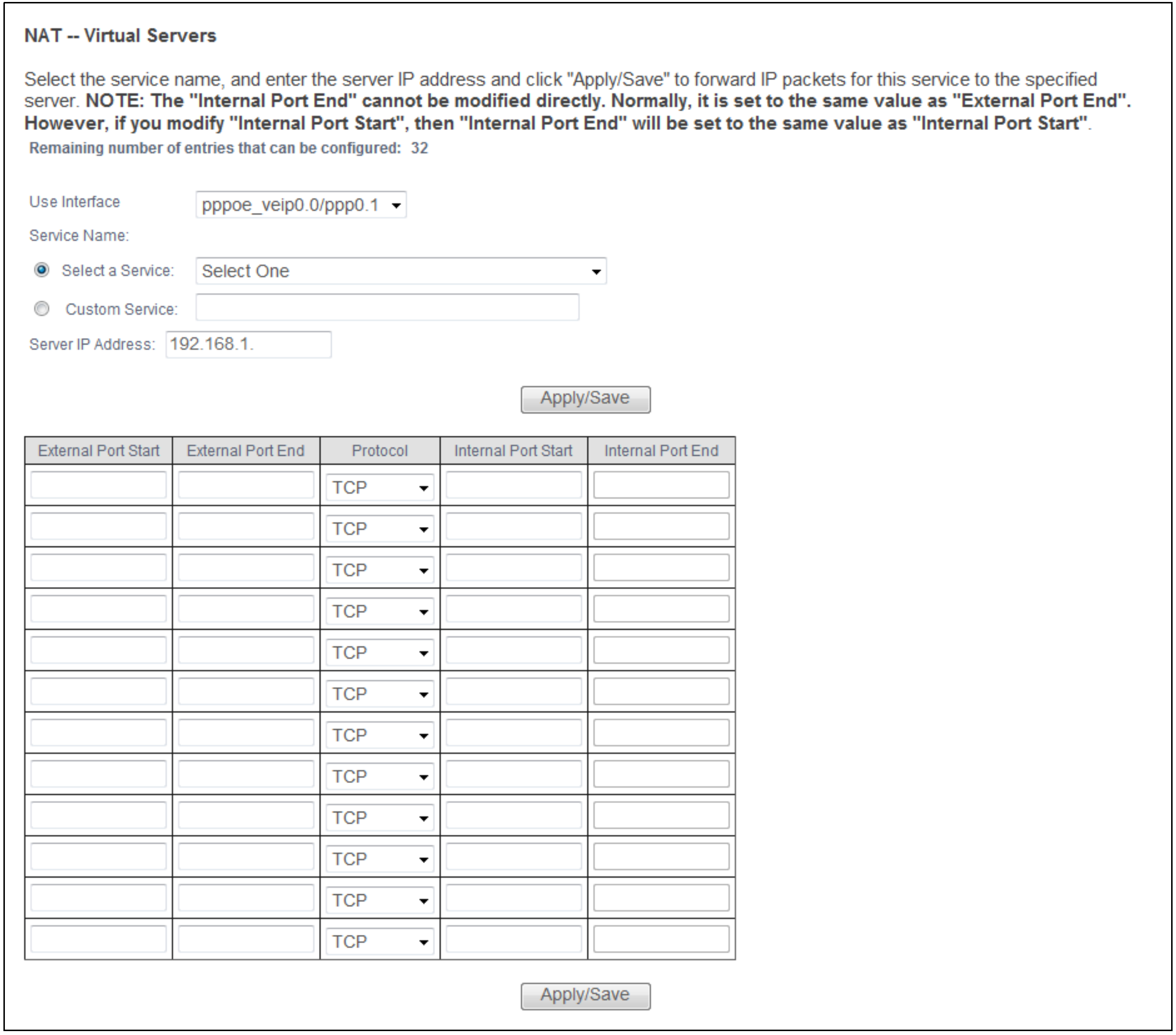
LABEL	DESCRIPTION
Server Name	This field displays the name of the service used by the packets for this virtual server.
External Port Start	This is the first external port number that identifies a service.
External Port End	This is the last external port number that identifies a service.
Protocol	This show whether the virtual server applies to TCP traffic, UDP traffic, or both.
Internal Port Start	This is the first internal port number that identifies a service.
Internal Port End	This is the last internal port number that identifies a service.
Server IP Address	This field displays the inside IP address of the server.
WAN Interface	This field displays the WAN interface through which the service is forwarded.
Current UPNP Rule Listing	Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. These are the rules the Router has created using UPnP.
External Port	This is the external port number that identifies a service.
Internal	This is the internal port number that identifies a service.
Client IP	This is the IP address of the device for which the Router created the UPnP rule.
Protocol	This is the protocol of the traffic for which the Router created the UPnP rule.

6.1.1 Virtual Servers Add

This screen lets you create or edit a virtual server rule. Click **Add** in the **Virtual Servers** screen to open the following screen.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Figure 35 Virtual Servers Add



NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".**

Remaining number of entries that can be configured: 32

Use Interface: pppoe_veip0.0/ppp0.1

Service Name:

● Select a Service: Select One

○ Custom Service:

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		

Table 33 Virtual Servers Add

LABEL	DESCRIPTION
Use Interface	Select a WAN interface for which you want to configure a virtual server rules.
Service Name	**Select a Service**: use the drop-down list to select a service. **Custom Service**: type a name to specify a different service.
Server IP Address	Enter the inside IP address of the LAN device to which the virtual server forwards traffic.
Apply/Save	Click this button to save your changes.
External Port Start	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
External Port End	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Internal Port Start	Enter the port number here to which you want the Router to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal Port End	Enter the last port of the translated port range.
Apply/Save	Click this button to save your changes.

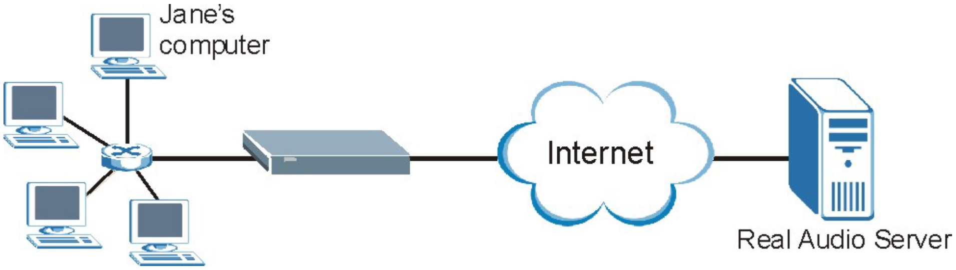
6.2 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Router records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Router's WAN port receives a response with a specific port number and protocol ("open" port), the Router forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

Figure 36 Trigger Port Forwarding Process: Example



1 Jane requests a file from the Real Audio server (port 7070).

2 Port 7070 is a "trigger" port and causes the Router to record Jane's computer IP address. The Router associates Jane's computer IP address with the "open" port range of 6970-7170.

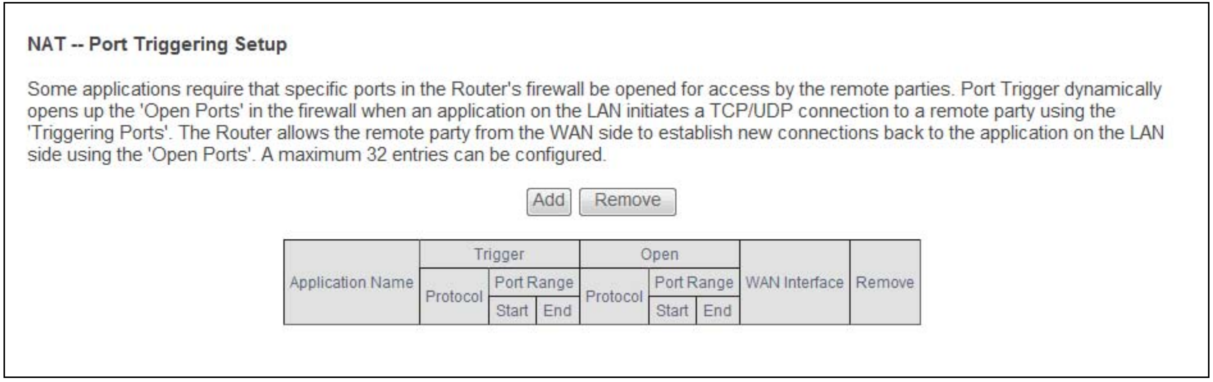
3 The Real Audio server responds using a port number ranging between 6970-7170.

4 The Router forwards the traffic to Jane's computer IP address.

5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Router times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Click **Advanced Setup > NAT > Port Triggering** to manage your Router's trigger port settings.

Figure 37 Port Triggering



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 Name	Trigger			Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range			
		Start	End		Start	End		

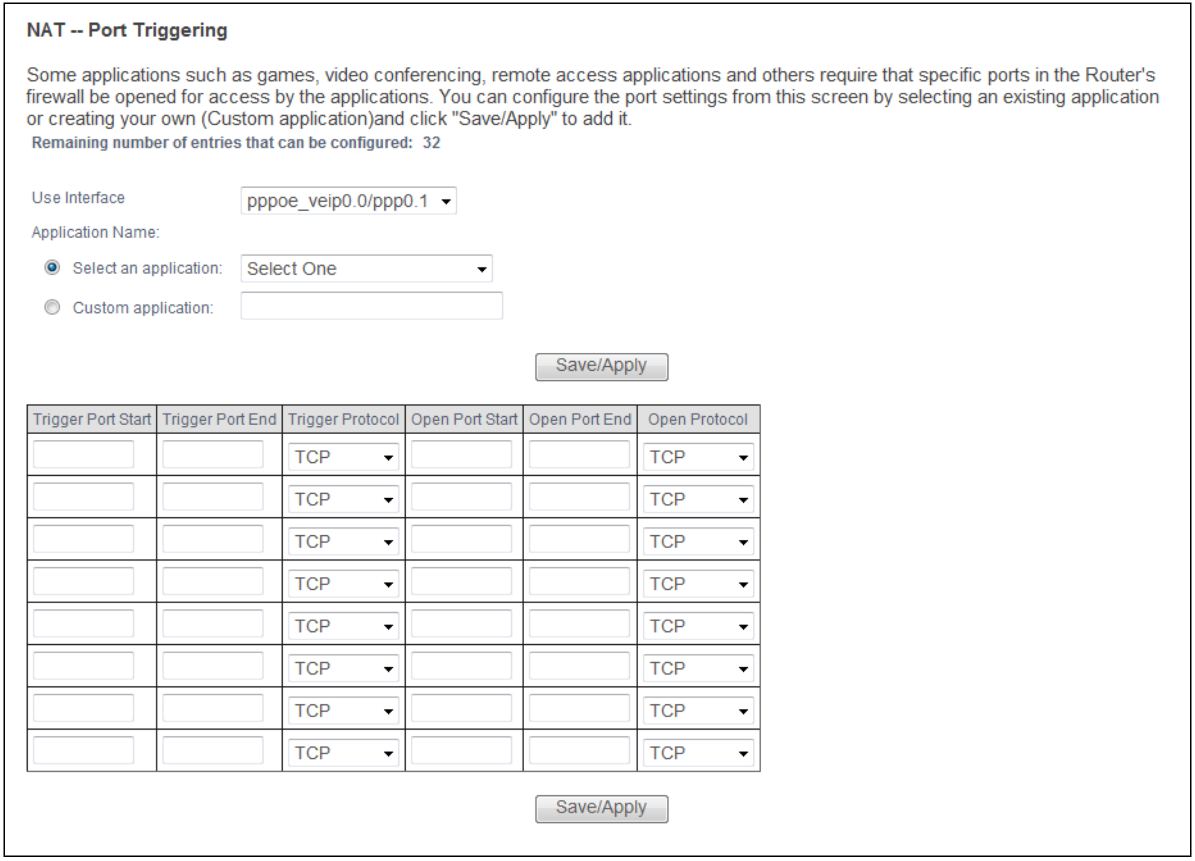
Table 34 Port Triggering

LABEL	DESCRIPTION
Add	Click this to create a new rule.
Remove	Select entries and click the **Remove** button to delete them.
#	This is the index number of the entry.
Status	This field displays whether the port triggering rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Application Name	This field displays the name of the service used by this rule.
Trigger Protocol	This is the trigger transport layer protocol.
Trigger Port Range Start	The trigger port is a port (or a range of ports) that causes (or triggers) the Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN. This is the first port number that identifies a service.
Trigger Port Range End	This is the last port number that identifies a service.
Open Protocol	This is the open transport layer protocol.
Open Port Range Start	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. This is the first port number that identifies a service.
Open Port Range End	This is the last port number that identifies a service.
WAN Interface	This field shows the WAN interface through which the service is forwarded.

6.2.1 Add Port Triggering Rule

This screen lets you create new port triggering rules. Click **Add** in the **Port Triggering** screen to open the following screen.

Figure 38 Port Triggering: Add



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

Use Interface: pppoe_veip0.0/ppp0.1

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

Table 35 Port Triggering: Add

LABEL	DESCRIPTION
User Interface	Select a WAN interface for which you want to configure port triggering rules.
Application Name	Choose an application from the drop-down list or select **Custom application** and enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
Save/Apply	Click this button to save your changes.
Trigger Port Start	The trigger port is a port (or a range of ports) that causes (or triggers) the Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN. Type a port number or the starting port number in a range of port numbers.

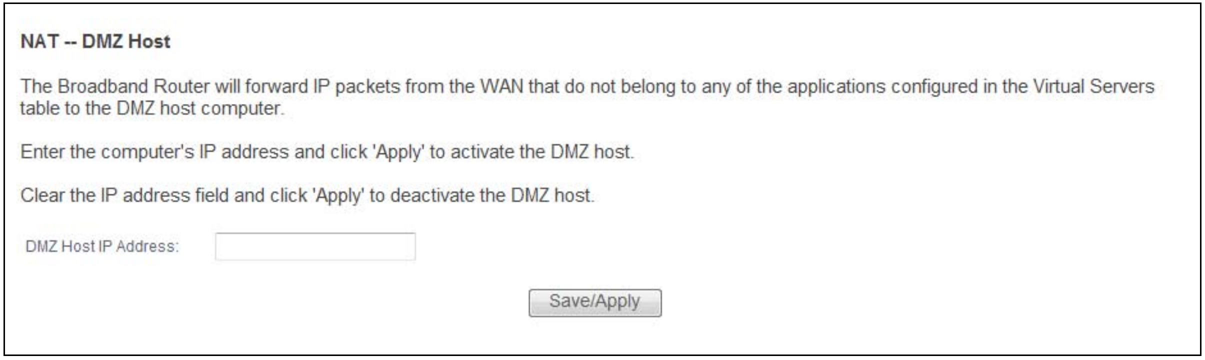
Table 35 Port Triggering: Add (continued)

LABEL	DESCRIPTION
Trigger Port End	Type a port number or the ending port number in a range of port numbers.
Trigger Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Open Port Start	The open port is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. Type a port number or the starting port number in a range of port numbers.
Open Port End	Type a port number or the ending port number in a range of port numbers.
Open Protocol	Select the transport layer protocol from **TCP**, **UDP**, or **TCP/UDP**.
Save/Apply	Click this button to save your changes.

6.3 DMZ Host

Click **Advanced Setup > NAT > DMZ Host** to specify the IP address of a default server to receive packets from ports not specified in the **Port Forwarding** screen.

Figure 39 DMZ Host



NAT -- DMZ Host

The Broadband 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:

Table 36 DMZ Host

LABEL	DESCRIPTION
DMZ Host IP Address	Enter the IP address which receives packets from ports that are not specified in the **Port Forwarding** screen. Note: If you do not assign a default server, the Router discards all packets received for ports not specified in the virtual server configuration.
Save/Apply	Click this button to save your changes.

6.4 SIP ALG

Click **Advanced Setup > NAT > SIP ALG** to enable and disable the NAT Application Layer Gateway (ALG) in the Router.

The SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Router registers with the SIP register server, the SIP ALG translates the Router's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Figure 40 SIP ALG

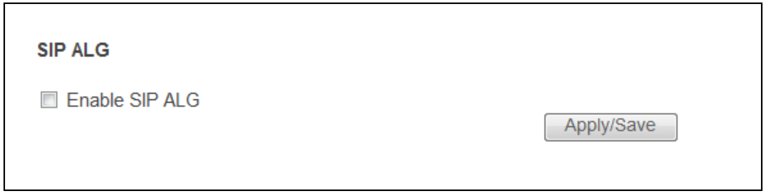


Table 37 SIP ALG

LABEL	DESCRIPTION
Enable SIP ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding.
Apply/Save	Click this button to save your changes.

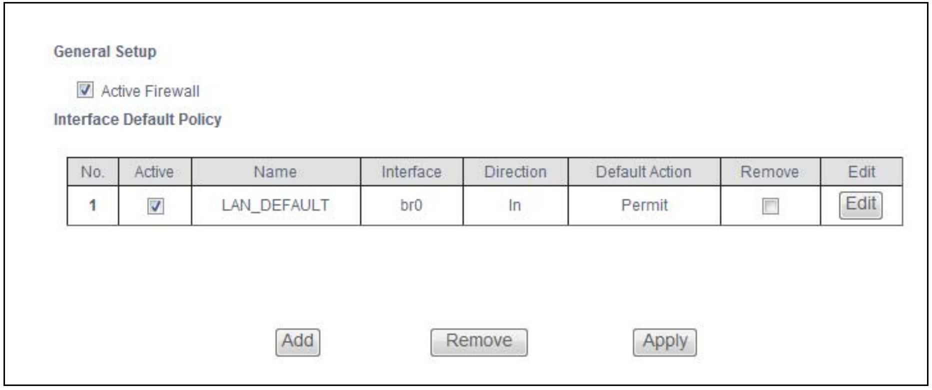
Firewall

Chapter 7

7.1 Firewall General

Use this screen to enable or disable the firewall and manage the default policies (filters). Click **Advanced Setup > Firewall** to open the **General** screen.

Figure 41 Firewall General



General Setup

☑ Active Firewall

Interface Default Policy

No.	Active	Name	Interface	Direction	Default Action	Remove	Edit
1	☑	LAN_DEFAULT	br0	In	Permit	□	Edit

Table 38 Firewall General

LABEL	DESCRIPTION
Active Firewall	Select this check box to activate the firewall. The Router performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. By default the firewall allows traffic from all interfaces to go to all interfaces. Configure firewall interface default policies to block specific traffic directions or firewall rules to block specific traffic.
No.	This displays the index number of the default firewall policy.
Active	This field displays whether a policy is turned on or not. Select the check box to enable the policy. Clear the check box to disable the policy.
Name	This displays the name of the policy.
Interface	This displays the LAN or WAN interface(s) to which this policy is applied.
Direction	This displays the direction of travel of packets (**In** and **Out**). Firewall rules are grouped based on the direction of travel of packets to which they apply.

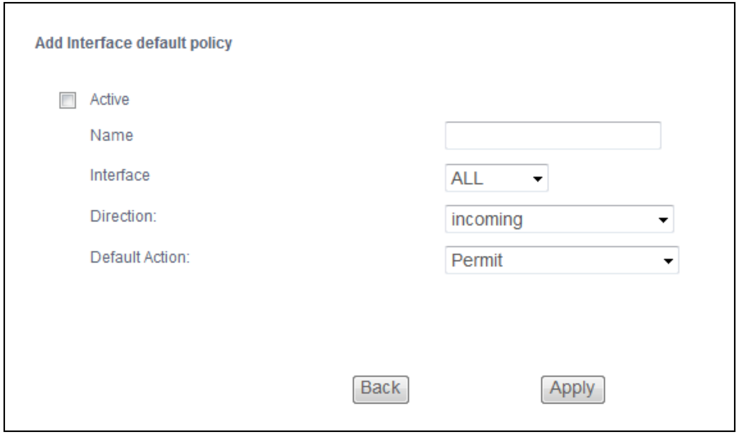
Table 38   Firewall General (continued)

LABEL	DESCRIPTION
Default Action	This displays the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. **Drop**: the Router silently discards the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender. **Permit**: the Router allows the passage of the packets.
Remove	Select entries and click the **Remove** button to delete them.
Edit	Click the **Edit** button to go to the screen where you can edit the rule.
Add	Click **Add** to create a new policy.
Apply	Click **Apply** to save your changes back to the Router.

7.1.1 Default Policy Configuration

In the **Firewall General** screen, click **Add** or click an entry's **Edit** icon to configure a firewall policy.

Figure 42 Default Policy



Add Interface default policy

□ Active	
Name	
Interface	ALL
Direction:	incoming
Default Action:	Permit

Table 39   Default Policy

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Name	Enter a descriptive name using printable English keyboard characters.
Interface	Select **All** to apply the policy to all interfaces on the Router or select the specific LAN or WAN interface to which this policy applies.
Direction	Specify the direction of travel of packets (**incoming** or **outgoing**) in this policy.

Table 39 Default Policy (continued)

LABEL	DESCRIPTION
Default Action	Specify whether the firewall silently discards packets (**Drop**) or allows the passage of packets (**Permit**).
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

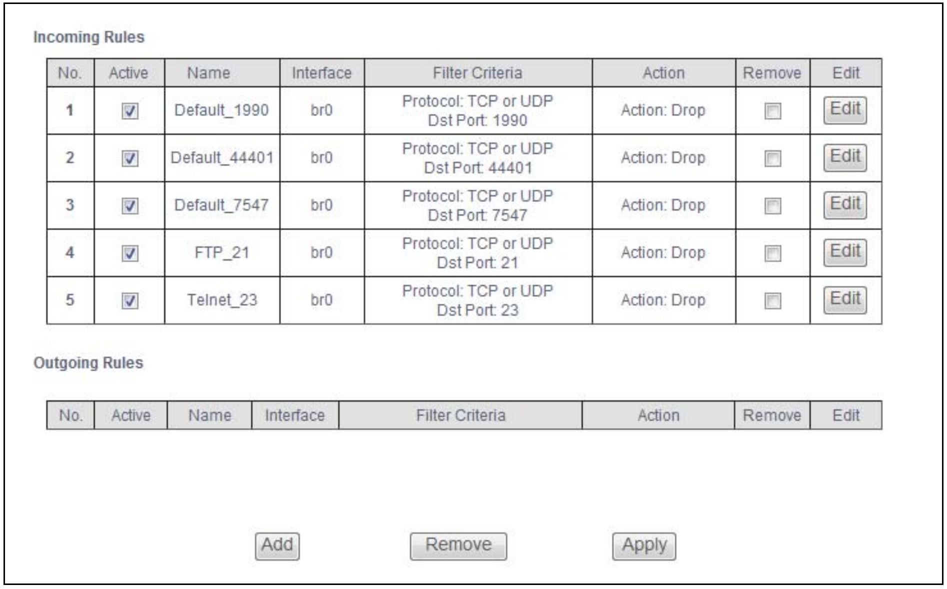
7.2 Firewall Rules

The ordering of your rules is very important as rules are applied in turn.

Click **Advanced Setup > Firewall > Rules** to display the following screen. This screen lists the configured incoming or outgoing firewall rules. Note the order in which the rules are listed.

The firewall rules that you configure here take priority over the general firewall action settings in the **General** screen.

Figure 43 Firewall Rules



Incoming Rules

No.	Active	Name	Interface	Filter Criteria	Action	Remove	Edit
1	☑	Default_1990	br0	Protocol: TCP or UDP Dst Port: 1990	Action: Drop	□	Edit
2	☑	Default_44401	br0	Protocol: TCP or UDP Dst Port: 44401	Action: Drop	□	Edit
3	☑	Default_7547	br0	Protocol: TCP or UDP Dst Port: 7547	Action: Drop	□	Edit
4	☑	FTP_21	br0	Protocol: TCP or UDP Dst Port: 21	Action: Drop	□	Edit
5	☑	Telnet_23	br0	Protocol: TCP or UDP Dst Port: 23	Action: Drop	□	Edit

Outgoing Rules

No.	Active	Name	Interface	Filter Criteria	Action	Remove	Edit

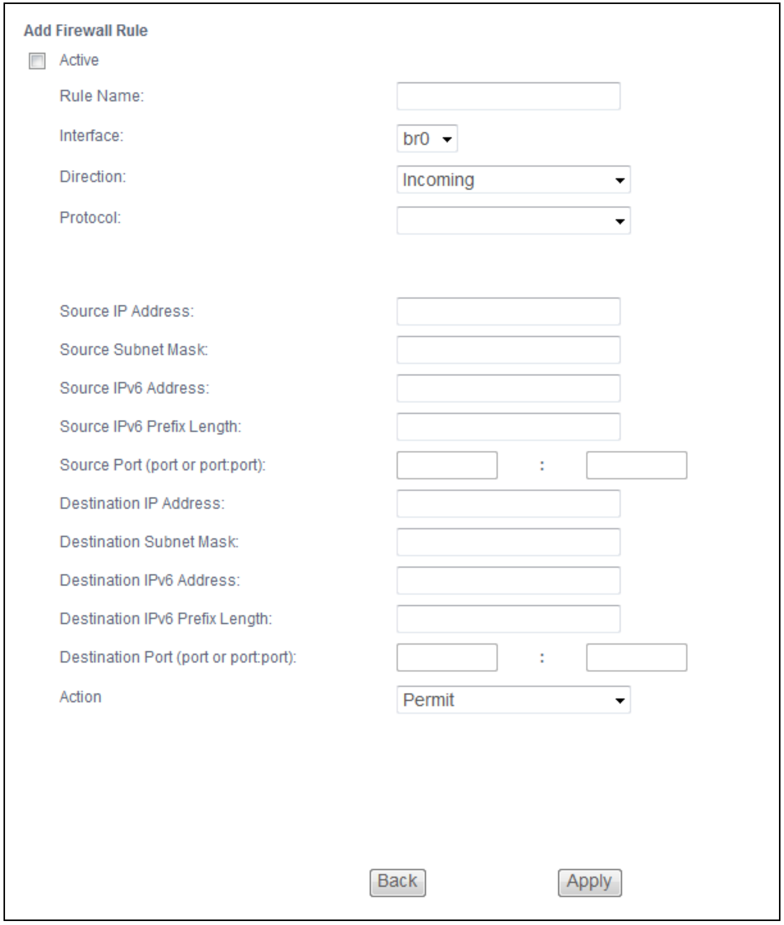
Table 40 Firewall Rules

LABEL	DESCRIPTION
Incoming/ Outgoing Rules	The following fields summarize the rules you have created that apply to traffic traveling in the selected packet direction.
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This field displays whether a firewall rule is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Name	This displays the name of the rule.
Interface	This displays the LAN or WAN interface(s) to which this rule is applied.
Filter Criteria	This displays the filtering criteria, such as the source or destination IP addresses and subnet mask to which this rule applies.
Action	This displays whether the firewall silently discards packets (**Drop**), discards packets and sends an ICMP message to the sender (**Reject**) or allows the passage of packets (**Permit**).
Remove	Select entries and click the **Remove** button to delete them.
Edit	Click the **Edit** button to go to the screen where you can edit the rule.
Add	Click **Add** to create a new rule.
Apply	Click **Apply** to save your changes back to the Router.

7.2.1 Firewall Rules Configuration

In the **Firewall Rules** screen, click **Add** or click a rule's **Edit** button to display this screen and refer to the following table for information on the labels.

Figure 44 Firewall Rules: Add



Add Firewall Rule

□ Active

Rule Name:	
Interface:	br0
Direction:	Incoming
Protocol:	
Source IP Address:	
Source Subnet Mask:	
Source IPv6 Address:	
Source IPv6 Prefix Length:	
Source Port (port or port:port):	:
Destination IP Address:	
Destination Subnet Mask:	
Destination IPv6 Address:	
Destination IPv6 Prefix Length:	
Destination Port (port or port:port):	:
Action	Permit

Table 41 Firewall Rules: Add

LABEL	DESCRIPTION
Active	Select this check box to enable the rule.
Rule Name	Enter a descriptive name of up to 16 printable English keyboard characters, including spaces. To add a firewall rule, you need to configure at least one of the following fields (except the **Interface** field).
Interface	Select an interface on the Router to which this rule applies.

Table 41 Firewall Rules: Add (continued)

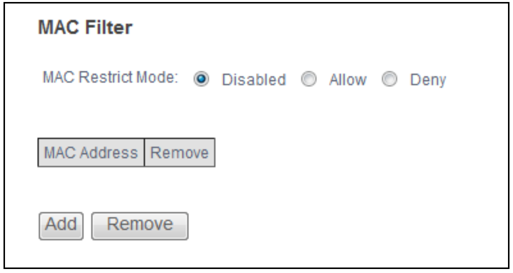
LABEL	DESCRIPTION
Direction	Select a direction of travel of packets for which you want to configure the firewall rule.
Protocol	Select the IP protocol (**TCP**, **UDP** or **ICMP**) and enter the protocol (service type) number in the port field.
Source IP Address	Enter the source IP address in dotted decimal notation.
Source Subnet Mask	Enter the source subnet mask.
Source IPv6 Address	Enter the source IPv6 address in dotted decimal notation.
Source IPv6 Prefix Length	Enter the IPv6 prefix length for the source IPv6 address. The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Source Port	Enter the single port number or the range of port numbers of the source.
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask.
Destination IPv6 Address	Enter the destination IPv6 address in dotted decimal notation.
Destination IPv6 Prefix Length	Enter the IPv6 prefix length for the destination IPv6 address. The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address. This field displays the bit number of the IPv6 subnet mask.
Destination Port	Enter the single port number or the range of port numbers of the destination.
Action	Use the drop-down list box to select whether to discard (**Drop**), deny and send an ICMP message to the sender of (**Reject**) or allow the passage of (**Permit**) packets that match this rule.
Reject Type	If you select **Reject**, specify the type of ICMP message to send to the sender.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.

7.3 MAC Filtering

Click **Advanced Setup > Firewall > MAC Filtering** to allow or block wireless and LAN clients access to the Router.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

Figure 45 MAC Filtering



MAC Filter

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

The following table describes the labels in this menu.

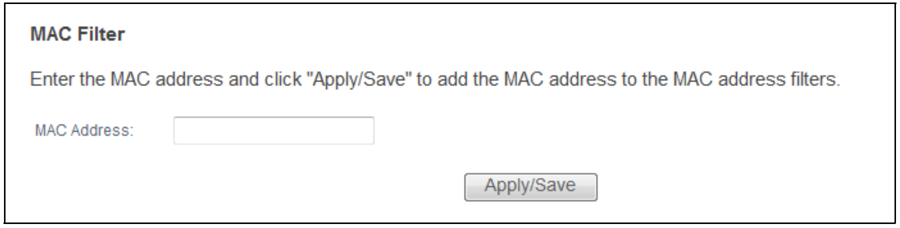
Table 42 MAC Filtering

LABEL	DESCRIPTION
MAC Restrict Mode	Select **Disabled** to turn off MAC address filtering. Select **Allow** to have the Router permit access from the listed wireless and LAN client MAC addresses and block access from MAC addresses not in the list. Select **Deny** to have the Router block access from the listed wireless and LAN client MAC addresses and allow access from MAC addresses not in the list.
MAC Address	These are the MAC addresses of LAN devices. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3.1 MAC Filtering Add

Click **Advanced Setup > Firewall > MAC Filtering > Add** to add a MAC address to the **MAC Filtering** screen’s list of wireless and LAN clients access to the Router.

Figure 46 MAC Filtering Add



MAC Filter

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

MAC Address:

The following table describes the labels in this menu.

Table 43 MAC Filtering Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply/Save	Click this button to save your changes.

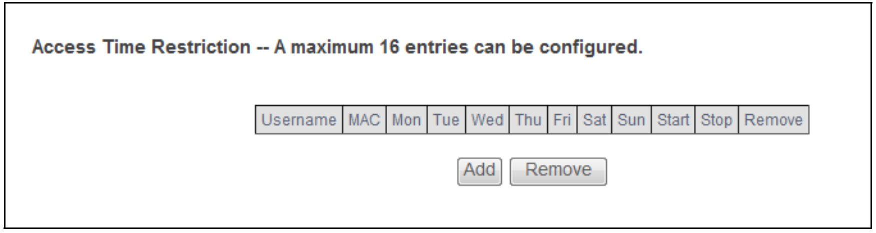
Parental Control

Chapter 8

8.1 Time Restriction

Click **Advanced Setup > Parental Control > Time Restriction** to configure access time schedules for specific users.

Figure 47 Time Restriction



Access Time Restriction -- A maximum 16 entries can be configured.

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

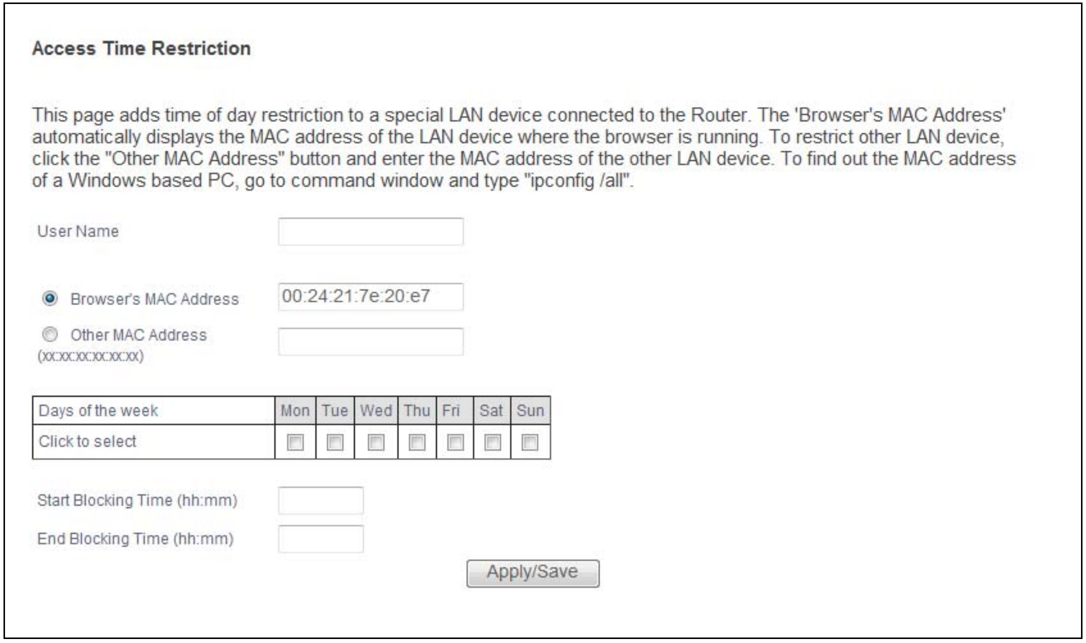
Table 44 Time Restriction

LABEL	DESCRIPTION
Username	This is the name of the user whose access the rule controls.
MAC	This is the MAC address of the LAN or wireless device whose access the rule controls.
Mon ~ Sun	This shows an “x” for every day of the week the schedule applies to.
Start	This shows the beginning of the access blocking time.
Stop	This shows the end of the access blocking time.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to add a new entry.

8.1.1 Add a Time Restriction Rule

Click **Add** in the **Time Restriction** screen to add a new rule. Use this screen to configure a restricted access schedule.

Figure 48 Time Restriction: Add



Access Time 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 00:24:21:7e:20:e7

○ 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)

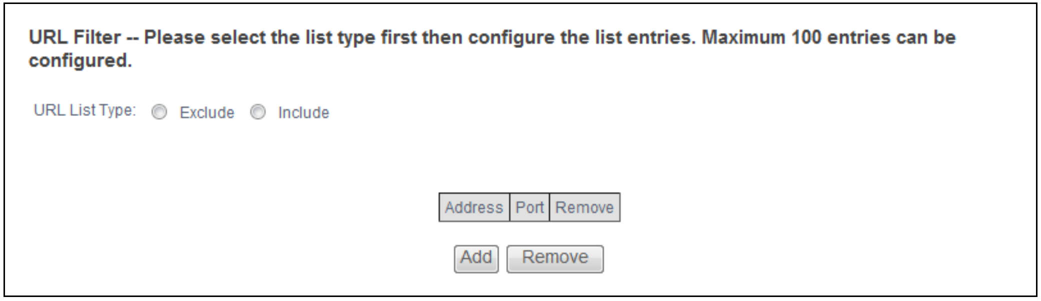
Table 45 Time Restriction: Add

LABEL	DESCRIPTION
Username	Specify the name of the user whose access the rule controls.
Browser's MAC Address	Select this to create the rule for the MAC address of the device with the browser you are using to configure the Router. 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. This is the MAC address of the LAN or wireless device whose access the rule controls.
Other MAC Address	Select this and enter the MAC address of another LAN device. To find out the MAC address of a Windows based PC, go to the command window and type "ipconfig / all".
Days of the week	Select check boxes for the days that you want the Router to perform parental control.
Start Blocking Time	Enter the time in 24-hour format to begin blocking access.
End Blocking Time	Enter the time in 24-hour format to stop blocking access.
Apply/Save	Click this button to save your changes.

8.2 URL Filter

Click **Advanced Setup > Parental Control > Url Filter** to use the **Url Filter** screen to block or allow access to specific web sites.

