User Guide

AXE11000 Wi-Fi 6E Gateway – CF60

Doc No. UG01465

Important notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless AXE11000 Wi-Fi 6E Gateway to transmit or receive such data.

Copyright

Note – This document is subject to change without notice.

Document history

This document relates to the following product:

NetComm AXE11000 Wi-Fi 6E Gateway – CF60

Ver.	Document description	Date
v1.00	Initial Document Release	5 December 2023
V1.01	Update branding	2 September 2025

Table i. – Document revision history

Contents

Overview

Introduction

This document provides you all the information you need to set up, configure and use the NetComm Wireless AXE11000 Wi-Fi 6E Gateway.

Prerequisites

To configure your Gateway a computing device with a web browser such as Microsoft® Edge, Mozilla Firefox® or Google Chrome™ is required.

Notation

The following symbols may be used in this document:

Note – This note contains useful information.

Important – This is important information that may require your attention.

Warning – This is a warning that may require immediate action in order to avoid damage or injury.

Setting up your Internet connection

Note – If you received your gateway from your service provider and they have provided you with their own instructions, refer to those to complete the setup. In some cases, the gateway has been pre-configured for you and is ready to use. Otherwise, you will need to complete the setup yourself.

Before you begin

Ensure that you have the following information from your service provider:

- How your Internet service will physically connect to your gateway.
- The settings specific to your type of service.

Connecting using Ethernet WAN

Ethernet WAN is the most common internet connection interface in Australia and New Zealand and covers most Australian NBN and New Zealand UFB network access technologies.

This type of Internet service uses the red WAN port on the back of the gateway to connect to the dedicated connection box installed by your wholesale provider, such as NBN.

Here's how things connect to the Ethernet WAN interface

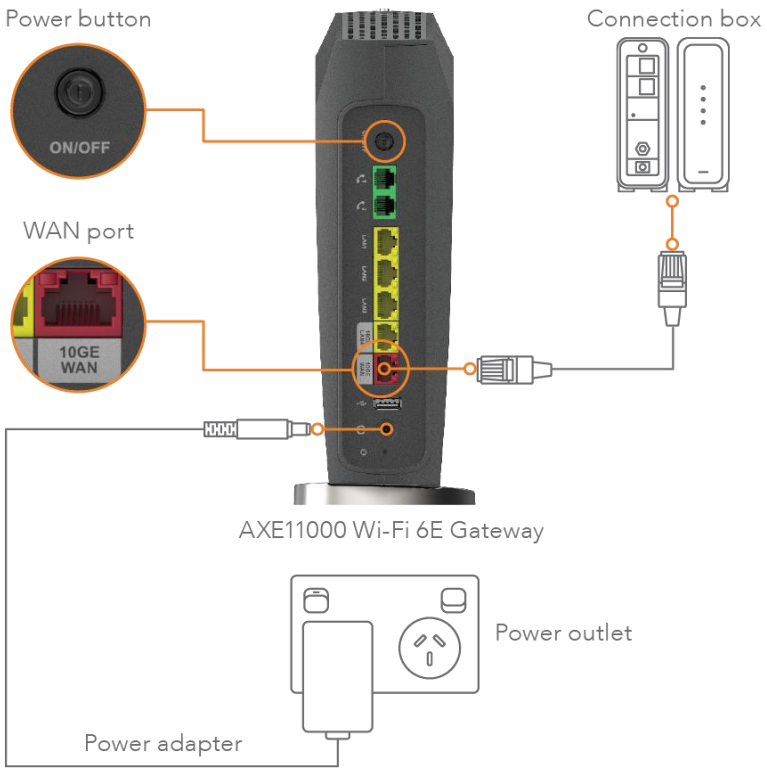


Figure 1 – Connecting to Ethernet WAN

Configuring your gateway

To complete the setup, you will need the following information from your service provider:

- Connection type (PPPoE/IPoE/Bridging)
- Other specifics depending on your connection type including 802.1P priority, VLAN Tag, WAN IP Address, Subnet Mask and DNS Servers
- VoIP settings from your service provider if you intend to use a phone with your service.

When you have the necessary information, follow these steps:

1. Push the power button on the rear of the gateway to turn it on. Wait a few minutes for it to complete start up.
2. Connect to the gateway using Wi-Fi, or by connecting an Ethernet cable from one of the LAN ports on the rear of the router to your Ethernet enabled computer.
3. Open a web browser and navigate to 192.168.20.1.
4. Follow the Basic Setup wizard to complete the configuration.

Connecting to Wi-Fi

Your Wi-Fi Security Card includes your unique network name and password. Type the information into your wireless device when connecting or scan the QR code that is printed on the card.

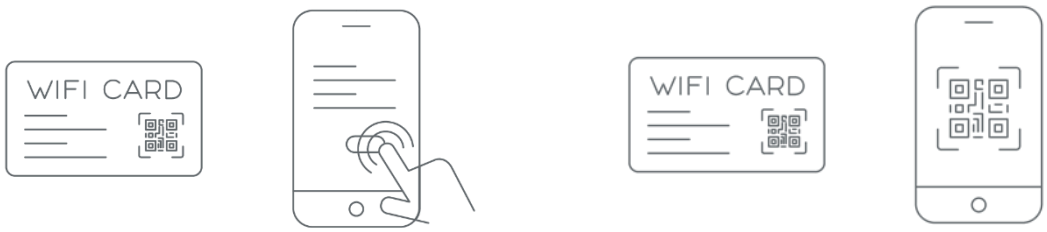


Figure 2 - Connecting with Wi-Fi

Turning Wi-Fi and lights on or off

To turn the Wi-Fi radio off and on, press the Wi-Fi button for **three** seconds then release. This is a quick way to completely disable / enable Wi-Fi on the gateway.

Figure 3 – Turning the Wi-Fi radio on and off

To turn the lights on the front of the device off and on, hold down the **WPS/LED** button for more than **six seconds** then release.

Figure 4 – Turning the LED lights on and off

Using WPS

Where supported by your devices, such as laptops and smart phones, you can use Wi-Fi Protected Setup (WPS) to connect your devices. To activate WPS on the gateway, press the WPS button for three seconds, then release. The WPS indicator blinks when WPS pairing mode is active. On your device, activate the WPS pairing functionality to complete the connection.

Figure 5 – Activating WPS

Connecting a telephone

Connect a regular telephone handset to the gateway as shown below. To use the phone, you will need to have a VoIP service from your carrier, complete the setup wizard and enter your VoIP settings.

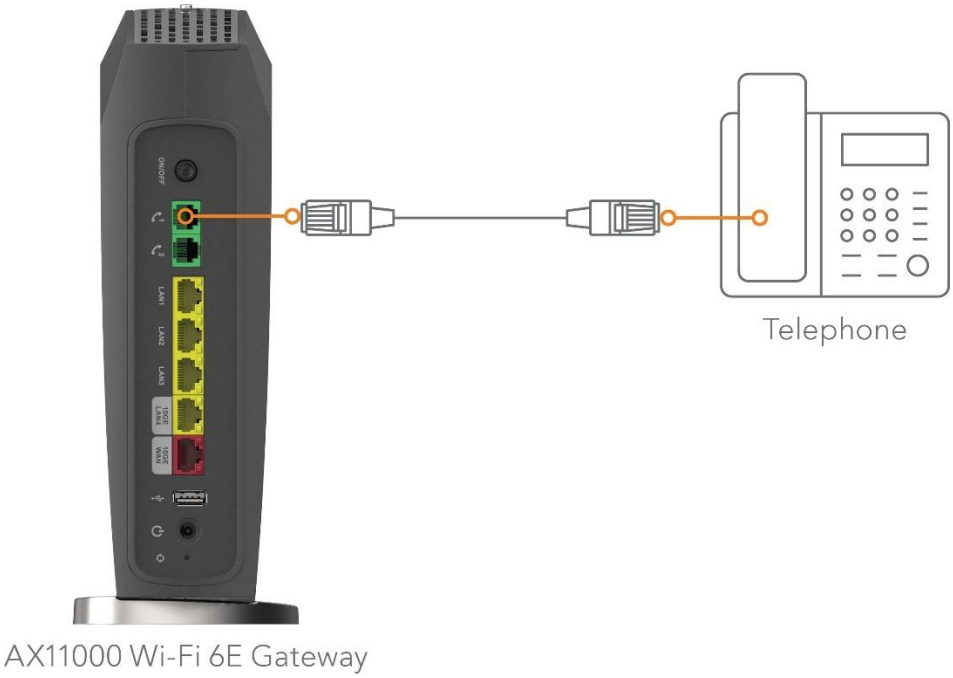


Figure 6 – Connecting a telephone

Interfaces

Front view

The front of the gateway is fitted with LED indicator lights to indicate the status of the gateway.

Figure 7 – Front LED lights

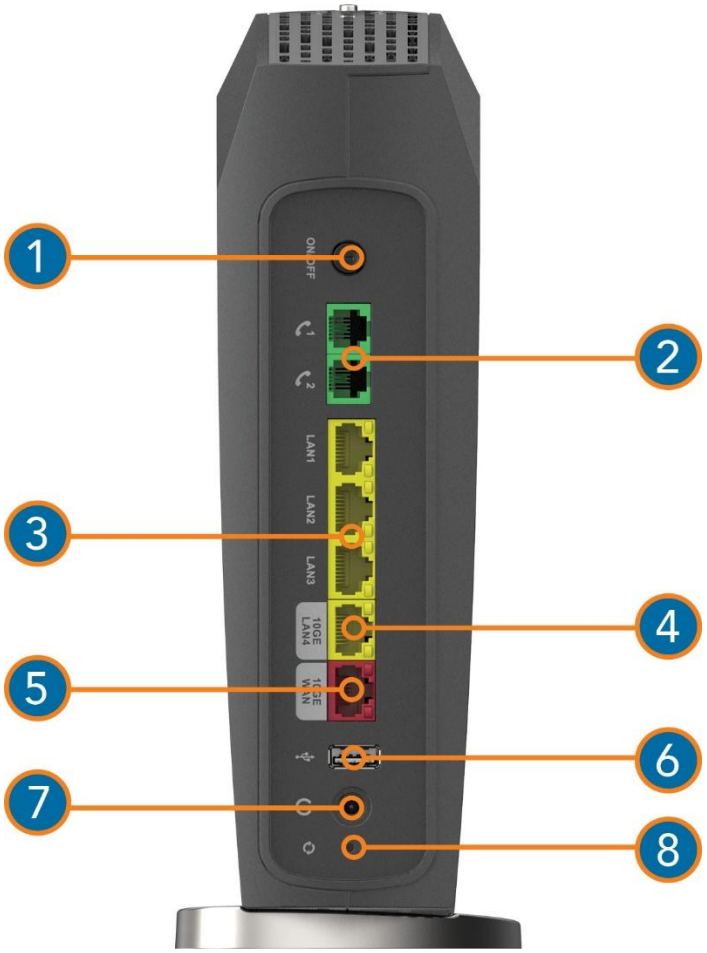
Front LED indicators

LED	Colour / Status		Description
Power		Blinking	The gateway is powered on and is initialising.
		Solid	The gateway is powered on and operating normally.
		Off	The gateway is powered off.
Internet		Solid	The gateway is connected to an internet service.
		Off	The gateway is not connected to the internet.
Wi-Fi		Solid	Wi-Fi is enabled.
		Blinking	WPS pairing triggered.
		Off	Wi-Fi is disabled.
Telephone		Solid	Telephone service (SIP) is operating normally.
		Blinking	Incoming call or the handset is in use.
		Off	Telephone service is disabled or not configured.

Table 1 – LED Indicators

Rear view

The power button, Ethernet ports and VoIP ports are located on the rear for easy organization.



No.	Item	Description
1	Power button	Push to turn the gateway on or off.
2	Phone ports	Connect standard telephones here for connection via a VoIP service.
3	LAN 1 – 3	Provides a 1 Gigabit network connection for local wired devices.
4	10GE LAN4	Provides a 10 Gigabit network connection for a local wired device. If you have a 10GE network adapter in your local device, connect it to this port for maximum speed.
5	10GE WAN	Connect your gateway to your internet service provider's equipment using this port. It provides a connection speed of up to 10 Gigabits per second.
6	USB port	Connect a storage device here to access it over the local network. The storage device must be formatted in NTFS, FAT or FAT32 file systems.
7	DC power jack	Connect the included power adapter here to power the gateway.
8	Reset button	Use a paperclip or similar object to hold the button down for 10 seconds to reset the gateway to the factory default settings.

Table 2 – Rear interfaces

Ethernet LED Indicators

Each of the Ethernet ports on the rear of the gateway include LED indicator lights to display the status of the physical Ethernet connection. The yellow LED indicator light indicates an Ethernet connection, and the green LED indicator light indicates data transfer.

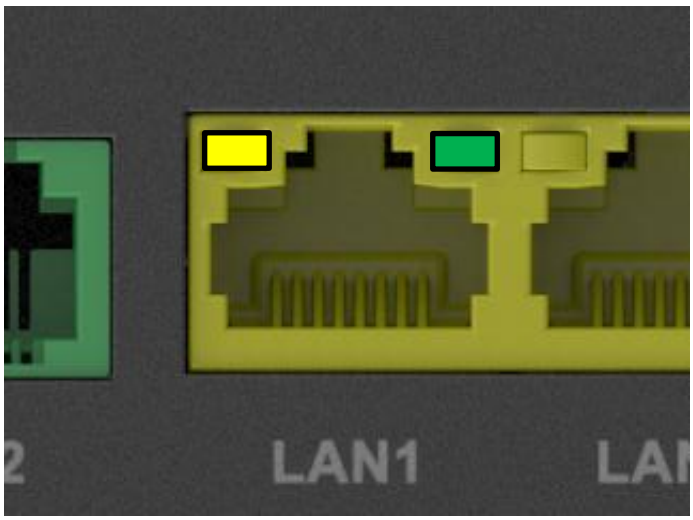


Figure 8 – Ethernet Port LED lights

LED	Colour / Status		Description
Yellow LED		Solid	Ethernet cable connected
		Off	Ethernet cable not connected or not functional
Green LED		Blinking	Data is being transferred over the Ethernet connection
		Off	No data currently being transferred over the Ethernet connection

Table 3 – Ethernet LED indicators

Safety and product care

Your gateway is an electronic device that sends and receives radio signals. Please take the time to read this list of precautions that should be taken when installing and using the router.

- Do not disassemble the gateway. There are no user-serviceable parts.
- Do not allow the gateway to come into contact with liquid or moisture at any time. To clean the device, wipe it with a damp cloth.
- Do not restrict airflow around the device. This can lead to the device overheating.
- Do not place the device in direct sunlight or in hot areas.

Transport and handling

When transporting the gateway, we recommend returning the product in its original packaging. This helps to reduce the risk of damage to the product.

Attention – In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

Placement of your Gateway

The wireless connection between your Gateway and your wireless devices will be strong when they are in close proximity and have direct line of sight. As your client device moves further away from the Gateway or solid objects block direct line of sight to the router, your wireless connection and performance may degrade. This may or may not be directly noticeable and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five metres from the Gateway to see if distance is the problem.

Note – While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this check list may help.

Avoiding obstacles and interference

Avoid placing your Gateway near devices that may emit radio “noise,” such as microwave ovens or other dense objects that can inhibit wireless communication, including:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal’s path (between your devices and the Gateway).

Cordless phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

Try moving cordless phones away from your Gateway and your wireless-enabled computers.