Figure 49 URL Filter



URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: ○ Exclude ○ Include

Address	Port	Remove

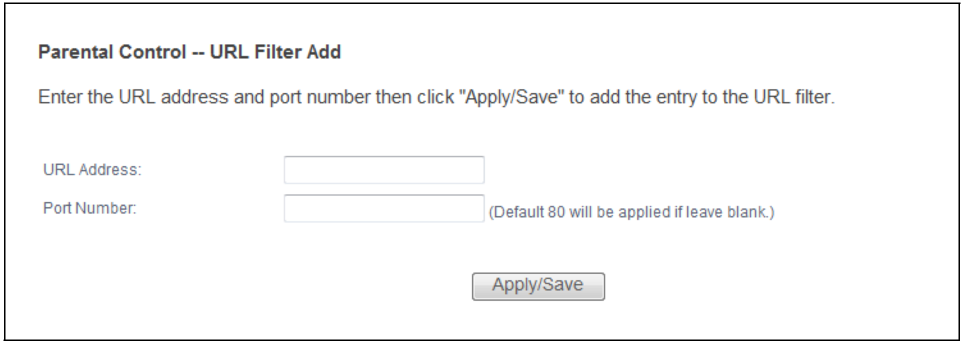
Table 46 URL Filter

LABEL	DESCRIPTION
URL List Type	Select **Exclude** to block access to the URLs in the list and allow access to other URLs. Select **Include** to allow access to the URLs in the list and block access to other URLs.
Address	This shows the website address (URL) to which the entry applies.
Port	This shows the port number for the URL list entry.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to add a new entry.

8.2.1 Add a URL Filter Rule

Click **Add** in the **URL Filter** screen to add a new entry. Use this screen to configure a URL filtering setting to control access to certain web sites.

Figure 50 URL Filter: Add



Parental Control -- URL Filter Add

Enter the URL address and port number then click "Apply/Save" to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Table 47 URL Filter: Add

LABEL	DESCRIPTION
URL Address	Specify a web site or URL to which to filter access.
Port Number	Specify the port number if you need to control access to one other than 80.
Apply/Save	Click this button to save your changes.

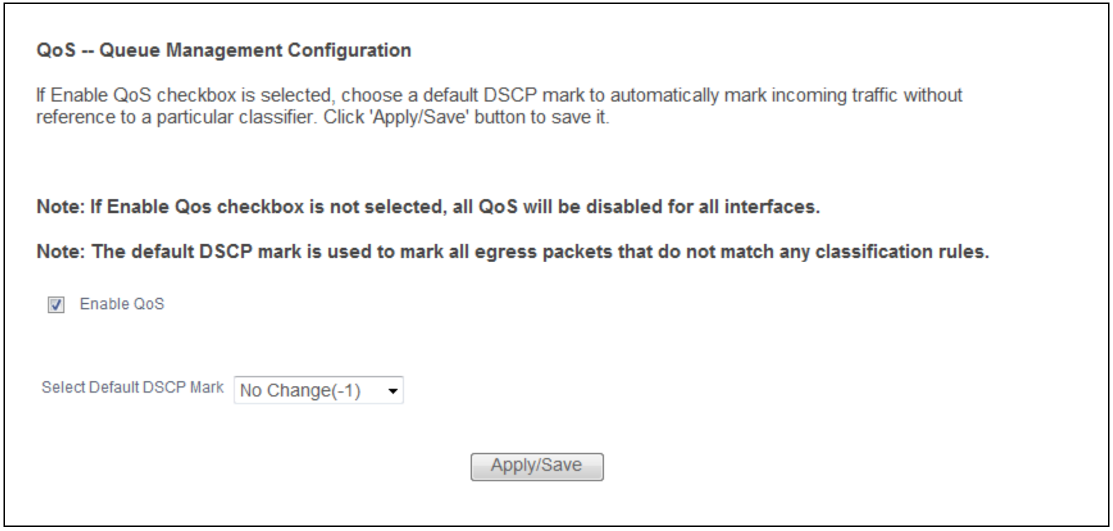
Quality of Service (QoS)

Chapter 9

9.1 QoS General

Click **Advanced Setup > Quality of Service** to enable or disable QoS, set the bandwidth, and select to have the Router automatically assign priority to upstream traffic according to the IP precedence or packet length.

Figure 51 QoS General



QoS -- Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

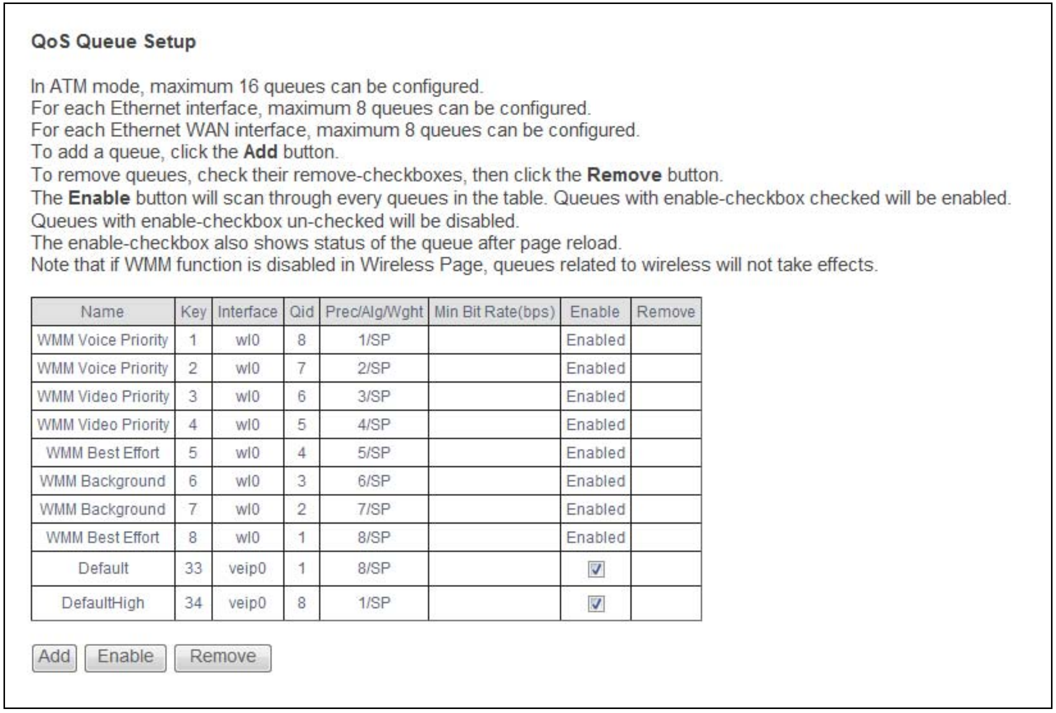
Table 48 QoS General

LABEL	DESCRIPTION
Enable QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the Router forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Select Default DSCP Mark	Set the default DSCP (DiffServ Code Point) value for outgoing packets that do not match any classification rules.
Apply/Save	Click this button to save your changes.

9.2 Queue Setup

Click **Advanced Setup > Quality of Service > Queue Setup** to use the **Queue Setup** screen to configure QoS queue assignment.

Figure 52 Queue Setup



QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
For each Ethernet interface, maximum 8 queues can be configured.
For each Ethernet WAN interface, maximum 8 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled.
Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
Note that if WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Min Bit Rate(bps)	Enable	Remove
WMM Voice Priority	1	wl0	8	1/SP		Enabled	
WMM Voice Priority	2	wl0	7	2/SP		Enabled	
WMM Video Priority	3	wl0	6	3/SP		Enabled	
WMM Video Priority	4	wl0	5	4/SP		Enabled	
WMM Best Effort	5	wl0	4	5/SP		Enabled	
WMM Background	6	wl0	3	6/SP		Enabled	
WMM Background	7	wl0	2	7/SP		Enabled	
WMM Best Effort	8	wl0	1	8/SP		Enabled	
Default	33	veip0	1	8/SP		☑	
DefaultHigh	34	veip0	8	1/SP		☑	

Table 49 Queue Setup

LABEL	DESCRIPTION
Name	This shows the descriptive name of this queue.
Key	This is the queue's index number.
Interface	This shows the name of the Router's interface through which traffic in this queue passes.
Qid	This shows the priority of this queue for the interface.
Prec/Alg/Wght	This displays the queue's default precedence, queue management algorithm, and weighted round robin weight. **SP** is strict priority.
Min Bit Rate (bps)	This shows the minimum transmission rate for traffic in this queue.
Enable	This shows whether the queue is active or not. For queues with a check box, select it and click the **Enable** button to turn them on. Clear the check box to turn a queue off.
Remove	Select entries and click the **Remove** button to delete them.

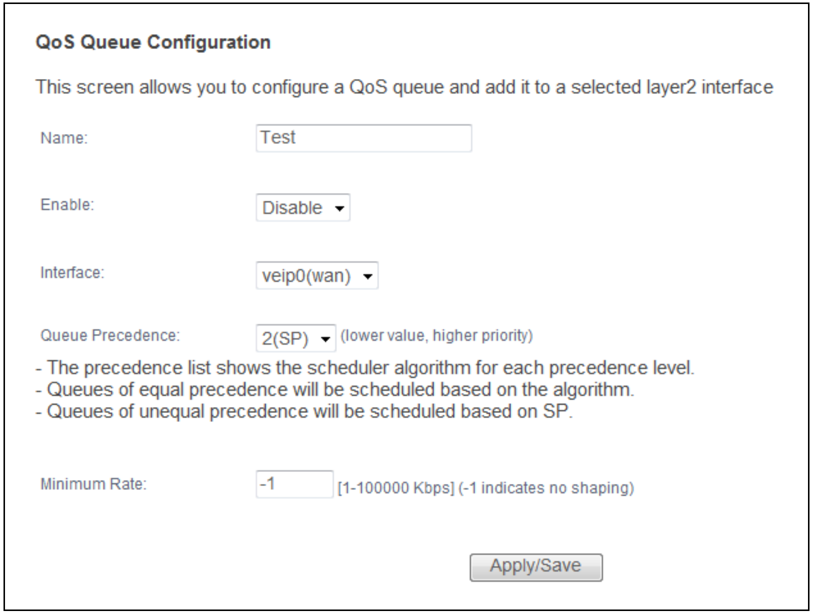
Table 49 Queue Setup (continued)

LABEL	DESCRIPTION
Add	Click **Add** to create a new queue.
Enable	Select disabled entries and click the **Enable** button to activate them.

9.2.1 Add a QoS Queue

Click the Add button in the QoS Queue screen to configure a new queue.

Figure 53 Queue Setup: Add



QoS Queue Configuration

This screen allows you to configure a QoS queue and add it to a selected layer2 interface

Name: Test

Enable: Disable

Interface: veip0(wan)

Queue Precedence: 2(SP) (lower value, higher priority)

- The precedence list shows the scheduler algorithm for each precedence level.
- Queues of equal precedence will be scheduled based on the algorithm.
- Queues of unequal precedence will be scheduled based on SP.

Minimum Rate: -1 [1-100000 Kbps] (-1 indicates no shaping)

Table 50 Queue Setup: Add

LABEL	DESCRIPTION
Name	Enter the descriptive name of this queue.
Enable	Select to enable or disable this queue.
Interface	Select the interface of this queue.

Table 50 Queue Setup: Add (continued)

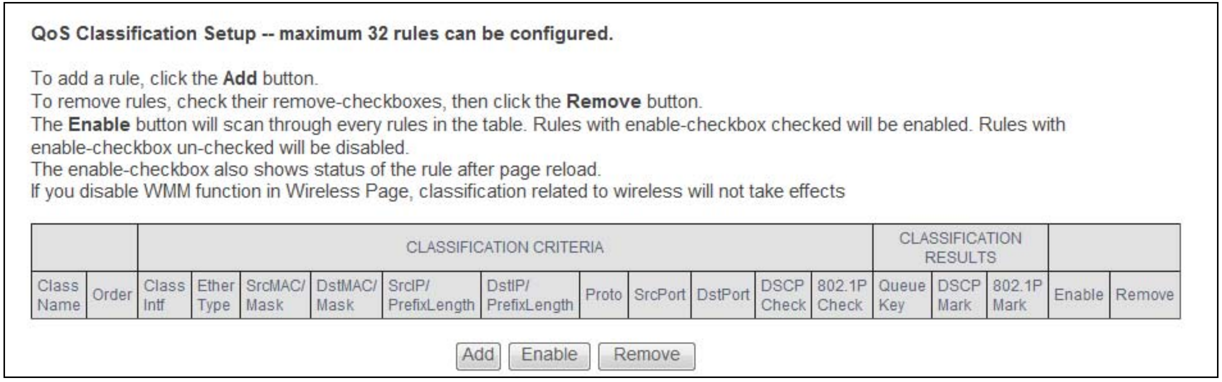
LABEL	DESCRIPTION
Queue Precedence	Select a queue precedence level (from 1 to 8) to configure for the selected interface. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested. If the queue precedence level already has a queue scheduler configured, it displays after the precedence level. The Router uses strict priority to service queues with different precedences.
Minimum Rate	This displays for GPON interface queues. Specify the minimum transmission rate (in **Kbps**) allowed for traffic on this queue.

9.3 Class Setup

Click **Advanced Setup > Quality of Service > Class Setup** to configure QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface.

You can give different priorities to traffic that the Router forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Figure 54 QoS Classification Setup



QoS Classification Setup -- maximum 32 rules can be configured.

To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the rule after page reload.
If you disable WMM function in Wireless Page, classification related to wireless will not take effects

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS				
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Enable	Remove

Table 51 QoS Classification Setup

LABEL	DESCRIPTION
Class Name	This displays the name of the classifier rule.
Order	This displays the rule’s place in the list of classifier rules. The Router checks traffic against classifiers in order until it matches one.

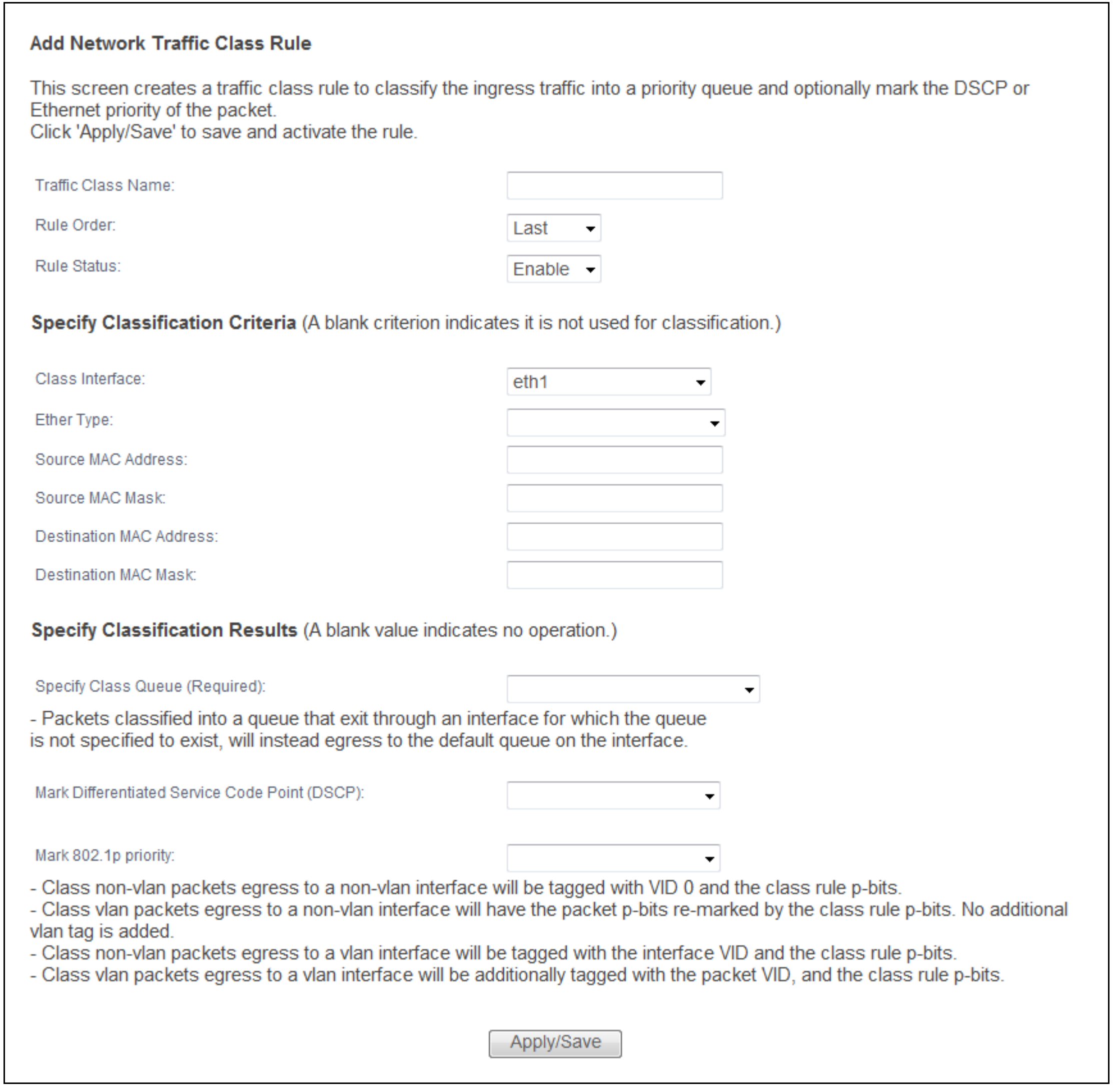
Table 51 QoS Classification Setup (continued)

LABEL	DESCRIPTION
CLASSIFICATION CRITERIA	These fields show the criteria specified in the classifier rule. For example the interface from which traffic of this class comes and the source MAC address of traffic that matches this classifier.
Class Intf	This displays the ingress interface to which the classifier applies.
Ether Type	This displays the type of Ethernet frames to which the classifier applies.
SrcMAC/ Mask	This displays the source MAC and network mask of traffic to which the classifier applies.
DstMAC/ Mask	This displays the destination MAC and network mask of traffic to which the classifier applies.
SrcIP/ PrefixLength	This displays the source IP address and prefix length of traffic to which the classifier applies.
DstIP/ PrefixLength	This displays the destination IP address and prefix length of traffic to which the classifier applies.
Proto	This displays the protocol of traffic to which the classifier applies.
SrcPort	This displays the source port of traffic to which the classifier applies.
DstPort	This displays the destination port of traffic to which the classifier applies.
DSCP Check	This displays the DSCP mark of traffic to which the classifier applies.
802.1P Check	This displays the IEEE 802.1p priority level of traffic to which the classifier applies.
CLASSIFICATION RESULTS	These fields show the changes the classifier rule applies to matching traffic.
Queue Key	This displays the number of the queue to which the Router adds traffic that matches this classifier.
DSCP Mark	This displays the DSCP mark the Router adds to traffic that matches this classifier.
802.1P Mark	This displays the IEEE 802.1p priority level the Router assigns to traffic that matches this classifier.
Enable	Select an entry’s **Enable** option and click the **Enable** button to turn it on.
Remove	Select an entry’s **Remove** option and click the **Remove** button to delete it.
Add	Click this button to create a new classifier rule.

9.3.1 Add QoS Class

Click **Add** in the **Class Setup** screen to configure a new classifier.

Figure 55 Add QoS Class



Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.
Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:	
Rule Order:	Last
Rule Status:	Enable

Specify Classification Criteria (A blank criterion indicates it is not used for classification.)

Class Interface:	eth1
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

Specify Classification Results (A blank value indicates no operation.)

Specify Class Queue (Required):

- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Table 52 Add QoS Class

LABEL	DESCRIPTION
Traffic Class Name	Enter a descriptive name of up to 15 printable English keyboard characters, not including spaces.
Rule Order	Select this classifier’s place in the list of classifiers. Select **Last** to put this rule in the back of the classifier list.
Rule Status	Turn this classifier on or off.

Table 52 Add QoS Class (continued)

LABEL	DESCRIPTION
Specify Classification Criteria	Configure these fields to identify the traffic to which the class applies. The fields available vary depending on the selected interface and Ether type. Leave a field blank to not apply that criterion.
Class Interface	Select the ingress interface to which the classifier applies.
Ether Type	Select the predefined application (IP, ARP, IPv6, PPPoE discovery, PPPoE session, 8865, 8866, or IEEE 802.1q) to which the classifier applies. The list of types available to choose from varies depending on the selected interface.
Source MAC Address	Enter a MAC address to apply the classifier to packets from that MAC address.
Source MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Destination MAC Address	Enter a MAC address to apply the classifier to packets destined for that MAC address.
Destination MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Source IP Address[/Mask]	Select this and enter an IP address to apply the classifier to packets from that IP address. You can also include a source subnet mask.
Vendor Class ID (DHCP Option 60)	Select this and enter the Vendor Class Identifier (Option 60) of the matched traffic, such as the type of the hardware or firmware.
User Class ID DHCP option 77	Select this and enter a string that identifies the user's category or application type in the matched DHCP packets.
Destination IP Address[/Mask]	Enter an IP address to apply the classifier to packets destined for that IP address. You can also include a destination subnet mask.
Differentiated Service Code Point (DSCP) Check	Select a DSCP mark of traffic to which to apply the classifier.
802.1p Priority Check	This field displays when you set the **Ether Type** field to **8021Q**. Select the IEEE 802.1p priority level (between 0 and 7) of traffic to which to apply the classifier. "0" is the lowest priority level and "7" is the highest.

Table 52 Add QoS Class (continued)

LABEL	DESCRIPTION
Specify Classification Results	Configure these fields to change traffic that matches the classifier. The fields available vary depending on the selected interface, Ether type, and sometimes on the selected class queue. Leave a field blank to not apply that type of change.
Specify Class Queue	Select the queue to which to add traffic that matches this classifier.
Mark Differentiated Service Code Point (DSCP):	Select the DSCP mark to add to traffic that matches this classifier. Use **Auto** marking to automatically apply a DSCP mark according to the type of traffic. Use **default** to leave the DSCP mark unchanged.
Mark 802.1p priority	Select the IEEE 802.1p priority level to assign to traffic that matches this classifier.
Set Rate Limit	Set the rate limit to apply to traffic that matches this classifier.
Apply/Save	Click this button to save your changes.

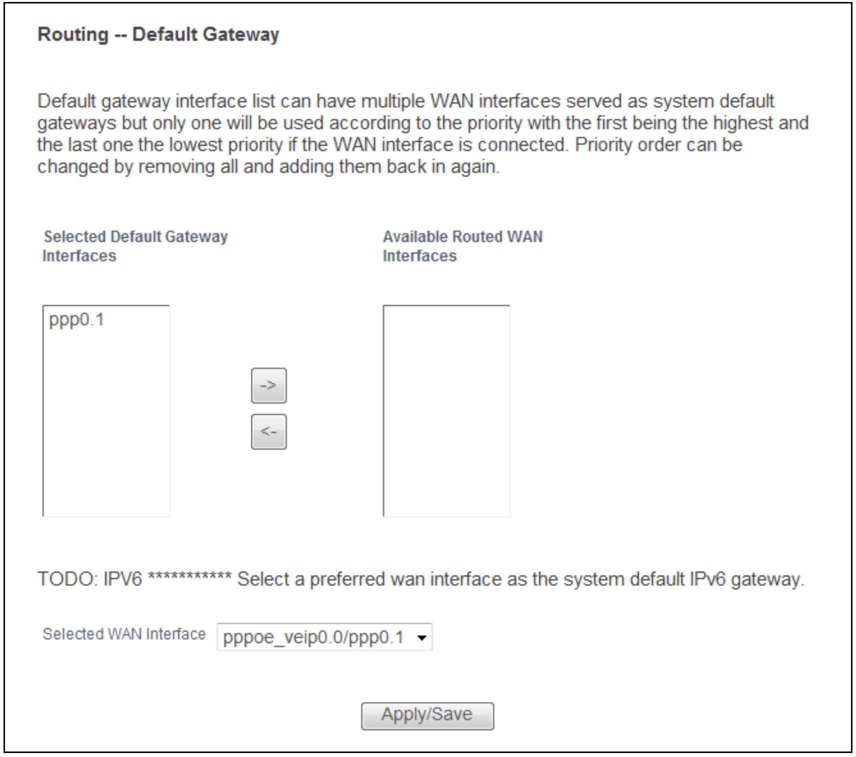
Routing

10 Chapter

10.1 Default Gateway

Click **Advanced Setup > Routing > Default Gateway** to open the **Default Gateway** screen. Use this screen to select WAN interfaces to serve as system default gateways.

Figure 56 Default Gateway



Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces: ppp0.1

Available Routed WAN Interfaces:

TODO: IPV6 *********** Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: pppoe_veip0.0/ppp0.1

Move the WAN interfaces to serve as system default gateways from **Available Routed WAN Interfaces** to **Selected Default Gateway Interfaces**.

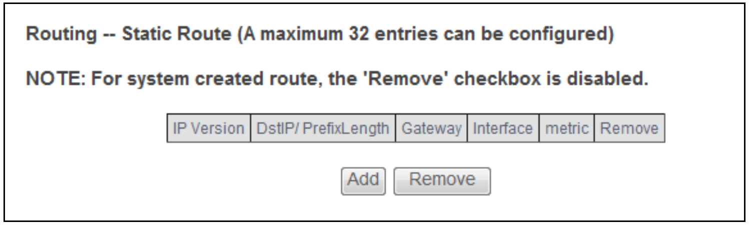
Use the **Selected WAN Interface** field to select the preferred WAN interface to server as the Router's default IPv6 gateway.

Click **Apply/Save** to save your changes.

10.2 Static Route

Click **Advanced Setup > Routing > Static Route** to view and configure the static route rules on the Router.

Figure 57 Static Route



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

NOTE: For system created route, the 'Remove' checkbox is disabled.

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

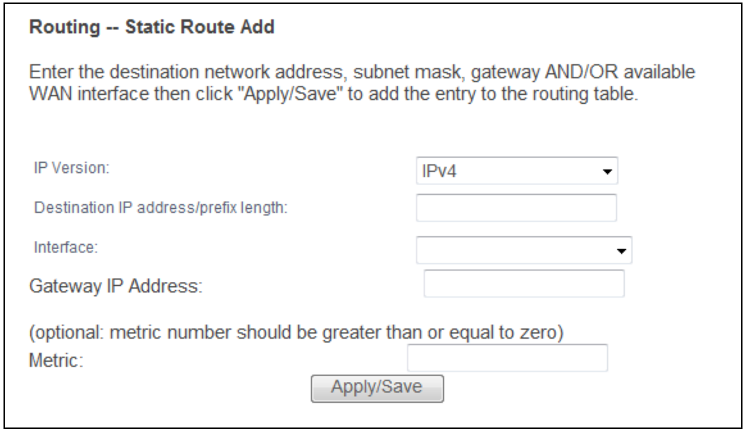
Table 53 Static Route

LABEL	DESCRIPTION
IP Version	This displays whether the entry uses IPv4 or IPv6.
DstIP/ PrefixLength	This specifies the IP network address and prefix length of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Interface	This is the interface this static route uses to forward traffic for the listed destination address.
metric	The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the number, the lower the "cost".
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to configure a new static route.

10.2.1 Add Static Route

Use this screen to add a static route. Click **Add** in the **Static Route** screen to display the following screen.

Figure 58 Static Route: Add



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

(optional: metric number should be greater than or equal to zero)

Metric:

Table 54 Static Route: Add

LABEL	DESCRIPTION
IP Version	Select whether your IP type is **IPv4** or **IPv6**.
Destination IP address/ prefix length	Enter the IPv4 or IPv6 address and network length of the final destination.
Interface	Select the interface through which this static route sends traffic.
Gateway IP Address	Enter the IP address of the gateway when you configure a static route that uses an IP-based interface (such as IPoE, IPoA, or LAN). The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Apply/Save	Click this button to save your changes.

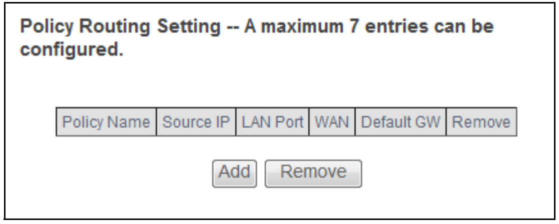
10.3 Policy Routing

Traditionally, routing is based on the destination address only and the Router takes the shortest path to forward a packet. Policy routing allows the Router to override the default routing behavior and alter the packet routing based on the policy defined by the network administrator. Policy-based routing is applied to outgoing packets, prior to the normal routing.

You can use source-based policy routing to direct traffic from different users through different connections or distribute traffic among multiple paths for load sharing.

Use the **Policy Routing** screen to view and configure routing policies on the Router. Click **Advanced Setup > Routing > Policy Routing** to open the following screen.

Figure 59 Policy Routing



Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

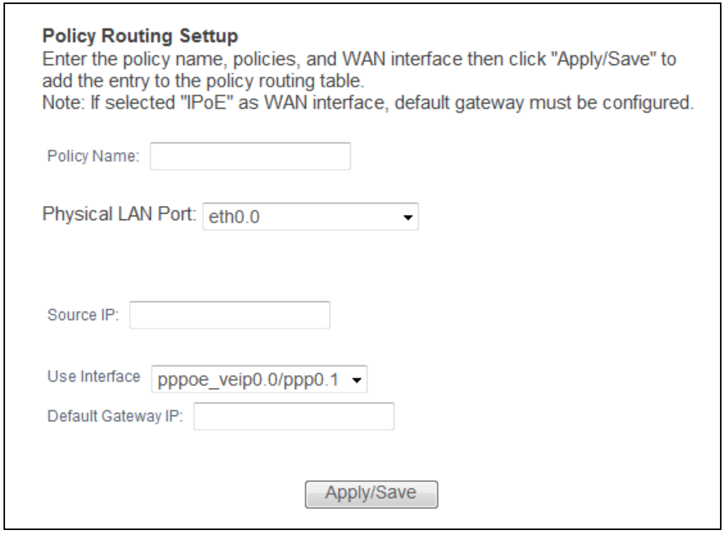
Table 55 Policy Routing

LABEL	DESCRIPTION
Policy Name	This displays the name of the rule.
Source IP	This displays the source IP address.
LAN Port	This displays the source LAN port number.
WAN	This displays the WAN interface through which the traffic is routed.
Default GW	This displays the default gateway IP address the route uses.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to create a new policy routing rule.

10.3.1 Add Policy Routing

Click **Add** in the **Policy Routing** screen to open the following screen. Use this screen to configure the required information for a policy route.

Figure 60 Policy Routing: Add



Policy Routing Setup

Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.

Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:

Physical LAN Port: eth0.0

Source IP:

Use Interface pppoe_veip0.0/ppp0.1

Default Gateway IP:

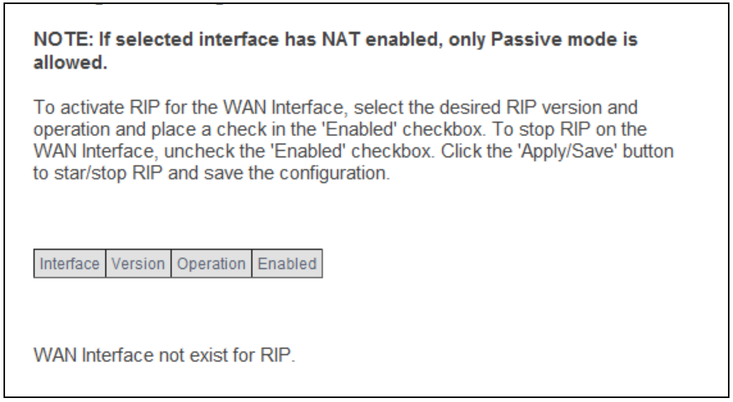
Table 56 Policy Routing: Add

LABEL	DESCRIPTION
Policy Name	Enter a descriptive name of printable English keyboard characters, not including spaces.
Physical LAN Port	Select the source LAN Ethernet port number.
Source IP	Enter the source IP address.
Use Interface	Select a WAN interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screens.
Default Gateway IP	Enter the default gateway IP address the route uses.
Apply/Save	Click this button to save your changes.

10.4 RIP

Click **Advanced Setup > Routing > RIP** to open the **RIP** screen. Use this screen to configure RIP settings. Routing Information Protocol (RIP, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers.

Figure 61 RIP



NOTE: If selected interface has NAT enabled, only Passive mode is allowed.

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled

WAN Interface not exist for RIP.

Table 57 RIP

LABEL	DESCRIPTION
Interface	This is the name of the interface in which the RIP setting is used.
Version	The RIP version controls the format and the broadcasting method of the RIP packets that the Router sends (it recognizes both formats when receiving). RIP version **1** is universally supported but RIP version **2** carries more information. RIP version **1** is probably adequate for most networks, unless you have an unusual network topology.
Operation	Select **Passive** to have the Router update the routing table based on the RIP packets received from neighbors but not advertise its route information to other routers in this interface. Select **Active** to have the Router advertise its route information and also listen for routing updates from neighboring routers.
Enabled	Select the check box to activate the settings.
Apply/Save	Click this button to save your changes.

DNS

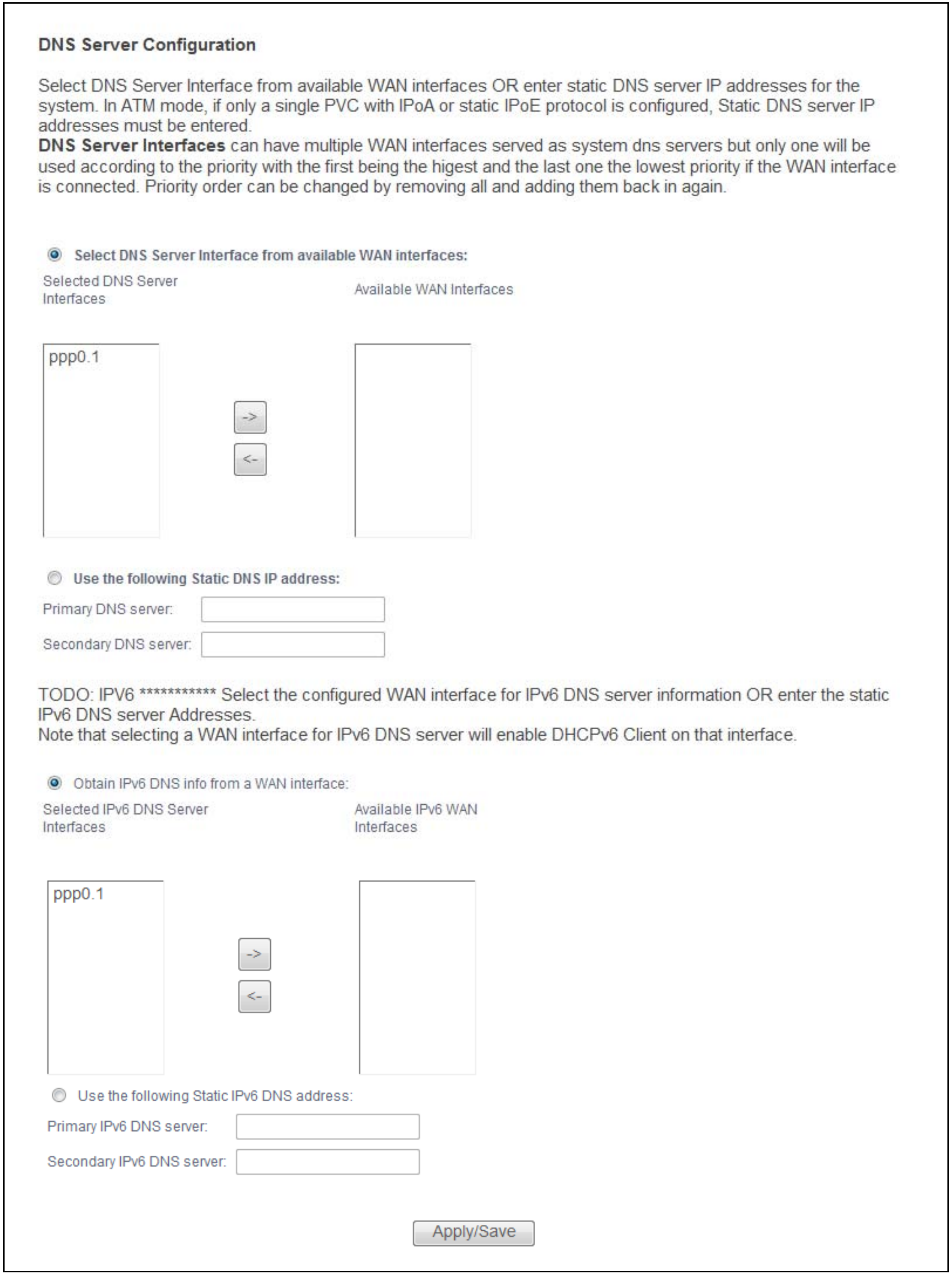
Chapter 11

11.1 DNS Server

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

Use this screen to view and configure DNS routes on the Router. Click **Advanced Setup > DNS > DNS Server** to open this screen.

Figure 62 DNS Server



DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

● **Select DNS Server Interface from available WAN interfaces:**

Selected DNS Server Interfaces: ppp0.1

Available WAN Interfaces:

○ **Use the following Static DNS IP address:**

Primary DNS server:

Secondary DNS server:

TODO: IPV6 *********** Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses.
Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.

● Obtain IPv6 DNS info from a WAN interface:

Selected IPv6 DNS Server Interfaces: ppp0.1

Available IPv6 WAN Interfaces:

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

The following table describes the fields in this screen.

Table 58 DNS Server

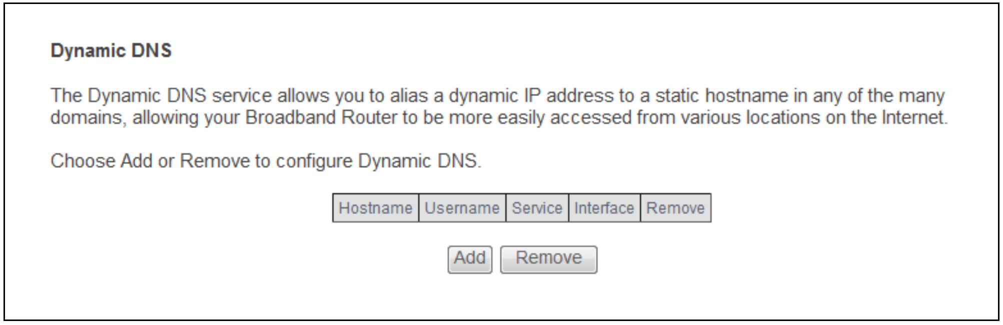
LABEL	DESCRIPTION
Select DNS Server Interface from available WAN interfaces	Select this to have the Router get the DNS server addresses from one of the Router’s WAN interfaces.
Selected DNS Server Interfaces	Select a WAN interface through which to get DNS server addresses. You can select multiple WAN interfaces for the device to try. The Router tries the WAN interfaces in the order listed and uses only the DNS server information of the first WAN interface that connects; there is no backup WAN function. To change the priority order remove them all and add them back in again.
Available WAN Interfaces	These are the WAN interfaces you can select from.
Use the following Static DNS IP address	Select this to have the Router use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Obtain IPv6 DNS info from a WAN interface	Select this to have the Router get the IPv6 DNS server addresses from the ISP automatically.
Selected IPv6 DNS Server Interfaces	Select an IPv6 WAN interface through which you want to obtain the IPv6 DNS related information.
Available IPv6 WAN Interfaces	These are the IPv6 WAN interfaces you can select from.
Use the following Static IPv6 DNS address	Select this to have the Router use the IPv6 DNS server addresses you configure manually.
Primary IPv6 DNS server	Enter the first IPv6 DNS server address assigned by the ISP.
Secondary IPv6 DNS server	Enter the second IPv6 DNS server address assigned by the ISP.
Apply/Save	Click this button to save your changes.

11.2 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services. You need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name.

Click **Advanced Setup > DNS > Dynamic DNS** to configure DDNS entries.

Figure 63 Dynamic DNS



Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

The following table describes the fields in this screen.

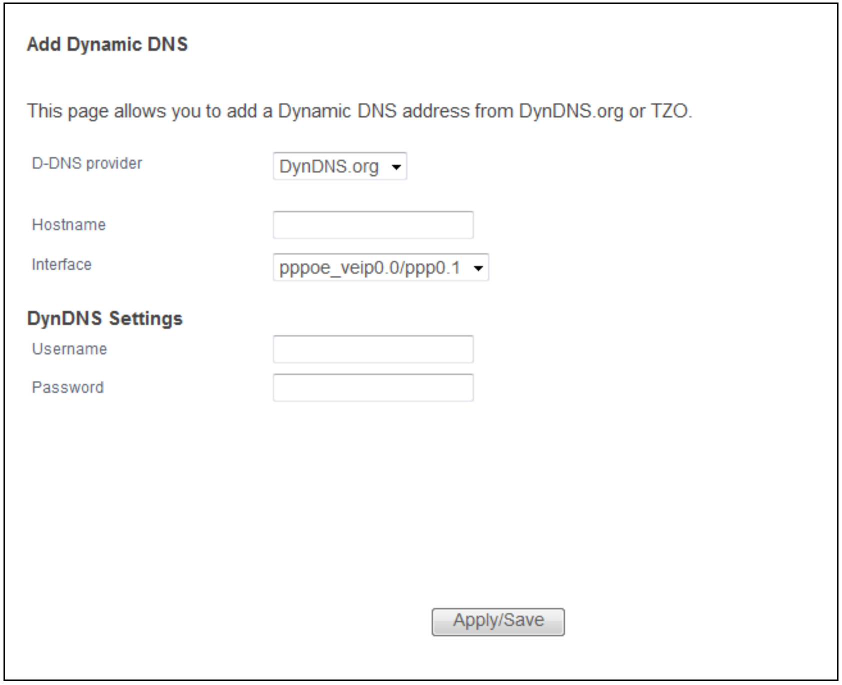
Table 59 Dynamic DNS

LABEL	DESCRIPTION
Hostname	This displays the entry’s domain name.
Username	This displays the entry’s user name.
Service	This displays the entry’s Dynamic DNS service provider.
Interface	This displays the interface the DDNS entry uses.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to create a new DDNS entry.

11.2.1 Dynamic DNS Add

Use this screen to create a DDNS entry. Click the **Dynamic DNS** screen's **Add** button to display the following screen.

Figure 64 Dynamic DNS Add



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Hostname:

Interface: pppoe_veip0.0/ppp0.1

DynDNS Settings

Username:

Password:

The following table describes the fields in this screen.

Table 60 Dynamic DNS Add

LABEL	DESCRIPTION
D-DNS provider	Select your Dynamic DNS service provider from the drop-down list box.
Hostname	Type the domain name assigned to your Router by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
Interface	Select the interface the DDNS entry uses.
Username	Type your user name.
Password	Type the password assigned to you.
Apply/Save	Click this button to save your changes.

UPnP

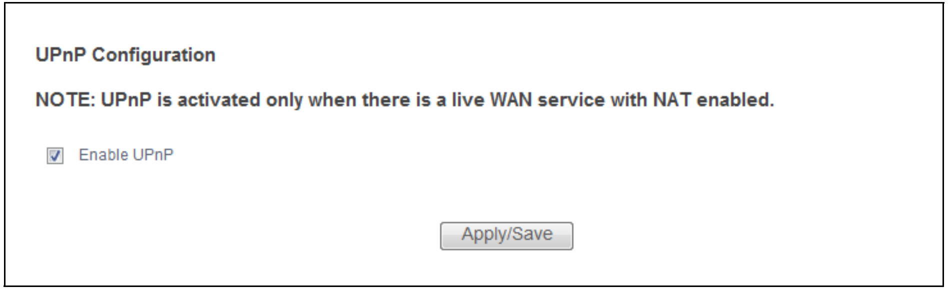
12 Chapter

12.1 UPnP

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

Use the **UPnP** screen to enable the UPnP feature on your Router. Click **Advanced Setup > UPnP**.

Figure 65 UPnP



UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

☑ Enable UPnP

Table 61 UPnP

LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Router's IP address (although you must still enter the password to access the web configurator).
Apply/Save	Click this button to save your changes.

DNS Proxy

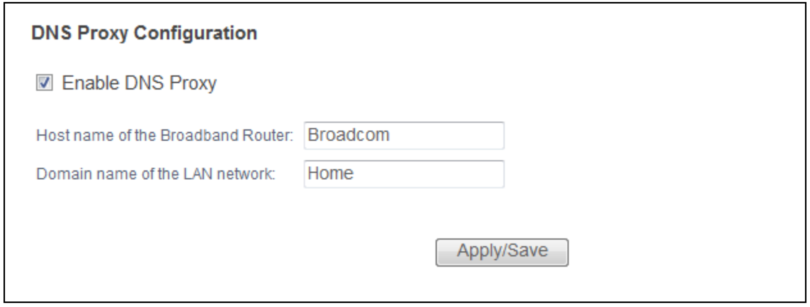
13 Chapter

13.1 DNS Proxy

Use DNS Proxy to have the Router send its own address to the LAN clients for them to use as the DNS server.

Click **Advanced Setup > DNS Proxy** to open the **DNS Proxy** screen.

Figure 66 DNS Proxy



DNS Proxy Configuration

☑ Enable DNS Proxy

Host name of the Broadband Router: Broadcom

Domain name of the LAN network: Home

Table 62 DNS Proxy

LABEL	DESCRIPTION
Enable DNS Proxy	Select this to have the Router send its own address to the LAN clients for them to use as the DNS server.
Host name of the Broadband Router	Enter a descriptive name for this Router.
Domain name of the LAN network	Enter the domain name of the LAN network.
Apply/Save	Click this button to save your changes.

Interface Grouping

Chapter 14

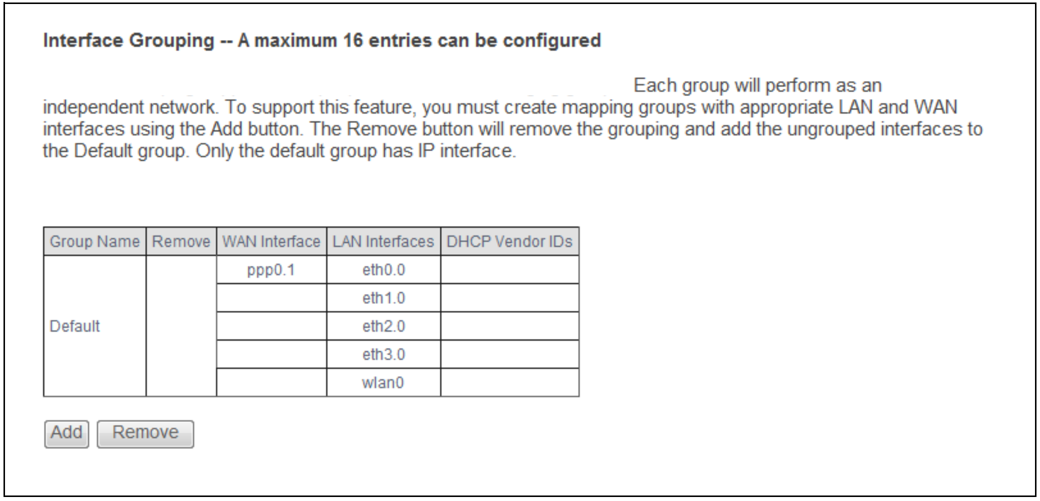
14.1 Interface Grouping

By default, all LAN and WAN interfaces on the Router are in the same group and can communicate with each other. Create interface groups to have the Router assign the IP addresses in different domains to different groups. Each group acts as an independent network on the Router. This lets devices connected to an interface group's LAN interfaces communicate through the interface group's WAN or LAN interfaces but not other WAN or LAN interfaces.

You can manually add a LAN interface to a new group. Alternatively, you can have the Router automatically add the incoming traffic and the LAN interface on which traffic is received to an interface group when its DHCP Vendor ID option information matches one listed for the interface group.

Use the **LAN** screen to configure the private IP addresses the DHCP server on the Router assigns to the clients in the default and/or user-defined groups. If you set the Router to assign IP addresses based on the client's DHCP Vendor ID option information, you must enable DHCP server and configure LAN TCP/IP settings for both the default and user-defined groups. Click **Advanced Setup > Interface Grouping** to open the following screen.

Figure 67 Interface Grouping



Interface Grouping -- A maximum 16 entries can be configured

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		ppp0.1	eth0.0	
			eth1.0	
			eth2.0	
			eth3.0	
			wlan0	

The following table describes the fields in this screen.

Table 63 Interface Grouping

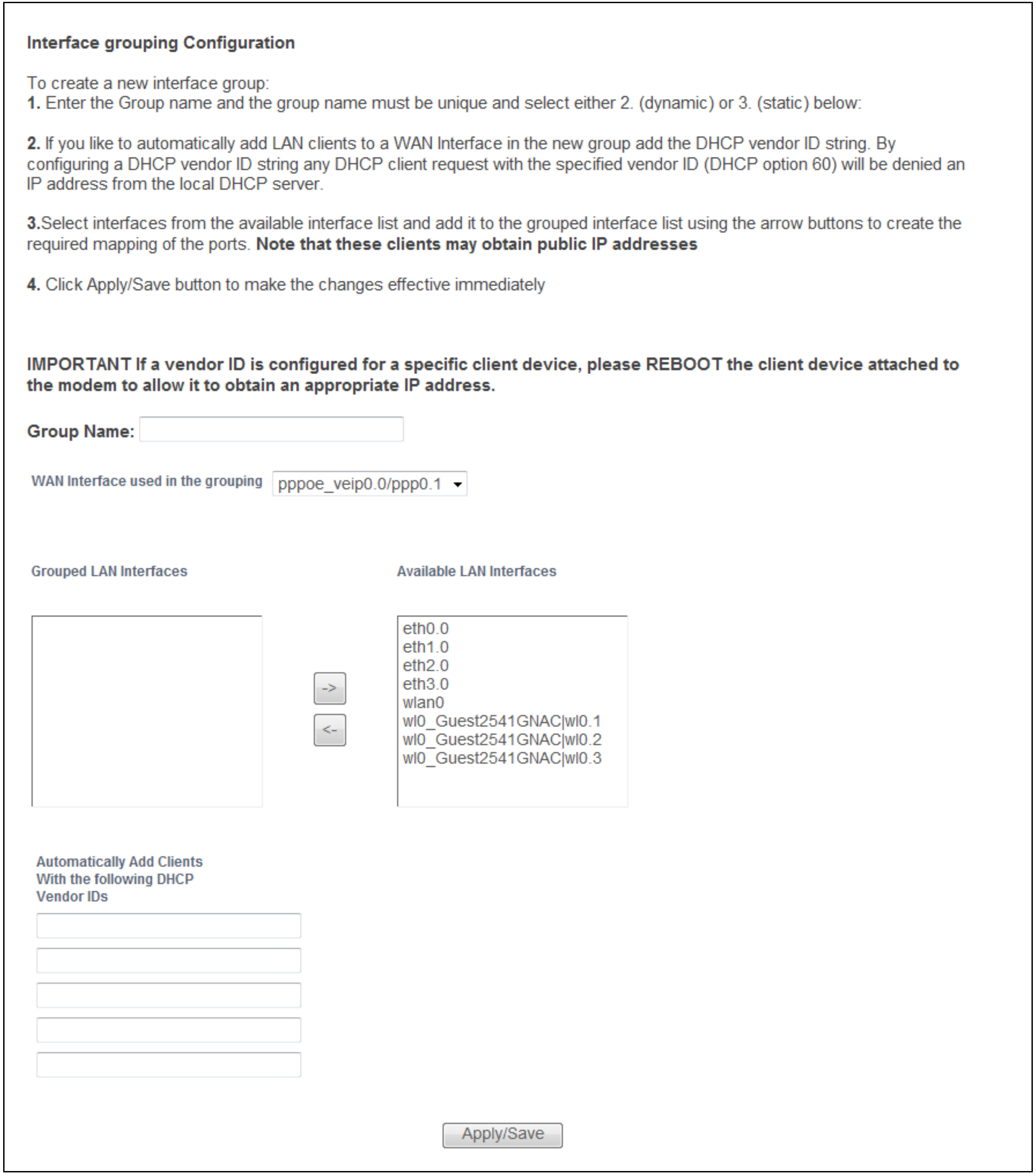
LABEL	DESCRIPTION
Group Name	This shows the descriptive name of the group.
Remove	Select this check box and click the **Remove** button to delete the group from the Router.
WAN Interface	This shows the WAN interfaces in the group.
LAN Interfaces	This shows the LAN interfaces in the group.
DHCP Vendor IDs	This shows the DHCP Vendor’s ID for the group.
Add	Click this button to create a new group.

14.1.1 Interface Group Configuration

Click the **Add** button in the **Interface Grouping** screen to open the following screen. Use this screen to create a new interface group.

ⓘ An interface can belong to only one group at a time.

Figure 68 Interface Grouping: Add



Interface grouping Configuration

To create a new interface group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

4. Click Apply/Save button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

WAN Interface used in the grouping: pppoe_veip0.0/ppp0.1

The following table describes the fields in this screen.

Table 64 Interface Grouping: Add

LABEL	DESCRIPTION
Group Name	Enter a name to identify this group. You can enter up to 30 characters. You can use letters, numbers, hyphens (-) and underscores (_). Spaces are not allowed.
WAN Interface used in the grouping	Select the WAN interface this group uses. Select **None** to not add a WAN interface to this group.
Grouped LAN Interfaces Available LAN Interfaces	Select one or more LAN interfaces (Ethernet LAN, HPNA or wireless LAN) in the **Available LAN Interfaces** list and use the left arrow to move them to the **Grouped LAN Interfaces** list to add the interfaces to this group. To remove a LAN or wireless LAN interface from the **Grouped LAN Interfaces**, use the right-facing arrow.
Automatically Add Clients With the following DHCP Vendor IDs	If you want LAN clients to get public IP addresses, you can list their DHCP vendor IDs here.
Apply/Save	Click **Apply/Save** to save your changes back to the Router.

IP Tunnel

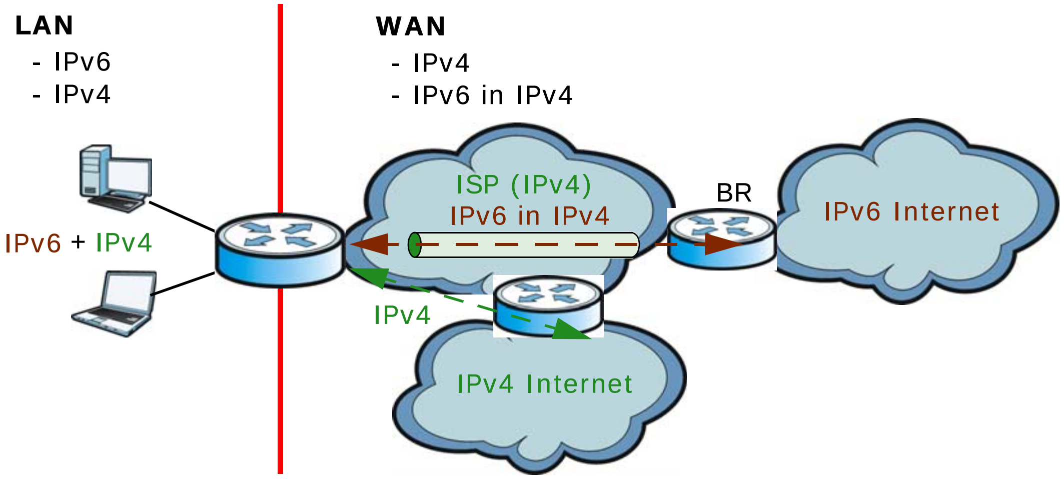
15 Chapter

15.1 IPv6inIPv4 (6RD)

Use IPv6 Rapid Deployment (6RD) when the local network uses IPv6 and the ISP has an IPv4 network. When the Router has an IPv4 WAN address and is configured to **IPv4 only**, you can enable 6RD to encapsulate IPv6 packets in IPv4 packets to cross the ISP's IPv4 network.

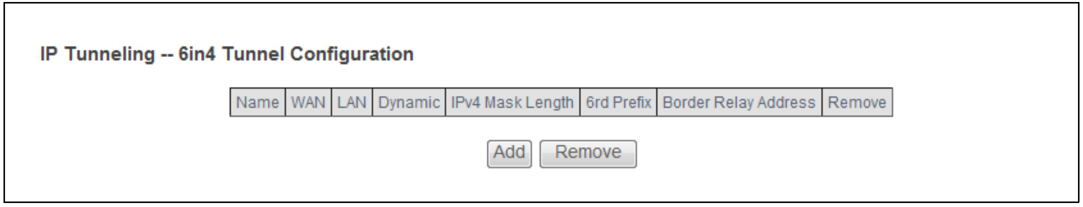
The Router generates a global IPv6 prefix from its IPv4 WAN address and tunnels IPv6 traffic to the ISP's Border Relay router (BR in the figure) to connect to the native IPv6 Internet. The local network can also use IPv4 services. The Router uses it's configured IPv4 WAN IP to route IPv4 traffic to the IPv4 Internet.

Figure 69 IPv6 Rapid Deployment



Click **Advanced Setup > IP Tunnel > IPv6inIPv4** to view and configure IPv6 through IPv4 tunneling. This will encapsulate IPv6 packets in IPv4 packets so they can travel through IPv4 networks.

Figure 70 IPv6inIPv4



IP Tunneling -- 6in4 Tunnel Configuration

Name	WAN	LAN	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove

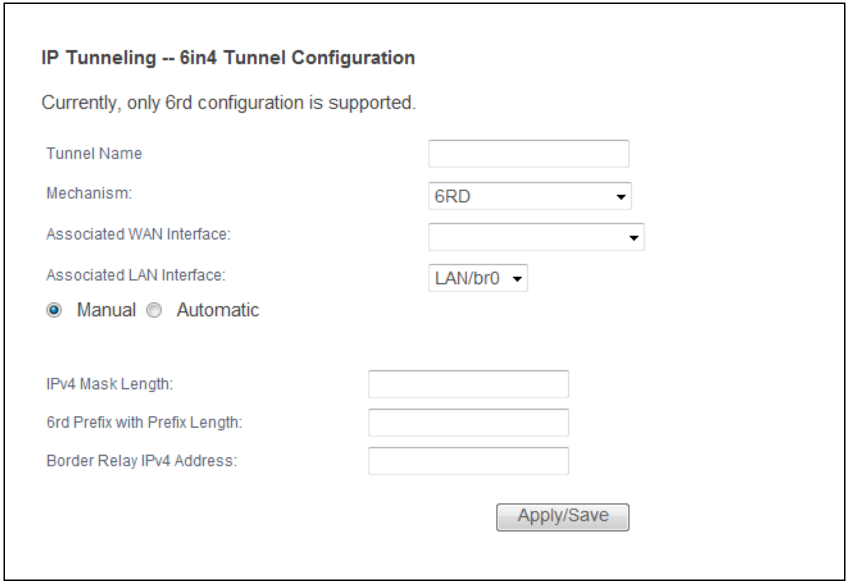
Table 65 IPv6inIPv4

LABEL	DESCRIPTION
Name	This displays the IPv6 to IPv4 tunnel's name.
WAN	This displays the associated WAN interface.
LAN	This displays the associated LAN interface.
Dynamic	This displays the type of 6RD.
IPv4 Mask Length	This displays the subnet mask number for the IPv4 network.
6rd Prefix	This displays the IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
Boarder Relay Address	This displays the relay server's IPv4 address.
Remove	Select an entry and click the **Remove** button to delete it.
Add	Click this to add a new IPv6 through IPv4 tunnel.

15.1.1 IPv6inIPv4 Configuration

Click the **Add** button in the **IPv6inIPv4 screen to add a new IPv6 through IPv4 tunnel entry.**

Figure 71 IPv6inIPv4: Add



IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name	
Mechanism:	6RD
Associated WAN Interface:	
Associated LAN Interface:	LAN/br0

● Manual ○ Automatic

IPv4 Mask Length:	
6rd Prefix with Prefix Length:	
Border Relay IPv4 Address:	

Table 66 IPv6inIPv4: Add

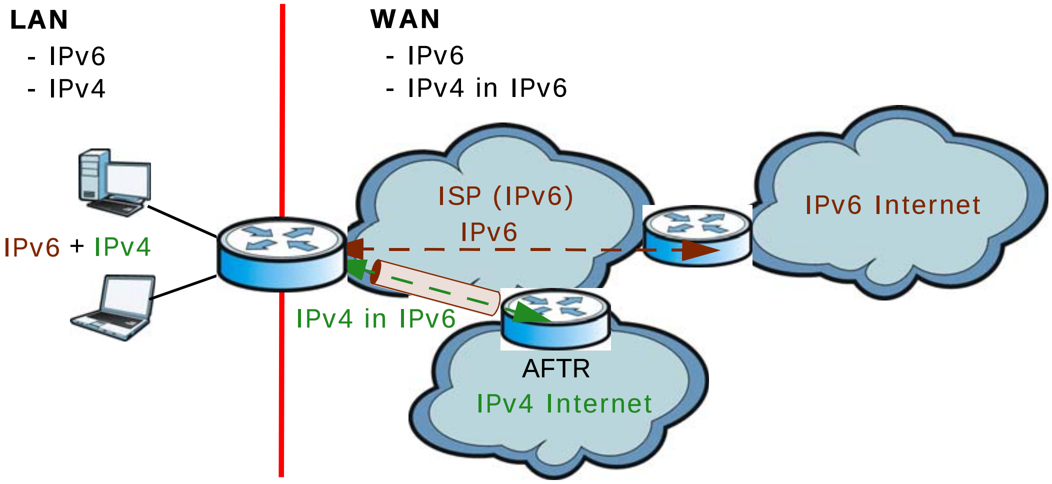
LABEL	DESCRIPTION
Tunnel Name	Enter a descriptive name for the IPv6 through IPv4 tunnel.
Mechanism	The current mechanism is set to **6RD** to tunnel IPv6 traffic from the local network through the ISP's IPv4 network.
Associated WAN Interface	Select a WAN interface to associate with the IPv6 to IPv4 tunnel.
Associated LAN Interface	Select a LAN interface to associate with the IPv6 to IPv4 tunnel.
Manual/ Automatic	Select the 6RD type. Select **Manual** to set the 6RD type to static. Select **Automatic** to have the Router detect it automatically through DHCP.
IPv4 Mask Length	Enter the subnet mask number (1~32) for the IPv4 network.
6rd Prefix with Prefix Length	Enter an IPv6 prefix for tunneling IPv6 traffic to the ISP's border relay router and connecting to the native IPv6 Internet.
Border Relay IPv4 Address	Specify the relay server's IPv4 address in this field.
Apply/Save	Click this button to save your changes.

15.2 IPv4inIPv6 (Dual Stack Lite)

Use DS-Lite (Dual Stack Lite) when local network computers use IPv4 and the ISP has an IPv6 network. When the Router has an IPv6 WAN address and is set to **IPv6 only**, you can enable Dual Stack Lite to use IPv4 computers and services.

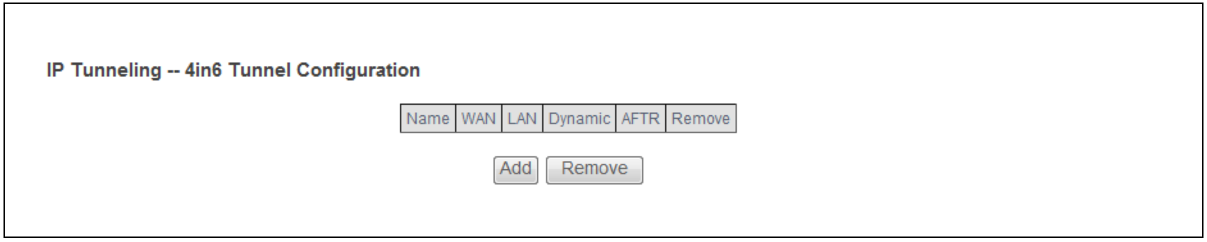
The Router tunnels IPv4 packets inside IPv6 encapsulation packets to the ISP's Address Family Transition Router (AFTR in the graphic) to connect to the IPv4 Internet. The local network can also use IPv6 services. The Router uses it's configured IPv6 WAN IP to route IPv6 traffic to the IPv6 Internet.

Figure 72 Dual Stack Lite



Click **Advanced Setup > IP Tunnel > IPv4inIPv6** to view and configure Dual Stack Lite to let local computers use IPv4 through an ISP's IPv6 network.

Figure 73 IPv4inIPv6



IP Tunneling -- 4in6 Tunnel Configuration

Name	WAN	LAN	Dynamic	AFTR	Remove

Table 67 IPv4inIPv6

LABEL	DESCRIPTION
Name	This displays the IPv4 through IPv6 tunnel's name.
WAN	This displays the associated WAN interface.
LAN	This displays the associated LAN interface.
Dynamic	This displays the type of 6RD.
AFTR	This displays the transition router's IPv6 address.

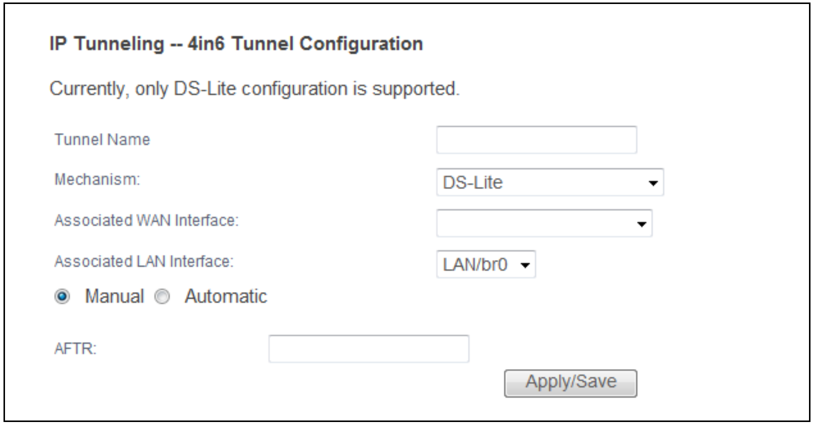
Table 67 IPv4inIPv6 (continued)

LABEL	DESCRIPTION
Remove	Select an entry and click the **Remove** button to delete it.
Add	Click this to add a new IPv4 through IPv6 tunnel.

15.2.1 IPv4inIPv6 Configuration

Click the **Add** button in the **IPv4inIPv6** screen to add a new IPv6 through IPv4 tunnel entry.

Figure 74 IPv4inIPv6: Add



IP Tunneling -- 4in6 Tunnel Configuration

Currently, only DS-Lite configuration is supported.

Tunnel Name

Mechanism: DS-Lite

Associated WAN Interface:

Associated LAN Interface: LAN/br0

● Manual ○ Automatic

AFTR:

Table 68 IPv4inIPv6: Add

LABEL	DESCRIPTION
Tunnel Name	Enter a descriptive name for the IPv4 to IPv6 tunnel.
Mechanism	The mechanism is set to **DS-Lite** to let local computers use IPv4 through an ISP’s IPv6 network.
Associated WAN Interface	Select a WAN interface to associate with the IPv4 to IPv6 tunnel.
Associated LAN Interface	Select a LAN interface to associate with the IPv4 to IPv6 tunnel.
Manual/Automatic	Select the 6RD type. Select **Manual** to set the 6RD type to static. Select **Automatic** to have the Router detect it automatically through DHCP.
AFTR	Specify the ISP’s Address Family Transition Router’s IPv6 address.
Apply/Save	Click this button to save your changes.

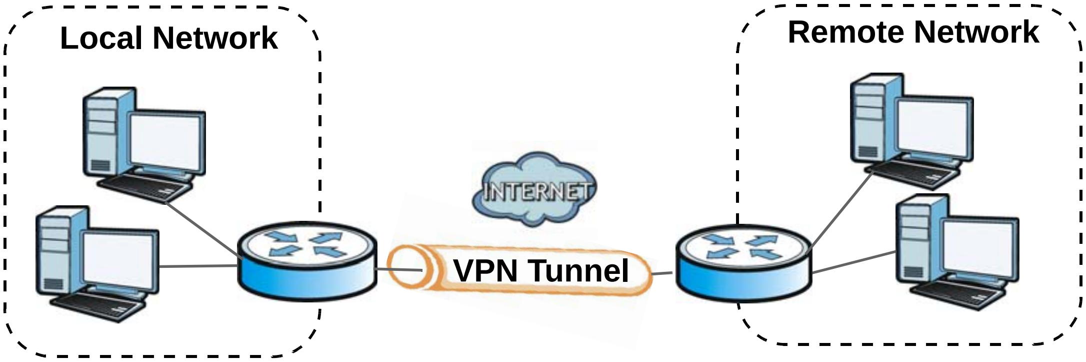
IPSec VPN

16 Chapter

16.1 IPSec VPN

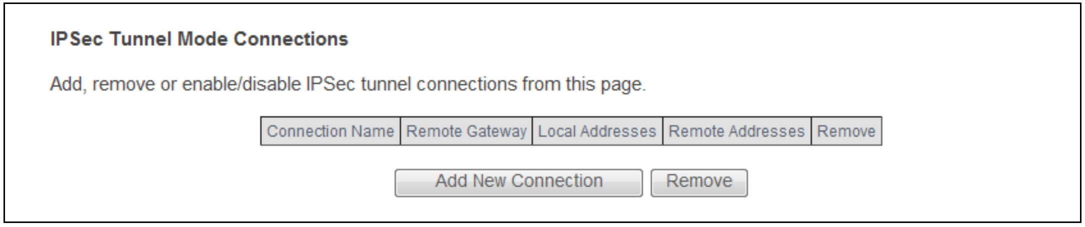
A virtual private network (VPN) provides secure communications over the the Internet. Internet Protocol Security (IPSec) is a standards-based VPN that provides confidentiality, data integrity, and authentication. This chapter shows you how to configure the Router's VPN settings.

Figure 75 IPSec Fields Summary



Click **Advanced Setup > IPSec VPN** to view and manage your VPN tunnel policies. The following figure helps explain the main fields in the web configurator.

Figure 76 IPSec VPN



IPSec Tunnel Mode Connections

Add, remove or enable/disable IPSec tunnel connections from this page.

Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Remove

This screen contains the following fields:

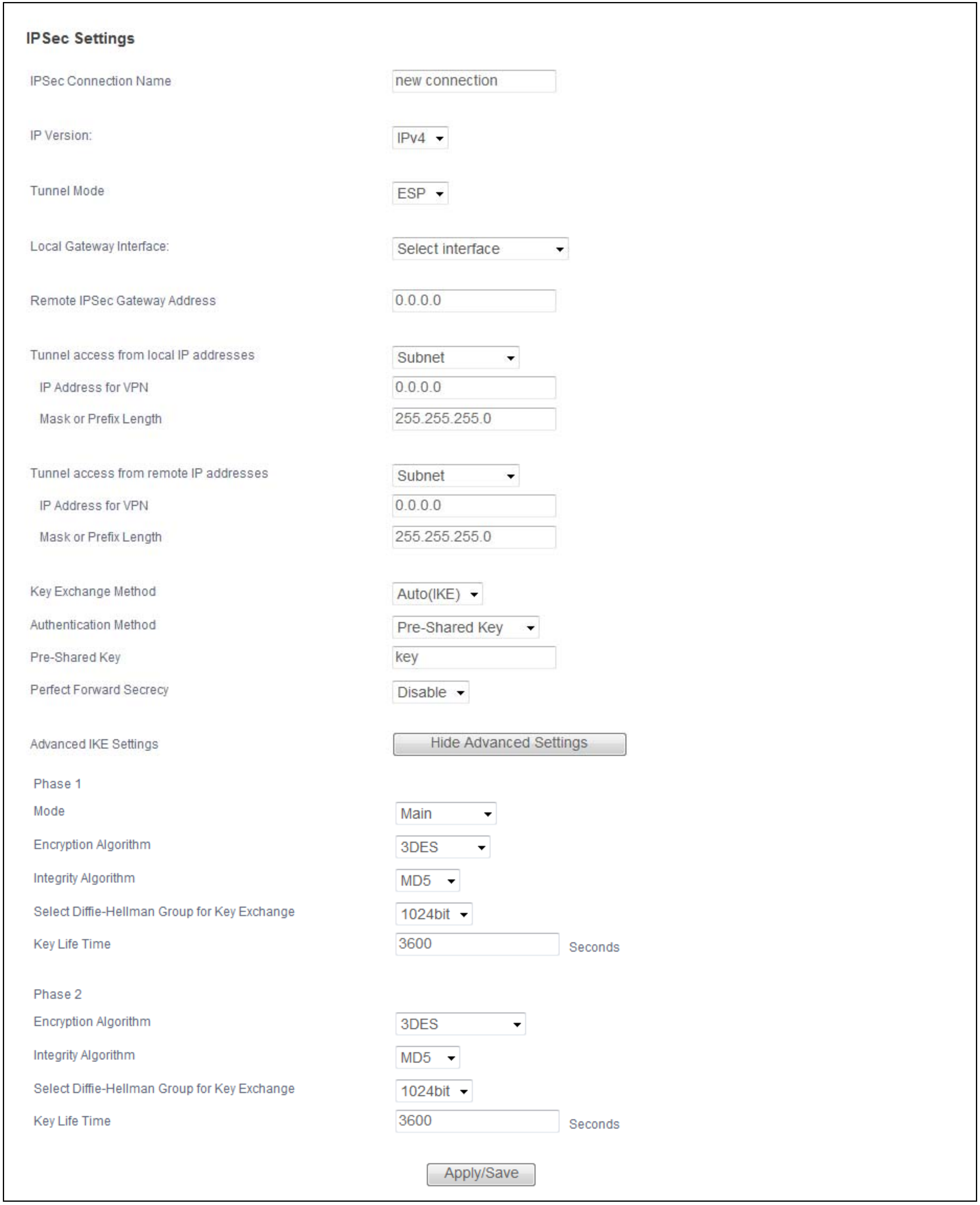
Table 69 IPSec VPN

LABEL	DESCRIPTION
Connection Name	The name of the VPN policy.
Remote Gateway	This is the IP address of the remote IPSec router in the IKE SA.
Local Addresses	This displays the IP address(es) on the LAN behind your Router.
Remote Addresses	This displays the IP address(es) on the LAN behind the remote IPSec's router.
Remove	Select entries and click the **Remove** button to delete them.
Add New Connection	Click this button to add an item to the list.