Unplug and remove the battery from any cordless phone that operates on the 2.4GHz or 5GHz band (check manufacturer’s information). If this fixes the problem, your phone may be interfering with the Gateway.

If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Gateway to channel 11. See your phone’s user manual for detailed instructions.

If necessary, consider switching to a 900MHz or 1800MHz cordless phone.

Advanced configuration of the Gateway

To perform advanced configuration of the Gateway, you can access its web interface:

1 Push the power button on the rear of the Gateway to turn it on. Wait a few minutes for it to complete starting up.

2 Open a web browser and navigate to 192.168.20.1.

3 At the login screen, admin into the Username field. In the Password field type the unique password printed on the label on the bottom of the Gateway, then select the Login button. If you have changed the password, enter your chosen password instead.

Figure 9 – Login

4 If this is your first time configuring the Gateway, select Basic Setup from the menu on the left side of the screen to run through the configuration wizard. See Basic Setup for further information regarding the Basic Setup configuration wizard.

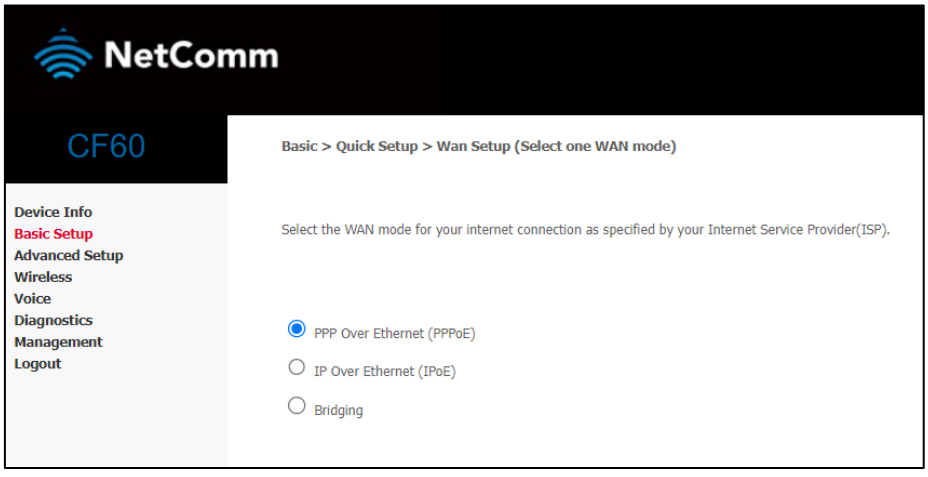
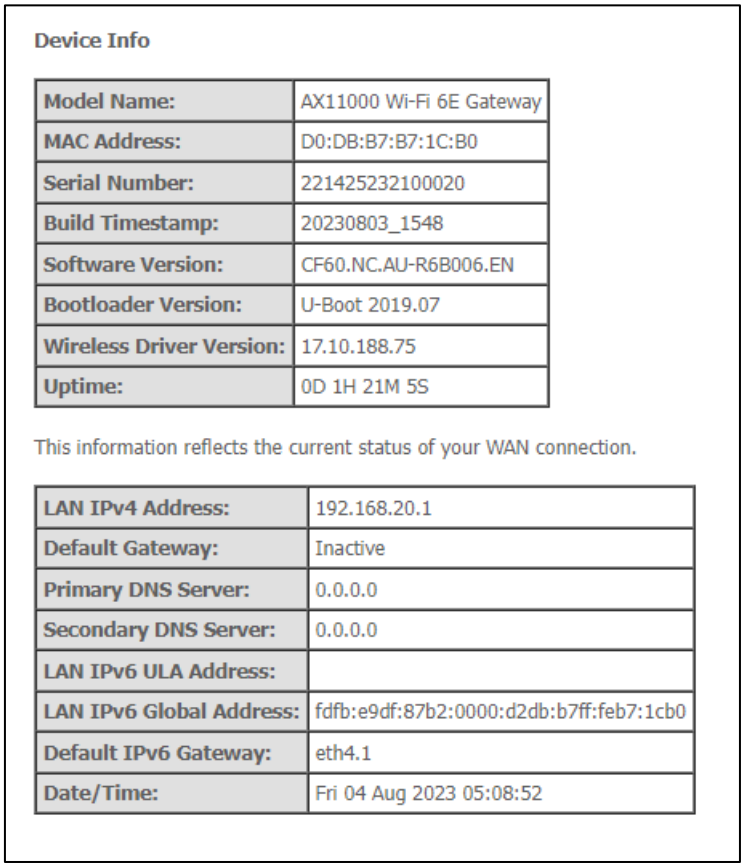


Figure 10 – Basic Setup

The Device Info - Summary page is first displayed after you have successfully logged into the Gateway. This page gives you an overview of important information regarding the gateway and WAN connection.



Device Info

Model Name:	AX11000 Wi-Fi 6E Gateway
MAC Address:	D0:DB:B7:B7:1C:B0
Serial Number:	221425232100020
Build Timestamp:	20230803_1548
Software Version:	CF60.NC.AU-R6B006.EN
Bootloader Version:	U-Boot 2019.07
Wireless Driver Version:	17.10.188.75
Uptime:	0D 1H 21M 5S

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.20.1
Default Gateway:	Inactive
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
LAN IPv6 Global Address:	fdfb:e9df:87b2:0000:d2db:b7ff:feb7:1cb0
Default IPv6 Gateway:	eth4.1
Date/Time:	Fri 04 Aug 2023 05:08:52

Figure 11 – Device Info

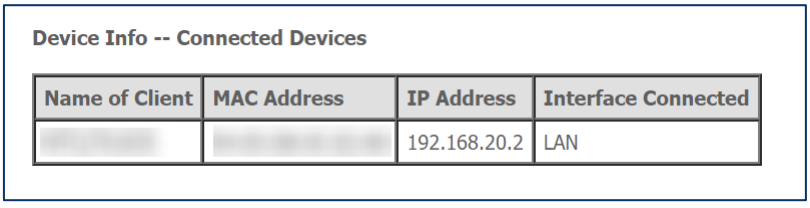
To navigate to other areas of the user interface for advanced configuration, select an item from the menu on the left side of the screen.

Device info

The Device Info pages provide detailed information on the status of the Gateway. The first page – Device Info summary, is detailed above.

Connected devices

The Connected devices page provides details about devices connected via both Wi-Fi and Ethernet to the Gateway.



Device Info -- Connected Devices

Name of Client	MAC Address	IP Address	Interface Connected
[redacted]	[redacted]	192.168.20.2	LAN

Figure 12 – Device Info - Connected Devices

WAN

The WAN page displays information about the WAN connection.

WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Proxy	Igmp Source	MLD Proxy	MLD Source	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address	Uptime
eth4.1 (Ethernet)	ipoe_eth4_eth4	IPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown		0D 0H 0M 0S
eth4.2 (Ethernet)	ipoe_eth4_eth4.10	IPoE	10	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown		0D 0H 0M 0S

Figure 13 – Device Info - WAN

Statistics

LAN and WLAN

The LAN and WAN page displays information about the LAN and Wi-Fi network connections. Select the Reset Statistics button to reset all of the statistics about the connections to 0.

Statistics -- LAN&WLAN

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
LAN1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LAN2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
LAN3	737480	5594	0	0	122114	790	4714	90	2367333	5912	0	0	39262	194	5242	476
LAN4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2.4G	0	0	0	14	0	0	0	0	100644	794	0	403	0	794	0	485
6G	0	0	0	14	0	0	0	0	95270	777	0	387	0	777	0	485
5G	0	0	0	14	0	0	0	0	95180	776	0	361	0	776	0	485

Reset Statistics

Figure 14 – Device Info - WAN

Route

The Route page displays the Routes on the Gateway.

Device Info -- Route

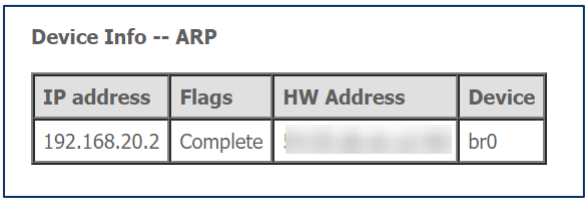
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.20.0	0.0.0.0	255.255.255.0	U	0	cpe-ipintf-1	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	cpe-ipintf-1	br0

Figure 15 – Device Info - Route

ARP

The ARP page displays the Adress Resolution Protocol (ARP) table for the Gateway. The ARP table displays a list of network interfaces connected to the gateway, including MAC addresses.



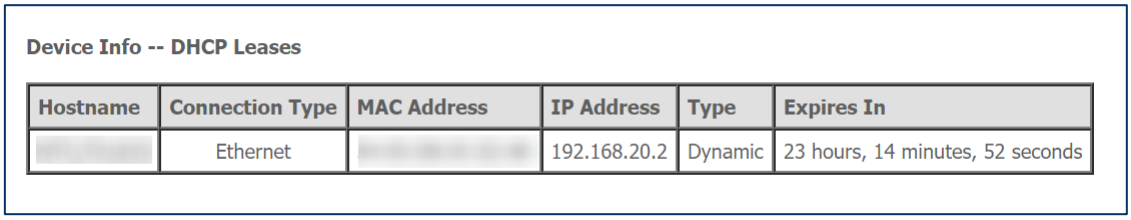
Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.20.2	Complete	[redacted]	br0

Figure 16 – Device Info - ARP

DHCP

The DHCP Leases page displays information about devices connected to the network using DHCP, including Hostname, MAC address, IP address type (Dynamic or Status) and the DHCP lease expiry time.



Device Info -- DHCP Leases

Hostname	Connection Type	MAC Address	IP Address	Type	Expires In
[redacted]	Ethernet	[redacted]	192.168.20.2	Dynamic	23 hours, 14 minutes, 52 seconds

Figure 17 – Device Info - ARP

CPU & Memory

The CPU & Memory page displays graphs of the current system resource usage on the Gateway.

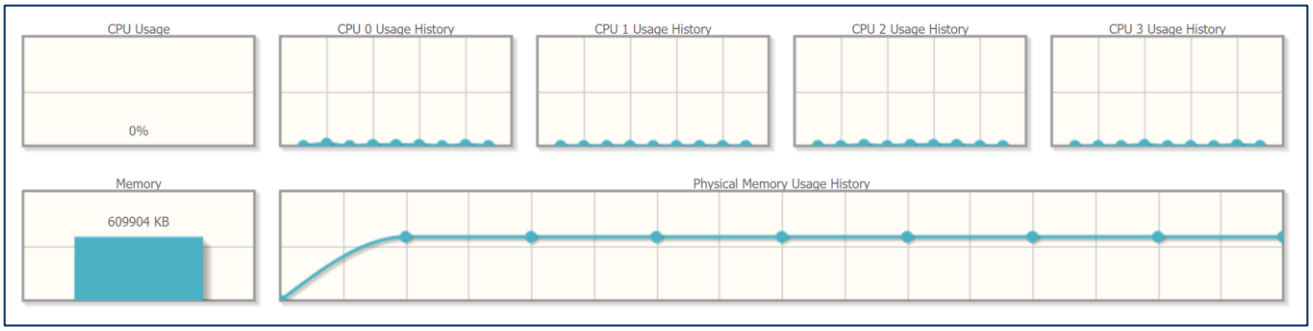


Figure 18 – Device Info – CPU and Memory

System info

The System Info page provides detailed information on the current system status, including CPU and memory usage and the inbuilt flash storage availability.

System info

CPU info

time	CPU number	usr(percentage)	sys(percentage)	iowait(percentage)	irq(percentage)	soft(percentage)	idle(percentage)
04:36:08	3	0.20	0.53	0.02	0.00	0.00	99.25
04:36:08	2	0.49	0.34	0.03	0.00	0.00	99.13
04:36:08	1	0.55	0.49	0.03	0.00	0.00	98.93
04:36:08	0	0.51	0.45	0.01	0.00	0.06	98.96

Flash info

Main space1 total(KB)	Main space1 used(KB)	Main space1 available(KB)	Main space2 total(KB)	Main space2 used(KB)	Main space2 available(KB)	Container space total(KB)	Container space used(KB)	Container space available(KB)
7608704	47512	7561192	7608704	47512	7561192	1983056	6012	1858260

Memory info

MemTotal(KB)	Main file system(KB)	VmHWMTotal(KB)	free(KB)
1019380	138547	498700	382133

Detail info about the memory:

Pid	VmPeak(KB)	VmHWM(KB)	VmExe/File size(KB)	Name
1	1300	4	1012	init
13623	1788	1240	12	systeminfo
13629	1300	4	1012	cat
1618	1884	80	8	lightbox
1632	2284	1380	16	vtp_pc

Figure 19 – Device Info – System info

Basic setup

The Basic Setup configuration wizard guides you through setting up your Internet connection. To complete the wizard, you will need some information about your connection from your Internet Service Provider, such as the WAN connection type, authentication methods, login credentials (if required) and other settings. To perform installation also ensure you have connected the WAN port on your Gateway to your ISP provided network termination device using the supplied Ethernet cable.

Note that in many cases, the gateway may have been pre-configured for you by your provider and therefore we recommend that you do not run the basic setup if everything is working.

1 Select the WAN mode for your connection as specified by your ISP. The available options are PPP over Ethernet (PPPoE), IP over Ethernet (IPoE) and Bridging.

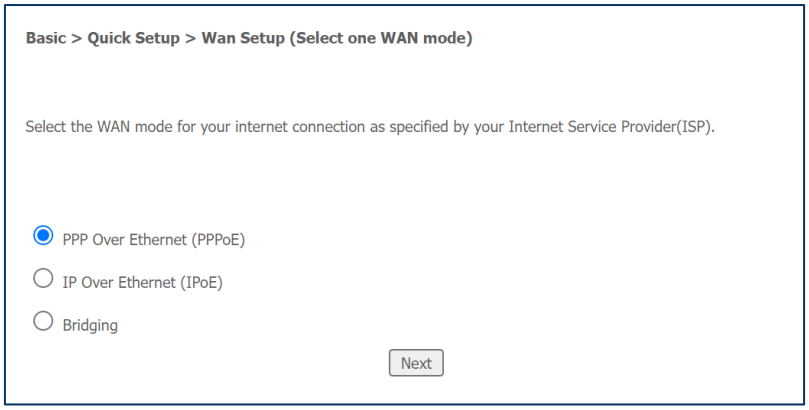


Figure 20 – Basic Setup – Select WAN mode

2 Set your VLAN tag if specified by your ISP.

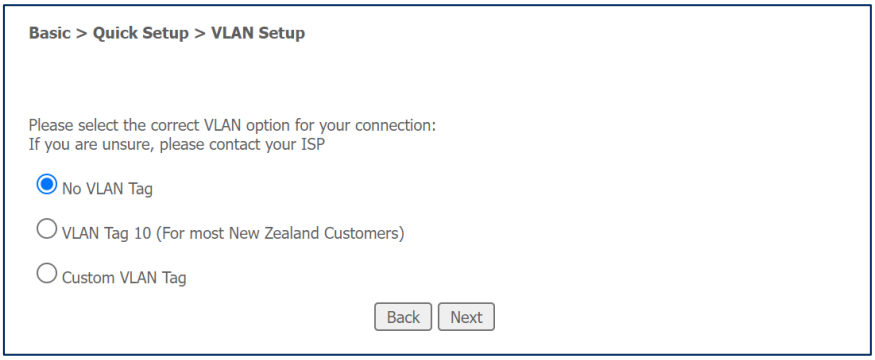


Figure 21 – Basic Setup – Set VLAN tag

3 If you are using PPPoE, enter the User ID and password associated with your connection.

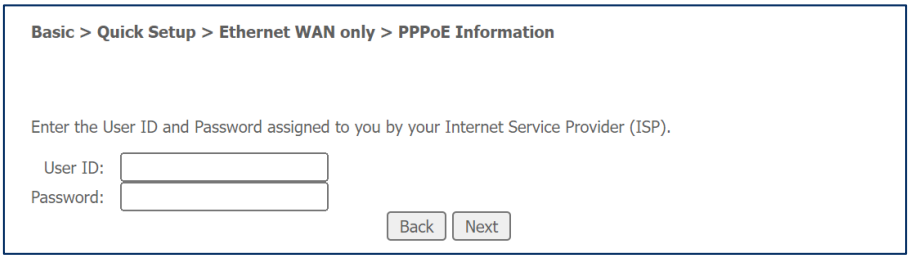


Figure 22 – Basic Setup – PPPoE Username and password

4 A summary of your settings will be displayed. Ensure they are correct, then select **Apply / Save** to create the connection.