16.2 IPSec VPN Add Screen

Use these settings to add IPSec VPN policies. Click the **Add New Connection** button in the **Advanced Setup > IPSec VPN** screen to open this screen as shown next.

Figure 77 IPSec VPN: Add



IPSec Settings

IPSec Connection Name	new connection
IP Version:	IPv4
Tunnel Mode	ESP
Local Gateway Interface:	Select interface
Remote IPSec Gateway Address	0.0.0.0
Tunnel access from local IP addresses	Subnet
IP Address for VPN	0.0.0.0
Mask or Prefix Length	255.255.255.0
Tunnel access from remote IP addresses	Subnet
IP Address for VPN	0.0.0.0
Mask or Prefix Length	255.255.255.0
Key Exchange Method	Auto(IKE)
Authentication Method	Pre-Shared Key
Pre-Shared Key	key
Perfect Forward Secrecy	Disable
Advanced IKE Settings	Hide Advanced Settings
Phase 1	
Mode	Main
Encryption Algorithm	3DES
Integrity Algorithm	MD5
Select Diffie-Hellman Group for Key Exchange	1024bit
Key Life Time	3600 Seconds
Phase 2	
Encryption Algorithm	3DES
Integrity Algorithm	MD5
Select Diffie-Hellman Group for Key Exchange	1024bit
Key Life Time	3600 Seconds

This screen contains the following fields:

Table 70 IPSec VPN: Add

LABEL	DESCRIPTION
IPSec Connection Name	Enter the name of the VPN policy.
IP Version	Set whether this policy uses IPv4 or IPv6.
Tunnel Mode	Select the security protocol to use in the IPSec SA. **AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. **ESP** (RFC 2406) - provides encryption and the same services offered by AH, but its authentication is weaker. The Router and remote IPSec router must use the same active protocol.
Remote IPSec Gateway Address	Enter the IP address of the remote IPSec router in the IKE SA.
Tunnel access from local IP addresses	Select **Single Address** to have only one local LAN IP address use the VPN tunnel. Select **Subnet** to specify local LAN IP addresses by their subnet mask.
IP Address for VPN	If **Single Address** is selected, enter a (static) IP address on the LAN behind your Router. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind your Router. Then enter the subnet mask to identify the network address.
Mask or Prefix Length	If **Subnet** is selected, enter the subnet mask (for IPv4) or prefix length (for an IPv6 address) to identify the network address. The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.
Tunnel access from remote IP addresses	Select **Single Address** to have only one remote LAN IP address use the VPN tunnel. Select **Subnet** to specify remote LAN IP addresses by their subnet mask.
IP Address for VPN	If **Single Address** is selected, enter a (static) IP address on the LAN behind the remote IPSec's router. If **Subnet** is selected, specify IP addresses on a network by their subnet mask by entering a (static) IP address on the LAN behind the remote IPSec's router. Then enter the subnet mask to identify the network address.
Mask or Prefix Length	If **Subnet** is selected, enter the subnet mask (for IPv4) or prefix length (for an IPv6 address) to identify the network address. The IPv6 prefix length specifies how many most significant bits (starting from the left) in the address compose the network address.

Table 70 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Key Exchange Method	Select the key exchange method: **Auto(IKE)** - Select this to use automatic IKE key management VPN connection policy. **Manual** - Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management. Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.
Authentication Method	Select **Pre-Shared Key** to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Select **Certificate (X.509)** to use a certificate for authentication.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x” (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself.
Perfect Forward Secrecy (PFS)	Select whether or not to enable Perfect Forward Secrecy (PFS). Both routers must enable it or disable it.
Advanced IKE Settings	Use the button to show or hide the advanced IKE settings.
Phase 1	
Mode	Select the negotiation mode to use to negotiate the IKE SA. Choices are: **Main** - this encrypts the Router’s and remote IPSec router’s identities but takes more time to establish the IKE SA. **Aggressive** - this is faster but does not encrypt the identities. The Router and the remote IPSec router must use the same negotiation mode.

Table 70 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: DES - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - **128** - a 128-bit key with the AES encryption algorithm **AES** - **196** - a 196-bit key with the AES encryption algorithm **AES** - **256** - a 256-bit key with the AES encryption algorithm The Router and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Integrity Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. SHA is generally considered stronger than MD5, but it is also slower.
Select Diffie-Hellman Group for Key Exchange	Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096, 6114, and 8192. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Key Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Phase 2	
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - **128** - a 128-bit key with the AES encryption algorithm **AES** - **192** - a 196-bit key with the AES encryption algorithm **AES** - **256** - a 256-bit key with the AES encryption algorithm Select **NULL Encryption** to set up a tunnel without encryption. You do not enter an encryption key with this option. The Router and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput.
Integrity Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5** and **SHA1**. SHA is generally considered stronger than MD5, but it is also slower.

Table 70 IPSec VPN: Add (continued)

LABEL	DESCRIPTION
Select Diffie-Hellman Group for Key Exchange	Select which Diffie-Hellman key group you want to use for encryption keys. Choices for number of bits in the random number are: 768, 1024, 1536, 2048, 3072, 4096, 6114, and 8192. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group.
Key Life Time	Define the length of time before an IPSec SA automatically renegotiates in this field. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
The following fields display if you select **Manual** in the **Key Exchange Method** field.	
Perfect Forward Secrecy (PFS)	Select whether or not to enable Perfect Forward Secrecy (PFS). Both routers must enable it or disable it.
Encryption Algorithm	Select which key size and encryption algorithm to use in the IKE SA. Choices are: **DES** - a 56-bit key with the DES encryption algorithm **3DES** - a 168-bit key with the DES encryption algorithm **AES** - AES-CBC encryption. CBC creates message authentication code from a block cipher.
Encryption Key	This field is applicable when you select an Encryption Algorithm. Enter the encryption key, which depends on the encryption algorithm. **DES** - type a unique key 16 hexadecimal characters long. **3DES** - type a unique key 48 hexadecimal characters long. **AES** - type a unique key 32, 48, or 64 hexadecimal characters long.
Authentication Algorithm	Select which hash algorithm to use to authenticate packet data. Choices are **MD5**, **SHA1**. SHA is generally considered stronger than MD5, but it is also slower.
Authentication Key	Enter the authentication key, which depends on the authentication algorithm. **MD5** - type a unique key 32 hexadecimal characters long **SHA1** - type a unique key 40 hexadecimal characters long
SPI	Type a unique SPI (Security Parameter Index) in hexadecimal characters. The SPI is used to identify the Router during authentication. The Router and remote IPSec router must use the same SPI.
Apply/Save	Click this button to save your changes.

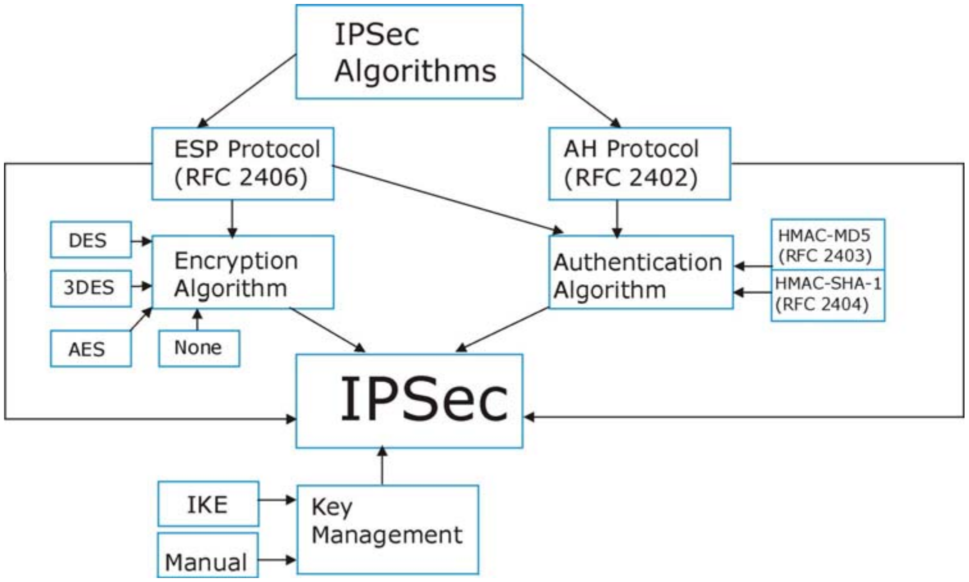
16.3 Technical Reference

This section provides some technical background information about the topics covered in this section.

16.3.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 78 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

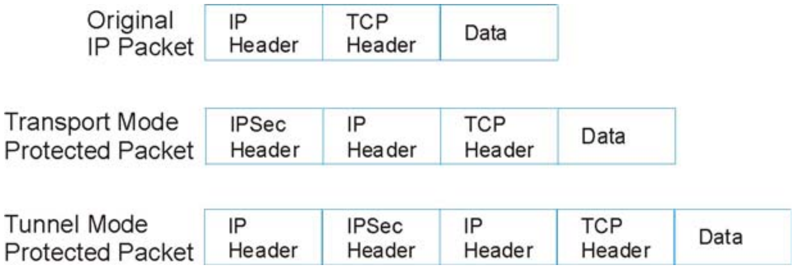
Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

16.3.2 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode. At the time of writing, the Router supports **Tunnel** mode only.

Figure 79 Transport and Tunnel Mode IPSec Encapsulation



Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel Mode

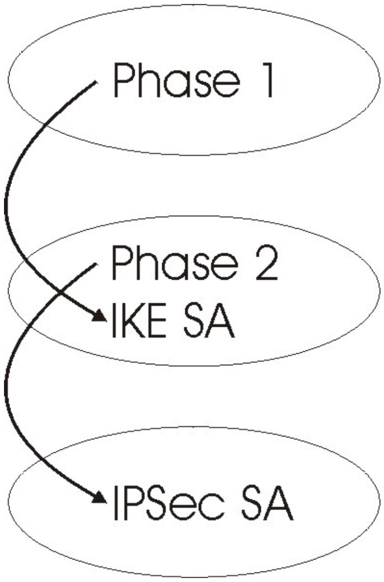
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

16.3.3 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 80 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose a Diffie-Hellman public-key cryptography key group.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Router automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

16.3.4 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

16.3.5 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Router.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 71 VPN and NAT

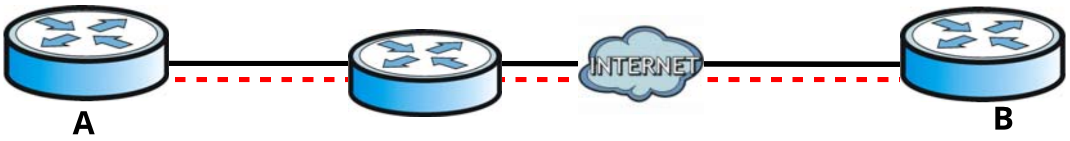
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

16.3.6 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the Router's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 81 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In the above figure, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.
- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 72 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the Router if you enable NAT traversal.

16.3.7 ID Type and Content

With aggressive negotiation mode (see Section 16.3.4 on page 124), the Router identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Router to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses.

Regardless of the ID type and content configuration, the Router does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 16.3.4 on page 124), the ID type and content are encrypted to provide identity protection. In this case the Router can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Router can distinguish up to 48 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and eight key groups when you configure a VPN rule (see Section 16.1 on page 114). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 73 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer.
DNS	Type a domain name (up to 31 characters) by which to identify this Router.

Table 73   Local ID Type and Content Fields (continued)

LOCAL ID TYPE=	CONTENT=
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Router.
	The domain name or e-mail address that you use in the **Local ID Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

16.3.7.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Routers in this example can complete negotiation and establish a VPN tunnel.

Table 74   Matching ID Type and Content Configuration Example

ROUTER A	ROUTER B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Remote ID type: IP	Remote ID type: E-mail
Remote ID content: 1.1.1.2	Remote ID content: tom@yourcompany.com

The two Routers in this example cannot complete their negotiation because Router B's **Local ID Type** is **IP**, but Router A's **Remote ID Type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 75   Mismatching ID Type and Content Configuration Example

ROUTER A	ROUTER B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.2
Remote ID type: E-mail	Remote ID type: IP
Remote ID content: aa@yahoo.com	Remote ID content: 1.1.1.0

16.3.8 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 16.3.3 on page 123 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

16.3.9 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

Certificates

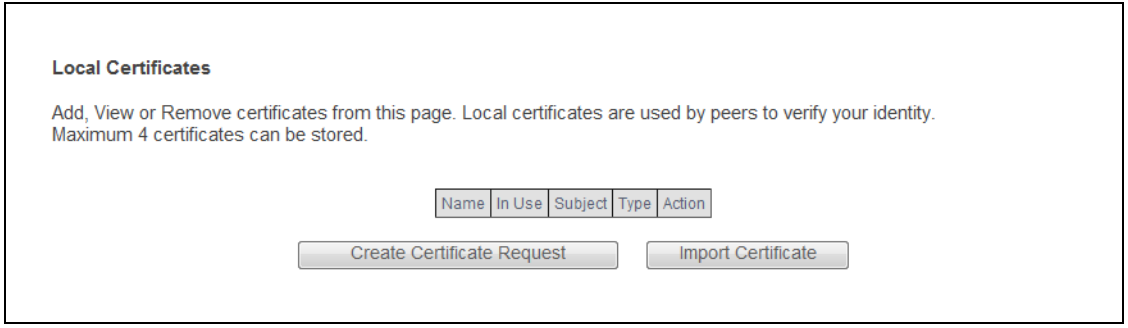
17 Chapter

17.1 Local Certificates

The Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner’s identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **Advanced Setup > Certificates > Local** to manage the Router’s list of certificates and certification requests.

Figure 82 Local Certificates



Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action

Table 76 Local Certificates

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
In Use	This field shows whether or not the Router currently uses the certificate.
Subject	This field displays identifying information about the certificate’s owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Type	This field displays whether the entry is for a certificate or a certificate request.

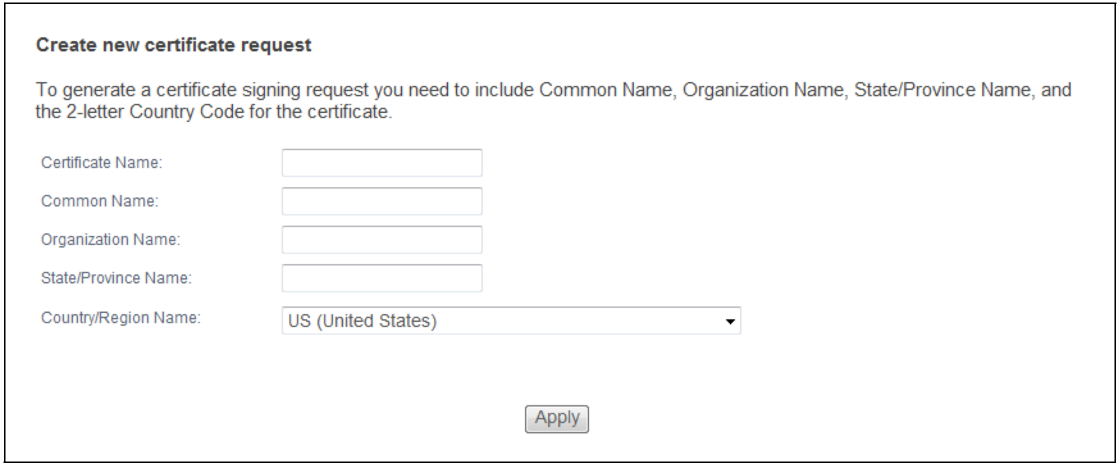
Table 76 Local Certificates (continued)

LABEL	DESCRIPTION
Action	Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request). For a certification request, click **Load Signed** to import the signed certificate. Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.
Create Certificate Request	Click this button to go to the screen where you can have the Router generate a certification request.
Import Certificate	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Router.

17.1.1 Create Certificate Request

Click the **Local Certificates** screen's **Create Certificate Request** button to open the following screen. Use this screen to have the Router generate a certification request.

Figure 83 Create Certificate Request



Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

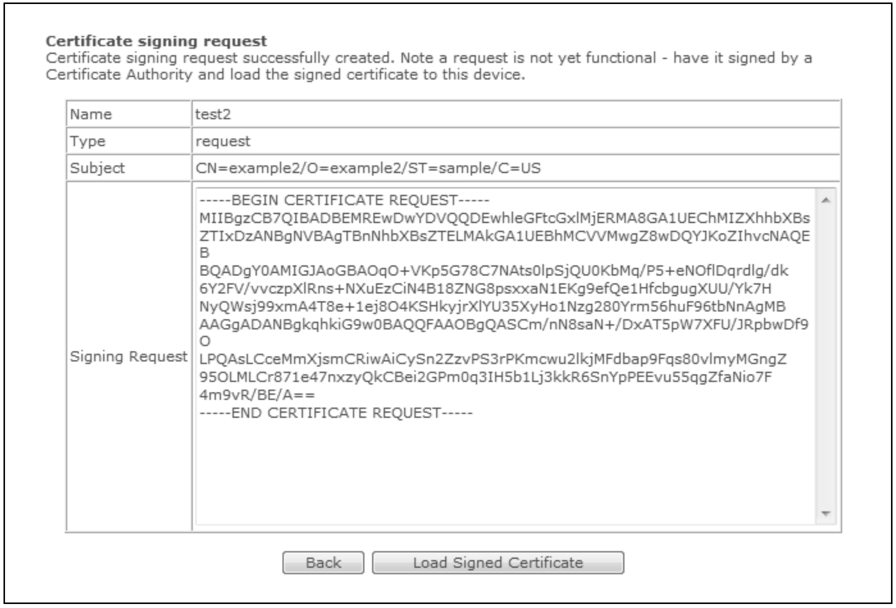
Certificate Name:	
Common Name:	
Organization Name:	
State/Province Name:	
Country/Region Name:	US (United States)

Table 77 Create Certificate Request

LABEL	DESCRIPTION
Certificate Name	Type up to 63 ASCII characters (not including spaces) to identify this certificate.
Common Name	Select **Auto** to have the Router configure this field automatically. Or select **Customize** to enter it manually. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organization Name	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the Router drops trailing spaces.
State/Province Name	Type up to 32 characters to identify the state or province where the certificate owner is located. You may use any character, including spaces, but the Router drops trailing spaces.
Country/Region Name	Select a country to identify the nation where the certificate owner is located.
Apply	Click **Apply** to save your changes.

After you click **Apply**, the following screen displays to notify you that you need to get the certificate request signed by a Certificate Authority. If you already have, click **Load_Signed** to import the signed certificate into the Router. Otherwise click **Back** to return to the **Local Certificates** screen.

Figure 84 Certificate Request Created



Certificate signing request

Certificate signing request successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and load the signed certificate to this device.

Name	test2
Type	request
Subject	CN=example2/O=example2/ST=sample/C=US
Signing Request	(see below)

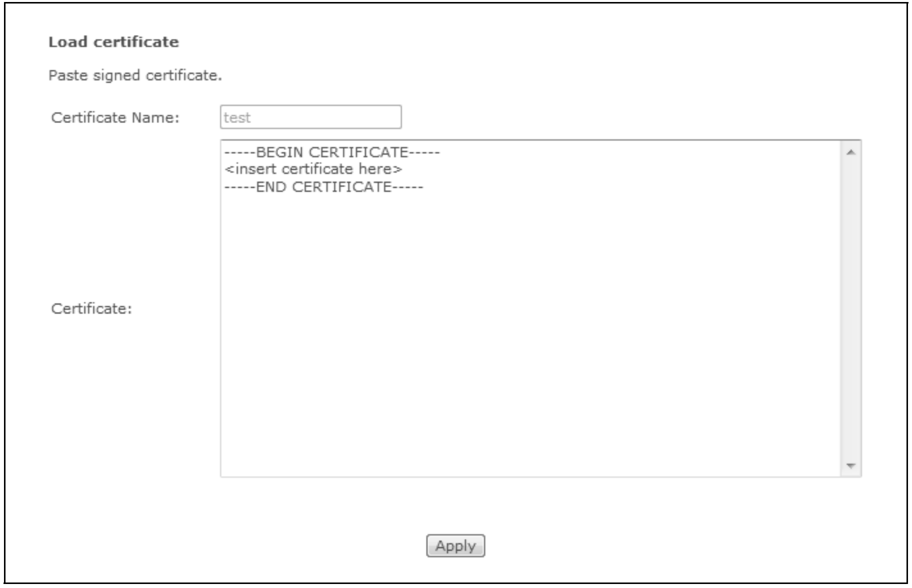
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBgzCB7QIBADBEMREwDwYDVQQDEwhleGFtcGxlMjERMA8GA1UEChMIZXhhbXBs
ZTIxDzANBgNVBAgTBnNhbXBsZTELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcNAQE
B
BQADgY0AMIGJAoGBAOqO+VKp5G78C7NAts0lpSjQU0KbMq/P5+eNOflDqrdlg/dk
6Y2FV/vvczpXlRns+NXuEzCiN4B18ZNG8psxxaN1EKg9efQe1HfcbgugXUU/Yk7H
NyQWsj99xmA4T8e+1ej8O4KSHkyjrXlYU35XyHo1Nzg280Yrm56huF96tbNnAgMB
AAGgADANBgkqhkiG9w0BAQQFAAOBgQASCm/nN8saN+/DxAT5pW7XFU/JRpbwDf9
O
LPQAsLCceMmXjsmCRiwAiCySn2ZzvPS3rPKmcwu2lkjMFdbap9Fqs80vlmyMGngZ
95OLMLCr871e47nxzyQkCBei2GPm0q3IH5b1Lj3kkR6SnYpPEEvu55qgZfaNio7F
4m9vR/BE/A==
-----END CERTIFICATE REQUEST-----
```

17.1.2 Load Signed Certificate

After you create a certificate request and have it signed by a Certificate Authority, in the **Local Certificates** screen click the certificate request's **Load Signed** button to import the signed certificate into the Router.

ⓘ You must remove any spaces from the certificate's filename before you can import it.

Figure 85 Load Signed Certificate



Load certificate

Paste signed certificate.

Certificate Name: test

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

Table 78 Load Signed Certificate

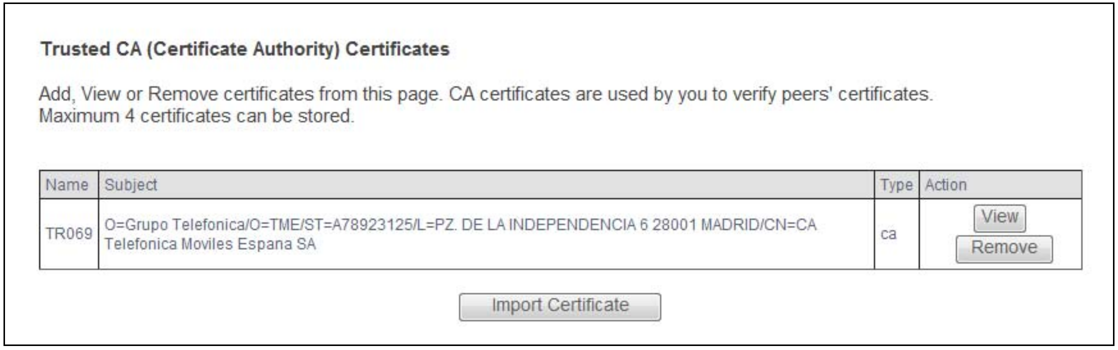
LABEL	DESCRIPTION
Certificate Name	This is the name of the signed certificate.
Certificate	Copy and paste the signed certificate into the text box to store it on the Router.
Apply	Click **Apply** to save your changes.

17.2 Trusted CA

Use the **Trusted CA** screen to view a summary list of certificates of the certification authorities that you have set the Router to accept as trusted. The Router accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Advanced Setup > Certificates > Trusted CA** to open the **Trusted CA** screen.

Figure 86 Trusted CA



Trusted CA (Certificate Authority) Certificates

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

Name	Subject	Type	Action
TR069	O=Grupo Telefonica/O=TME/ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/CN=CA Telefonica Moviles Espana SA	ca	View Remove

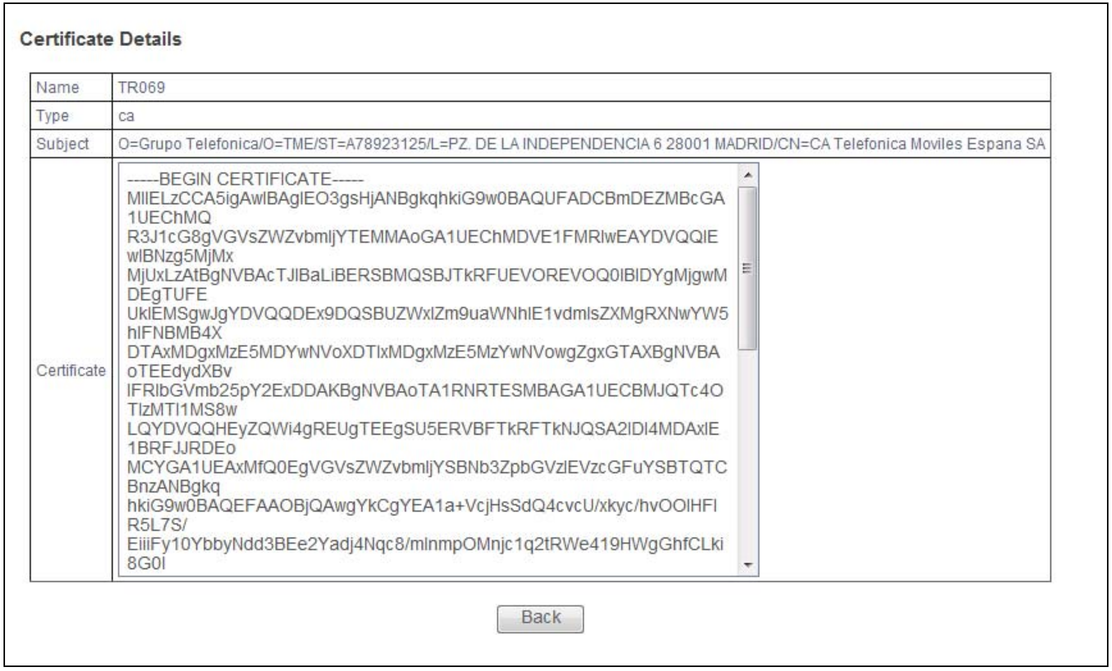
Table 79 Trusted CA

LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click the **View** button to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Remove** button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Router.

17.2.1 View Trusted CA Certificate

Click the **View** icon in the **Trusted CA** screen to open the following screen. Use this screen to view in-depth information about the certification authority's certificate.

Figure 87 Trusted CA: View



Certificate Details

Name	TR069
Type	ca
Subject	O=Grupo Telefonica/O=TME/ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/CN=CA Telefonica Moviles Espana SA

Certificate

```
-----BEGIN CERTIFICATE-----
MIIELzCCA5igAwIBAgIEO3gsHjANBgkqhkiG9w0BAQUFADCBmDEZMBcGA
1UEChMQ
R3J1cG8gVGVsZWZvbmljYTEMMAoGA1UEChMDVE1FMRIwEAYDVQQIE
wIBNzg5MjMx
MjUxLzAtBgNVBAcTJIBaLiBERSBMQSBJTkRFUEVOREVOQ0lBIDYgMjgwM
DEgTUFE
UklEMSgwJgYDVQQDEx9DQSBUZWxlZm9uaWNhIE1vdmlsZXMgRXNwYW5
hIFNBMB4X
DTAxMDgxMzE5MDYwNVoXDTIxMDgxMzE5MzYwNVowgZgxGTAXBgNVBA
oTEEdydXBv
IFRlbGVmb25pY2ExDDAKBgNVBAoTA1RNRTESMBAGA1UECBMJQTc4O
TIzMTI1MS8w
LQYDVQQHEyZQWi4gREUgTEEgSU5ERVBFTkRFTkNJQSA2IDI4MDAxIE
1BRFJJRDEo
MCYGA1UEAxMfQ0EgVGVsZWZvbmljYSBNb3ZpbGVzIEVzcGFuYSBTQTC
BnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA1a+VcjHsSdQ4cvcU/xkyc/hvOOlHFI
R5L7S/
EiiiFy10YbbyNdd3BEe2Yadj4Nqc8/mInmpOMnjc1q2tRWe419HWgGhfCLki
8G0I
```

The following table describes the fields in this screen.

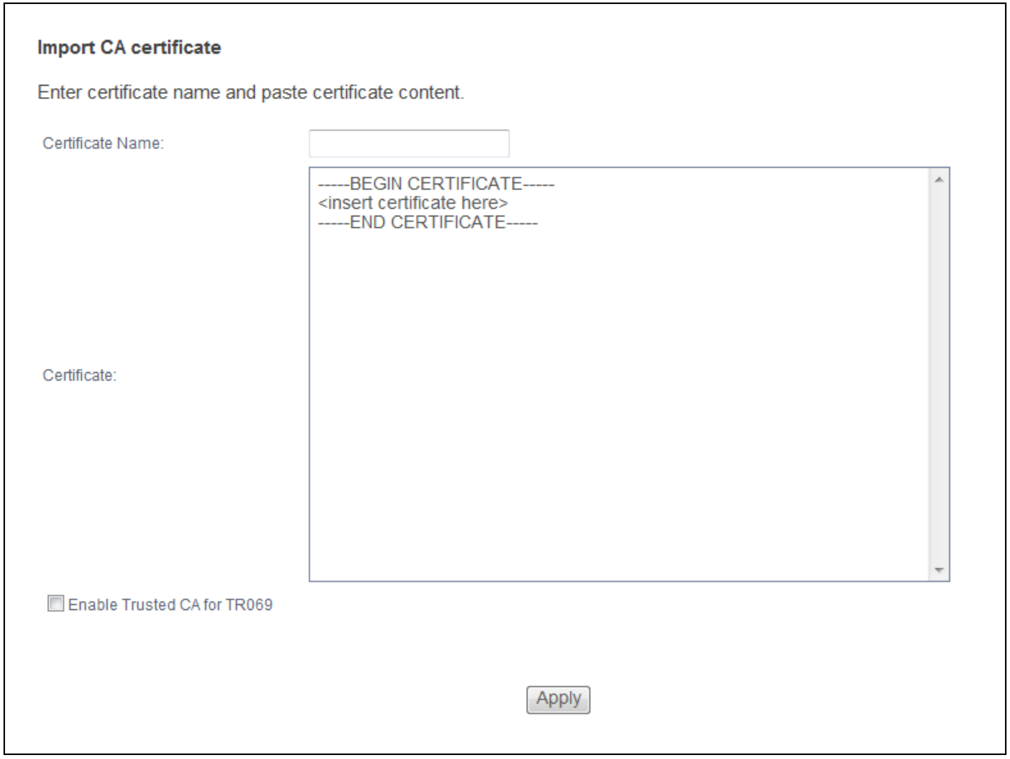
Table 80 Trusted CA: View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Certificate	This read-only text box displays the certificate in Privacy Enhanced Mail (PEM) format. PEM uses base 64 to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click **Back** to return to the previous screen.

17.2.2 Import Trusted CA Certificate

Click the **Trusted CA** screen's **Import Certificate** button to open the following screen. The Router trusts any valid certificate signed by any of the imported trusted CA certificates.

Figure 88 Trusted CA: Import Certificate



Import CA certificate

Enter certificate name and paste certificate content.

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<insert certificate here>
-----END CERTIFICATE-----
```

□ Enable Trusted CA for TR069

The following table describes the fields in this screen.

Table 81 Trusted CA: Import Certificate

LABEL	DESCRIPTION
Certificate Name	Type a name for the signed certificate.
Certificate	Copy and paste the certificate into the text box to store it on the Router.
Enable Trusted CA for TR069	Select this to have the Router use this trusted CA certificate to authenticate TR069 connections.
Apply	Click this to save your changes.

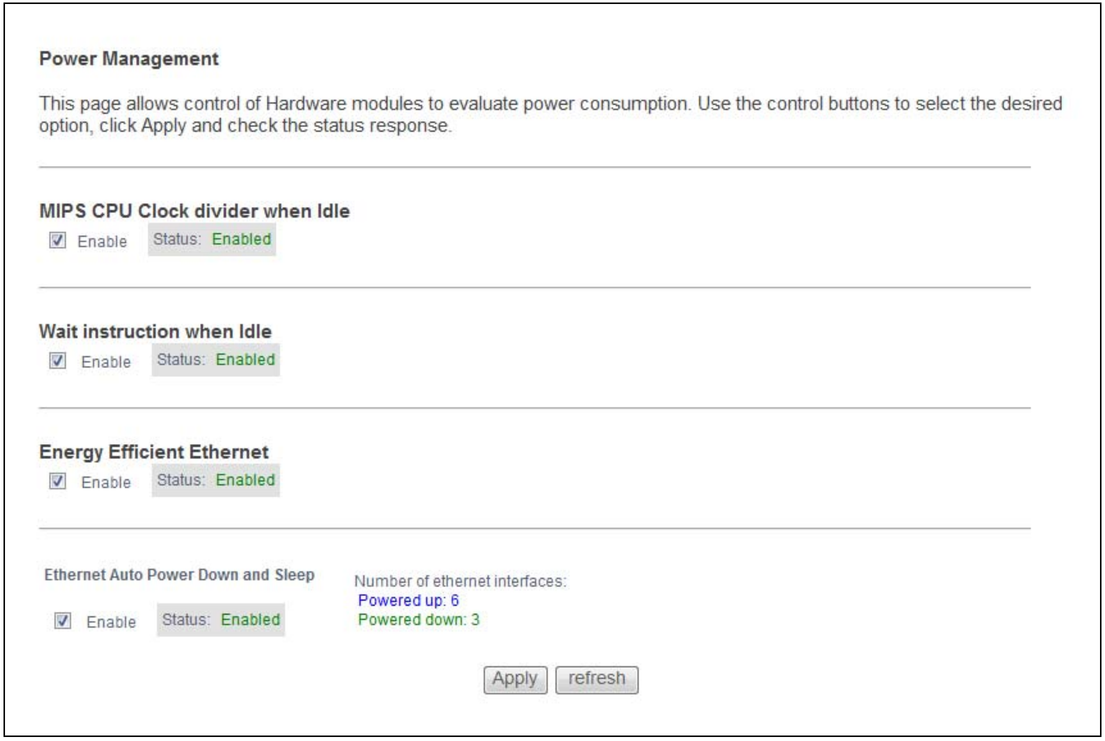
Power Management

18 Chapter

18.1 Power Management

Click **Advanced Setup > Power Management** to control hardware modules to reduce power consumption. Use the control buttons to select the desired option, click **Apply** and check the status response.

Figure 89 Power Management



Power Management

This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

MIPS CPU Clock divider when Idle

☑ Enable Status: Enabled

Wait instruction when Idle

☑ Enable Status: Enabled

Energy Efficient Ethernet

☑ Enable Status: Enabled

Ethernet Auto Power Down and Sleep

☑ Enable Status: Enabled

Number of ethernet interfaces:
Powered up: 6
Powered down: 3

Table 82 Power Management

LABEL	DESCRIPTION
MIPS CPU Clock divider when Idle	Select **Enable** to reduce the MIPS CPU's clock when idle to reduce power usage. Clear this to always run the MIPS CPU at full speed.
Wait instruction when Idle	Select **Enable** to put the CPU to sleep when idle to reduce power usage. Clear this to always keep the CPU running.
Energy Efficient Ethernet	Select **Enable** to set the Ethernet interfaces to power saving mode. Clear this to turn off power saving on the Ethernet interfaces.
Ethernet Auto Power Down and Sleep	Select **Enable** to power down Ethernet interfaces when idle to reduce power usage. Clear this to keep the Ethernet interfaces always on. The screen shows how many Ethernet interfaces are running and how many are powered down.
Apply	Click this button to save and apply your changes.
Refresh	Click this button to update the display in this screen.