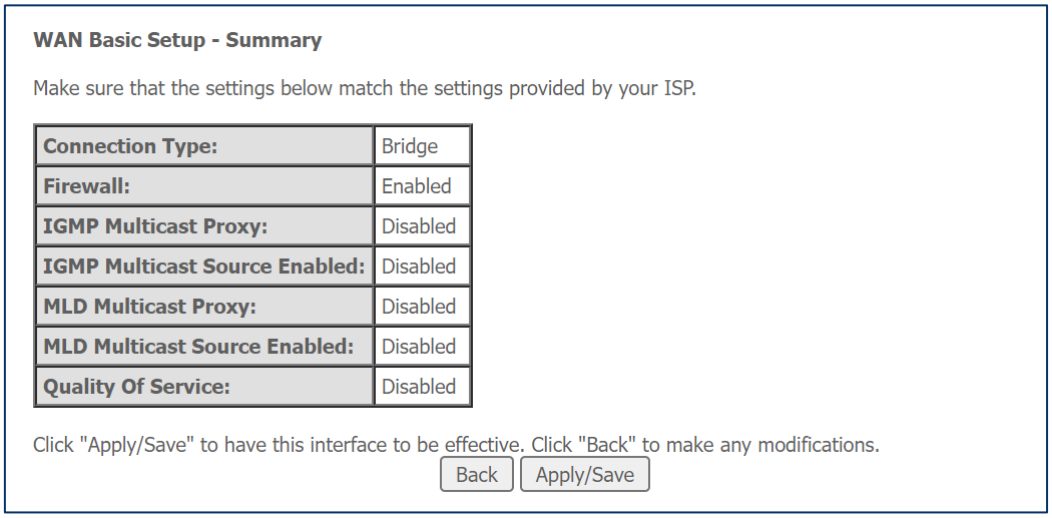


Figure 23 – Basic Setup – Save configuration

5 Ensure your internet connection is working by navigating to a website such as https://www.google.com. If you are experiencing issues, contact your ISP to validate your connection is active and that the required settings are correct.

Advanced setup

This section provides a variety of options for configuring the gateway for advanced functions. These include settings related to the WAN service, Local Area Network (LAN), Network Address Translation (NAT), MAC filtering, Parental control, Firewall, Quality of Service (QoS), Routing and more. In most cases, you will not need to modify settings in the Advanced setup section, and we recommend that you do not change any of the settings unless you are sure of the effect that the changes will have, and have a backup of your current working configuration.

Layer2 Interface

ETH Interface

The ETH interface page allows you to add or remove ETH WAN interfaces.

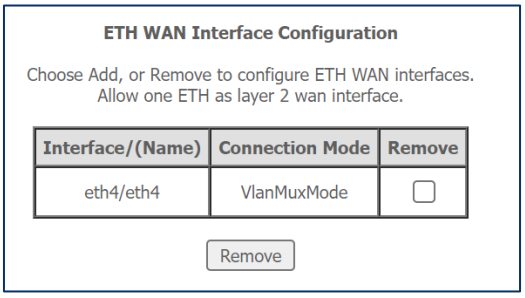


Figure 24 – Layer2 Interface – ETH Interface

Note – When the eth4 - ETH WAN Layer 2 interface is removed, the ETH WAN port will behave as an additional Ethernet LAN port.

WAN Service

The WAN Service page displays the current Wide Area Network service setup and allows you to configure the Gateway's connection to the Internet. In most circumstances a WAN connection will be preconfigured by your ISP.

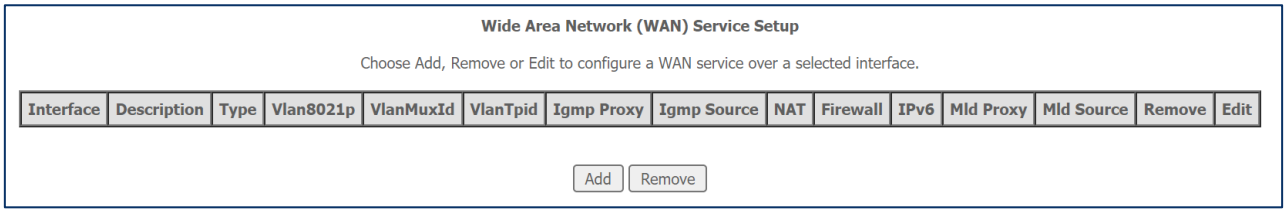


Figure 25 – WAN Service

To add a WAN service:

1 Select the Add button. The WAN Service Interface Configuration page is shown. Select an Interface for the WAN service.

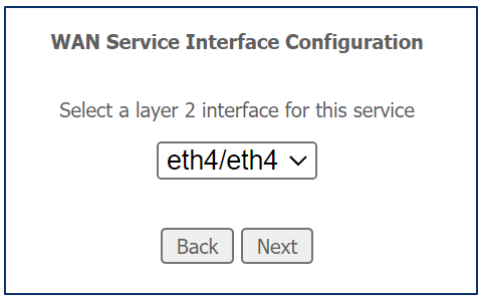


Figure 26 – WAN Service - Interface Configuration

2 Select a WAN service type to use with the WAN connection. The available options are **PPP over Ethernet (PPPoE)**, **IP over Ethernet (IPoE)** and **Bridging**. Enter a **Service Description** to identify the connection, an **802.1P Priority**, an **802.1Q VLAN ID** and a **VLAN TPID**. If using PPPoE or IPoE enter the **Internet Selection Protocol**. Depending on your chosen type, refer to the below sections for your connection type to complete the WAN configuration.

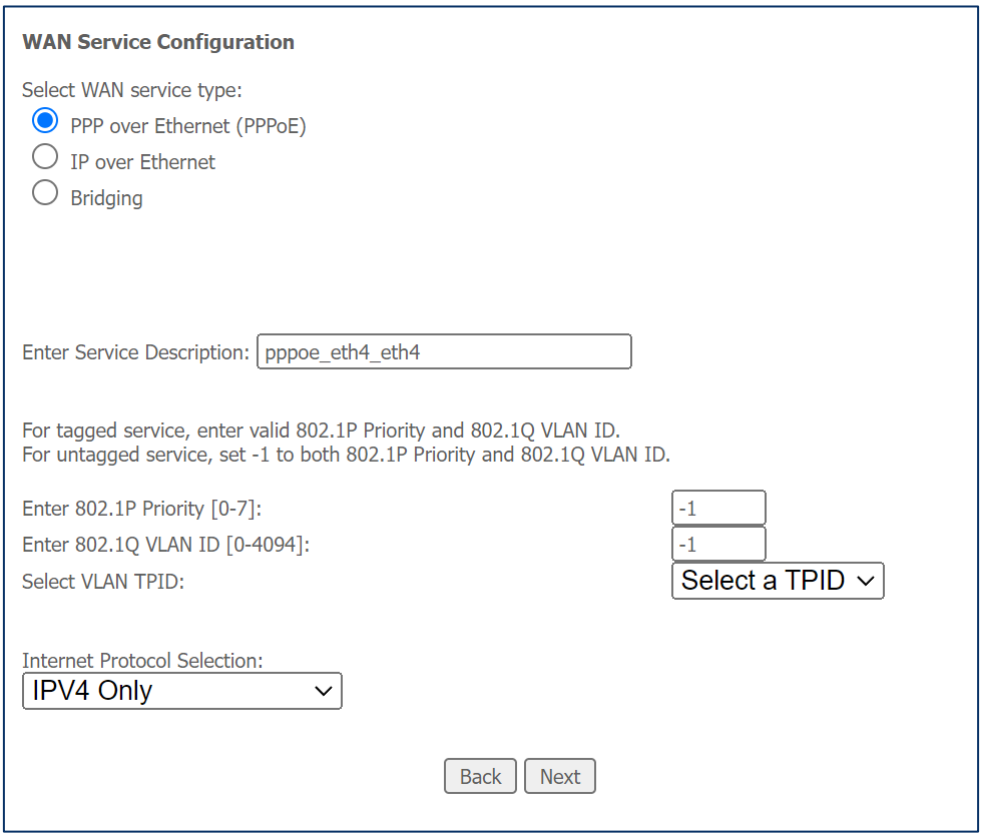


Figure 27 – WAN Service – WAN Service Configuration

PPPoE

If configuring the WAN connection for PPPoE:

1 Enter the Username and Password information. Select if you require NAT, Firewall, Static IP address or IGMP Multicast. This information may be provided by your ISP.

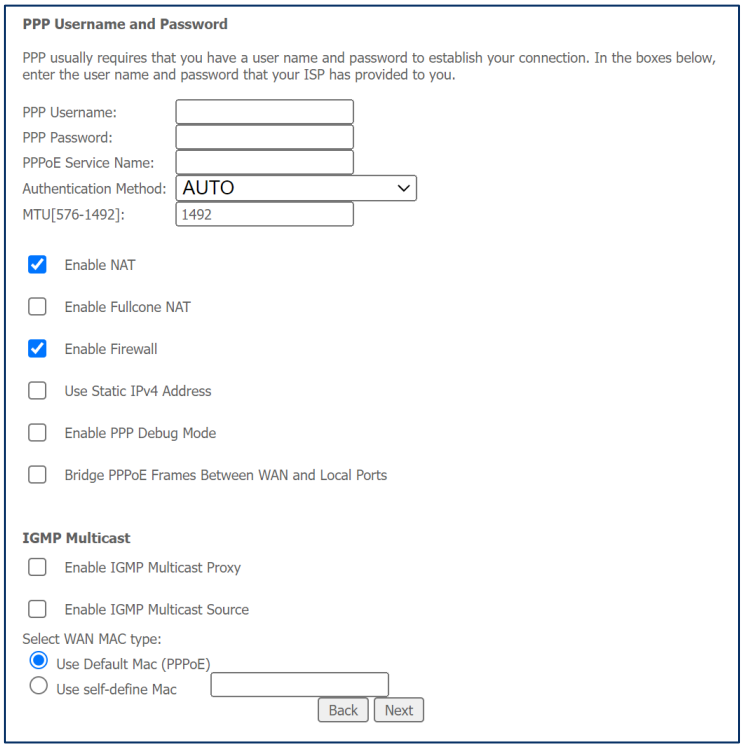


Figure 28 – WAN Service – WAN Service Configuration PPPoE

2 Select the Default Gateway for the connection. If multiple Gateways are available, they can be added to the Available Routed WAN Interfaces list in order of priority by using the arrow buttons.

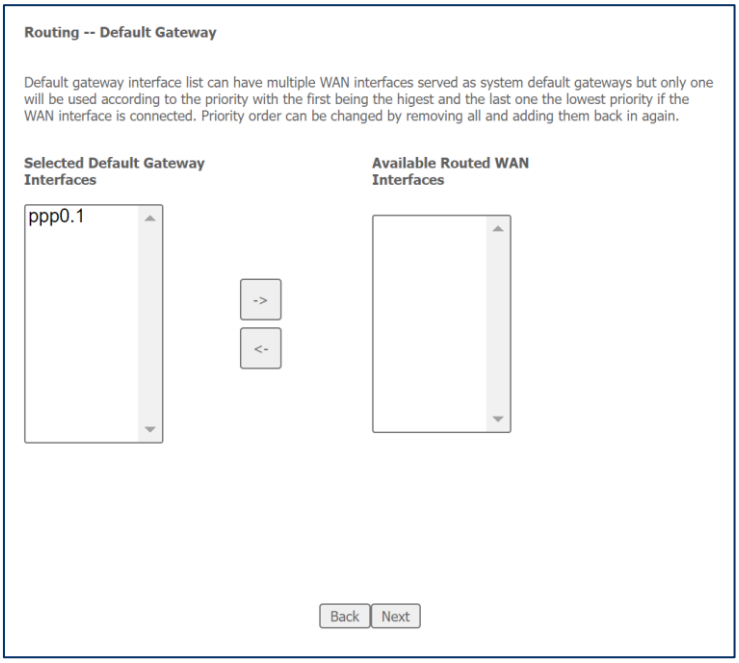


Figure 29 – WAN Service – WAN Service Configuration PPPoE

3 Configure where the DNS Server for the interface should be received from. To use the PPPoE WAN connection, use the first option. If you wish to use static DNS servers, such as Google or Cloudflare, enter them in the Static DNS IP addresses fields.

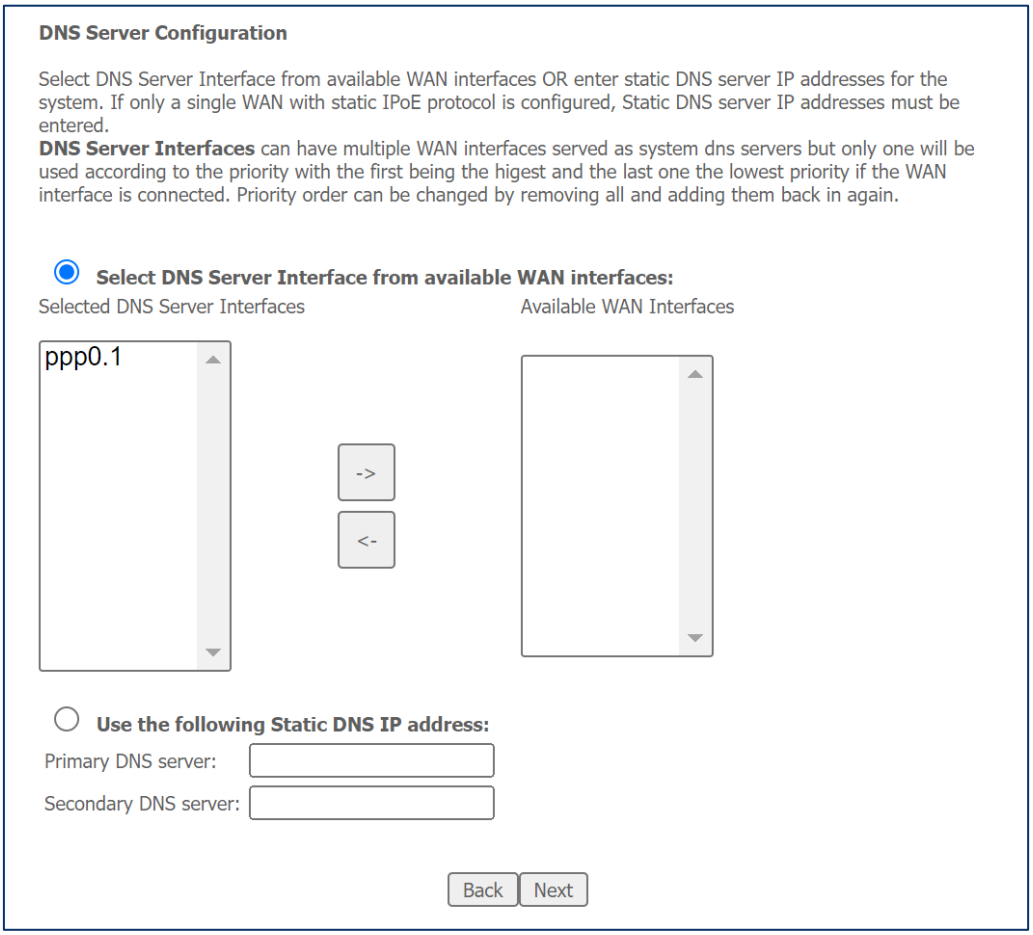


Figure 30 – WAN Service – WAN Service Configuration PPPoE

4 Review the WAN Setup – Summary page, then select Apply/Save to create the WAN connection.

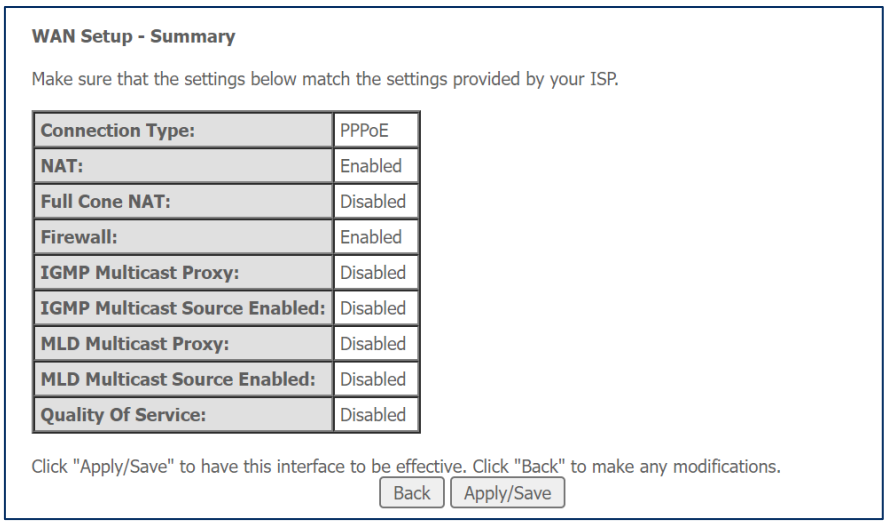


Figure 31 – WAN Service – WAN Service Configuration PPPoE

IPoE

If configuring the WAN connection for IPoE:

1 Enter information for the WAN IP.

If setting the Gateway to **Obtain an IP address automatically**, enter any IP options where they are provided by your ISP.

If setting the Gateway to **Use a static IP address** enter the WAN IP address, mask, gateway and DNS configuration as supplied by your ISP.

If required by your ISP, set a MAC address for the interface.

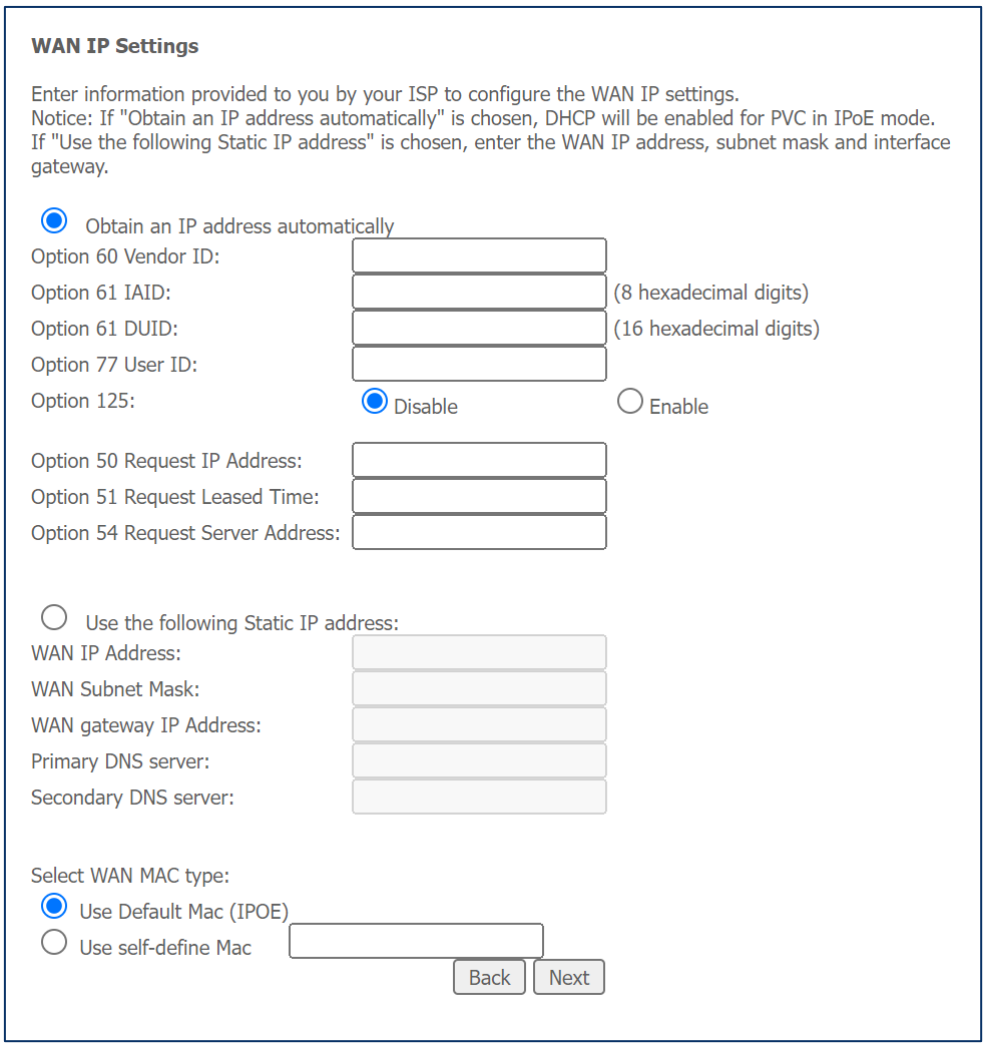


Figure 32 – WAN Service – WAN Service Configuration IPoE

2 Configure if NAT, Fullcone NAT or Firewall should be enabled on the WAN connection. Enter the MTU for connection. If required enable the IGMP Multicast Proxy and IGMP Multicast Source.

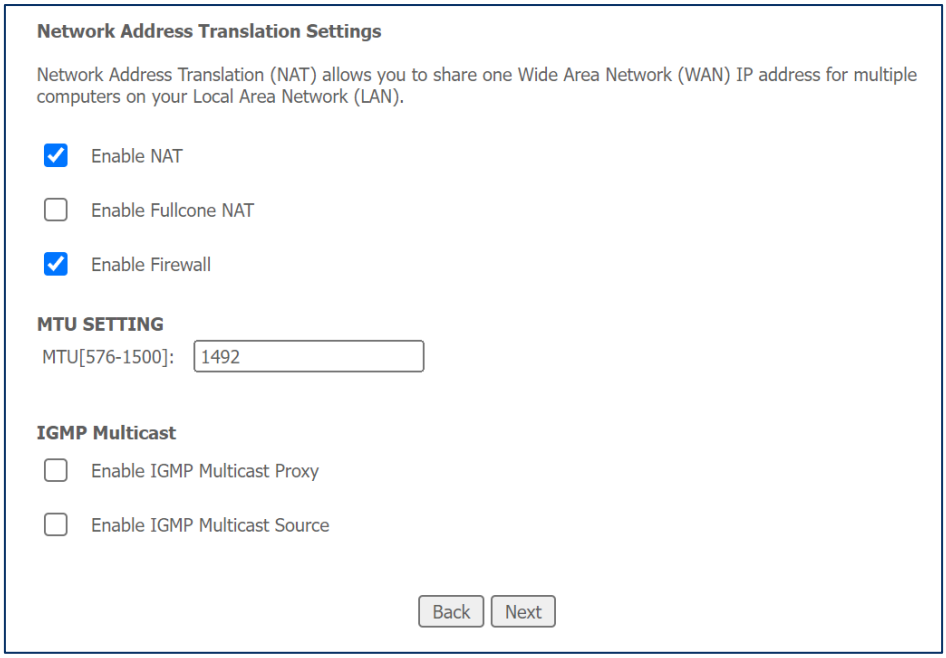


Figure 33 – WAN Service – WAN Service Configuration IPoE

3 Select the Default Gateway for the connection. If multiple Gateways are available, they can be added to the Available Routed WAN Interfaces list in order of priority by using the arrow buttons.

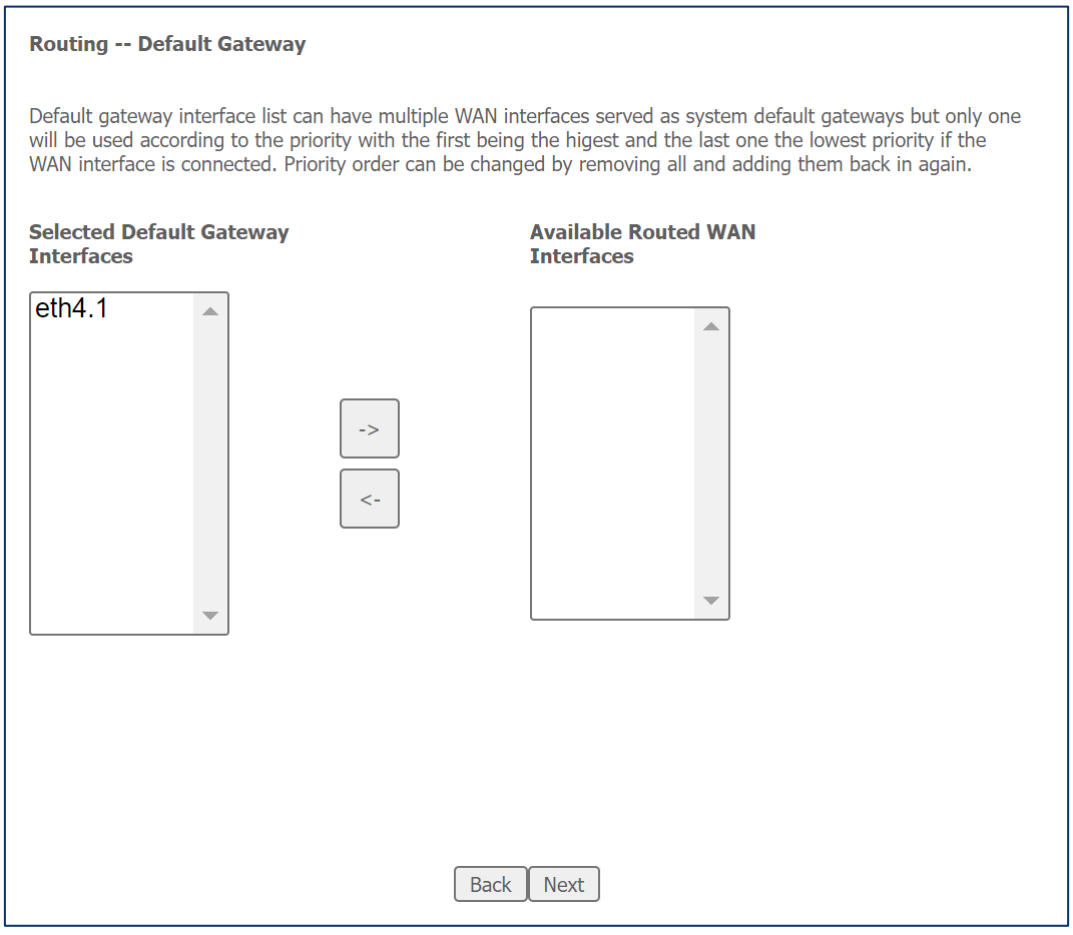


Figure 34 – WAN Service – WAN Service Configuration IPoE

4 Configure where the DNS Server for the interface should be received from. To use the IPoE WAN connection, use the first option. If you wish to use static DNS servers, such as Google or Cloudflare, enter them in the Static DNS IP addresses fields.