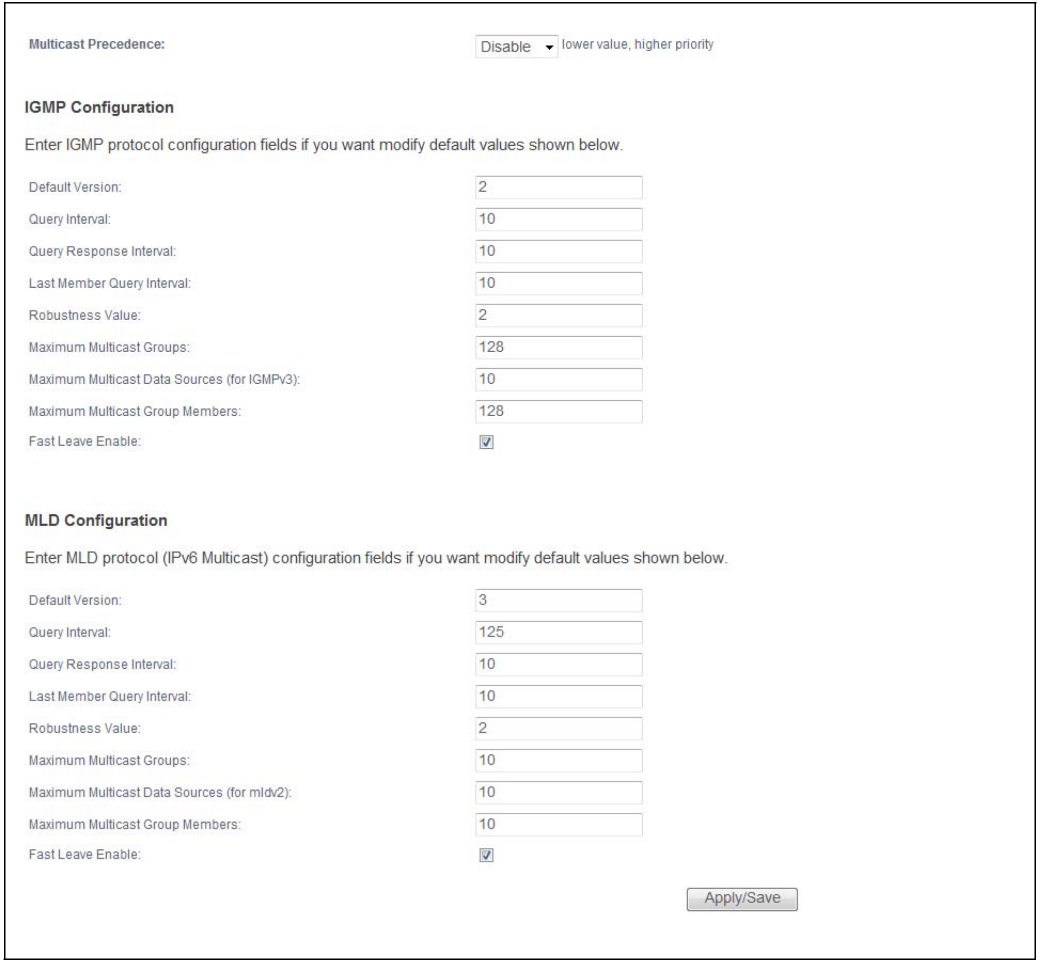
Multicast

19 Chapter

19.1 Multicast

Click **Advanced Setup > Multicast** to configure multicast and IGMP and MLD group settings.

Figure 90 Multicast



Multicast Precedence:	Disable ▾ lower value, higher priority

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	2
Query Interval:	10
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	128
Maximum Multicast Data Sources (for IGMPv3):	10
Maximum Multicast Group Members:	128
Fast Leave Enable:	☑

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	3
Query Interval:	125
Query Response Interval:	10
Last Member Query Interval:	10
Robustness Value:	2
Maximum Multicast Groups:	10
Maximum Multicast Data Sources (for mldv2):	10
Maximum Multicast Group Members:	10
Fast Leave Enable:	☑

Table 83 Multicast

LABEL	DESCRIPTION
Multicast Precedence	Set the Router's multicast precedence (1 to 9) or disable multicast on the Router. The lower the number, the higher the Router's multicast priority.
IGMP/MLD Configuration	
Default Version	Enter the version of IGMP (1~3) and MLD (1~2) that you want the Router to use on the WAN.
Query Interval	Specify how many seconds since the last query the Router waits before it queries all directly connected networks to gather multicast group membership.
Query Response Interval	Enter the maximum number of seconds the Router can wait to receive a General Query message. Multicast routers use general queries to learn which multicast groups have members.
Last Member Query Interval	Enter the maximum number of seconds the Router can wait for receiving a response to a Group-Specific Query message. Multicast routers use group-specific queries to learn whether any member remains in a specific multicast group.
Robustness Value	Enter the number of times (1~7) the Router can resend a packet if packet loss occurs due to network congestion.
Maximum Multicast Groups	Enter a number to limit the number of multicast groups an interface on the Router is allowed to join. Once a multicast member is registered in the specified number of multicast groups, any new IGMP or MLD join report frames are dropped by the interface.
Maximum Multicast Data Sources	Enter a number to limit the number of multicast data sources (1-24) a multicast group is allowed to have. Note: The setting only works for IGMPv3 and MLDv2.
Maximum Multicast Group Members	Enter a number to limit the number of multicast members a multicast group can have.
Fast Leave Enable	Select this option to set the Router to remove a port from the multicast tree immediately (without sending an IGMP or MLD membership query message) once it receives an IGMP or MLD leave message. This is helpful if a user wants to quickly change a TV channel (multicast group change) especially for IPTV applications.
Apply/Save	Click this button to save your changes.

Wireless

20 Chapter

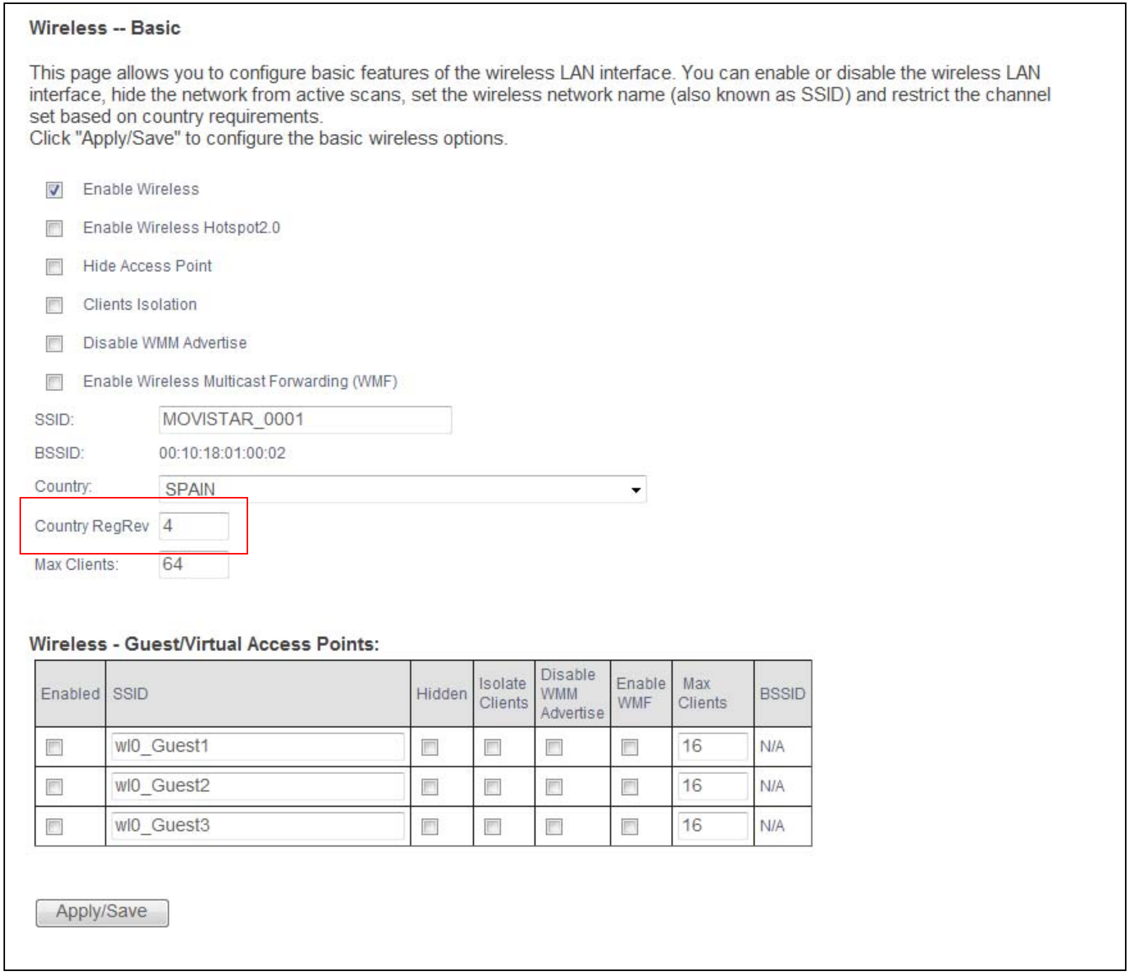
20.1 Wireless Basic

Use the **Advanced Setup > Wireless** screens to configure the 2.4 GHz wireless network.

Click **Advanced Setup > Wireless** to enable or disable the 2.4 GHz Wireless LAN and configure basic settings.

ⓘ If you are configuring the Router from a computer connected to the wireless LAN and you change the Router’s SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Router’s new settings.

Figure 91 Wireless Basic



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/Save" to configure the basic wireless options.

☑ Enable Wireless

□ Enable Wireless Hotspot2.0

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise

□ Enable Wireless Multicast Forwarding (WMF)

SSID:	MOVISTAR_0001
BSSID:	00:10:18:01:00:02
Country:	SPAIN
Country RegRev	4
Max Clients:	64

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	wl0_Guest1	□	□	□	□	16	N/A
□	wl0_Guest2	□	□	□	□	16	N/A
□	wl0_Guest3	□	□	□	□	16	N/A

Table 84 Wireless Basic

LABEL	DESCRIPTION
Enable Wireless	Select this check box to activate the wireless LAN.
Enable Wireless Hotspot2.0	
Hide Access Point	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Clients Isolation	Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router.
Disable WMM Advertise	WMM (Wifi MultiMedia) automatically prioritizes services according to the ToS value in the IP header of packets. Turn off WMM if your wireless clients are not able to associate with an AP using WMM.

Table 84 Wireless Basic (continued)

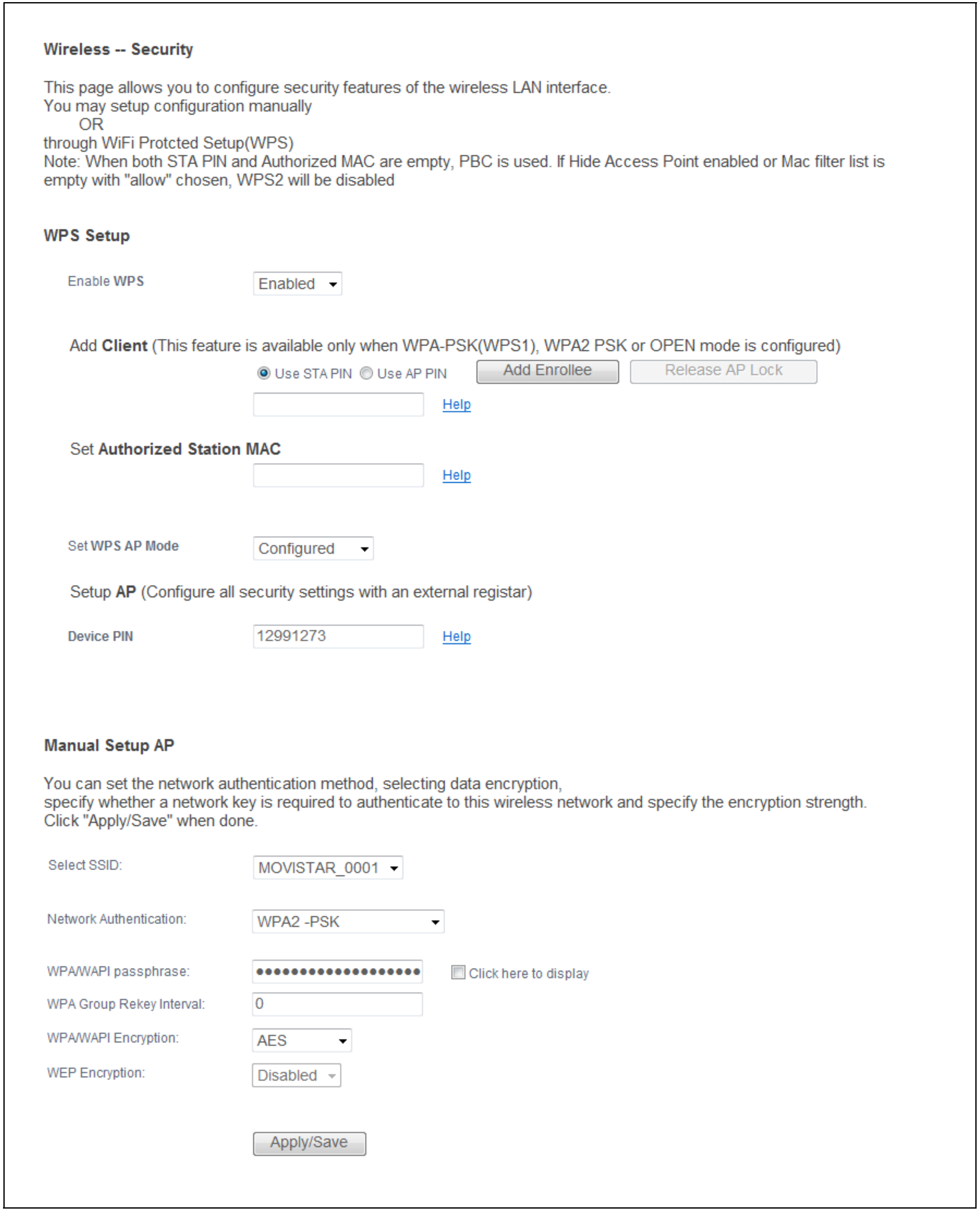
LABEL	DESCRIPTION
Enable Wireless Multicast Forwarding	Select this check box to have the Router convert wireless multicast traffic (IGMP version 2 or 3) into wireless unicast traffic to reduce the traffic load. This function can improve the transmission quality of video services (for example, IPTV).
SSID	Enter a descriptive name for the wireless LAN.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Country	Select the country you have the Router in. This has the Router use the correct frequency bands.
Country RegRev	Specify the sub-revision of the regulatory locale table for the country code.
Max Clients	Set a limit for how many wireless clients can connect to the Router at a time.
Wireless Guest/ Virtual Access Points	Use this section to enable and configure multiple wireless networks on the Router.
Enabled	Select this to activate the wireless network.
SSID	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the Router from a computer connected to the wireless LAN and you change the Router’s SSID or WEP settings, you will lose your wireless connection when you press **Save/Apply** to confirm. You must then change the wireless settings of your computer to match the Router’s new settings.
Hidden	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Isolate Clients	Select this to isolate wireless clients from accessing others in the same wireless network.
Enable WMF	Select this check box to improve the wireless transmission quality for multicast frames. It is recommended to select this for video streaming application.
Max Clients	Set a limit for how many wireless clients can connect to the wireless network at a time.
BSSID	This shows the MAC address of the wireless network on the Device when the wireless network is enabled.
Apply/Save	Click this button to save your changes.

20.2 Wireless Security

Click **Wireless > Security** to open the **Security** screen. Set **Network Authentication** to **Open** and **WEP Encryption** to **Disabled** to allow wireless stations to communicate with the Router without any data encryption or authentication.

ⓘ If you do not enable any wireless security on your Router, your network is accessible to any wireless networking device that is within range.

Figure 92 Wireless Security



Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protcted Setup(WPS)
Note: When both STA PIN and Authorized MAC are empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled

WPS Setup

Enable **WPS**: Enabled

Add **Client** (This feature is available only when WPA-PSK(WPS1), WPA2 PSK or OPEN mode is configured)

● Use STA PIN ○ Use AP PIN

Set **Authorized Station MAC**

Set **WPS AP Mode**: Configured

Setup **AP** (Configure all security settings with an external registar)

Device PIN: 12991273

Manual Setup AP

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.
Click "Apply/Save" when done.

Select SSID:	MOVISTAR_0001
Network Authentication:	WPA2 -PSK
WPA/WAPI passphrase:	●●●●●●●●●●●●●●●●●●●● □ Click here to display
WPA Group Rekey Interval:	0
WPA/WAPI Encryption:	AES
WEP Encryption:	Disabled

Table 85 Wireless Security

LABEL	DESCRIPTION
Enable WPS	Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time.
Add Client	Use this section to add a wireless client to the wireless network. Select **Use STA PIN** to add a client by entering the client's Personal Identification Number (PIN) in the field that displays when you select this option. Select **Use AP PIN** to add a client by entering the AP's PIN from the **Device PIN** field in the client's WPS configuration.
Add Enrollee	Click this to use WPS to add a wireless client to your wireless network. Note: You must also activate WPS on the client within two minutes.
Release AP Lock	Click this to unlock the Router's AP function if WPS locked it due to unauthorized wireless access attempts.
Set Authorized Station MAC	If you select **Enter STA PIN** as your method to add a client, you may enter the MAC address of an authorized wireless client here.
Set WPS AP Mode	**Configured** uses the Router's current wireless security settings for WPS. **Unconfigured** has the Router change its wireless security settings when you do one of the following: • Add a wireless enrollee. The Router automatically uses WPA2-PSK and a random key. The **WPS AP Mode** automatically changes to **Configured**. • Use **Setup AP** to have an external registrar (like Windows Vista) configure the Router's wireless security settings. The **WPS AP Mode** automatically changes to **Configured**. • Manually configure the Router's wireless security settings. Then you can manually set the **WPS AP Mode** to **Configured**.
Device PIN	This shows the Router's PIN. Enter this PIN in the external registrar within two minutes of clicking **Generate PIN**. Enter this PIN in the client's WPS configuration if you selected **Use AP PIN**.
Select SSID	Select an SSID for which to configure wireless security settings.
Network Authentication	Use the strongest authentication method that the wireless clients all support. **WPA2-PSK** uses a common password for all clients. **Mixed WPA2/WPA -PSK** supports WPA2-PSK and WPA-PSK simultaneously. While WPA2-PSK offers stronger security, more wireless clients support WPA-PSK. **Shared** - encrypts the wireless communications using a shared (WEP) password. Choose **Open** to allow all wireless connections without authentication.

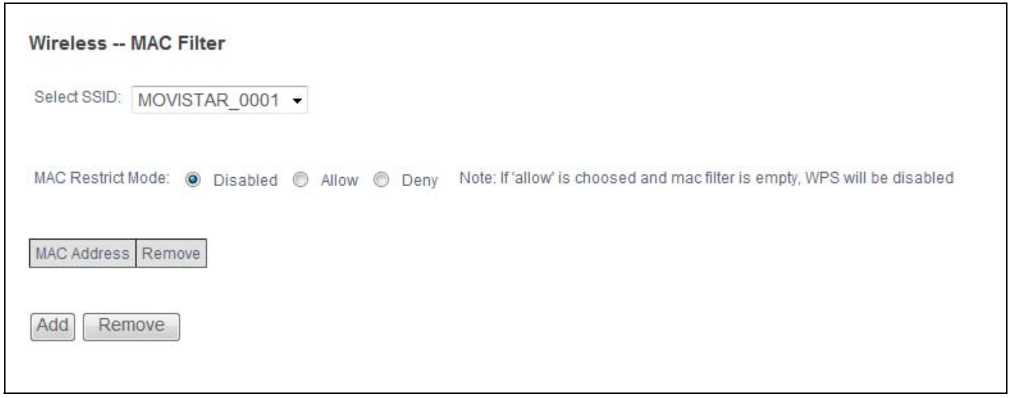
Table 85 Wireless Security

LABEL	DESCRIPTION
WPA/WAPI passphrase	This field displays when you select WPA2-PSK or Mixed WPA2/WPA -PSK. Use the automatically generated password or enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. Click the link to display the password.
WPA Group Rekey Interval	Set the rate at which the AP (if using WPA2/WPA-PSK key management) or RADIUS server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.
WPA/WAPI Encryption	Select the encryption type (**AES** or **TKIP+AES**) for data encryption. Select **AES** if your wireless clients can all use AES. Select **TKIP+AES** to allow the wireless clients to use either TKIP or AES.
WEP Encryption	This field displays when you set **Network Authentication** to **Open**. Enable WEP encryption to scramble the wireless data transmissions between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key. Note: WEP is extremely insecure. Attackers can break it using widely-available software. It is strongly recommended that you use a more effective security mechanism.
Encryption Strength	If you are using WEP encryption, select **64-bit** or **128-bit** to set the length of the encryption key.
Current Network Key	This field displays when you enable WEP encryption. Configure up to four 64-bit or 128-bit WEP keys. Use this field to select which one the network uses.
Network Key 1~4	These fields display when you enable WEP encryption. WEP uses a network key to encrypt data. The Router and wireless clients must use the same network key (password). If you chose **64-bit** WEP, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit** WEP, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). You must configure at least one password.
Apply/Save	Click this button to save your changes.

20.3 Wireless MAC Filter

Click **Wireless > MAC Filter** to open the **MAC Filter** screen. This screen allows you to configure the Router to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Router **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address assigned at the factory. It consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Figure 93 Wireless MAC Filter



Wireless -- MAC Filter

Select SSID: MOVISTAR_0001

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny Note: If 'allow' is choosed and mac filter is empty, WPS will be disabled

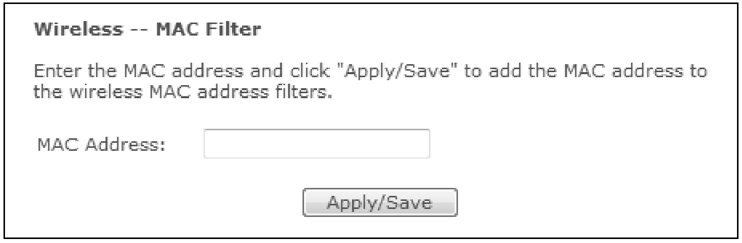
Table 86 Wireless MAC Filter

LABEL	DESCRIPTION
Select SSID	Select an SSID for which to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disabled** to turn off MAC filtering. Select **Allow** to permit access to the Router. MAC addresses not listed will be denied access to the Router. Select **Deny** to block access to the Router. MAC addresses not listed will be allowed to access the Router.
MAC Address	This displays the MAC addresses of the wireless devices that are allowed or denied access to the Router.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to add a new MAC address entry to the table.

20.3.1 Wireless MAC Filter Add

Use this screen to add MAC address entries. Click **Wireless > MAC Filter > Add** to open the following screen.

Figure 94 Wireless MAC Filter Add



Wireless -- MAC Filter

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

MAC Address:

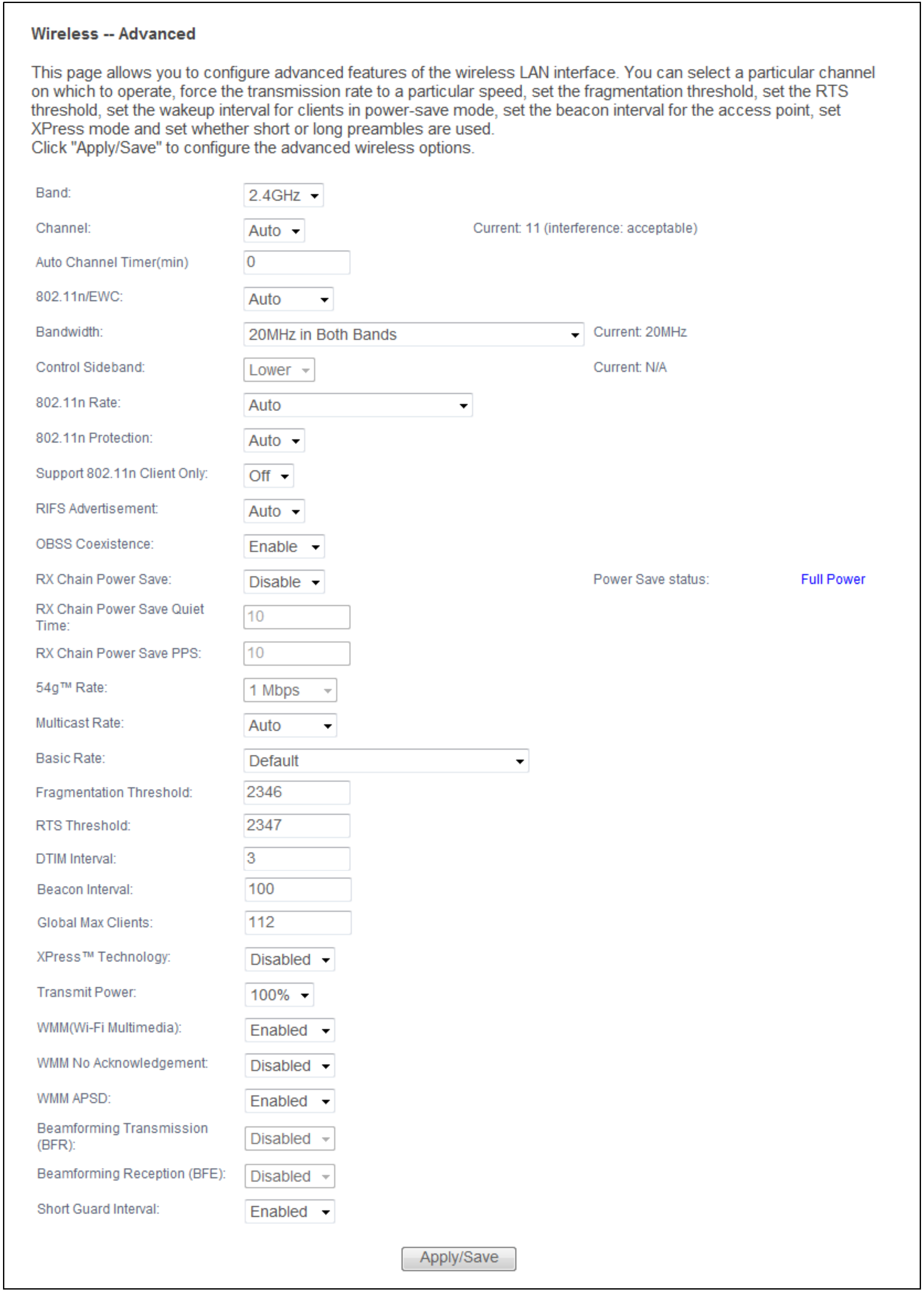
Table 87 Wireless MAC Filter Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of the wireless device that is to be allowed or denied access to the Router. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Save/Apply	Click this button to save the changes and have the Router start using them.

20.4 Wireless Advanced

Click **Wireless > Advanced** to configure advanced wireless settings.

Figure 95 Wireless Advanced



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/Save" to configure the advanced wireless options.

Band:	2.4GHz		
Channel:	Auto	Current: 11 (interference: acceptable)	
Auto Channel Timer(min)	0		
802.11n/EWC:	Auto		
Bandwidth:	20MHz in Both Bands	Current: 20MHz	
Control Sideband:	Lower	Current: N/A	
802.11n Rate:	Auto		
802.11n Protection:	Auto		
Support 802.11n Client Only:	Off		
RIFS Advertisement:	Auto		
OBSS Coexistence:	Enable		
RX Chain Power Save:	Disable	Power Save status:	Full Power
RX Chain Power Save Quiet Time:	10		
RX Chain Power Save PPS:	10		
54g™ Rate:	1 Mbps		
Multicast Rate:	Auto		
Basic Rate:	Default		
Fragmentation Threshold:	2346		
RTS Threshold:	2347		
DTIM Interval:	3		
Beacon Interval:	100		
Global Max Clients:	112		
XPress™ Technology:	Disabled		
Transmit Power:	100%		
WMM(Wi-Fi Multimedia):	Enabled		
WMM No Acknowledgement:	Disabled		
WMM APSD:	Enabled		
Beamforming Transmission (BFR):	Disabled		
Beamforming Reception (BFE):	Disabled		
Short Guard Interval:	Enabled		

Table 88 Wireless Advanced

LABEL	DESCRIPTION
Band	Select an operating band to use.
Channel	Select an operating channel to use. The choices depend on your particular region. Either select a channel or use **Auto** to have the Router automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible.
Auto Channel Timer	If you set the channel to **Auto**, specify the interval in minutes for how often the Router scans for the best channel. Enter 0 to disable the periodical scan.
802.11n/EWC	Select whether to enable (**Auto**) or disable (**Disabled**) the use of the wireless 802.11n modes defined by the Enhanced Wireless Consortium (EWC). These modes can enhance speeds although the wireless clients must also support the EWC modes.
Bandwidth	**20MHz in Both Bands** uses a single radio channel in the 2.4 GHz band and a single radio channel in the 5.0 GHz band. Use this if the wireless clients do not support channel bonding. **40MHz in Both Bands** bonds two adjacent radio channels in the 2.4 GHz band and two adjacent radio channels in the 5.0 GHz band. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. **20MHz in 2.4G Band and 40MHz in 5G Band** uses a single radio channel in the 2.4 GHz band and bonds two adjacent radio channel in the 5.0 GHz band. Use this if you have IEEE 802.11b and/or g clients that do not support 40 MHz and IEEE 802.11n clients that do.
Control Sideband	This is available for some regions when you select a specific channel and set the **Bandwidth** field to **40MHz in Both Bands**. Set whether the control channel (set in the **Channel** field) should be in the **Lower** or **Upper** range of channel bands.
802.11n Rate	Select a fixed transmission rate or select **Auto** to have the system configure it automatically.
802.11n Protection	Enable this feature to help prevent collisions in mixed-mode networks (networks with both IEEE 802.11n and IEEE 802.11g traffic). Select **Auto** to have the wireless devices transmit data after a RTS/CTS handshake. This helps improve IEEE 802.11n performance. Select **Off** to disable IEEE 802.11n protection. The transmission rate of your Router might be reduced in a mixed-mode network.
Support 802.11n Client Only	Select this to only allow IEEE 802.11n wireless clients to connect to the Router. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the Router.
RIFS Advertisement	Select **Auto** to enable the Reduced Inter-frame Spacing (RIFS) feature. It improves the Router’s performance by reducing the amount of dead time required between OFDM transmissions.

Table 88 Wireless Advanced (continued)

LABEL	DESCRIPTION
OBSS Co-Existance	Select **Enable** to allow coexistence between 20 MHZ and 40 MHZ Overlapping Basic Service Sets (OBSS) in wireless local area networks.
RX Chain Power Save	Select **Enable** to activate the RX Chain Power Save feature. It turns off one of the Receive chains to save power.
RX Chain Power Save Quiet Time	Specify the number of seconds the traffic must be below the PPS value before the Rx Chain Power Save feature is activated.
RX Chain Power Save PPS	Specify the maximum number of packets per second that can be processed by the WLAN interface for a time period (specified in the **RX Chain Power Save Quiet Time** field) before the Rx Chain Power Save feature is activated.
54g™ Rate	This field is available when **802.11n/EWC** is set to **Disabled**. Select a fixed wireless transmission rate or let the Router and the wireless client automatically select a rate.
Multicast Rate	Select a data rate at which the Router transmits wireless multicast traffic. If you select a high rate, multicast traffic may occupy all the bandwidth and cause network congestion.
Basic Rate	Select a minimum transmission rate.
Fragmentation Threshold	This is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
RTS Threshold	Use CTS/RTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions). A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS equal to or higher than the fragmentation threshold to turn RTS off.
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
Global Max Clients	Specify the maximum number (from 1 to 64) of the wireless stations that may connect to the Router.
XPress™ Technology	Select this for higher speeds, especially if you have both IEEE 802.11b and IEEE 802.11g wireless clients. The wireless clients do not have to support XPress™ Technology, although the performance enhancement is greater if they do.

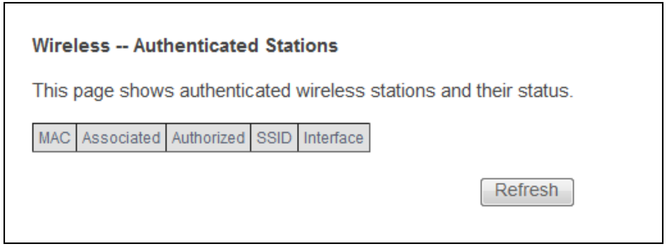
Table 88 Wireless Advanced (continued)

LABEL	DESCRIPTION
Transmit Power	Set the output power of the Router. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs.
WMM (Wi-Fi Multimedia)	Use WMM (Wifi MultiMedia) to prioritize services in wireless traffic. Select **Auto** to automatically prioritize services according to the ToS value in the IP header of packets. Select **Enable** to prioritize services according to the Router's Quality of Service settings. Select **Disable** to not prioritize services in wireless traffic.
WMM No Acknowledgement	When using WMM, you can enable this to have the Router not re-send data if an error occurs. This can increase throughput speed but may also increase errors, especially in an environment with a lot of Radio Frequency (RF) noise. Otherwise leave it disabled.
WMM APSD	When using WMM, enable APSD (Automatic Power Save Delivery) to have the Router manage radio usage to help increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval. For example, web browsing or using e-mail does not require a short packet exchange interval but Voice Over IP (VoIP) does. The wireless client must also support APSD for there to be any affect on the battery life.
Beamforming Transmission	Enable beamforming to have the Router focus the wireless signal and aim it directly at the wireless clients. Clear this option to disable beamforming. You may need to do this if beamforming causes issues with IEEE 802.11 N, G, or B devices.
Short Guard Interval	Enable short guard interval option to set the Router to use a reduced guard interval. This increases throughput at the cost of an increased error rate in certain network environments with greater radio interference.
Apply/Save	Click this to save your changes back to the Router.

20.5 Wireless Station Info

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) the Router. To open the station monitor, click **Wireless** > **Station Info**. The screen appears as shown.

Figure 96 Wireless Station Info



Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

The following table describes the labels in this menu.

Table 89 Wireless Station Info

LABEL	DESCRIPTION
MAC	This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station.
Associated	This is the time that the wireless client associated with the Router.
Authorized	This is the time that the wireless client’s connection to the Router was authorized.
SSID	This is the name of the wireless network on the Router to which the wireless client is connected.
Interface	This is the name of the wireless LAN interface on the Router to which the wireless client is connected.
Refresh	Click this button to update the information in the screen.

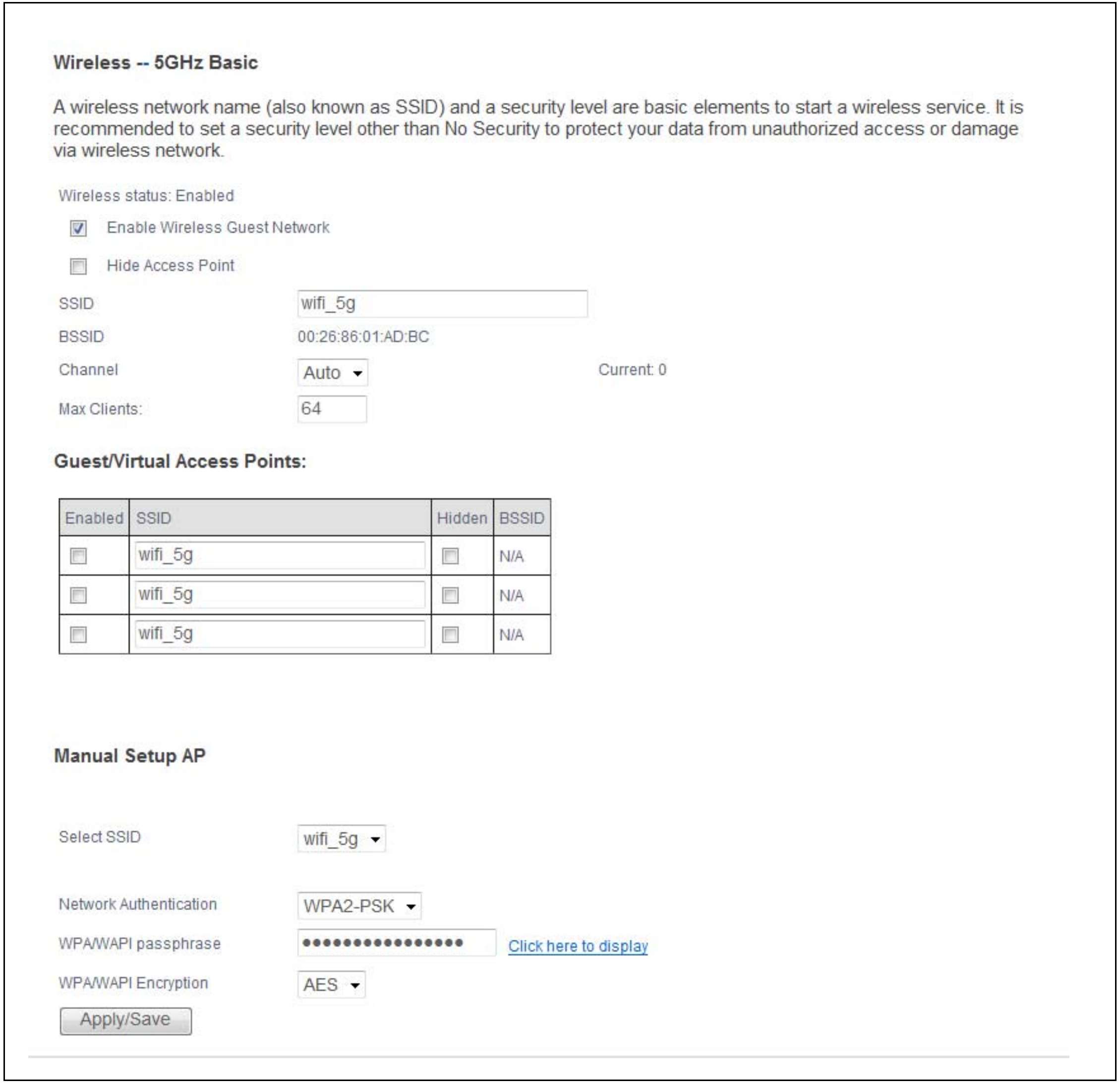
20.6 Wireless 5GHz Basic

Use the **Advanced Setup > Wireless 5GHz** screens to configure the 5 GHz wireless network.