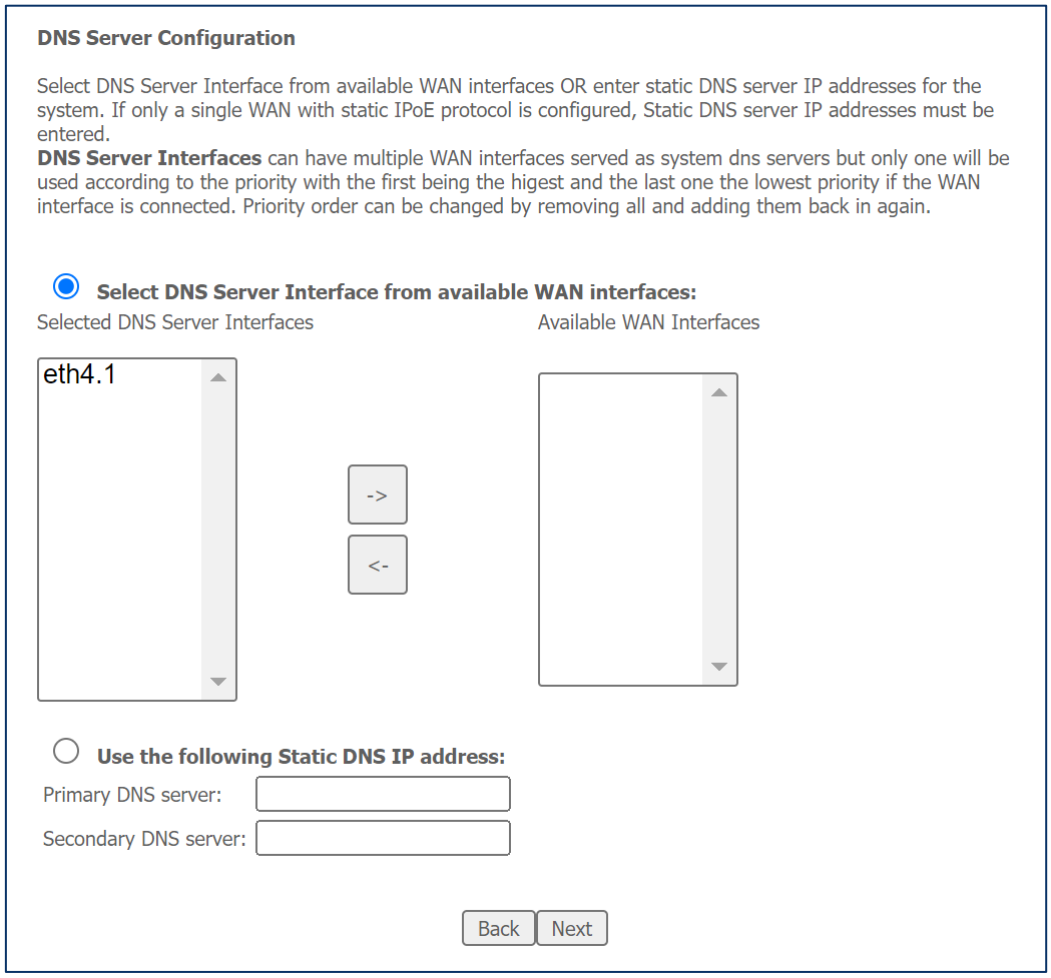


Figure 35 – WAN Service – WAN Service Configuration IPoE

5 Review the WAN Setup – Summary page, then select Apply/Save to create the WAN connection.

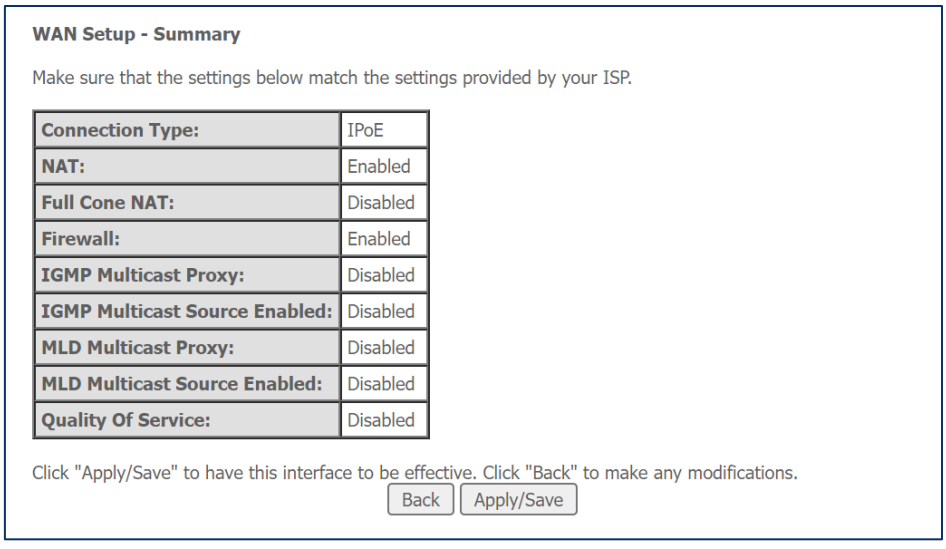


Figure 36 – WAN Service – WAN Service Configuration IPoE

Bridging

If configuring the WAN connection as Bridging:

1 Review the WAN Setup – Summary page, then select Apply/Save to create the WAN connection.

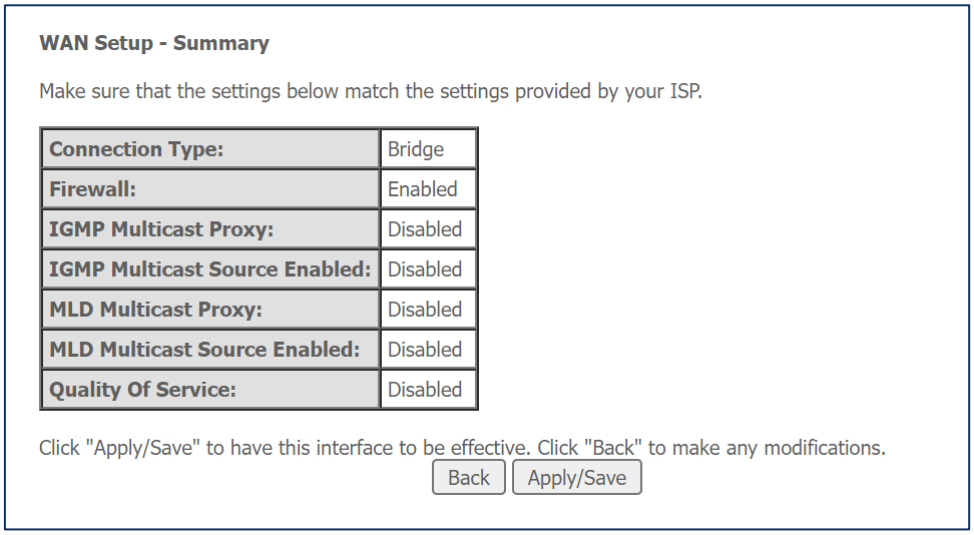


Figure 37 – WAN Service – WAN Service Configuration Bridging

LAN

IPv4 Autoconfig

The LAN page allows you to modify settings for the Local Area Network (LAN).

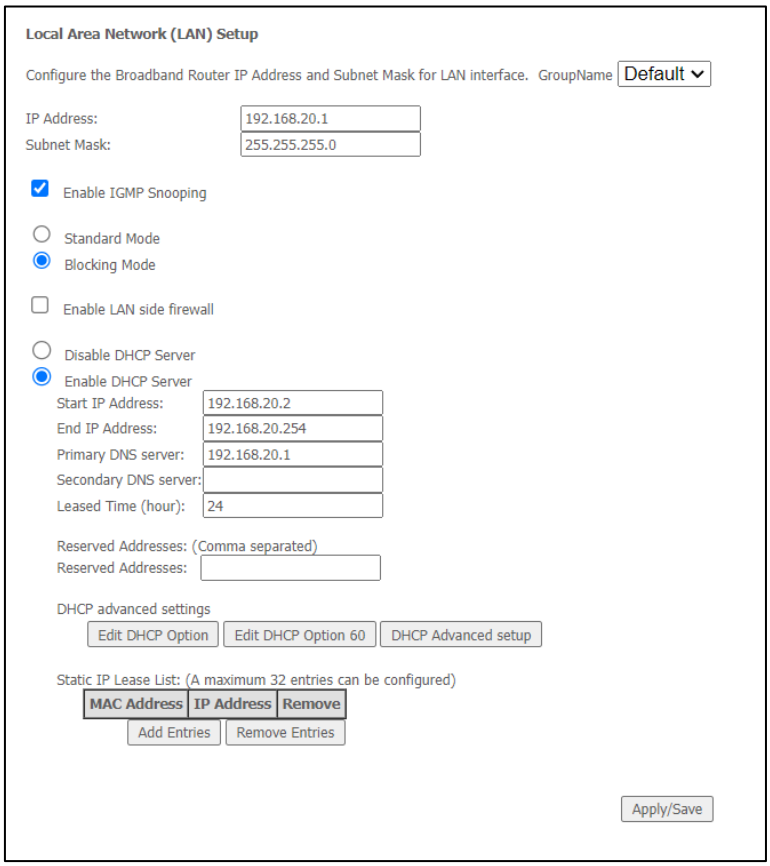


Figure 38 – LAN – IPv4 Autoconfig

The following options are available to configure:

Parameter	Definition
IP Address	Enter the Local IP Address to use for the Gateway.
Subnet Mask	Enter the subnet mask to define the subnet of the Local Network.
Enable IGMP Snooping	Enable IGMP Snooping and select the IGMP Snooping mode to use. Standard: allow all multicast traffic to LAN clients. Blocking: only allow multicast subscribed clients to receive multicast packets.
Enable LAN side Firewall	Enable the LAN side firewall to restrict network traffic between hosts on the local network. The LAN side firewall is helpful for situations where other devices on the LAN should not be able to interact with each other, for example, if the router is deployed in a café or as a public Wi-Fi access point.
Enable DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool. Note – Do not disable the DHCP server unless you understand that you will have to manually assign IP addresses to devices.

Table 4 – IPv4 Autoconfig settings table

Configuring the DHCP Server

The DHCP server on the Gateway allows you to automatically assign addresses to devices on the network. In most circumstances you will not need to modify these settings.

Note – Do not disable the DHCP server unless you understand that you will have to manually assign IP addresses to devices.

The following parameters can be modified:

Parameter	Definition
Enable / Disable DHCP Server	Select to Enable or Disable the DHCP server.
Start IP address	The first IP address in a range that should be issued to clients. E.g. 192.168.20.100
End IP address	The last IP address in a range that should be issued to clients. E.g. 192.168.20.200
Primary DNS server	The DNS server that clients should use. This will usually be the IP address of the gateway.
Secondary DNS server	A secondary DNS server that clients can use in the event the first is unavailable.
Lease time (hour)	The amount of time that the IP address should be valid on the client.
Reserved Addresses	A comma separated list of IP addresses in the range that should not be issued to clients e.g. 192.168.20.105,192.168.20.110

Table 5 – DHCP settings table

Creating static addresses for your devices

In certain circumstances you may want to ensure one of your devices always receives the same IP address.

To add a static IP address:

1 Select the Add Entries button. The Add Entries page opens.

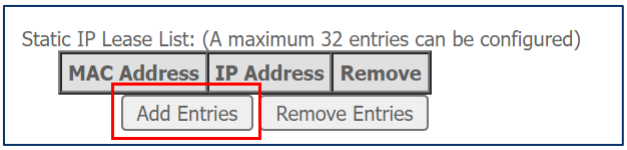


Figure 39 – LAN – IPv4 Autoconfig – Static IP address

2 In the **MAC Address** field, enter the MAC address of the device.

3 In the **IP Address** field, enter the IP address (within the DHCP range) that you wish to assign to the device.

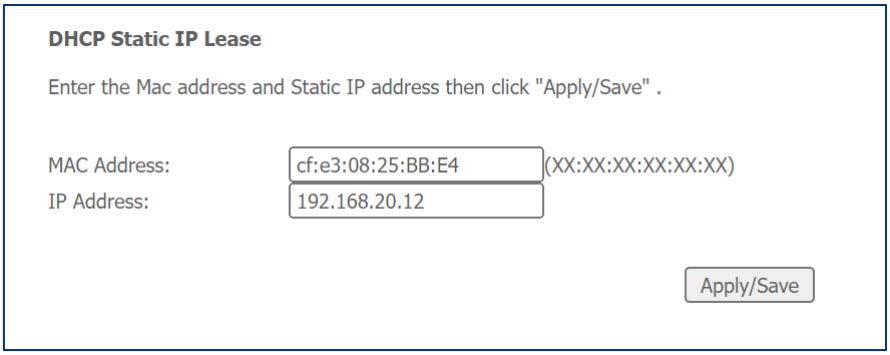


Figure 40 – LAN – IPv4 Autoconfig – Add Entries

4 Select Apply / Save to create the entry.

IPv6 Autoconfig

The IPv6 LAN Auto Configuration page allows you to configure IPv6 on the LAN.

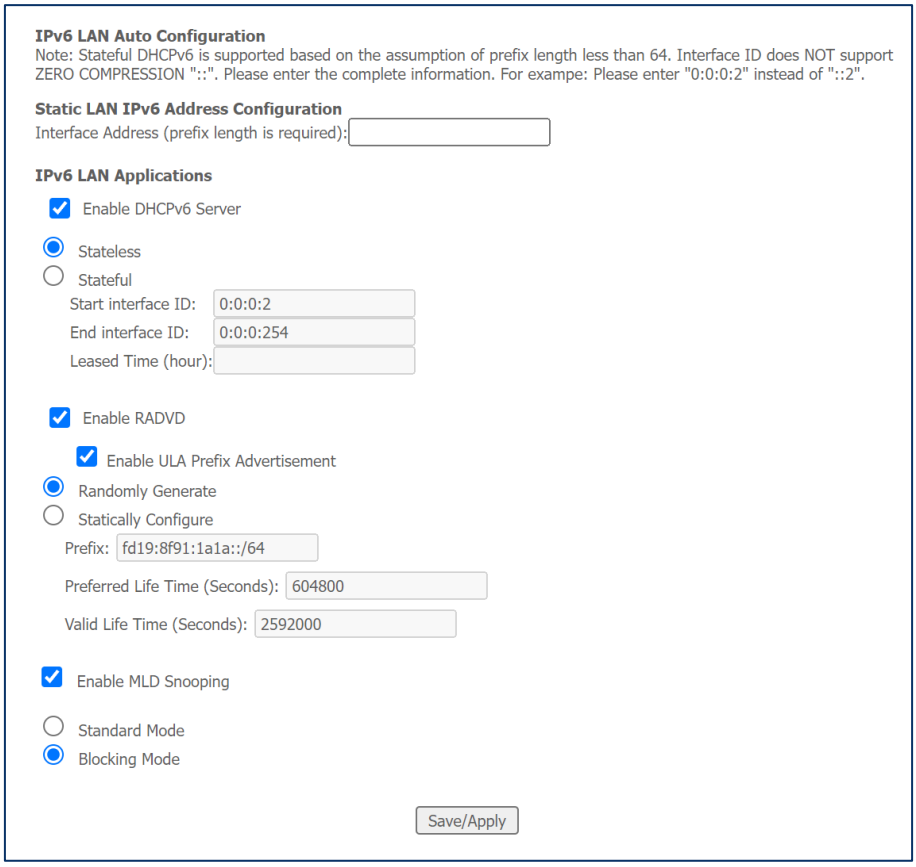


Figure 41 – LAN – IPv6 Autoconfig

The following parameters are configurable on the page:

Option	Definition
Static LAN IPv6 Address Configuration	Enter an IPv6 address that the Gateway should always use. This field is optional.

Enable DHCPv6 Server	Select the checkbox to enable the DHCPv6 Server.
Stateless (for DHCPv6 Server)	IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. This type of configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.
Stateful (for DHCPv6 Server)	This configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.
Enable RADVD	The Router Advertisement Daemon (radvd) is an open-source software product that implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbour Discovery Protocol (NDP) as specified in RFC 2461. The Router Advertisement Daemon is used by system administrators in stateless auto-configuration methods of network hosts on Internet Protocol version 6 networks. When IPv6 hosts configure their network interfaces, they broadcast router solicitation (RS) requests onto the network to discover available routers. The radvd software answers requests with router advertisement (RA) messages. In addition, radvd periodically broadcasts RA packets to the attached link to update network hosts. The router advertisement messages contain the routing prefix used on the link, the link maximum transmission unit (MTU), and the address of the responsible default router.
Enable Unique Local Addresses (ULA) Prefix Advertisement	Enable the use of unique local addresses. The router will advertise the IPv6 /64 prefix to new devices on the network.
Randomly Generate	Randomly generates the unique local addresses and the prefix.
Statically Configure	Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider (ISP).
Enable MLD Snooping	Select whether to enable or disable MLD Snooping on the router. The Multicast Listener Discovery (MLD) snooping function constrains the flooding of IPv6 multicast traffic on LANs on the router.
Standard / Blocking Mode	Select the mode for MLD snooping. Setting the mode to Blocking means that IPv6 multicast traffic will be dropped on the Gateway.

Table 6 – DHCPv6 settings table

VLAN Setting

The VLAN Setting page allows you to specify VLAN tagging on a specific Ethernet port.

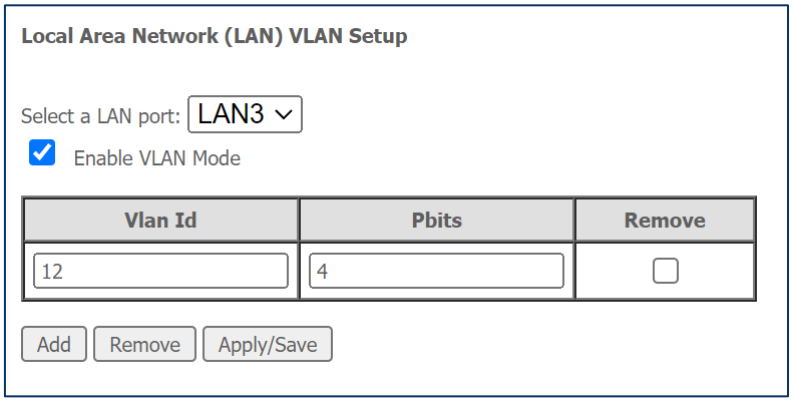


Figure 42 – LAN – VLAN Tagging

Select the LAN port using the drop-down menu, then Select the Add button. Enter the VLAN ID, then, in the Pbits field, enter a value from 0-7 indicating the priority bits that dictates the priority of the VLAN.