Click **Advanced Setup > Wireless 5GHz** to enable the 5 GHz Wireless LAN and set the wireless security.

If you are configuring the Router from a computer connected to the wireless LAN and you change the Router's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Router's new settings.

Figure 97 Wireless 5GHz Basic



Wireless -- 5GHz Basic

A wireless network name (also known as SSID) and a security level are basic elements to start a wireless service. It is recommended to set a security level other than No Security to protect your data from unauthorized access or damage via wireless network.

Wireless status: Enabled

☑ Enable Wireless Guest Network

□ Hide Access Point

SSID	wifi_5g	
BSSID	00:26:86:01:AD:BC	
Channel	Auto ▾	Current: 0
Max Clients:	64	

Guest/Virtual Access Points:

Enabled	SSID	Hidden	BSSID
□	wifi_5g	□	N/A
□	wifi_5g	□	N/A
□	wifi_5g	□	N/A

Manual Setup AP

Select SSID	wifi_5g ▾	
Network Authentication	WPA2-PSK ▾	
WPA/WAPI passphrase	●●●●●●●●●●●●●●●●	Click here to display
WPA/WAPI Encryption	AES ▾	

Table 90 Wireless 5GHz Basic

LABEL	DESCRIPTION
Enable Wireless Guest Network	Select this check box to activate the guest wireless LAN.
Hide Access Point	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

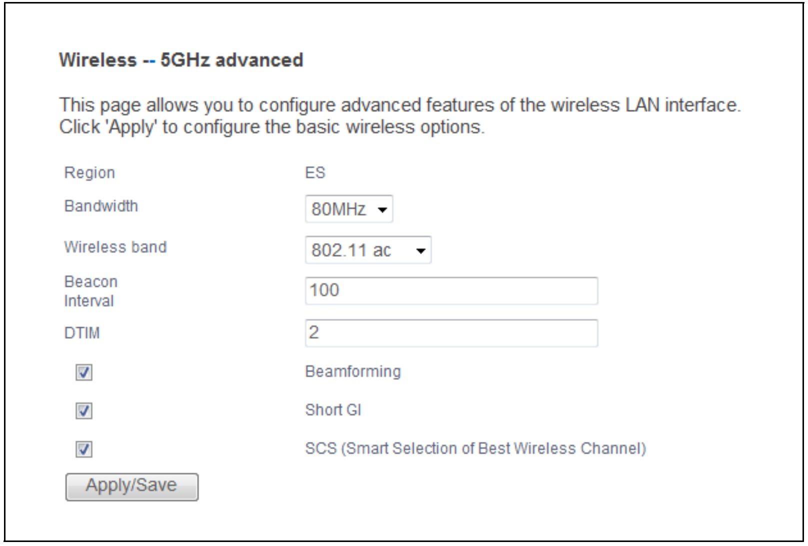
Table 90 Wireless 5GHz Basic (continued)

LABEL	DESCRIPTION
SSID	Enter a descriptive name for the wireless LAN.
BSSID	This shows the MAC address of the wireless interface on the Device when wireless LAN is enabled.
Country	Select the country you have the Router in. This has the Router use the correct frequency bands.
Channel	Select an operating channel to use. The choices depend on your particular region. Either select a channel or use **Auto** to have the Router automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible.
Max Clients	Set a limit for how many wireless clients can connect to the Router at a time.
Guest/Virtual Access Points	Use this section to enable and configure multiple wireless networks on the Router.
Enabled	Select this to activate the wireless network.
SSID	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Note: If you are configuring the Router from a computer connected to the wireless LAN and you change the Router's SSID or WEP settings, you will lose your wireless connection when you press **Save/Apply** to confirm. You must then change the wireless settings of your computer to match the Router's new settings.
Hidden	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless network on the Device when the wireless network is enabled.
Select SSID	Select an SSID for which to configure wireless security settings.
Network Authentication	Use the strongest authentication method that the wireless clients all support. **WPA2-PSK** uses a common password for all clients. While WPA2-PSK offers stronger security, more wireless clients support WPA-PSK. Choose **Open** to allow all wireless connections without authentication.
WPA/WAPI passphrase	This field displays when you select WPA2-PSK Use the automatically generated password or enter 16 to 63 alphanumeric characters (0-9, A-Z, with no spaces). It must contain both letters and numbers and is case-sensitive. Click the link to display the password.
WPA/WAPI Encryption	Select the encryption type for data encryption. Select **AES** if your wireless clients can all use AES.
Apply/Save	Click this button to save your changes.

20.7 Wireless 5GHz Advanced Screen

Click **Wireless 5GHz > Advanced** to configure advanced 5 GHz wireless settings.

Figure 98 Wireless 5GHz Advanced



Wireless -- 5GHz advanced

This page allows you to configure advanced features of the wireless LAN interface.
Click 'Apply' to configure the basic wireless options.

Region	ES
Bandwidth	80MHz ▾
Wireless band	802.11 ac ▾
Beacon Interval	100
DTIM	2
☑	Beamforming
☑	Short GI
☑	SCS (Smart Selection of Best Wireless Channel)

Table 91 Wireless 5GHz Advanced

LABEL	DESCRIPTION
Region	Select an operating band to use.
Bandwidth	Select whether the Device uses a wireless channel width of 20MHz, 40MHz, or 80MHz. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps, and a 80MHz channel uses only one channel and offers speeds of up to 433 Mbps. A wider band enables higher transmission rates. A 40MHz (channel bonding or dual channel) channel bonds two adjacent radio channels to increase throughput. An 80MHz channel bonds two adjacent 40 MHz channels to get even higher data rates. The wireless clients must also support 40 MHz or 80 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. Select **20MHz** to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding.
Wireless band	Select whether to use IEEE 802.11 ac or IEEE 802.11 ac and IEEE 802.11n wireless.
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.

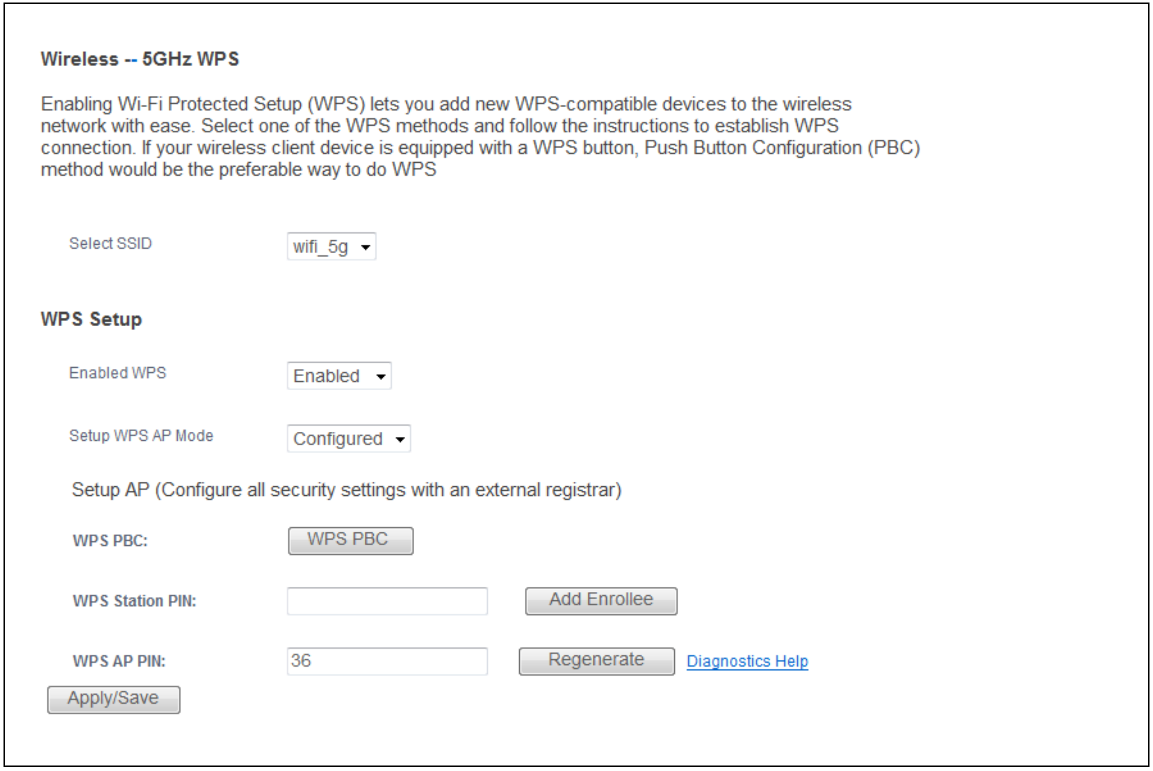
Table 91 Wireless 5GHz Advanced (continued)

LABEL	DESCRIPTION
DTIM	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
Beamforming	Select this option to have the Router focus the wireless signal and aim it directly at the wireless clients. Clear this option to disable beamforming. You may need to do this if beamforming causes issues with IEEE 802.11 N, G, or B devices.
Short GI	Select this option to set the Router to use a reduced guard interval. This increases throughput at the cost of an increased error rate in certain network environments with greater radio interference.
SCS	Select this to have the Router automatically determine and select the most suitable wireless channel.
Apply/Save	Click this to save your changes back to the Router.

20.8 Wireless 5GHz WPS

Click **Wireless 5GHz > WPS** to open the **WPS** screen. Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease.

Figure 99 Wireless 5GHz WPS



Wireless -- 5GHz WPS

Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS

Select SSID: wifi_5g

WPS Setup

Enabled WPS: Enabled

Setup WPS AP Mode: Configured

Setup AP (Configure all security settings with an external registrar)

WPS PBC:

WPS Station PIN:

WPS AP PIN: 36

Table 92 Wireless 5GHz WPS

LABEL	DESCRIPTION
Enable WPS	Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time.
Add Client	Use this section to add a wireless client to the wireless network. Select **Use STA PIN** to add a client by entering the client's Personal Identification Number (PIN) in the field that displays when you select this option. Select **Use AP PIN** to add a client by entering the AP's PIN from the **Device PIN** field in the client's WPS configuration.
Add Enrollee	Click this to use WPS to add a wireless client to your wireless network. Note: You must also activate WPS on the client within two minutes.
Release AP Lock	Click this to unlock the Router's AP function if WPS locked it due to unauthorized wireless access attempts.
Set Authorized Station MAC	If you select **Enter STA PIN** as your method to add a client, you may enter the MAC address of an authorized wireless client here.

Table 92 Wireless 5GHz WPS (continued)

LABEL	DESCRIPTION
Select SSID	Select an SSID for which to configure security settings.
Enabled WPS	Use WiFi Protected Setup (WPS) to quickly set up a wireless network without having to manually configure settings. Set up each WPS connection between two devices at a time. WPS is not available when using WPA or WPA 2.
Setup WPS AP Mode	Use an external registrar (like Windows Vista) configure the Router's wireless security settings. The **WPS AP Mode** automatically changes to **Configured**.
WPS PBC	Click this to initiate push button configuration. Use PBC on each WPS-enabled device, and allow them to connect automatically. See Section 20.8.1 on page 159 for details.
WPS Station PIN	Add a client to the wireless network by entering the client's Personal Identification Number (PIN) in the field and clicking the **Add Enrollee** button. Note: You must also activate WPS on the client within two minutes.
WPS AP PIN	Add a client by entering the AP's PIN from this field in the client's WPS configuration. Click **Regenerate** to refresh it.
Apply/Save	Click this button to save your changes.

20.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1 Ensure that the two devices you want to set up are within wireless range of one another.

2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this).

3 Press the button on one of the devices (it doesn't matter which). For the Router you must press the WPS button for more than three seconds.

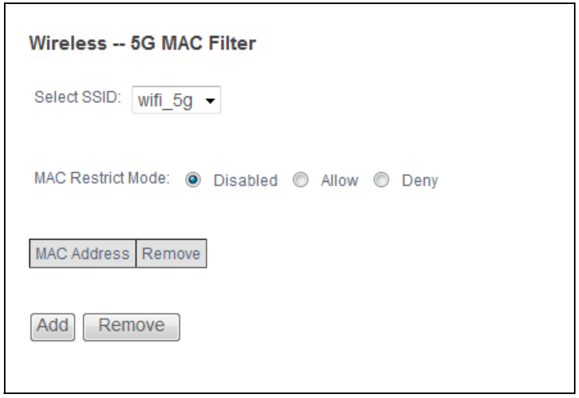
4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

20.9 Wireless 5GHz MAC Filter

Click **Wireless 5GHz > MAC Filter** to open the **MAC Filter** screen. This screen allows you to configure the Router to give exclusive access to specific devices **(Allow)** or exclude specific devices from accessing the Router **(Deny)**. Every Ethernet device has a unique MAC (Media Access Control) address assigned at the factory. It consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

Figure 100 Wireless 5GHz MAC Filter



Wireless -- 5G MAC Filter

Select SSID: wifi_5g

MAC Restrict Mode: ● Disabled ○ Allow ○ Deny

MAC Address	Remove

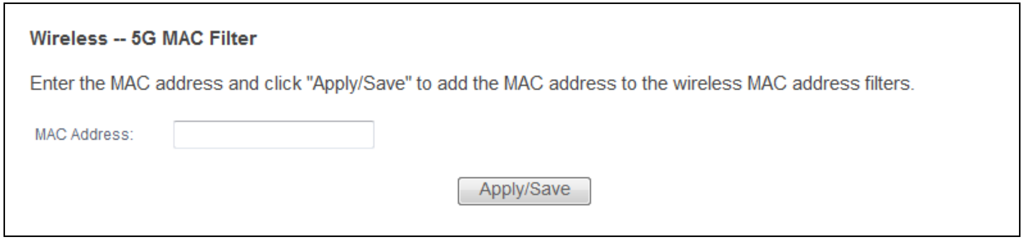
Table 93 Wireless 5GHz MAC Filter

LABEL	DESCRIPTION
Select SSID	Select an SSID for which to configure MAC filter settings.
MAC Restrict Mode	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Disabled** to turn off MAC filtering. Select **Allow** to permit access to the Router. MAC addresses not listed will be denied access to the Router. Select **Deny** to block access to the Router. MAC addresses not listed will be allowed to access the Router.
MAC Address	This displays the MAC addresses of the wireless devices that are allowed or denied access to the Router.
Remove	Select entries and click the **Remove** button to delete them.
Add	Click this to add a new MAC address entry to the table.

20.9.1 Wireless MAC Filter Add

Use this screen to add MAC address entries. Click **Wireless > MAC Filter > Add** to open the following screen.

Figure 101 Wireless MAC Filter Add



Wireless -- 5G MAC Filter

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

MAC Address:

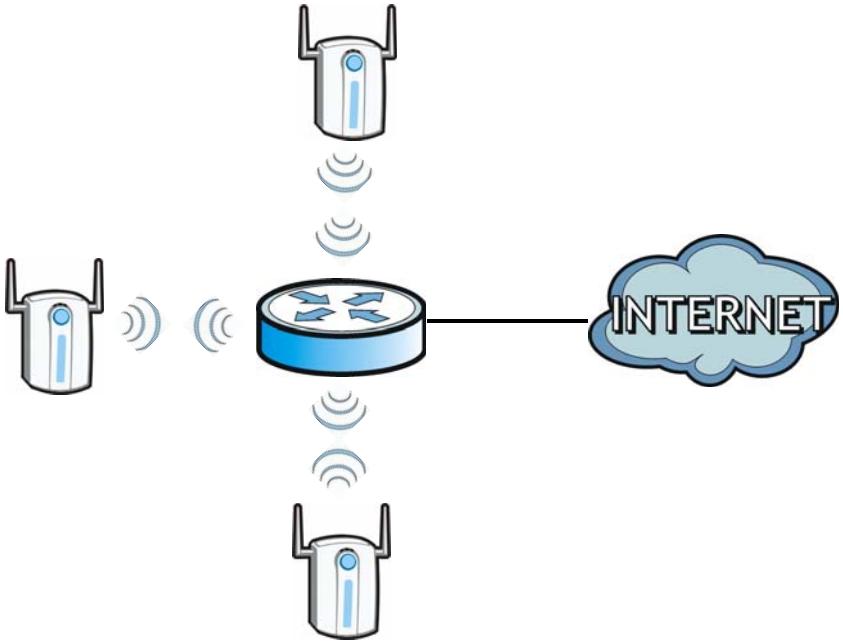
Table 94 Wireless MAC Filter Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of the wireless device that is to be allowed or denied access to the Router. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Save/Apply	Click this button to save the changes and have the Router start using them.

20.10 Wireless 5GHz Bridge

The Router can function as a wireless network bridge to wirelessly connect two or more APs.

Figure 102 Connecting Wireless Networks Using WDS



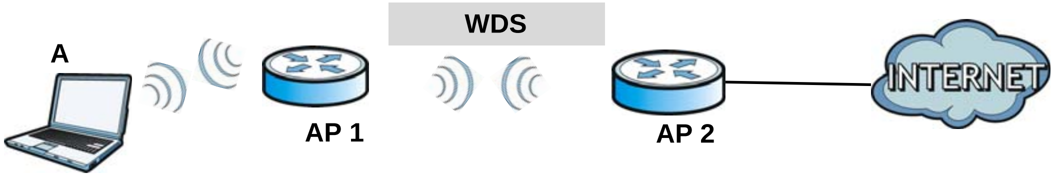
Use this screen to set up your Wireless Distribution System (WDS) links between the Router and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made.

Wireless Bridge Limitations

- At the time of writing, WDS is compatible with other APs of the same brand only. Not all models support WDS links.

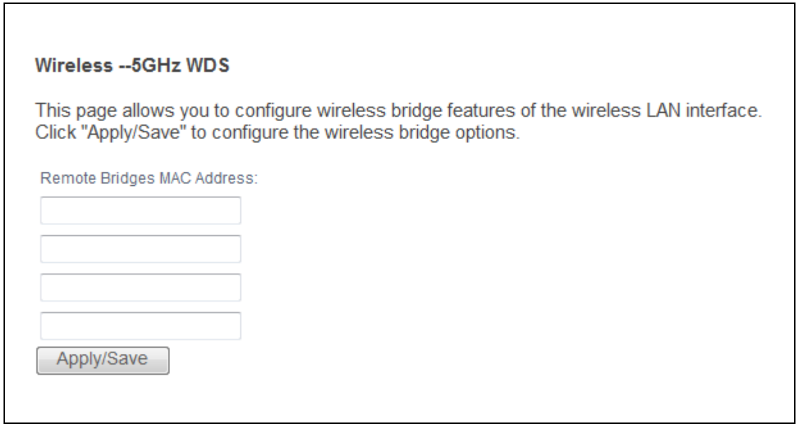
The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but can establish a WDS link with access point **AP 2**, which does. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

Figure 103 WDS Link Example



Click **Wireless 5GHz > Wireless Bridge** to display the following screen.

Figure 104 Wireless 5GHz Bridge



Wireless --5GHz WDS

This page allows you to configure wireless bridge features of the wireless LAN interface. Click "Apply/Save" to configure the wireless bridge options.

Remote Bridges MAC Address:

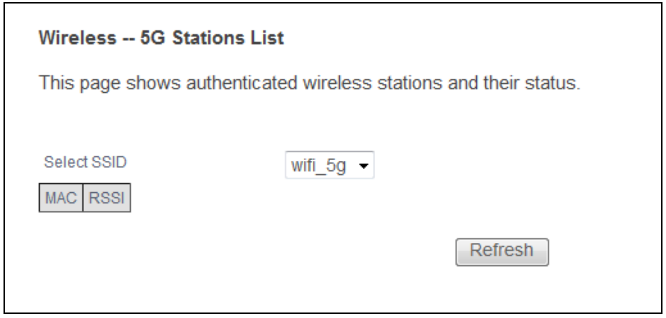
Table 95 Wireless Bridge

LABEL	DESCRIPTION
Remote Bridges MAC Address	Type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
Apply/Save	Click this to save and apply your changes.

20.11 Wireless 5GHz Station Info

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) the Router. To open the station monitor, click **Wireless 5GHz** > **Station Info** to display this screen.

Figure 105 Wireless 5GHz Station Info



Wireless -- 5G Stations List

This page shows authenticated wireless stations and their status.

Select SSID: wifi_5g

MAC	RSSI

The following table describes the labels in this menu.

Table 96   Wireless 5GHz Station Info

LABEL	DESCRIPTION
Select SSID	Select an SSID for which to display the authenticated wireless stations and their status.
MAC	This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station.
RSSI	This displays the Received Signal Strength Indication of the wireless station’s connection to the 5 GHz network.
Refresh	Click this button to update the information in the screen.

Voice

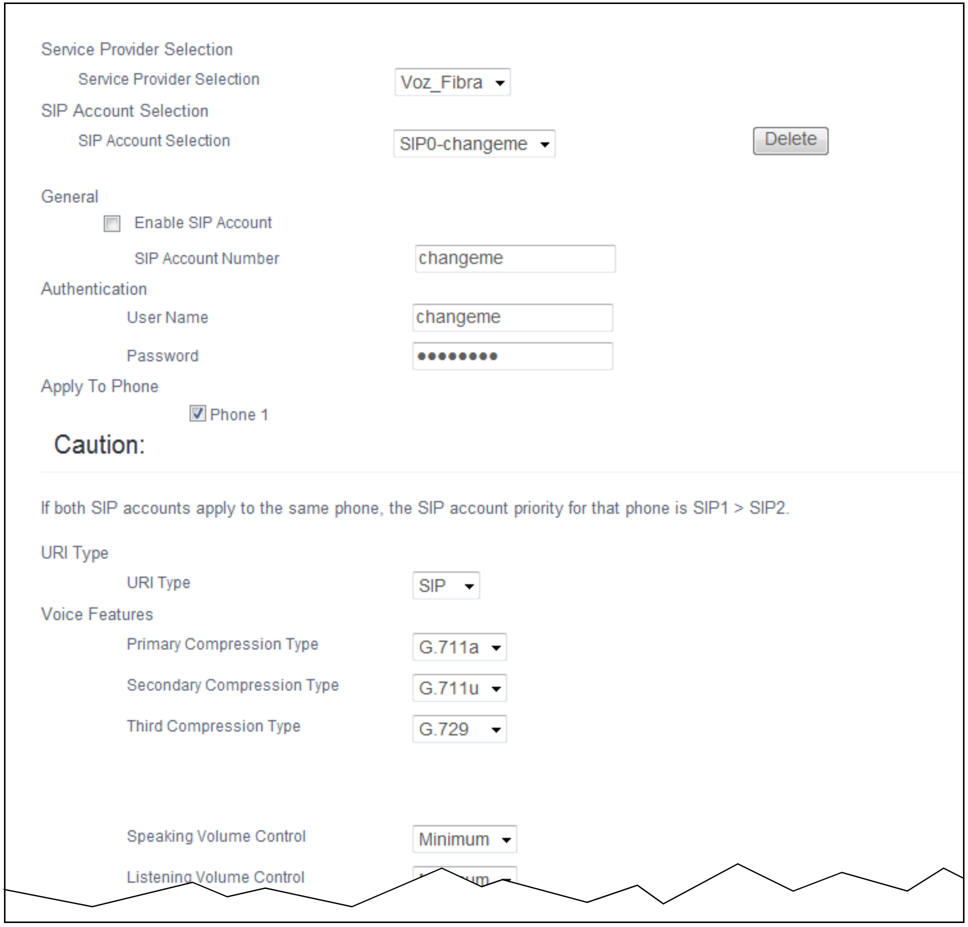
Chapter 21

21.1 SIP Account

The Router uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your Router to connect to your VoIP service provider.

Use this screen to maintain information about each SIP account. You can also enable and disable each SIP account. To access this screen, click **Voice > SIP Account**.

Figure 106 SIP Account



Service Provider Selection

Service Provider Selection: Voz_Fibra

SIP Account Selection

SIP Account Selection: SIP0-changeme

General

□ Enable SIP Account

SIP Account Number: changeme

Authentication

User Name: changeme

Password: ●●●●●●●●

Apply To Phone

☑ Phone 1

Caution:

If both SIP accounts apply to the same phone, the SIP account priority for that phone is SIP1 > SIP2.

URI Type

URI Type: SIP

Voice Features

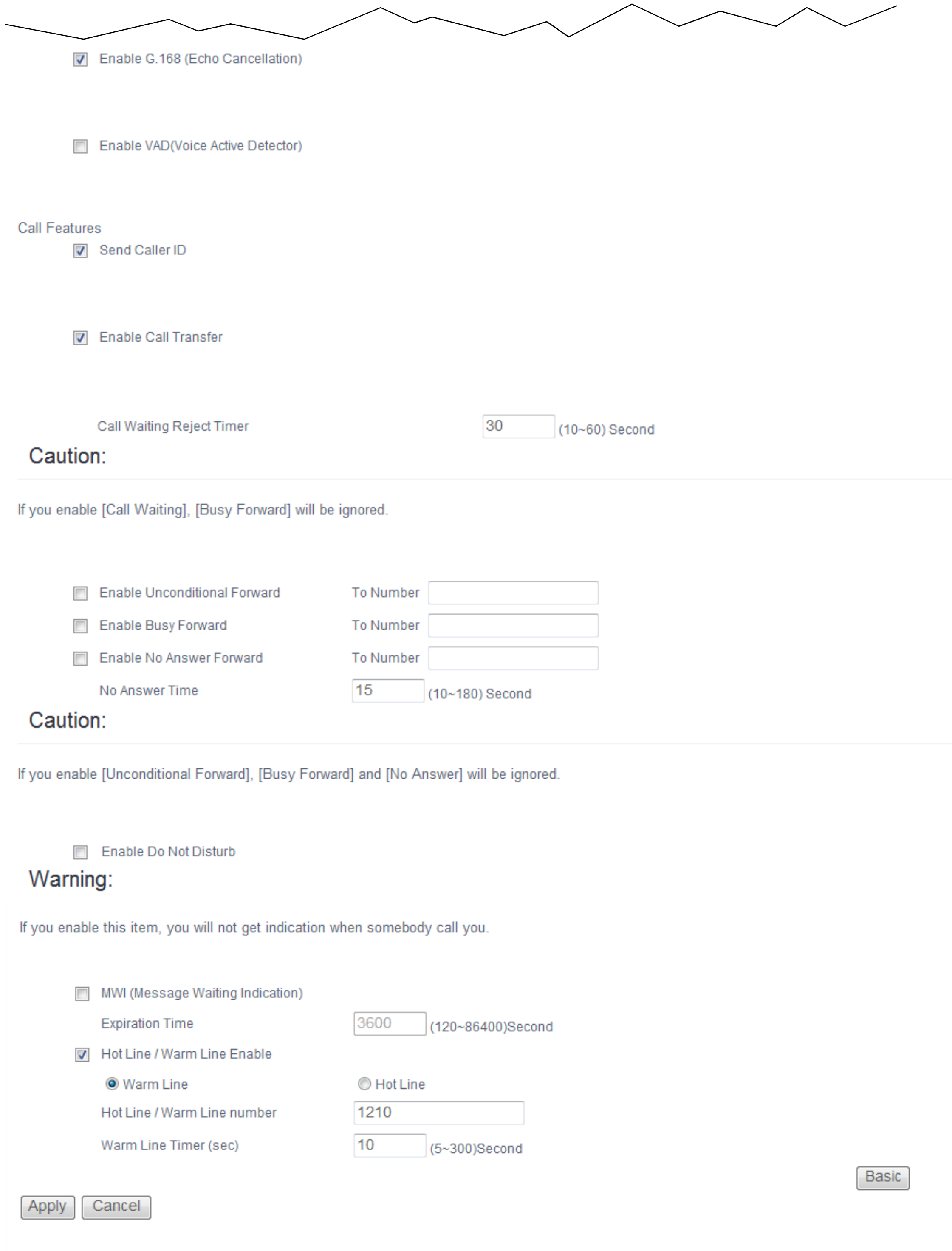
Primary Compression Type: G.711a

Secondary Compression Type: G.711u

Third Compression Type: G.729

Speaking Volume Control: Minimum

Listening Volume Control



☑ Enable G.168 (Echo Cancellation)

□ Enable VAD(Voice Active Detector)

Call Features

☑ Send Caller ID

☑ Enable Call Transfer

Call Waiting Reject Timer 30 (10~60) Second

Caution:

If you enable [Call Waiting], [Busy Forward] will be ignored.

□ Enable Unconditional Forward	To Number	
□ Enable Busy Forward	To Number	
□ Enable No Answer Forward	To Number	
No Answer Time	15	(10~180) Second

Caution:

If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

□ Enable Do Not Disturb

Warning:

If you enable this item, you will not get indication when somebody call you.

□ MWI (Message Waiting Indication)

Expiration Time 3600 (120~86400)Second

☑ Hot Line / Warm Line Enable

● Warm Line ○ Hot Line

Hot Line / Warm Line number 1210

Warm Line Timer (sec) 10 (5~300)Second

Each field is described in the following table.

Table 97 SIP Account

LABEL	DESCRIPTION
Service Provider Selection	Select the SIP service provider profile you want to use for the SIP account you configure in this screen. If you change this field, the screen automatically refreshes.
SIP Account Selection	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes. Select **ADD_NEW** to create a new SIP account on the Router.
Delete	Click this button to remove the SIP account selected in the **SIP Account Selection** field. This button is not available when you select **ADD_NEW** in the **SIP Account Selection** field.
General	
Enable SIP Account	Select this if you want the Router to use this account. Clear it if you do not want the Router to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
Apply To Phone	Select a phone port on which you want to make or receive phone calls for this SIP account. If you map a phone port to more than one SIP account, there is no way to distinguish between the SIP accounts when you receive phone calls. The Router uses the most recently registered SIP account first when you make an outgoing call. If a phone port is not mapped to a SIP account, you cannot receive or make any calls on the phone connected to this phone port.
Advanced/Basic	Click **Advanced** to display and edit more information for the SIP account. Click **Basic** to display and configure the basic SIP account settings.
URI Type	Select whether or not to include the SIP service domain name when the Router sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	

Table 97 SIP Account (continued)

LABEL	DESCRIPTION
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the Router to use. G.711 provides high voice quality but requires more bandwidth (64 kbps). G.711 is the default codec used by phone companies and digital handsets. • **G.711a** is typically used in Europe. • **G.711u** is typically used in North America and Japan. • **G.711a_VBD** is used in fax transmission. If both sides support the Voice Band Data (VBD) codec defined in ITU-T Recommendation V.152, they automatically use it instead of T.38. **G.722** is a 7 KHz wideband voice codec that operates at 48, 56 and 64 kbps. By using a sample rate of 16 kHz, G.722 can provide higher fidelity and better audio quality than narrowband codecs like G.711, in which the voice signal is sampled at 8 KHz. **G.726** operates at **24** or **32** kbps. The Router must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. Select the Router's first choice for voice coder/decoder. Select the Router's second choice for voice coder/decoder. Select **None** if you only want the Router to accept the first choice. Select the Router's third choice for voice coder/decoder. Select **None** if you only want the Router to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the Router uses for speech that it sends to the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Listening Volume Control	Enter the loudness that the Router uses for speech that it receives from the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Enable G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Enable VAD (Voice Active Detector)	Select this if the Router should stop transmitting when you are not speaking. This reduces the bandwidth the Router uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Enable Call Transfer	Select this to enable call transfer on the Router. This allows you to transfer an incoming call (that you have answered) to another phone.
Call Waiting Reject Timer	Specify a time of seconds that the Router waits before rejecting the second call if you do not answer it.

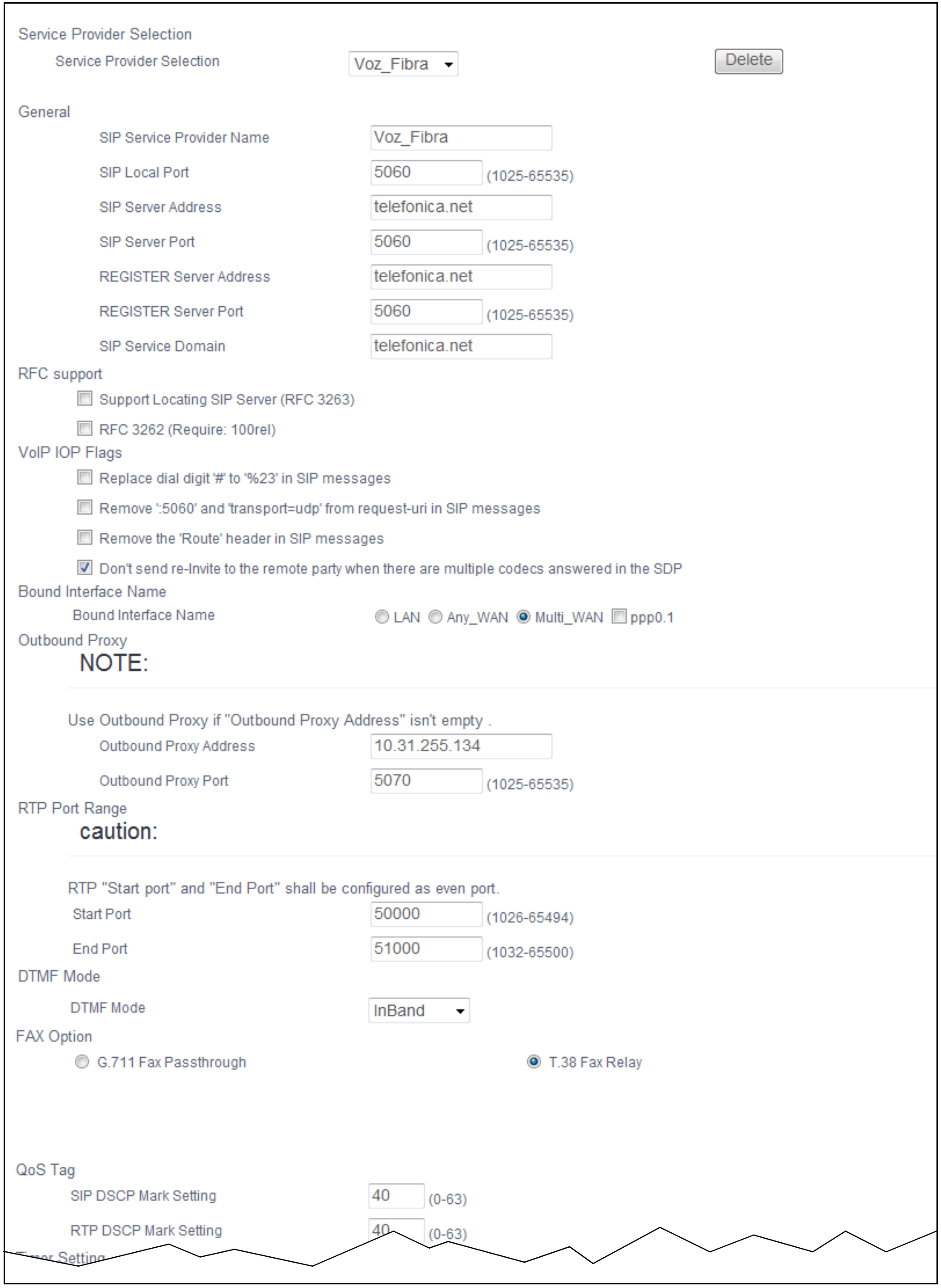
Table 97 SIP Account (continued)

LABEL	DESCRIPTION
Enable Unconditional Forward	Select this if you want the Router to forward all incoming calls to the specified phone number. Specify the phone number in the **To Number** field on the right.
Enable Busy Forward	Select this if you want the Router to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the **To Number** field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Enable No Answer Forward	Select this if you want the Router to forward incoming calls to the specified phone number if the call is unanswered. (See **No Answer Time**.) Specify the phone number in the **To Number** field on the right.
No Answer Time	This field is used by the **Active No Answer Forward** feature. Enter the number of seconds the Router should wait for you to answer an incoming call before it considers the call is unanswered.
Enable Do Not Disturb	Select this to set your phone to not ring when someone calls you.
MWI (Message Waiting Indication)	Select this if you want to hear a waiting (beeping) dial tone on your phone when you have at least one voice message. Your VoIP service provider must support this feature.
Expiration Time	Keep the default value for this field, unless your VoIP service provider tells you to change it. Enter the number of seconds the SIP server should provide the message waiting service each time the Router subscribes to the service. Before this time passes, the Router automatically subscribes again.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the Router.
Warm Line	Select this to have the Router dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the Router dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the Router to dial.
Warm Line Timer	Enter a number of seconds that the Router waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Apply	Click this to save your changes and to apply them to the Router.
Cancel	Click this to set every field in this screen to its last-saved value.

21.2 SIP Server

Click **Voice > SIP Server** to open the **SIP Server** screen. Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions, and dialing plan.