Select Apply/Save when you have finished.

NAT

Virtual Servers

Virtual Servers (also commonly referred to as port forwarding) allows for the direction of incoming traffic from the WAN side to an Internal network host with a private IP address on the LAN side.

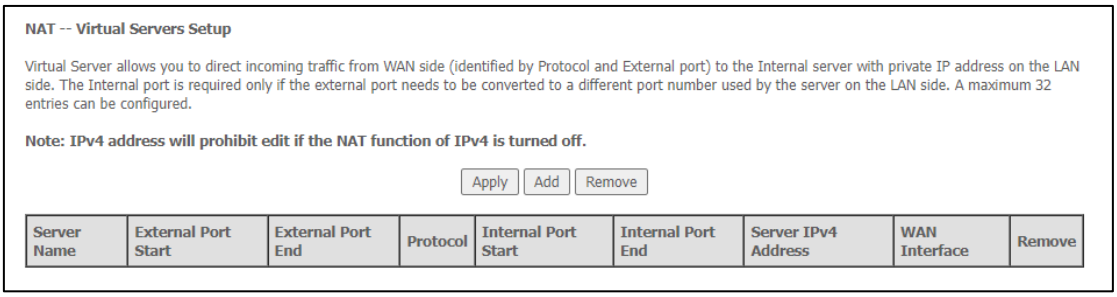


Figure 43 – NAT – Virtual Servers

Select the Add button to add a virtual server.

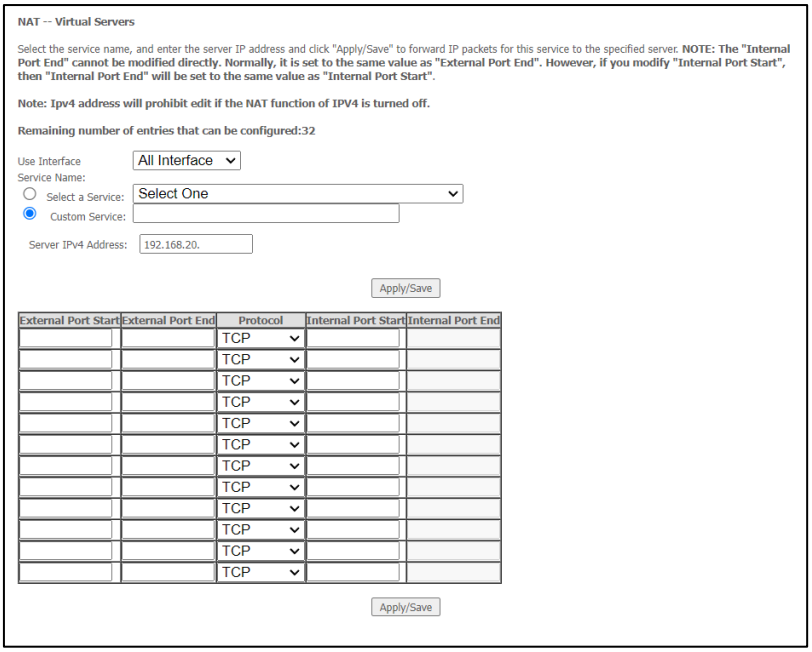


Figure 44 – NAT – Virtual Servers – Add virtual server

Field	Description
Select a Service or custom Server	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Server IP Address	Enter the IP address of the local server/host.
External Port Start	Enter the starting external port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
External Port End	Enter the ending external port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
Protocol	Options include TCP, UDP or TCP/UDP
Internal Port Start	Enter the starting internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
Internal Port End	Enter the ending internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.

Table 7 – NAT -- Virtual Server settings table

Select Save/Apply to save your settings when you have finished creating virtual servers.

Port Triggering

Some applications require specific ports in the Gateway's firewall to be open for access by remote parties. Port Triggering opens ports in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'.

The Gateway allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum of 32 entries can be configured.

This is a list of specific ports in the router's firewall that are open for access by remote parties.

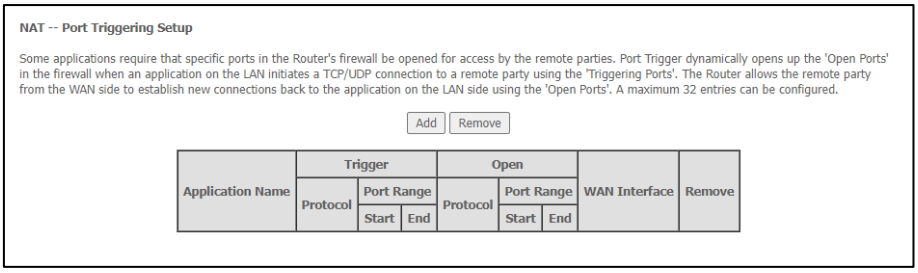


Figure 45 – NAT – Port triggering

Select the Add button and configure the port settings from an existing application in the drop-down list or create your own custom application.

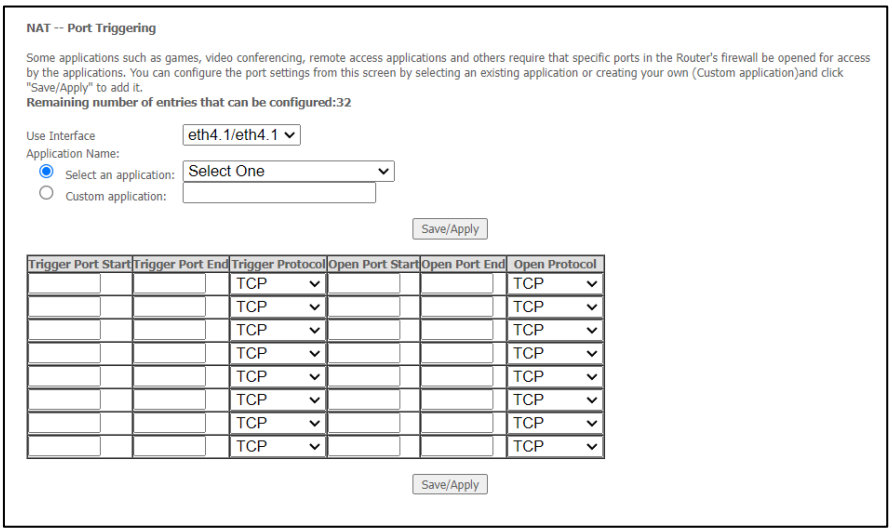


Figure 46 – NAT – Port triggering – Add port triggering rule

Field	Description
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Port End	Enter the ending trigger port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Trigger Protocol	Options include TCP, UDP or TCP/UDP.
Open Port Start	Enter the starting open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Open Port End	Enter the ending open port number (when you select Custom Application). When an application is selected the port range values are automatically entered.
Open Protocol	Options include TCP, UDP or TCP/UDP.

Table 8 – NAT -- Port Trigger Configuration settings

DMZ Host

DMZ stands for Demilitarized Zone. When the DMZ is configured, the Gateway will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table or being used in the Virtual Server table to the DMZ host.

Enter the DMZ Host IP address and select Apply to activate the DMZ host. To deactivate the DMZ Host function, clear the IP address field and select the Save/Apply button.

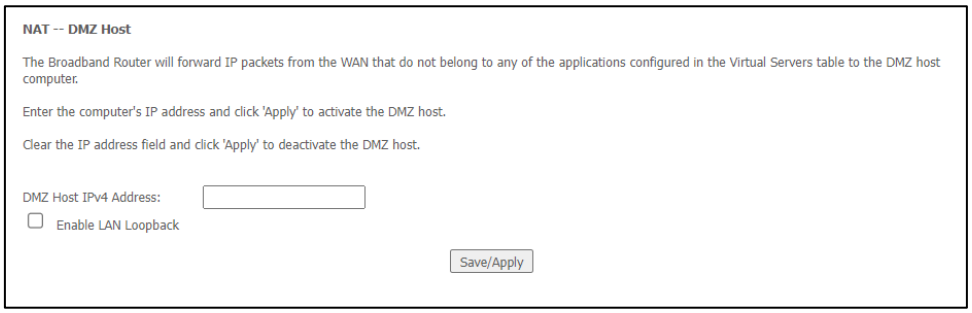


Figure 47 – NAT – DMZ Host

LAN Loopback can also be enabled.

LAN Loopback allows the LAN host to access another LAN host/server via the external IP Address of the router. Without NAT loopback you must use the internal IP address of the device when on the LAN side.

ALG

The Application Layer Gateway (ALG) is a feature which enables the Gateway to parse application layer packets and support address and port translation for certain protocols. We recommend that you leave these protocols enabled unless you have a specific reason for disabling them.

Figure 48 – NAT - ALG

Security

IP Filtering

MAC Filtering

The Gateway offers the ability to use MAC Address filtering when the WAN connection type is set to Bridged mode. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow all connections.

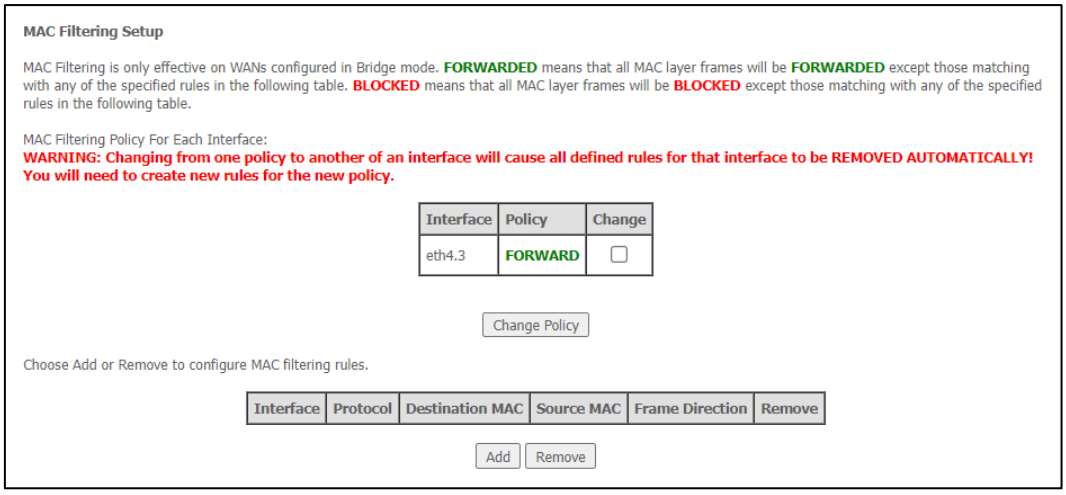


Figure 49 – Security – MAC filtering

Select **Add** to enter a new MAC Address filter.

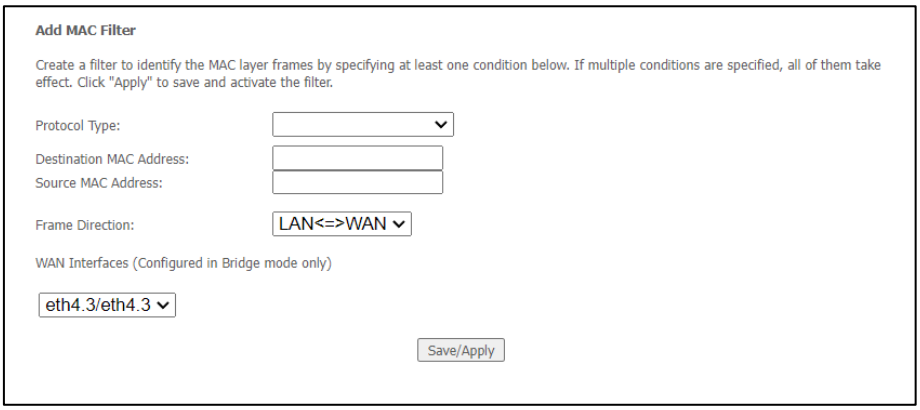


Figure 50 – Security – MAC filtering – Add MAC filtering rule

1 Enter the **Protocol type** to which the filter should apply.

2 Enter the **Source** and **Destination MAC Address.**

3 Enter the **Frame Direction** of the traffic to filter.

4 Select the **WAN interface** to which the filter should apply.

5 Select **Apply/Save** to save the new MAC filtering configuration.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure the devices connected to the network are can only access the internet when and how you decide.

Time restriction

This Parental Control function allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the router on selected days and at certain times. Make sure to activate the Internet Time server synchronization as described in the SNTP section, so that the scheduled times match your local time.

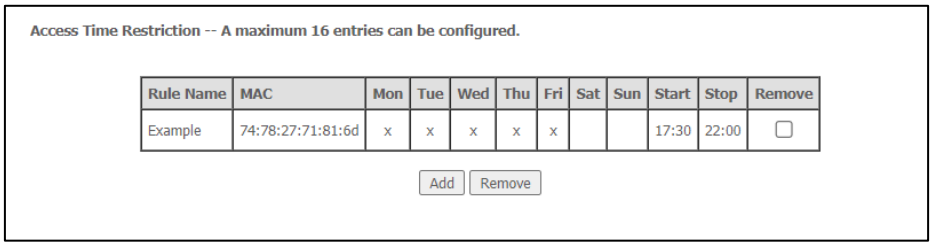


Figure 51 – Parental Control

To add a time restriction rule, select the Add button. The following screen appears:

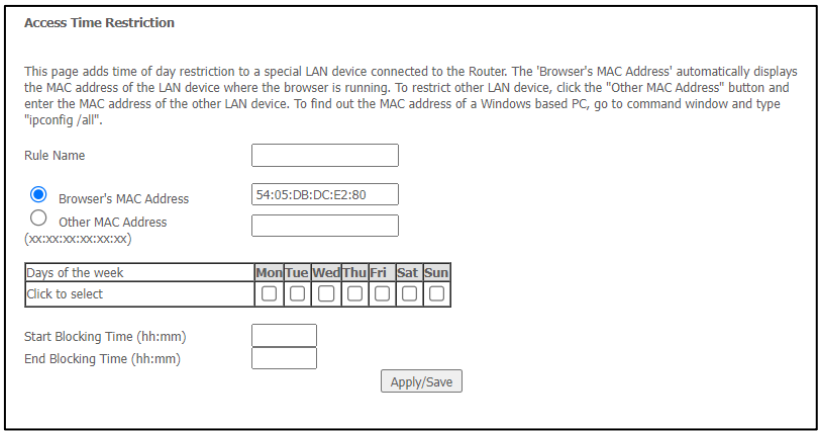


Figure 52 – Parental Control – Add time restriction rule

Field	Description
Rule Name	A user defined name for the time restriction rule.
Browser's MAC Address	The MAC address of the network card of the computer running the browser.
Other MAC Address	The MAC address of another device connected to the network.
Days of the Week	The days of the week for which the rules apply.
Start Blocking Time	The time of day when the restriction starts. (24 hour time: 00:00–23:59)
End blocking time	The time of day when the restriction ends. (24 hour time: 00:00–23:59)
Apply/Save button	Select the Apply/Save button to save a time restriction rule.

Table 9 – Parental Control – Add Time Restriction Settings

URL filter

With the URL filter, you can add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the Gateway.

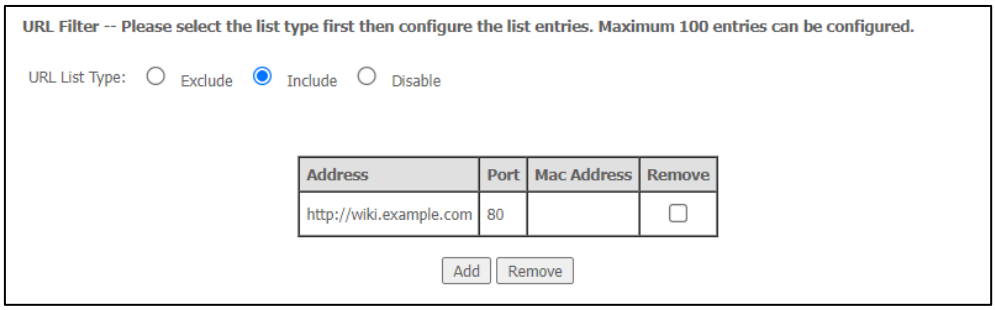


Figure 53 – Parental Control – URL filter

Select the Exclude (to block) or Include (to allow) option and then click Add to enter the URL that should be added to the URL Filter list.

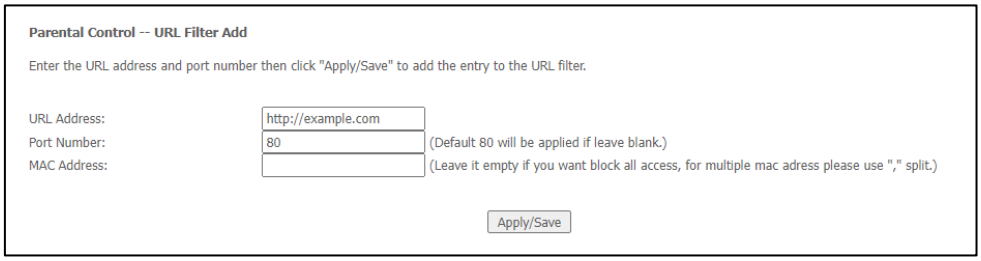


Figure 54 – Parental Control – URL filter – Add filter

Field	Description
URL Address	The URL address of the site you want to block or include.
Port Number	The Port Number (Default is 80).
MAC Address	If the address should only apply to a particular device via MAC address.
Apply/Save button	Select the Apply/Save button to apply the rule.

Table 10 – Parental Control – URL filter settings

Firewall

The Firewall page allows you to configure the firewall on the Gateway, including creating custom rules to allow specific traffic to transverse the Gateway. Select the Enabled checkbox to enable the Firewall.

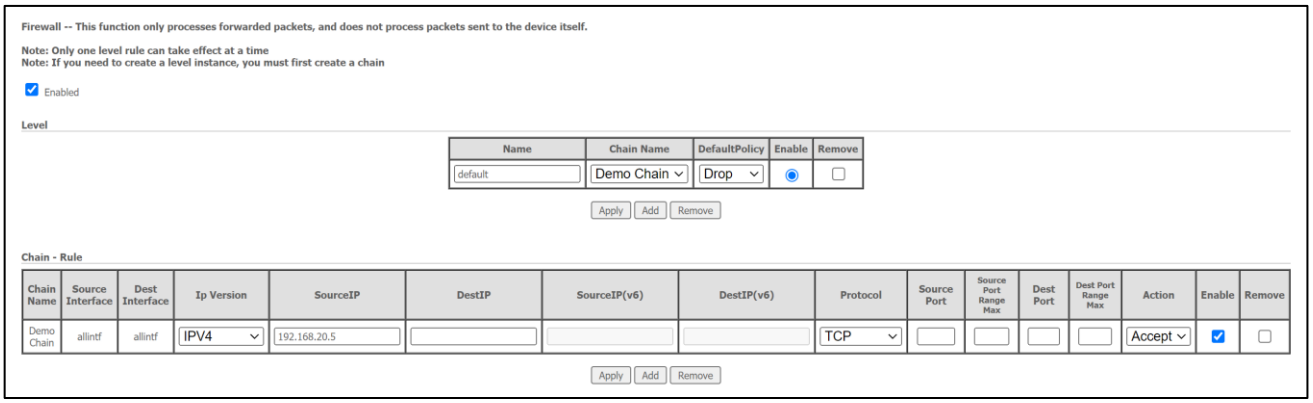


Figure 55 – Firewall

Level Rule

The Level Rule allows you to enable or disable a specific Chain Level. To use a Level Rule, you first need to define a Chain Rule, see the below section. Select the Enable button to Enable the Level Rule. Select the Remove button to remove the level rule.

Chain Rule

The Chain Rule allows you to define individual rules for different IP addresses. Each rule can be associated with an existing chain, or with its own individual chain, which can be updated in the Level Rule.

Details displayed in the Chain Rule list include the type of service as well as whether the rule is to exclude access to the specified connections (Drop) or include access to them (Accept).

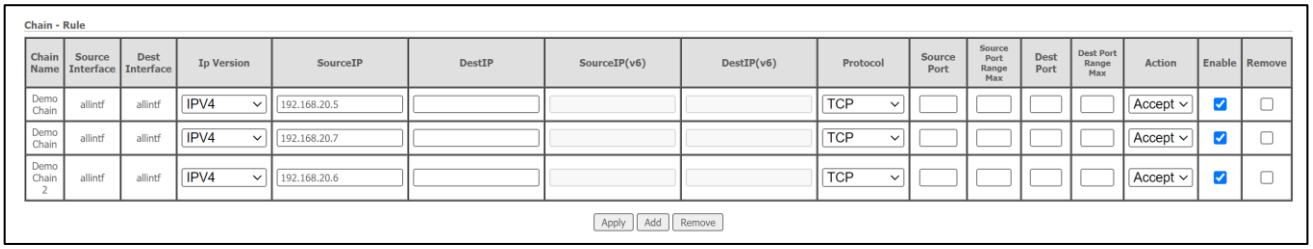


Figure 56 – Firewall – Chain Rule

To add a chain rule select the Add button to view the Add rule page.

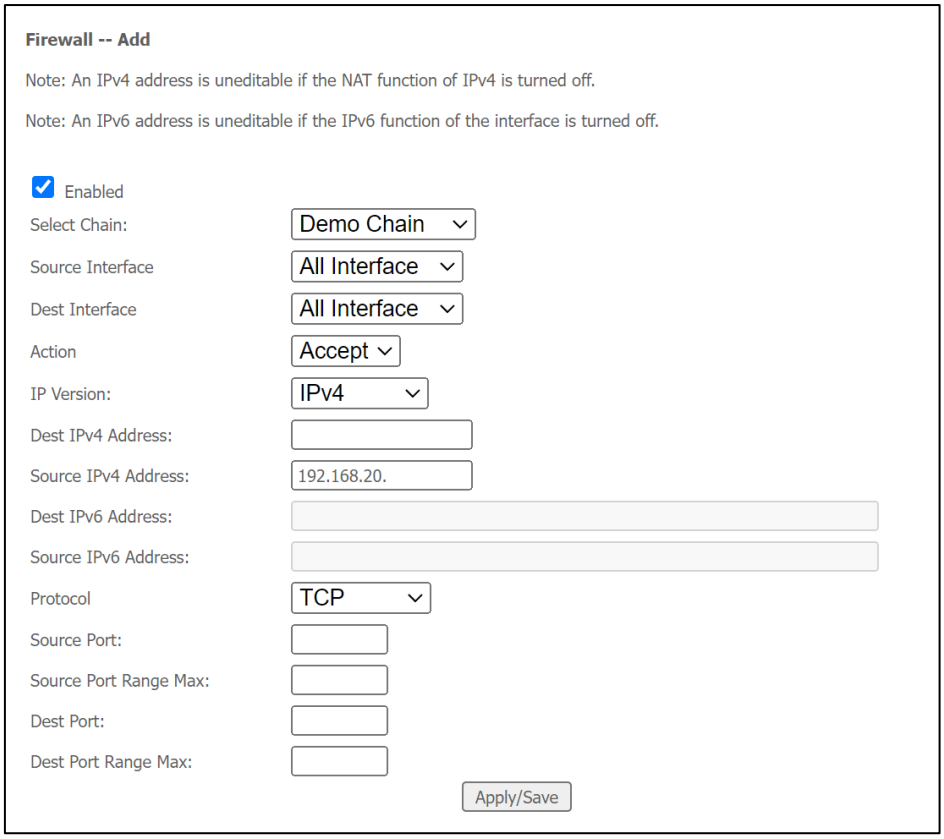


Figure 57 – Firewall – Add Chain Rule

Use the following parameters to create a rule:

Field	Description
Select Chain	If this rule should apply to an existing chain, select the chain from the dropdown. If the rule should start a new chain, select New Chain from the dropdown.
Chain Name	Add a name to identify the chain. This field only appears if you are creating a new chain.
Source Interface	Select the interface for the source IP address or All Interface from the drop-down menu.
Dest Interface	Select the interface for the destination IP address or All Interface from the drop-down menu.
Action	Select Drop to prevent the connection of any addresses included in the rule definition. Select Accept to allow the connection of any addresses included in the rule definition.
IP Version	Select: IPv4, IPv6 or IPv4/IPv4
Dest IPv4 Address	The destination address when IPv4 or IPv4/IPv6 is the selected version.
Source IPv4 Address	The source address when IPv4 or IPv4/IPv6 is the selected version.
Dest IPv6 Address	The destination address when IPv6 or IPv4/IPv6 is the selected version.
Source IPv6 Address	The source address when IPv4 or IPv4/IPv6 is the selected version.

Protocol	Select: TCP, UDP or TCP/UDP
Source Port	Specify a source port.
Source Port Range Max	Specify a range of possible source ports.
Dest Port	Specify a destination port.
Dest Port Range Max	Specify a range of possible destination ports.
Apply/Save button	Select the Apply/Save button to save the firewall rule and add it to the Chain Rule table, see previous.

Table 11 – Firewall – Add Rule parameters

Quality of Service

The Quality of Service (QoS) option found in the Advanced Setup drop-down menu configures access related parameters for the following:

- QoS Queue
- QoS Classification
- QoS Port Shaping

Quality of Service offers a defined level of performance on your home network – for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video conferencing is not disrupted by other network traffic. This means that if you are on a video call and someone else in your home begins downloading a large file, the download won't disrupt the flow of video traffic.

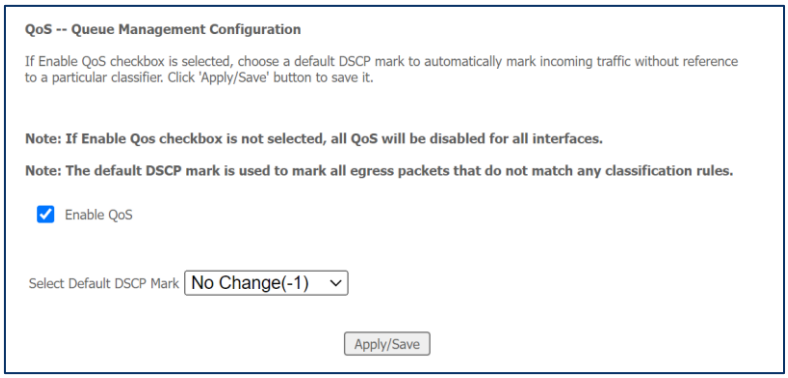


Figure 58 – Quality of Service

To enable QoS select the Enable QoS checkbox and set the Default DSCP (Differentiated Services Code Point) Mark. Then select the Apply/Save button.

QoS Queue

The QoS Queue page allows you to configure the Quality-of-Service Queue. The QoS Queue defines which traffic should be prioritized for delivery on the network, and which traffic should be placed in a buffer for delivery when bandwidth is available.

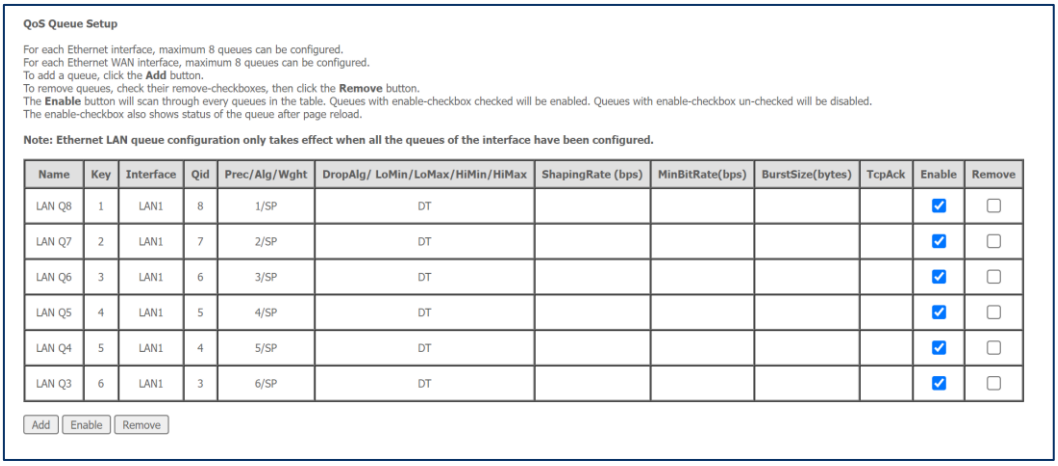


Figure 59 – Quality of Service – QoS Queue

Queue Configuration

Select the **Add** button to add a QoS Queue. The QoS Queue Configuration page is shown.

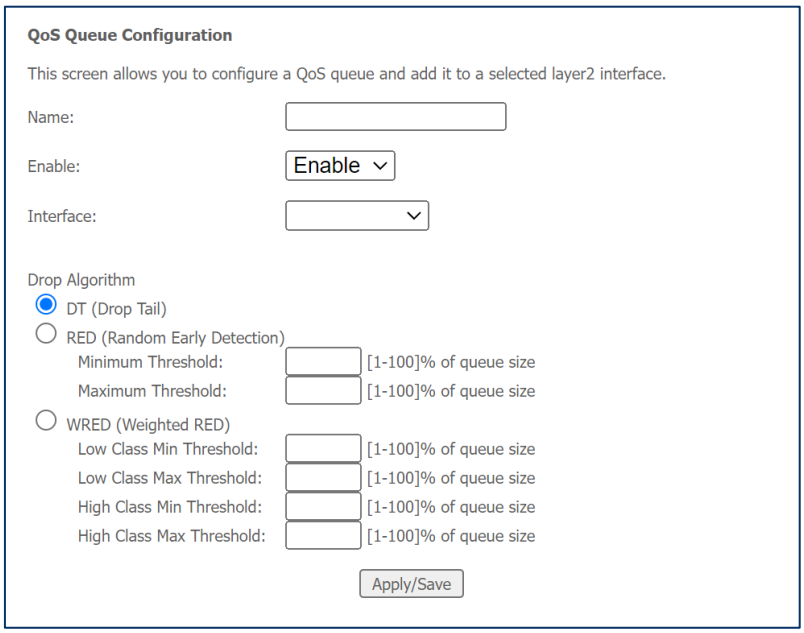


Figure 60 – Quality of Service – QoS Queue Configuration

The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.