Figure 107 SIP Server



Service Provider Selection

Service Provider Selection	Voz_Fibra ▾	Delete

General

SIP Service Provider Name	Voz_Fibra	
SIP Local Port	5060	(1025-65535)
SIP Server Address	telefonica.net	
SIP Server Port	5060	(1025-65535)
REGISTER Server Address	telefonica.net	
REGISTER Server Port	5060	(1025-65535)
SIP Service Domain	telefonica.net	

RFC support

☐ Support Locating SIP Server (RFC 3263)

☐ RFC 3262 (Require: 100rel)

VoIP IOP Flags

☐ Replace dial digit '#' to '%23' in SIP messages

☐ Remove ':5060' and 'transport=udp' from request-uri in SIP messages

☐ Remove the 'Route' header in SIP messages

☑ Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP

Bound Interface Name

Bound Interface Name ○ LAN ○ Any_WAN ● Multi_WAN ☐ ppp0.1

Outbound Proxy

NOTE:

Use Outbound Proxy if "Outbound Proxy Address" isn't empty .

Outbound Proxy Address	10.31.255.134	
Outbound Proxy Port	5070	(1025-65535)

RTP Port Range

caution:

RTP "Start port" and "End Port" shall be configured as even port.

Start Port	50000	(1026-65494)
End Port	51000	(1032-65500)

DTMF Mode

DTMF Mode InBand ▾

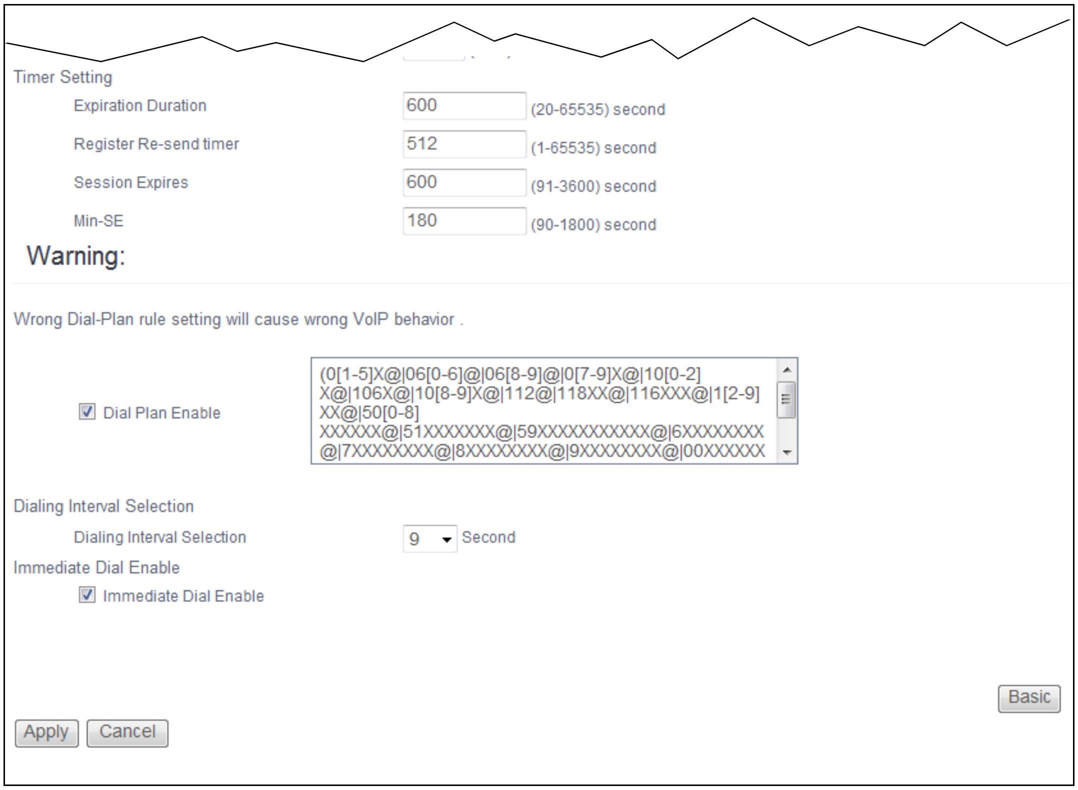
FAX Option

○ G.711 Fax Passthrough ● T.38 Fax Relay

QoS Tag

SIP DSCP Mark Setting	40	(0-63)
RTP DSCP Mark Setting	40	(0-63)

Timer Setting



Timer Setting

Expiration Duration: 600 (20-65535) second

Register Re-send timer: 512 (1-65535) second

Session Expires: 600 (91-3600) second

Min-SE: 180 (90-1800) second

Warning:

Wrong Dial-Plan rule setting will cause wrong VoIP behavior .

☑ Dial Plan Enable

```
(0[1-5]X@|06[0-6]@|06[8-9]@|0[7-9]X@|10[0-2]
X@|106X@|10[8-9]X@|112@|118XX@|116XXX@|1[2-9]
XX@|50[0-8]
XXXXXX@|51XXXXXXX@|59XXXXXXXXXXX@|6XXXXXXXX
@|7XXXXXXXX@|8XXXXXXXX@|9XXXXXXXX@|00XXXXXX
```

Dialing Interval Selection

Dialing Interval Selection: 9 Second

Immediate Dial Enable

☑ Immediate Dial Enable

Each field is described in the following table.

Table 98 SIP Server

LABEL	DESCRIPTION
Service Provider Selection	Select the SIP service provider profile you want to see in this screen. If you change this field, the screen automatically refreshes. Select **ADD_NEW** to create a new SIP service provider profile on the Router.
Delete	Click this button to remove the SIP service provider profile selected in the **Service Provider Selection** field. This button is not available when you select **ADD_NEW** in the **Service Provider Selection**.
General	
SIP Service Provider Name	Enter a descriptive name of up to 63 printable characters for this SIP service provider profile. Spaces are not allowed.
SIP Local Port	Enter the Router’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server’s listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.

Table 98 SIP Server (continued)

LABEL	DESCRIPTION
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RFC support	
Support Locating SIP Server (RFC 3263)	Select this option to have the Router use DNS procedures to resolve the SIP domain and find the SIP server's IP address, port number and supported transport protocol(s). The Router first uses DNS Name Authority Pointer (NAPTR) records to determine the transport protocols supported by the SIP server. It then performs DNS Service (SRV) query to determine the port number for the protocol. The Router resolves the SIP server's IP address by a standard DNS address record lookup. The **SIP Server Port** and **REGISTER Server Port** fields are grayed out and not applicable and the **Transport Type** can also be set to **AUTO** if you select this option.
RFC 3262	RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method. Select this to have the Router include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the Router receives a SIP response message indicating that the phone it called is ringing, the Router sends a PRACK message to have both sides confirm the message is received. If you select this option, the peer device should also support the option tag 100rel to send provisional responses reliably.
VoIP IOP Flags	Use this section to modify the header or some information in SIP messages in order to resolve interoperability issues with some SIP servers.
Replace dial digit '#' to '%23' in SIP messages	Replace a dial digit "#" with "%23" in the INVITE messages.
Remove ':5060' and 'transport=udp' from request-uri in SIP messages	Remove ":5060" and "transport=udp" from the "Request-URI" string in the REGISTER and INVITE packets.
Remove the 'Route' header in SIP messages	Remove the 'Route' header in SIP packets.

Table 98 SIP Server (continued)

LABEL	DESCRIPTION
Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP	Do not send a re-Invite packet to the remote party when the remote party answers that it can support multiple codecs??
Bound Interface Name	
Bound Interface Name	If you select **LAN** or **Any_WAN**, the Router automatically activates the VoIP service when any LAN or WAN connection is up. If you select **Multi_WAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.
Outbound Proxy	
Outbound Proxy Address	Enter the IP address or domain name of the SIP outbound proxy server if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Router to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Router to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Outbound Proxy Port	Enter the SIP outbound proxy server’s listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
DTMF Mode	
DTMF Mode	Control how the Router handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **InBand** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIPInfo** - send the DTMF tones in SIP messages.

Table 98 SIP Server (continued)

LABEL	DESCRIPTION
FAX Option	This field controls how the Router handles fax messages. Select **G.711 Fax Passthrough** to have the use G.711 to send fax messages. The peer devices must also use G.711. Select **T.38 Fax Relay** to have the Router send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
QoS Tag	
SIP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for SIP voice transmissions. The Router creates Class of Service (CoS) priority tags with this number to voice traffic that it transmits.
RTP DSCP Mark Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Router creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Router automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the Router waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Router accepts.
Phone Key Config	
Call Return	Specify the key combinations that you can enter to place a call to the last number that called you.
One Shot Caller Display Call	Specify the key combinations that you can enter to activate caller ID for the next call only.
One Shot Caller Hidden Call	Specify the key combinations that you can enter to deactivate caller ID for the next call only.
One Shot Call Waiting Enable	Specify the key combinations that you can enter to put a call on hold when you are answering another.
Call Waiting Enable	Specify the key combinations that you can enter to turn on the call waiting function.
Call Waiting Disable	Specify the key combinations that you can enter to turn off the call waiting function.

Table 98 SIP Server (continued)

LABEL	DESCRIPTION
Internal Call	Specify the key combinations that you can enter to call the phone(s) connected to the Router.
Call Transfer	Specify the key combinations that you can enter to transfer a call to another phone.
Unconditional Call Forward Enable	Specify the key combinations that you can enter to forward all incoming calls to the phone number you specified in the **SIP > SIP Account** screen.
Unconditional Call Forward Disable	Specify the key combinations that you can enter to turn the unconditional call forward function off.
No Answer Call Forward Enable	Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the calls are unanswered.
No Answer Call Forward Disable	Specify the key combinations that you can enter to turn the no answer call forward function off.
Call Forward When Busy Enable	Specify the key combinations that you can enter to forward incoming calls to the phone number you specified in the **SIP > SIP Account** screen if the phone port is busy.
Call Forward When Busy Disable	Specify the key combinations that you can enter to turn the busy forward function off.
One Shot Call Waiting Disable	Specify the key combinations that you can enter to deactivate call waiting on the next call only.
Do Not Disturb Enable	Specify the key combinations that you can enter to set your phone not to ring when someone calls you.
Do Not Disturb Disable	Specify the key combinations that you can enter to turn this function off.
Call Completion on Busy Subscriber (CCBS) Deactivate	Specify the key combinations that you can enter to disable CCBS on a call.
Outgoing SIP	Specify the key combinations that you can enter to select the SIP account that you use to make outgoing calls. If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the Router uses the first SIP account to call 12345678.
Dial Plan	
Dial Plan Enable	Select this to activate the dial plan rules you specify in the text box provided. See Section 21.2.1 on page 176 for how to set up a rule.

Table 98 SIP Server (continued)

LABEL	DESCRIPTION
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the Router should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Immediate Dial Enable**, you can press the pound key (#) to tell the Router to make the phone call immediately, regardless of this setting.
Immediate Dial Enable	
Immediate Dial Enable	Select this if you want to use the pound key (#) to tell the Router to make the phone call immediately, instead of waiting the number of seconds you selected in the **Dialing Interval Selection** field. If you select this, dial the phone number, and then press the pound key. The Router makes the call immediately, instead of waiting. You can still wait, if you want.
Apply	Click this to save your changes and to apply them to the Router.
Cancel	Click this to set every field in this screen to its last-saved value.

21.2.1 Dial Plan Rules

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee’s number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the Router makes the call.

The Router initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- “x” stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.
- The dot “.” appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.

- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,

  (<:1212> xxxxxxx) means the Router automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.

  (<9:> xxx xxxxxxx) means the Router automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.

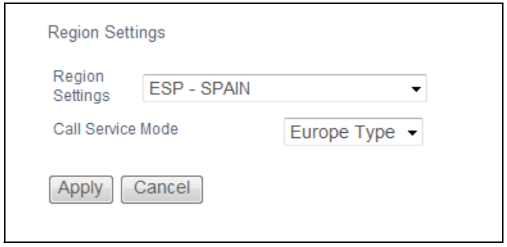
  (xx<123:456>xxxx) means the Router automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the @ character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

21.3 Phone Region

Use this screen to maintain settings that depend on which region of the world the Router is in. To access this screen, click **Voice > Phone**.

Figure 108 Phone Region



Region Settings

Region Settings: ESP - SPAIN

Call Service Mode: Europe Type

Each field is described in the following table.

Table 99 Phone Region

LABEL	DESCRIPTION
Region Settings	Select the place in which the Router is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. **Europe Type** - use supplementary phone services in European mode **USA Type** - use supplementary phone services American mode You might have to subscribe to these services to use them. Contact your VoIP service provider.

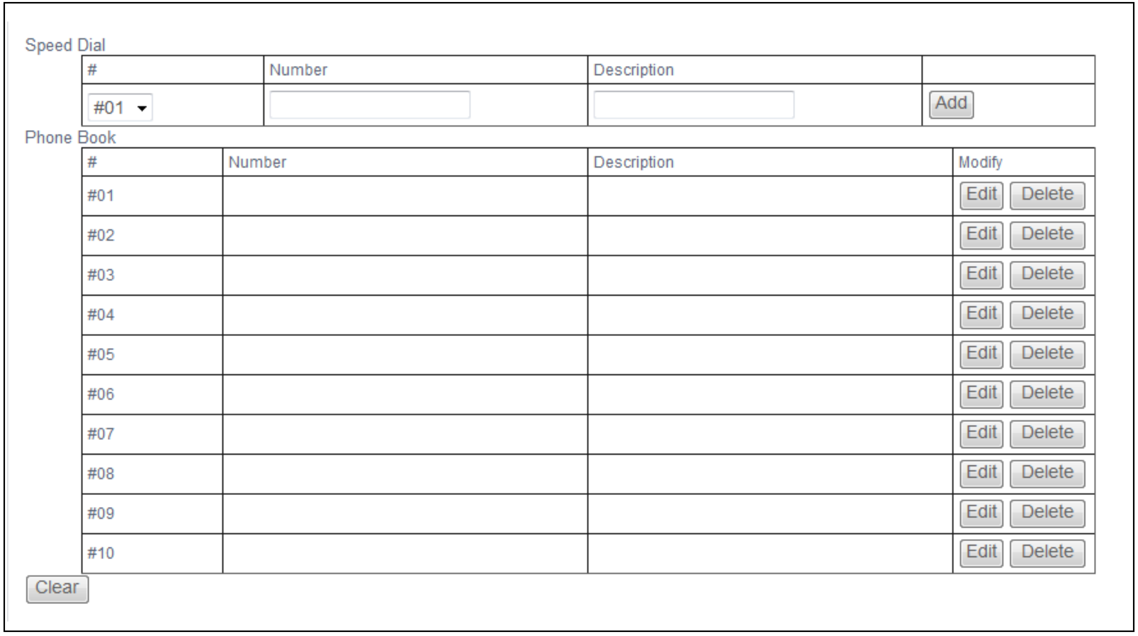
Table 99 Phone Region

LABEL	DESCRIPTION
Apply	Click this to save your changes and to apply them to the Router.
Cancel	Click this to set every field in this screen to its last-saved value.

21.4 Call Rule

Click **Voice > Call Rule** to manage speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Figure 109 Call Rule



Speed Dial

#	Number	Description	
#01 ▾			Add

Phone Book

#	Number	Description	Modify
#01			Edit Delete
#02			Edit Delete
#03			Edit Delete
#04			Edit Delete
#05			Edit Delete
#06			Edit Delete
#07			Edit Delete
#08			Edit Delete
#09			Edit Delete
#10			Edit Delete

Each field is described in the following table.

Table 100 Call Rule

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the Router to call when you dial the speed-dial number.

Table 100 Call Rule

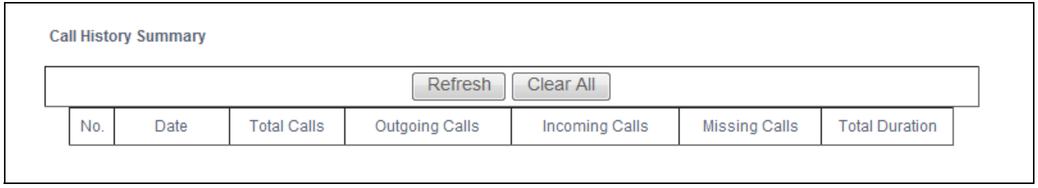
LABEL	DESCRIPTION
Description	Enter a name to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the **Speed Dial** section to update the **Phone Book** section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the Router calls when you dial the speed-dial number.
Description	This field displays the name of the party you call when you dial the speed-dial number.
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** button to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click the **Delete** button to erase this speed-dial entry.
Clear	Click this to erase all the speed-dial entries.

21.5 Call History Summary

The Router logs calls from or to your SIP numbers. This screen allows you to view the summary of received, dialed and missed calls.

Click **Voice > Summary**. The following screen displays.

Figure 110 Call History Summary



Call History Summary

No.	Date	Total Calls	Outgoing Calls	Incoming Calls	Missing Calls	Total Duration

Each field is described in the following table.

Table 101 Call History Summary

LABEL	DESCRIPTION
Refresh	Click this button to renew the call history list.
Clear All	Click this button to remove all entries from the call history list.

Table 101 Call History Summary

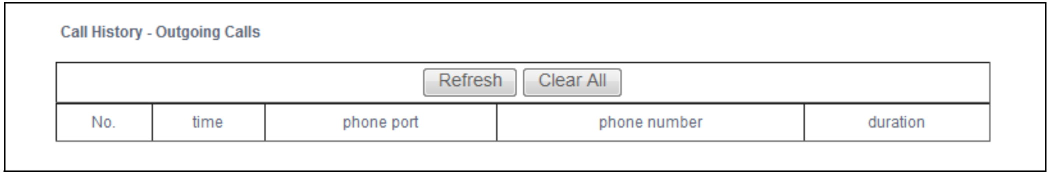
LABEL	DESCRIPTION
No.	This is a read-only index number.
Date	This is the date when the calls were made.
Total Calls	This displays the total number of calls from or to your SIP numbers that day.
Outgoing Calls	This displays how many calls originated from you that day.
Incoming Calls	This displays how many calls you received that day.
Missing Calls	This displays how many incoming calls were not answered that day.
Total Duration	This displays how long all calls lasted that day.

21.6 Outgoing Calls

Use this screen to see detailed information for each outgoing call you made.

Click **Voice > Outgoing**. The following screen displays.

Figure 111 Outgoing Calls



Call History - Outgoing Calls

No.	time	phone port	phone number	duration

Each field is described in the following table.

Table 102 Outgoing Calls

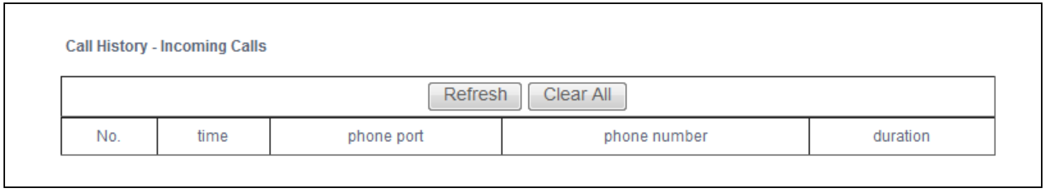
LABEL	DESCRIPTION
Refresh	Click this button to renew the dialed call list.
Clear All	Click this button to remove all entries from the dialed call list.
No.	This is a read-only index number.
time	This is the date and time when the call was made.
phone port	This is the phone port on which you made the call.
phone number	This is the SIP number you called.
duration	This displays how long the call lasted.

21.7 Incoming Calls

Use this screen to see detailed information for each incoming call from someone calling you.

Click **Voice > Incoming**. The following screen displays.

Figure 112 Incoming Calls



Call History - Incoming Calls

No.	time	phone port	phone number	duration

Each field is described in the following table.

Table 103 Incoming Calls

LABEL	DESCRIPTION
Refresh	Click this button to renew the received call list.
Clear All	Click this button to remove all entries from the received call list.
No.	This is a read-only index number.
time	This is the date and time when the call was made.
phone port	This is the phone port on which you received the call. **Missed** means the call was unanswered.
phone number	This is the SIP number that called you.
duration	This displays how long the call lasted.

21.8 Technical Reference

This section contains background material relevant to the **VoIP** screens.

VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each Router is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the Router). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The Router attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the Router attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC 3261, "SIP: Session Initiation Protocol").

SIP Servers

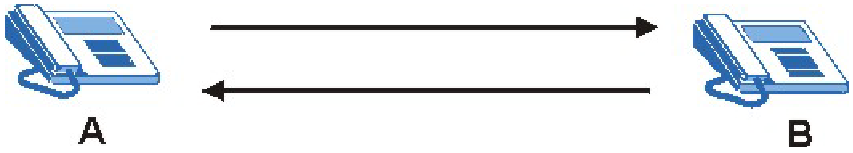
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 113 SIP User Agent



SIP Proxy Server

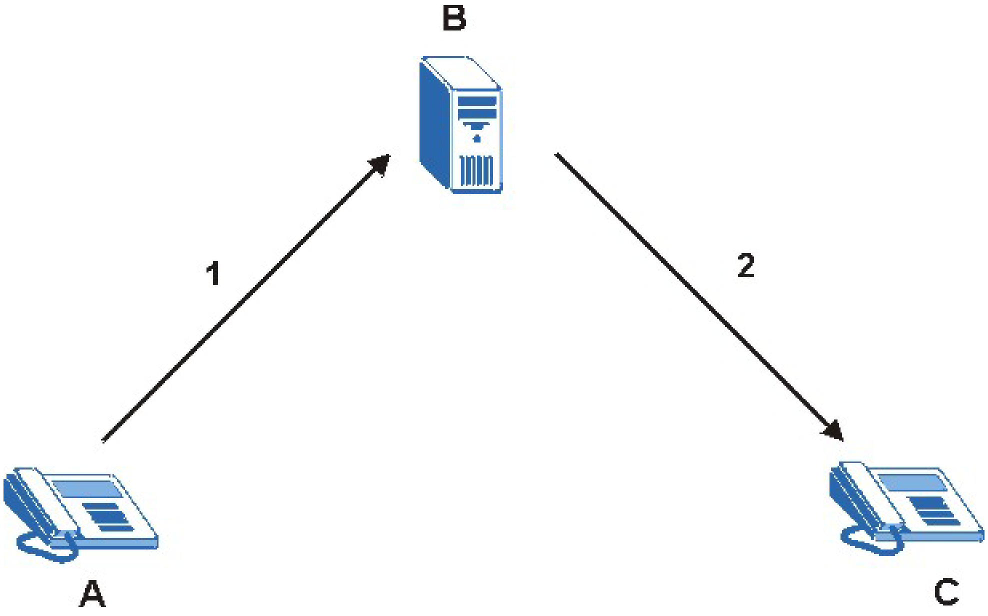
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 114 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

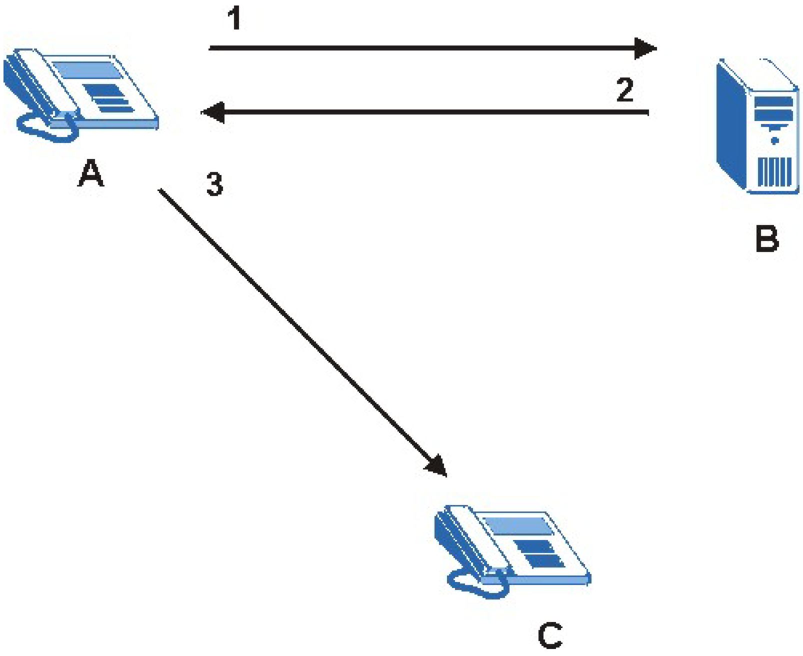
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 115 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 104 SIP Call Progression

A	B
1. INVITE ⟶	
⟵	2. Ringing

Table 104 SIP Call Progression (continued)

A		B
	←	3. OK
4. ACK	→	
	5.Dialogue (voice traffic)	
6. BYE	→	
	←	7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

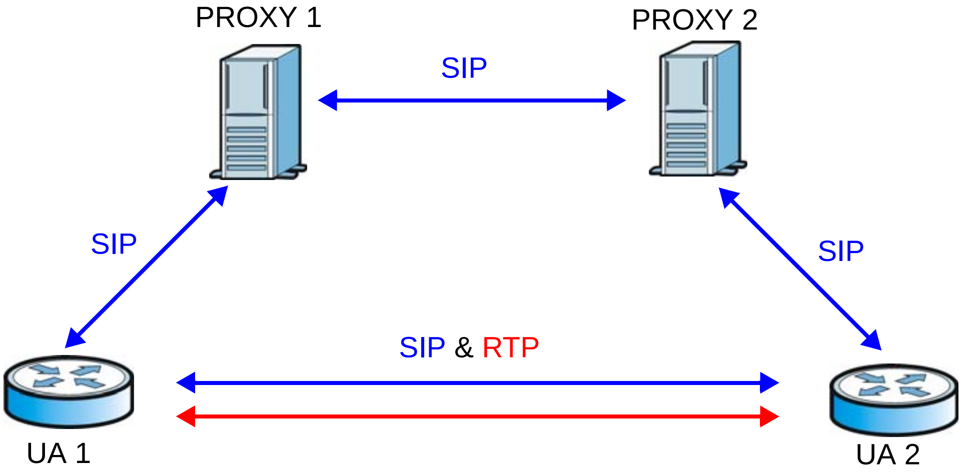
SIP Call Progression Through Proxy Servers

Usually, the SIP UAC sets up a phone call by sending a request to the SIP proxy server. Then, the proxy server looks up the destination to which the call should be forwarded (according to the URI requested by the SIP UAC). The request may be forwarded to more than one proxy server before arriving at its destination.

The response to the request goes to all the proxy servers through which the request passed, in reverse sequence. Once the session is set up, session traffic is sent between the UAs directly, bypassing all the proxy servers in between.

The following figure shows the SIP and session traffic flow between the user agents (**UA 1** and **UA 2**) and the proxy servers (this example shows two proxy servers, **PROXY 1** and **PROXY 2**).

Figure 116 SIP Call Through Proxy Servers



The following table shows the SIP call progression.

Table 105 SIP Call Progression

UA 1	PROXY 1	PROXY 2	UA 2
Invite →			
	Invite →		
	← 100 Trying	Invite →	
		← 100 Trying	
			← 180 Ringing
		← 180 Ringing	
	← 180 Ringing		
			← 200 OK
		← 200 OK	
	← 200 OK		
ACK →			
RTP ↔			RTP

Table 105 SIP Call Progression

UA 1	PROXY 1	PROXY 2	UA 2
	←	←	BYE
200 OK	→	→	

1 **User Agent 1** sends a SIP INVITE request to **Proxy 1**. This message is an invitation to **User Agent 2** to participate in a SIP telephone call. **Proxy 1** sends a response indicating that it is trying to complete the request.

2 **Proxy 1** sends a SIP INVITE request to **Proxy 2**. **Proxy 2** sends a response indicating that it is trying to complete the request.

3 **Proxy 2** sends a SIP INVITE request to **User Agent 2**.

4 **User Agent 2** sends a response back to **Proxy 2** indicating that the phone is ringing. The response is relayed back to **User Agent 1** via **Proxy 1**.

5 **User Agent 2** sends an OK response to **Proxy 2** after the call is answered. This is also relayed back to **User Agent 1** via **Proxy 1**.

6 **User Agent 1** and **User Agent 2** exchange RTP packets containing voice data directly, without involving the proxies.

7 When **User Agent 2** hangs up, he sends a BYE request.

8 **User Agent 1** replies with an OK response confirming receipt of the BYE request, and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The Router supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Router reduce the bandwidth that a call uses by not transmitting “silent packets” when you are not speaking.

Comfort Noise Generation

When using VAD, the Router generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Router. The Router allows you to record custom tones for the **Early Media** and **Music On Hold** functions. The same recordings apply to both the caller ringing and on hold tones.

Table 106 Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	900 seconds for all custom tones combined
Maximum Time per Individual Tone	180 seconds
Total Number of Tones Recordable	5 You can record up to 5 different custom tones but the total time must be 900 seconds or less.

Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1101~1105 on your phone followed by the “#” key.

3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.

4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Listening to Custom Tones

Do the following to listen to a custom tone:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.

3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

Deleting Custom Tones

Do the following to delete a custom tone:

1 Pick up the phone and press “****” on your phone’s keypad and wait for the message that says you are in the configuration menu.

2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.

You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

21.8.1 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the Router) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[1]

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 117 DiffServ: Differentiated Service Field

DSCP	Unused
(6-bit)	(2-bit)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

21.8.2 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The Router supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Three-Way Conference
- Internal Calls
- Call Park and Pickup
- Do not Disturb

To take full advantage of the supplementary phone services available through the Router's phone ports, you may need to subscribe to the services from your VoIP service provider.

[1] The Router does not support DiffServ at the time of writing.

21.8.2.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the Router.

You can invoke all the supplementary services by using the flash key.

21.8.2.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 107 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

21.8.2.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 108 USA Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1. Press the flash key to put the caller on hold.
2. When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call.
3. After you hear the ring signal or the second party answers it, hang up the phone.

USA Three-Way Conference

Use the following steps to make three-way conference calls.

1 When you are on the phone talking to someone (party A), press the flash key to put the caller on hold and get a dial tone.

2 Dial a phone number directly to make another call (to party B).

3 When party B answers the second call, press the flash key to create a three-way conversation.

4 Hang up the phone to drop the connection.

5 If you want to separate the activated three-way conference into two individual connections (with party A on-line and party B on hold), press the flash key.

6 If you want to go back to the three-way conversation, press the flash key again.

7 If you want to separate the activated three-way conference into two individual connections again, press the flash key. This time the party B is on-line and party A is on hold.

21.8.2.4 Phone Functions Summary

The following table shows the key combinations you can enter on your phone's keypad to use certain features.

Table 109 Phone Functions Summary

ACTION	FUNCTION	DESCRIPTION
*98#	Call transfer	Transfer a call to another phone. See Section 21.8.2.2 on page 192 (Europe type) and Section 21.8.2.3 on page 194 (USA type).
*66#	Call return	Place a call to the last person who called you.
*95#	Enable Do Not Disturb	Use these to set your phone not to ring when someone calls you, or to turn this function off.
#95#	Disable Do Not Disturb	
*41#	Enable Call Waiting	Use these to allow you to put a call on hold when you are answering another, or to turn this function off.
#41#	Disable Call Waiting	
****	IVR	Use these to set up Interactive Voice Response (IVR). IVR allows you to record custom caller ringing tones (the sound a caller hears before you pick up the phone) and on hold tones (the sound someone hears when you put their call on hold).
####	Internal Call	Call the phone(s) connected to the Router.
*82	One Shot Caller Display Call	Activate or deactivate caller ID for the next call only.
*67	One Shot Caller Hidden Call	

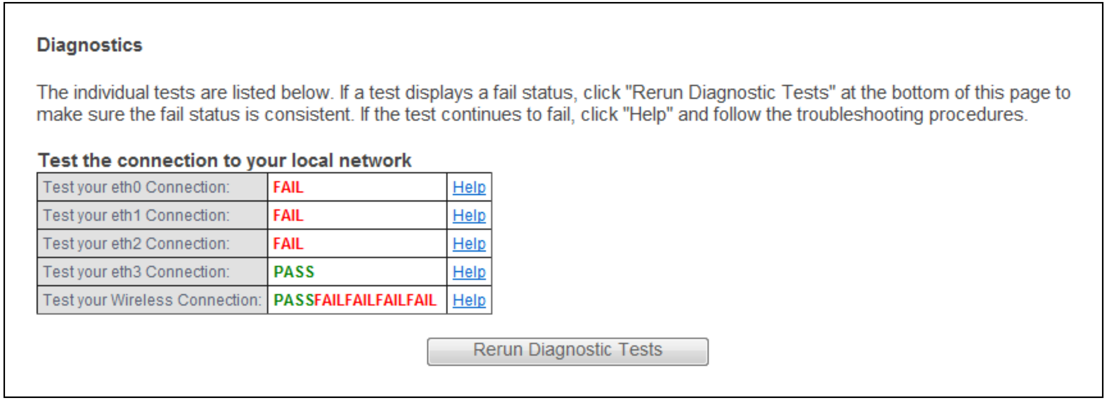
Diagnostics

22 Chapter

22.1 Diagnostics

Click **Diagnostics** to test the Router’s connections.

Figure 118 Diagnostics



Diagnostics

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 eth0 Connection:	FAIL	Help
Test your eth1 Connection:	FAIL	Help
Test your eth2 Connection:	FAIL	Help
Test your eth3 Connection:	PASS	Help
Test your Wireless Connection:	PASSFAILFAILFAILFAIL	Help

Click **Rerun Diagnostic Tests** to perform the tests again.

22.2 Ping/TraceRoute/Nslookup

Ping, traceroute, and nslookup help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Diagnostics > Ping&TraceRoute&Nslookup** to open the screen shown next.

Figure 119 Ping/TraceRoute/Nslookup

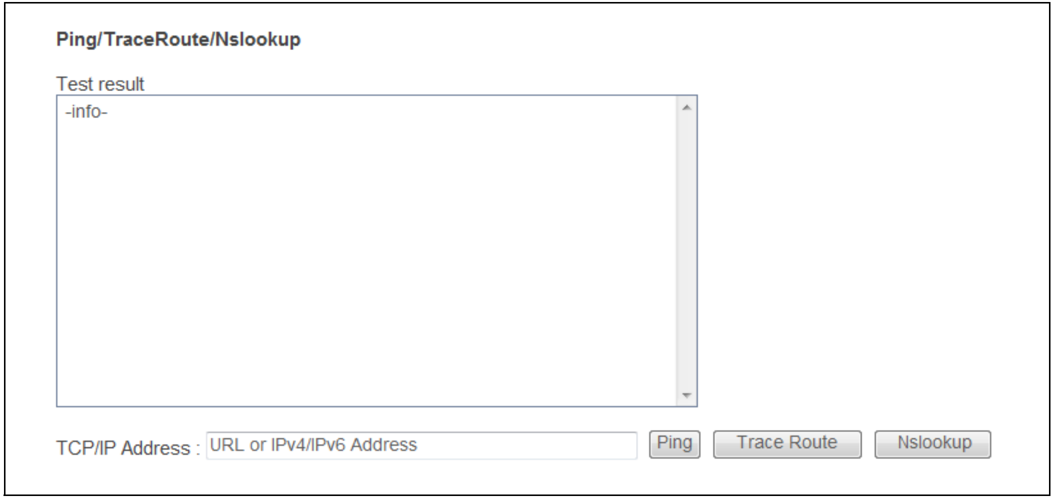


Table 110 Ping/TraceRoute/Nslookup

LABEL	DESCRIPTION
Ping	Type an IPv4 or IPv6 address to which to test a connection. Click **Ping** and the ping statistics will show in the diagnostic.
TraceRoute	Click this to show the path that packets take from the system to the IP address that you entered.
Nslookup	Click this button to perform a DNS lookup on the IP address that you entered.

Settings

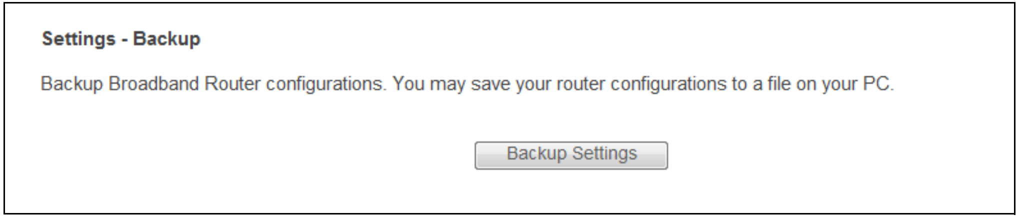
23 Chapter

This chapter describes how to manage your Router's configuration.

23.1 Backup Configuration Using the Web Configurator

Click **Management > Settings > Backup** to open the following screen. Use this screen to back up (save) the Router's current configuration to a file on your computer. Once your Router is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Figure 120 Settings: Backup



Settings - Backup

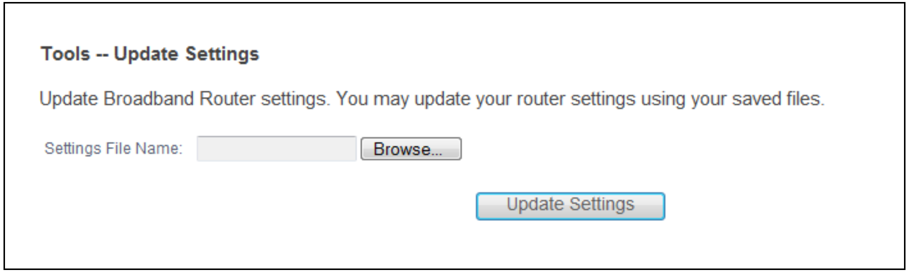
Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Click **Backup Settings** to save the Router's current configuration to your computer.

23.2 Restore Configuration Using the Web Configurator

Click **Management > Settings > Update** to open the following screen. Use this screen to upload a new or previously saved configuration file from your computer to your Router.

Figure 121 Settings: Update



Tools -- Update Settings

Update Broadband Router settings. You may update your router settings using your saved files.

Settings File Name:

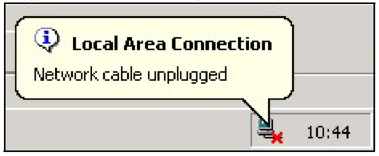
Table 111 Settings: Update

LABEL	DESCRIPTION
Settings File Name	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Update Settings	Click this to begin the upload process.

Do not turn off the Router while configuration file upload is in progress

You must then wait before logging into the Router again. The Router automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 122 Temporarily Disconnected



Local Area Connection

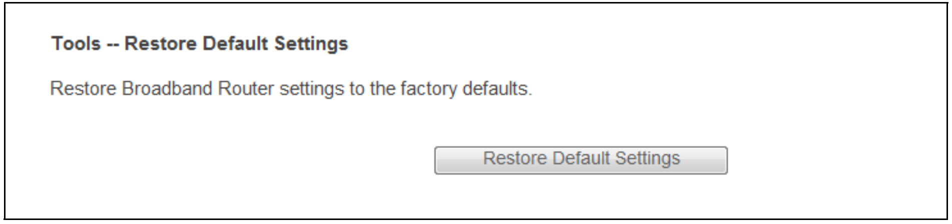
Network cable unplugged

You may need to change the IP address of your computer to be in the same subnet as that of the Router’s IP address (192.168.1.1). See the appendix for details on how to set up your computer’s IP address.

23.3 Restoring Factory Defaults

Click **Management > Settings > Restore Default** to open the following screen.

Figure 123 Management > Settings > Restore Default



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Click **Restore Default Settings** to clear all user-entered configuration information and return the Router to its factory defaults.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Router.

You may need to change the IP address of your computer to be in the same subnet as that of the default Router IP address (192.168.1.1). See the appendix for details on how to set up your computer's IP address.

Logs

24 Chapter

24.1 Logs

The Web Configurator allows you to choose which categories of events and/or alerts to have the Router log and then display the logs or have the Router send them to an administrator (as e-mail) or to a syslog server.

24.1.1 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 112 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.

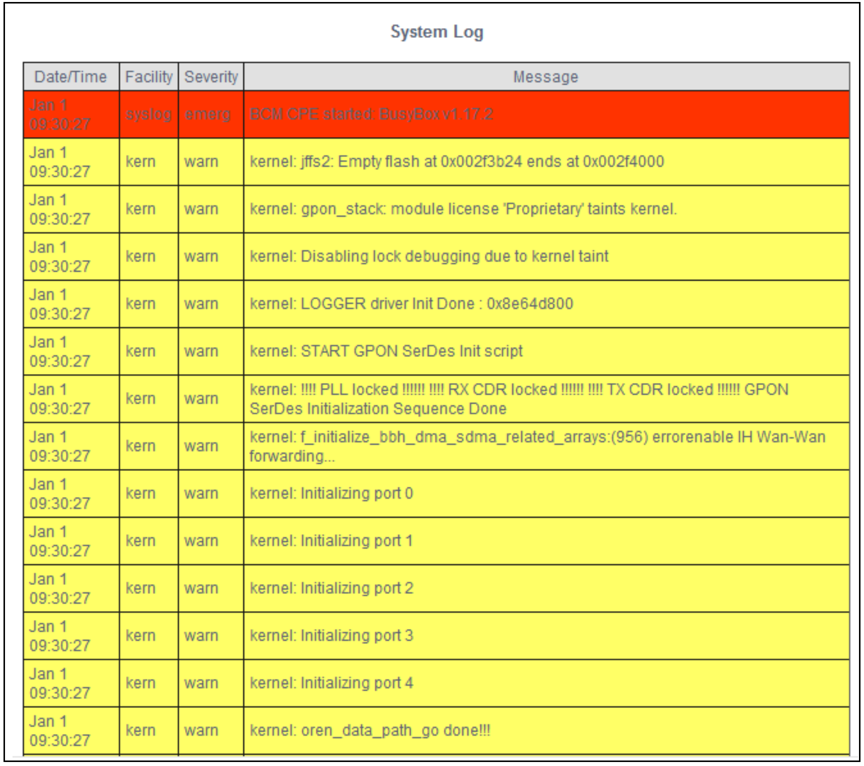
Table 112 Syslog Severity Levels (continued)

CODE	SEVERITY
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

24.2 System Log

Use the **System Log** screen to see the system logs. Click **Management > System Log > View System Log** to open the **System Log** screen.

Figure 124 System Log



System Log

Date/Time	Facility	Severity	Message
Jan 1 09:30:27	syslog	emerg	BCM CPE started: BusyBox v1.17.2
Jan 1 09:30:27	kern	warn	kernel: jffs2: Empty flash at 0x002f3b24 ends at 0x002f4000
Jan 1 09:30:27	kern	warn	kernel: gpon_stack: module license 'Proprietary' taints kernel.
Jan 1 09:30:27	kern	warn	kernel: Disabling lock debugging due to kernel taint
Jan 1 09:30:27	kern	warn	kernel: LOGGER driver Init Done : 0x8e64d800
Jan 1 09:30:27	kern	warn	kernel: START GPON SerDes Init script
Jan 1 09:30:27	kern	warn	kernel: !!!! PLL locked !!!!!! !!!! RX CDR locked !!!!!! !!!! TX CDR locked !!!!!! GPON SerDes Initialization Sequence Done
Jan 1 09:30:27	kern	warn	kernel: f_initialize_bbh_dma_sdma_related_arrays:(956) errorenable IH Wan-Wan forwarding...
Jan 1 09:30:27	kern	warn	kernel: Initializing port 0
Jan 1 09:30:27	kern	warn	kernel: Initializing port 1
Jan 1 09:30:27	kern	warn	kernel: Initializing port 2
Jan 1 09:30:27	kern	warn	kernel: Initializing port 3
Jan 1 09:30:27	kern	warn	kernel: Initializing port 4
Jan 1 09:30:27	kern	warn	kernel: oren_data_path_go done!!!

The following table describes the fields in this screen.

Table 113 System Log

LABEL	DESCRIPTION
Date/Time	This field displays when the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Severity	This field displays the severity level of the logs that the device is to send to this syslog server.

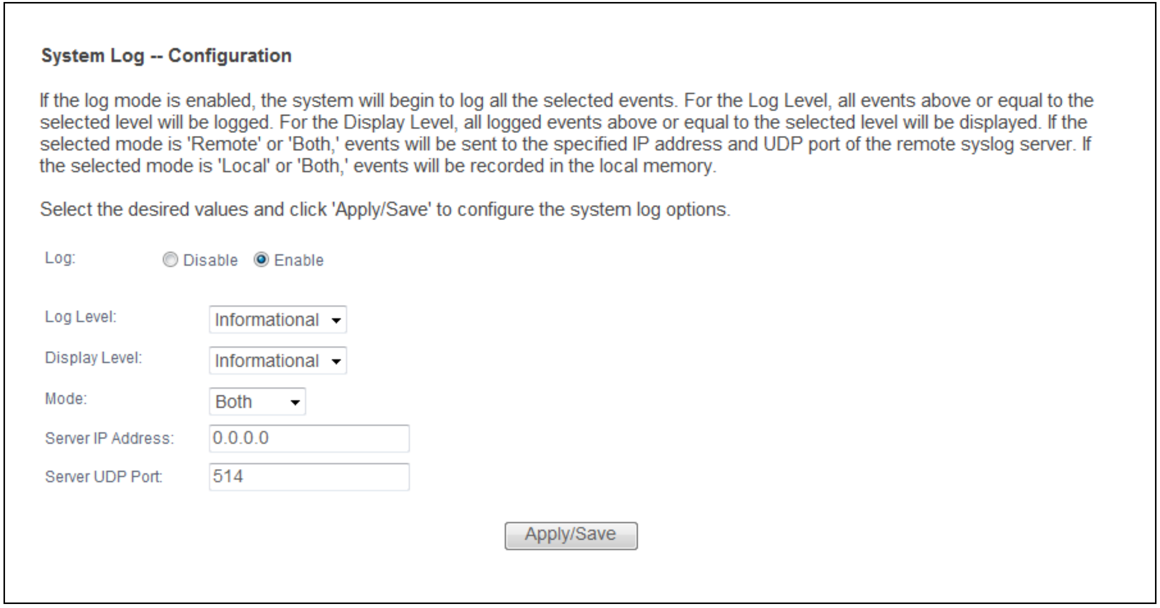
Table 113 System Log (continued)

LABEL	DESCRIPTION
Messages	This field states the reason for the log.
Refresh	Click this to renew the log screen.
Close	Click this to close the log screen.

24.3 System Log Configuration

To change your Router's log settings, click **Management > System Log > Configure System Log**. The screen appears as shown.

Figure 125 System Log Configuration



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 'Apply/Save' to configure the system log options.

Log: ○ Disable ● Enable

Log Level: Informational

Display Level: Informational

Mode: Both

Server IP Address: 0.0.0.0

Server UDP Port: 514

The following table describes the fields in this screen.

Table 114 System Log Configuration

LABEL	DESCRIPTION
Log	Select **Enable** to have the Router log events.
Log Level	Select the severity level of events to log.
Display Level	Select the severity level of events to display in the log.
Mode	Select the syslog destination from the drop-down list box. Select **Remote**, the log(s) to send logs only to a remote syslog server. Select **Local** to save the logs in a local file. To send the log(s) to a remote syslog server and save it in a local file, select **Both**.

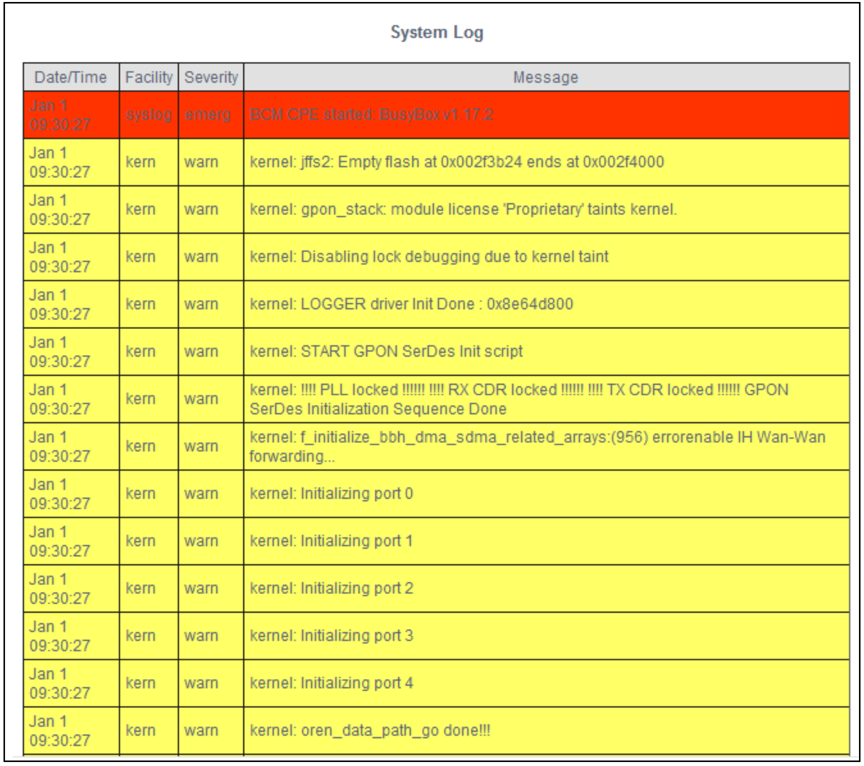
Table 114 System Log Configuration (continued)

LABEL	DESCRIPTION
Server IP Address	Enter the IP address of the syslog server that will log the selected categories of logs.
Server UDP Port	Enter the port number used by the syslog server.
Apply/Save	Click this button to save your changes.

24.4 Security Log

Use the **Security Log** screen to see the system logs. Click **Management > Security Log > View** to open the **Security Log** screen.

Figure 126 Security Log



System Log

Date/Time	Facility	Severity	Message
Jan 1 09:30:27	syslog	emerg	BCM CPE started: BusyBox v1.17.2
Jan 1 09:30:27	kern	warn	kernel: jffs2: Empty flash at 0x002f3b24 ends at 0x002f4000
Jan 1 09:30:27	kern	warn	kernel: gpon_stack: module license 'Proprietary' taints kernel.
Jan 1 09:30:27	kern	warn	kernel: Disabling lock debugging due to kernel taint
Jan 1 09:30:27	kern	warn	kernel: LOGGER driver Init Done : 0x8e64d800
Jan 1 09:30:27	kern	warn	kernel: START GPON SerDes Init script
Jan 1 09:30:27	kern	warn	kernel: !!!! PLL locked !!!!!! !!!! RX CDR locked !!!!!! !!!! TX CDR locked !!!!!! GPON SerDes Initialization Sequence Done
Jan 1 09:30:27	kern	warn	kernel: f_initialize_bbh_dma_sdma_related_arrays:(956) errorenable IH Wan-Wan forwarding...
Jan 1 09:30:27	kern	warn	kernel: Initializing port 0
Jan 1 09:30:27	kern	warn	kernel: Initializing port 1
Jan 1 09:30:27	kern	warn	kernel: Initializing port 2
Jan 1 09:30:27	kern	warn	kernel: Initializing port 3
Jan 1 09:30:27	kern	warn	kernel: Initializing port 4
Jan 1 09:30:27	kern	warn	kernel: oren_data_path_go done!!!

The following table describes the fields in this screen.

Table 115 Security Log

LABEL	DESCRIPTION
Date/Time	This field displays when the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Severity	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.
Refresh	Click this to renew the log screen.
Close	Click this to close the log screen.

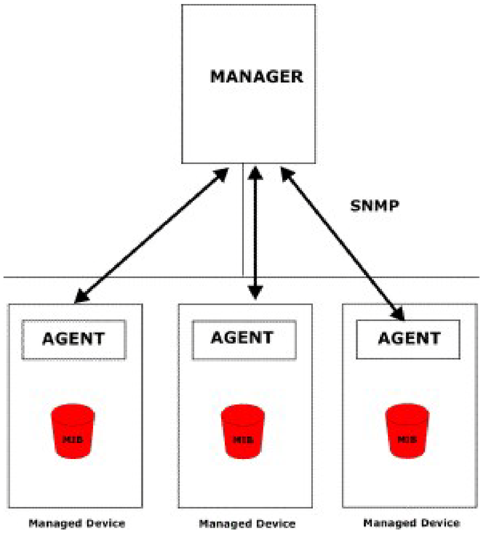
SNMP

25 Chapter

25.1 SNMP Agent

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your Router supports SNMP agent functionality, which allows a manager station to manage and monitor the Router through the network. The Router supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

Figure 127 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Router). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

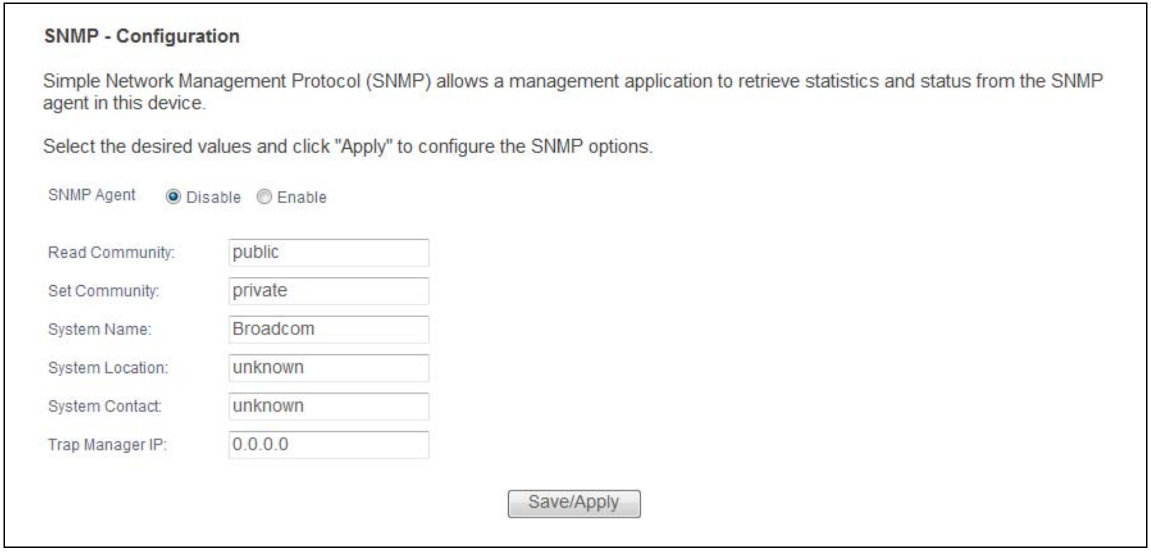
The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Click **Management > SNMP Agent** to open the following screen. Use this screen to configure the Router SNMP settings.

Figure 128 Management > SNMP Agent



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:	Broadcom
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

The following table describes the fields in this screen.

Table 116 Management > SNMP Agent

LABEL	DESCRIPTION
SNMP Agent	Select **Enable** to let the Router act as an SNMP agent, which allows a manager station to manage and monitor the Device through the network. Select **Disable** to turn this feature off.
Read Community	Enter the **Read Community**, which is the password for the incoming Get and GetNext requests from the management station.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station.
System Name	Enter the SNMP system name.
System Location	Enter the SNMP system location.

Table 116 Management > SNMP Agent (continued)

LABEL	DESCRIPTION
System Contact	Enter the SNMP system contact.
Trap Manager IP	Type the IP address of the station to send your SNMP traps to.
Save/Apply	Click this to save your changes back to the Router.

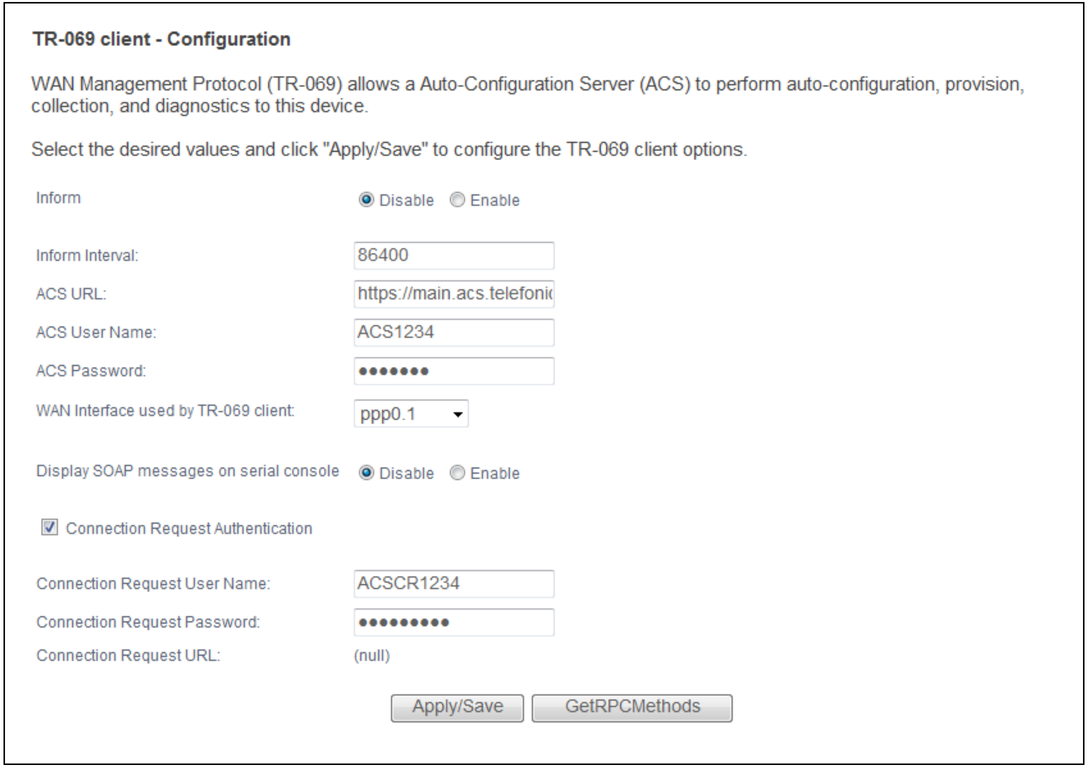
TR-069 Client

26 Chapter

26.1 TR-069 Client

Click **Management > TR-069 Client** to open the following screen. Use this screen to configure your Router to be managed by an ACS (Auto Configuration Server).

Figure 129 TR-069 Client



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform	● Disable ○ Enable
Inform Interval:	86400
ACS URL:	https://main.acs.telefoni
ACS User Name:	ACS1234
ACS Password:	•••••••
WAN Interface used by TR-069 client:	ppp0.1
Display SOAP messages on serial console	● Disable ○ Enable
☑ Connection Request Authentication	
Connection Request User Name:	ACSCR1234
Connection Request Password:	•••••••••
Connection Request URL:	(null)

Table 117 TR-069 Client

LABEL	DESCRIPTION
Inform	Select **Enable** for the Router to send periodic inform via TR-069 on the WAN. Otherwise, select **Disable**.
Inform Interval	Enter the time interval (in seconds) at which the Router sends information to the auto-configuration server.
ACS URL	Enter the URL or IP address of the auto-configuration server.

Table 117 TR-069 Client (continued)

LABEL	DESCRIPTION
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
WAN Interface used by TR-069 client	Select a WAN interface through which the TR-069 traffic passes. If you select **Any_WAN**, you should also select the pre-configured WAN connection(s).
Display SOAP messages on serial console	Select **Enable** to show the SOAP messages on the console.
Connection Request Authentication	Select this option to enable authentication when there is a connection request from the ACS.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Router, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Router, this password is used to authenticate the ACS.
Connection Request URL	This shows the connection request URL. The ACS can use this URL to make a connection request to the Router.
Apply/Save	Click this button to save your changes.
GetRPCMethods	In TR-069, a Remote Procedure Call (RPC) mechanism is used for bidirectional communication between a CPE and the auto-configuration server. The RPC method is used to initiate the transfer (download or upload) between them. Click this button to discover the method supported by the ACS, such as Inform, TransferComplete or RequestDownload.

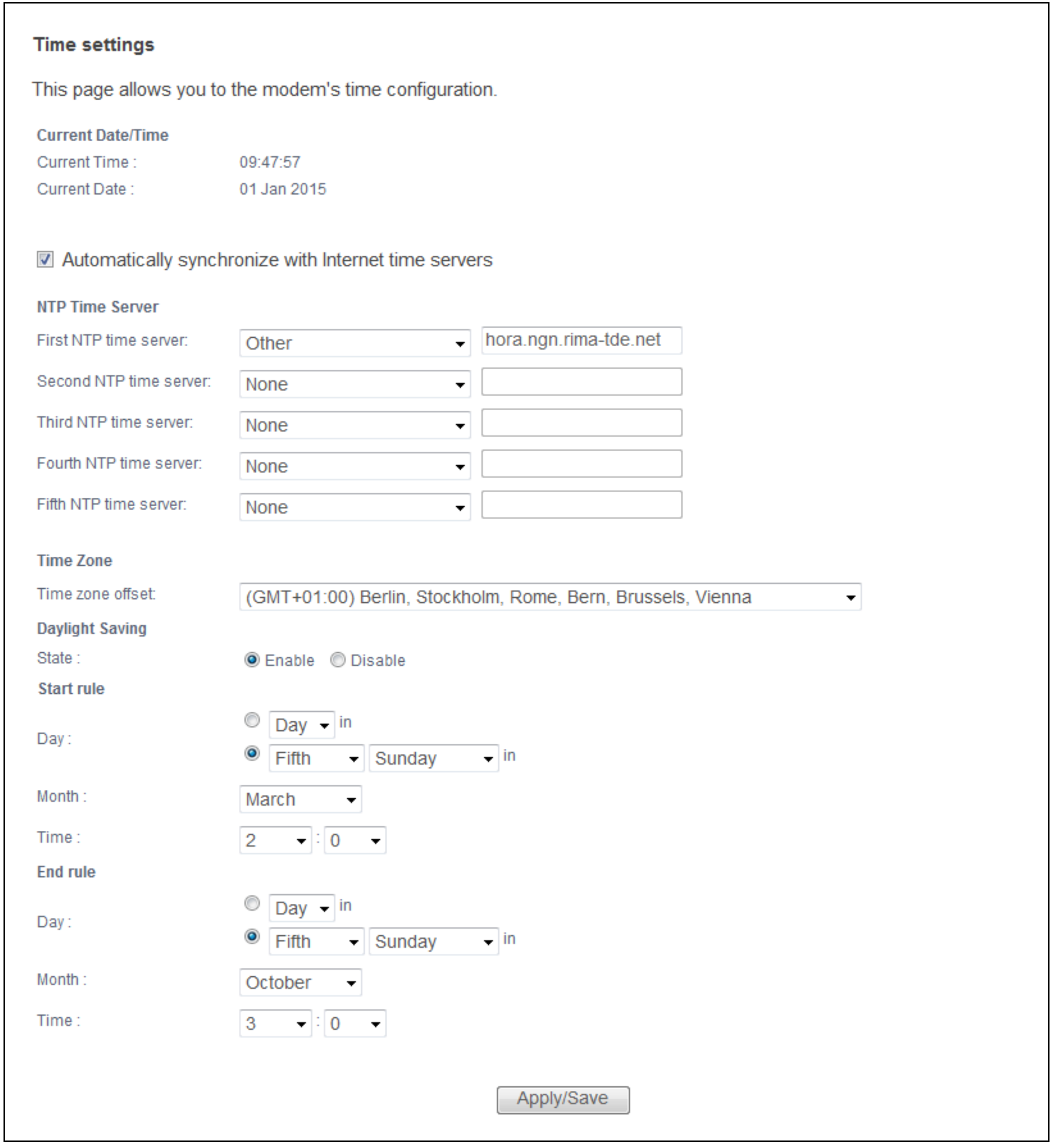
Internet Time

27 Chapter

27.1 Internet Time

Click **Management > Internet Time** to configure the Router to get the time from time servers on the Internet.

Figure 130 Internet Time



Time settings

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

Current Date/Time

Current Time : 09:47:57

Current Date : 01 Jan 2015

☑ Automatically synchronize with Internet time servers

NTP Time Server

First NTP time server:	Other	hora.ngn.rima-tde.net
Second NTP time server:	None	
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Time Zone

Time zone offset: (GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vienna

Daylight Saving

State : ● Enable ○ Disable

Start rule

Day : ○ Day in
● Fifth Sunday in

Month : March

Time : 2 : 0

End rule

Day : ○ Day in
● Fifth Sunday in

Month : October

Time : 3 : 0

The following table describes the fields in this screen.

Table 118 Internet Time

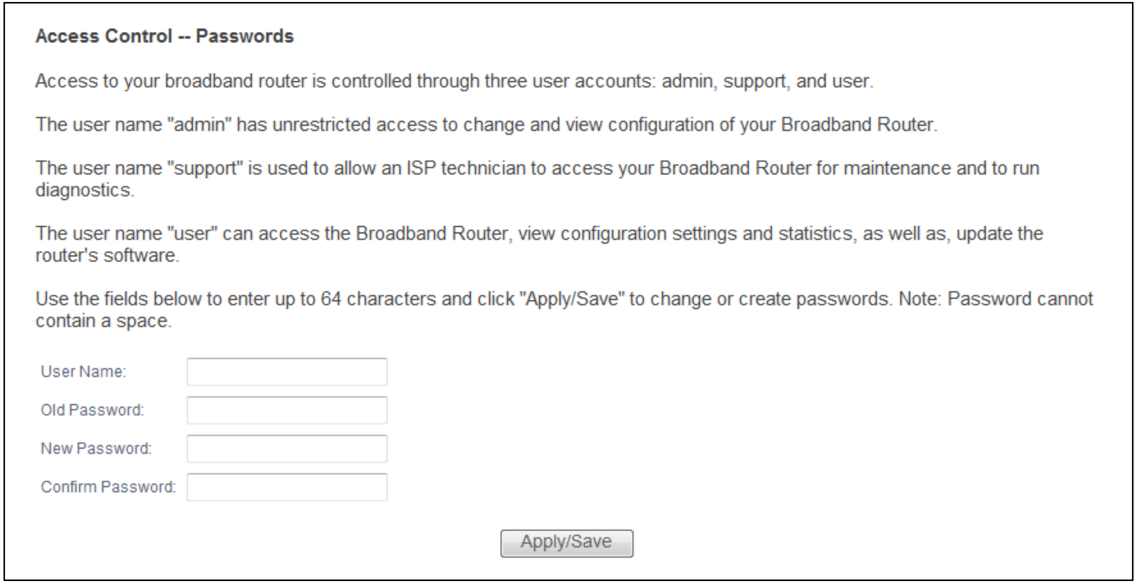
LABEL	DESCRIPTION
Automatically synchronize with Internet time servers	Select this to have the Router get the time from the specified Internet time servers.
First ~ Fifth NTP time server	Select an NTP time server from the drop-down list box. Otherwise, select **Other** and enter the IP address or URL (up to 29 extended ASCII characters in length) of your time server. Select **None** if you don't want to configure the time server. Check with your ISP/network administrator if you are unsure of this information.
Time zone offset	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start/End Date	Configure the day and time when Daylight Saving Time starts/ends if you enabled daylight saving. The **Time** fields use the 24 hour format.
Apply/Save	Click this button to save your changes.

User Passwords

28 Chapter

28.1 User Passwords

Click **Management > Access Control > Passwords** to change the login password.



Access Control -- Passwords

Access to your broadband router is controlled through three user accounts: admin, support, and user.

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

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

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

Use the fields below to enter up to 64 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Figure 131 Use Passwords

Table 119 User Passwords

LABEL	DESCRIPTION
User Name	Enter the name of one of the Router system accounts.
Old Password	Type the account’s default password or existing password.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Router.
Retype to confirm	Type the new password again for confirmation.
Apply/Save	Click this button to save your changes.

GPON Password

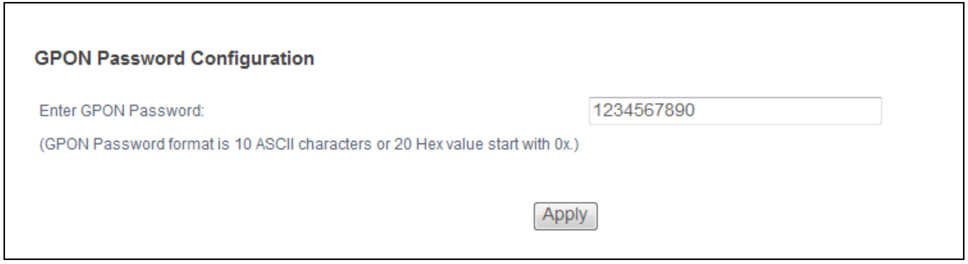
29

Chapter

29.1 GPON Password

Click **Management > GPON Password** to enter the password for your GPON Internet access account.

Figure 132 GPON Password



GPON Password Configuration

Enter GPON Password: 1234567890

(GPON Password format is 10 ASCII characters or 20 Hex value start with 0x.)

Table 120 GPON Password

LABEL	DESCRIPTION
Enter GPON Password	Enter the password for your GPON Internet access account.
Apply	Click this button to save and apply your changes.

Update Software

30 Chapter

30.1 Update Software

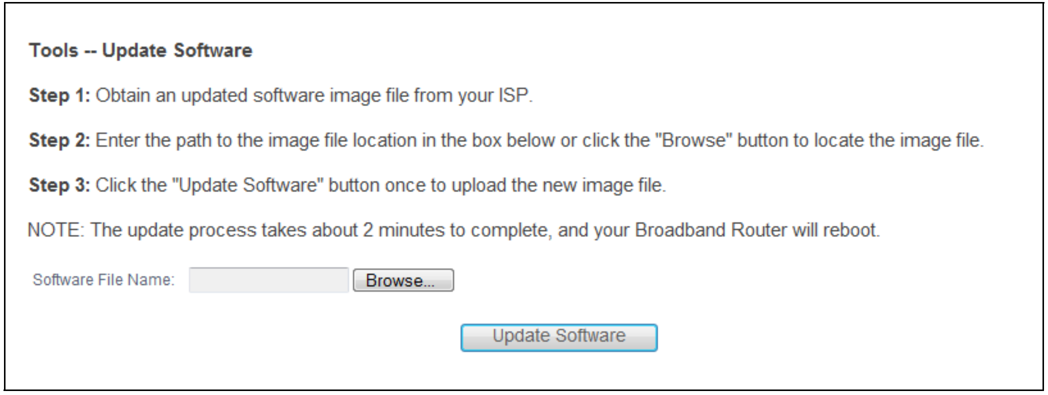
Click **Management > Update Software** to open the following screen where you can upload new software to your Router. You can download new software releases from your ISP to use to upgrade your device's performance.

Only use software for your device's specific model. Refer to the label on the bottom of your Router.

The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the Router while software upload is in progress!

Figure 133 Update Software



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 Broadband Router will reboot.

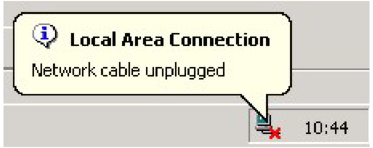
Table 121 Update Software

LABEL	DESCRIPTION
Software File Name	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Update Software	Click this to begin the upload process. This process may take up to two minutes.

After you see the software updating screen, wait two minutes before logging into the Router again.

The Router automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 134 Network Temporarily Disconnected



Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new software version in the **Device Info** screen.

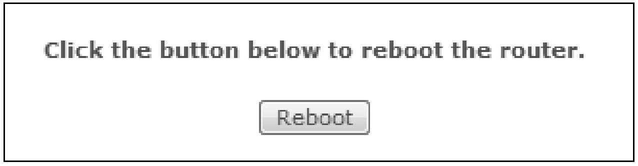
Reboot

31 Chapter

31.1 Restart Using the Web Configurator

Click **Management > Reboot** to open the following screen. Use this screen to restart the .

Figure 135 Reboot



Click the button below to reboot the router.

Troubleshooting

32 Chapter

32.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- Router Access and Login
- Internet Access
- Wireless Internet Access
- Phone Calls and VoIP
- UPnP

32.2 Power, Hardware Connections, and LEDs

The Router does not turn on. None of the LEDs turn on.

1 Make sure the Router is turned on.

2 Make sure you are using the power adaptor or cord included with the Router.

3 Make sure the power adaptor or cord is connected to the Router and plugged in to an appropriate power source. Make sure the power source is turned on.

4 Turn the Router off and on.

5 If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.3 on page 11.

2 Check the hardware connections. See Section 1.2 on page 9.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the Router off and on.

5 If the problem continues, contact the vendor.

32.3 Router Access and Login

I forgot the IP address for the Router.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the Router by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Router (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.2 on page 9.

I forgot the password.

1 The default password is random. Please refer to the label sticker at the bottom of the device.

2 If you can’t remember the password, you have to reset the device to its factory defaults. See Section 1.2 on page 9.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address (Section 4.1 on page 46), use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the Router.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.2 on page 9.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.

4 Reset the device to its factory defaults, and try to access the Router with the default IP address. See Section 1.2 on page 9.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Router using another service, such as Telnet. If you can access the Router, check the remote management settings and firewall rules to find out why the Router does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the Router.

1. Make sure you have entered the user name and password correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. You cannot log in to the web configurator while someone is using Telnet to access the Router. Log out of the Router in the other session, or ask the person who is logged in to log out.
3. Turn the Router off and on.
4. If this does not work, you have to reset the device to its factory defaults. See Section 32.2 on page 219.

I cannot Telnet to the Router.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

32.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.3 on page 11.
2. Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.

4. If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **Wifi/WPS** button or the **Network Setting > Wireless > General** screen.

5. Disconnect all the cables from your device, and follow the directions in Section 1.2 on page 9. again.

6. If the problem continues, contact your ISP.

🛠 I cannot access the Internet anymore. I had access to the Internet (with the Router), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See Section 1.3 on page 11.

2. Turn the Router off and on.

3. If the problem continues, contact your ISP.

🛠 The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.3 on page 11. If the Router is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2. Turn the Router off and on.

3. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

32.5 Wireless Internet Access

🛠 What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

What wireless security modes does my Router support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your Router are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

32.6 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1 Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

1 The **Telf** light should come on. Make sure that your telephone is connected to the **Telf1** port.

2 You can also check the VoIP status in the **System Info** screen.

3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

32.7 UPnP

🛠 When using UPnP and the Router reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the Router’s LAN port or from your computer.

2 Re-connect the Ethernet cable.

🛠 The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

🛠 I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

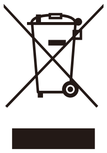
2 Restart the applications.

Appendix A

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Federal Communications Commission (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 generate, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one 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.

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, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

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

RF exposure warning

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.