Note – Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority.

WLAN Queue

The QoS WLAN Queue page displays a summary of the QoS Configuration.

QoS Wlan Queue Setup

Note: If WMM function is disabled in Wireless Page, queues related to wireless will not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
WMM Video Priority	900003	2.4G	6	3/SP	Enabled
WMM Video Priority	900004	2.4G	5	4/SP	Enabled
WMM Background	900006	2.4G	3	6/SP	Enabled
WMM Best Effort	900008	2.4G	1	8/SP	Enabled
WMM Voice Priority	900033	6G	8	1/SP	Enabled
WMM Voice Priority	900034	6G	7	2/SP	Enabled
WMM Video Priority	900035	6G	6	3/SP	Enabled
WMM Video Priority	900036	6G	5	4/SP	Enabled
WMM Best Effort	900037	6G	4	5/SP	Enabled
WMM Background	900039	6G	2	7/SP	Enabled
WMM Best Effort	900040	6G	1	8/SP	Enabled
WMM Voice Priority	900065	5G	8	1/SP	Enabled
WMM Voice Priority	900066	5G	7	2/SP	Enabled
WMM Best Effort	900069	5G	4	5/SP	Enabled
WMM Background	900070	5G	3	6/SP	Enabled
WMM Background	900071	5G	2	7/SP	Enabled

Figure 61 – Quality of Service – WLAN Queue

QoS Classification

The QoS Classification page manages the QoS classification configuration on the Gateway. QoS Classification is the process of identifying and classifying the different types of traffic which are transiting the Gateway, so it can be correctly processed in the QoS queue.

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	Policer Key	DSCP Mark	802.1P Mark	Enable	Remove
DemoClass	1	LAN	IP										33		auto	0	☑	☐

Add Enable Remove

Figure 62 – Quality of Service – QoS Classification

Select the Add button to add a QoS classification.

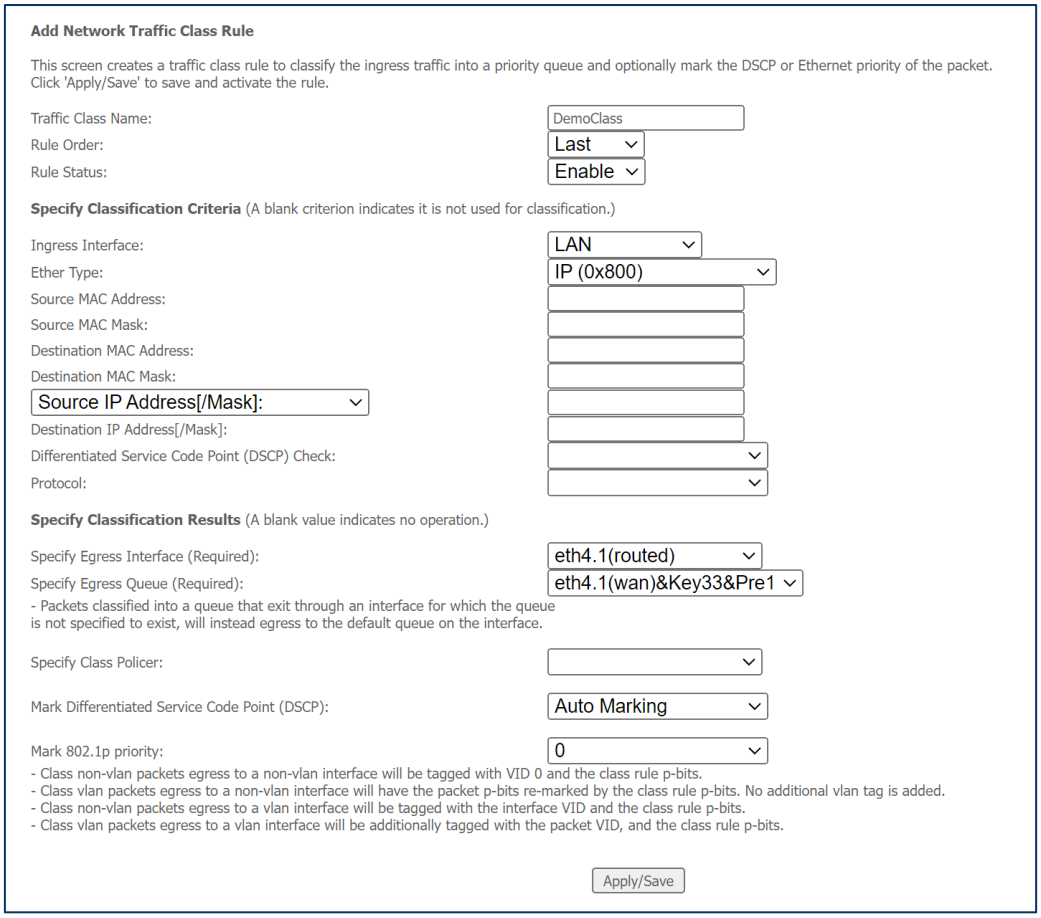


Figure 63 – Quality of Service – Add Network Traffic Class Rule

The Add Network Traffic Class Rule page creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Select the Apply/Save button to save and activate the rule.

QoS Port Shaping

Port Shaping allows the limiting of continuous network speed without affecting burst traffic. For example, when your browser loads a web page, this is a type burst traffic as the browser aims to fetch small amounts of data quickly and then leaves the connection idle. Limiting port speed alone will affect the speed at which web pages are loaded, causing users to feel that their overall internet connection speed is slow.

By configuring QoS Port Shaping with a Burst size, web pages are allowed to load using the burst speed, while continuous traffic such as file downloads will be shaped at a lower rate.

To identify the best way to configure shaping rate and burst size, consider the equation below:

```
Time window = Burst size / rate
```

For example. if a 200 Mbps bandwidth limit is configured with a 5 ms burst window, the calculation becomes 200 Mbps x 5 ms = 125 Kbytes, which is approximately eighty-three (83) 1500-byte packets. If the 200 Mbps bandwidth limit is configured on a Gigabit Ethernet interface, the burst duration is 125000 bytes / 1 Gbps =

1ms at the Gigabit Ethernet line rate. After 1ms of burst data at full gigabit speed, the speed is shaped to 200Mbps.

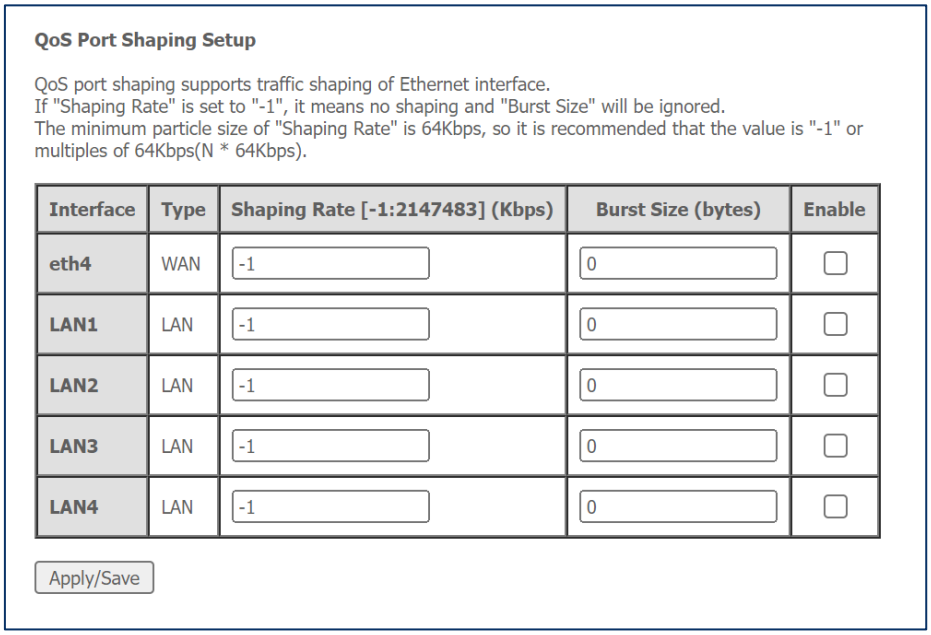


Figure 64 – Quality of Service – QoS Port Shaping Setup

The following table explains the parameters on the QoS Port Shaping Setup page:

Item	Description
Interface	Identifies the interface. Each of the interfaces corresponds with a port on the Gateway.
Type	Identifies the connection type.
Shaping Rate	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size	Burst size should be more than 10x MTU (>=15000 bytes)
Apply/Save button	Click to save and apply your changes

Table 12 – Quality of Service – QoS Port Shaping

Routing

The Routing option found in the Advanced Setup drop-down menu configures access related parameters for the following:

- Default Gateway
- Static Route
- Policy Routing
- RIP

Default Gateway

Select your preferred WAN interface from the available options.

Use the arrow buttons to move the available Routed WAN Interfaces listed on the right to the group of required **Default Gateway Interfaces** in the list on the left.

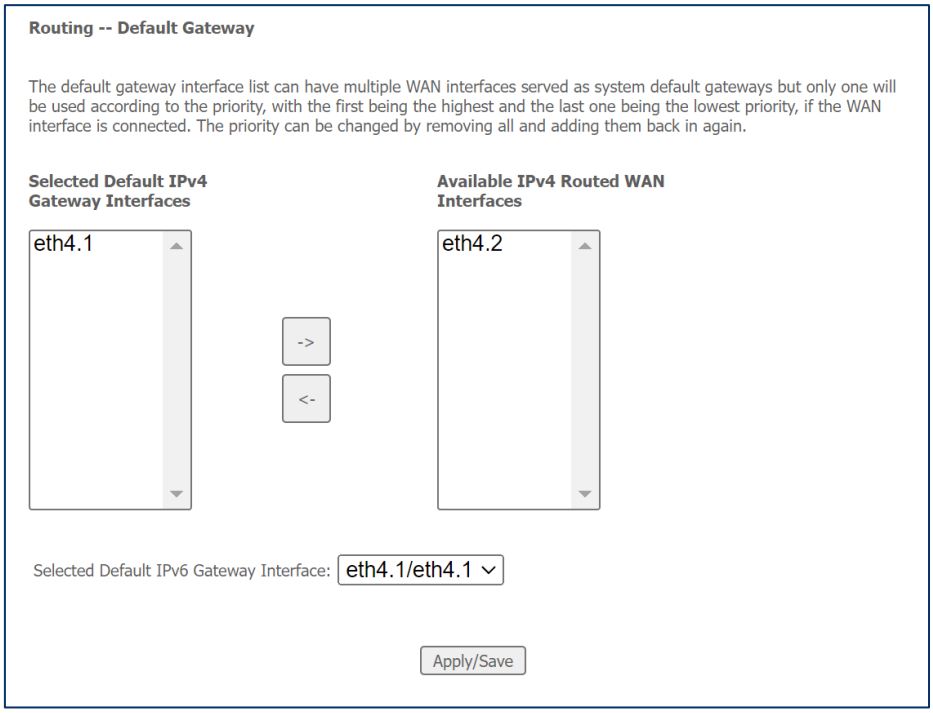


Figure 65 – Routing – Default Gateway

Static Route

The Static Route page allows static routes to be configured on the Gateway.

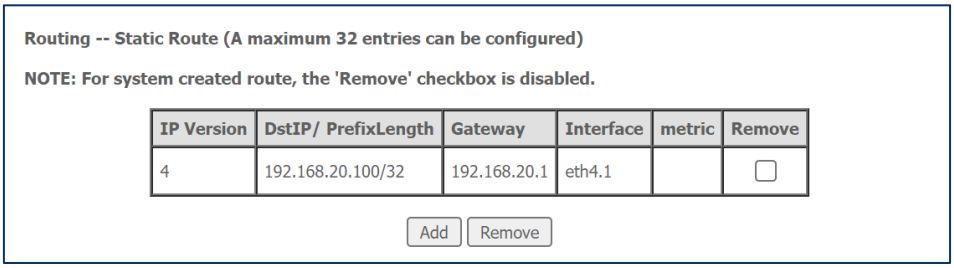


Figure 66 – Routing – Static Route

To add a static route:

1 Select the Add button to add a static route. The Static Route Add page opens.

2 Select the IP Version from the drop-down menu, enter the Destination Network Address, select an Interface, and enter the Gateway IP Address.

3 Optionally enter a number in the Metric field to set a priority for this route, the lower the number the higher will be its priority.

4 Select Apply/Save to add the entry to the routing table.

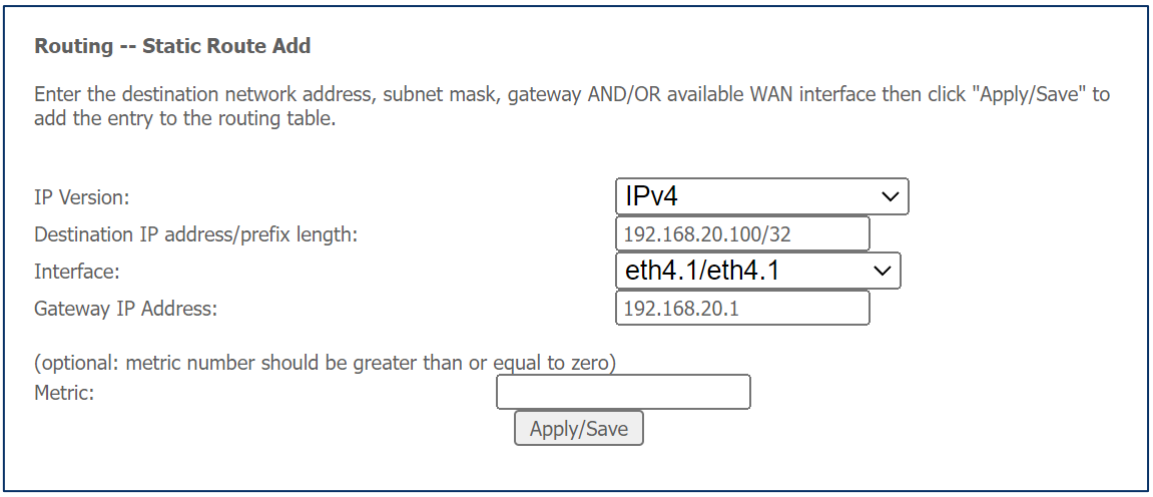


Figure 67 – Routing – Static Route – Add static route

Policy Routing

The **Policy Routing** page allows you to add policy rules to certain situations.

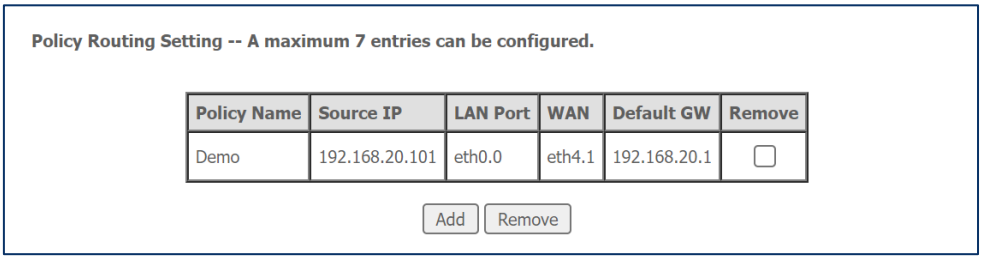


Figure 68 – Routing – Policy Routing

To add a policy route:

1 Select the **Add** button to add a policy route. The Policy Routing Setup page is displayed.

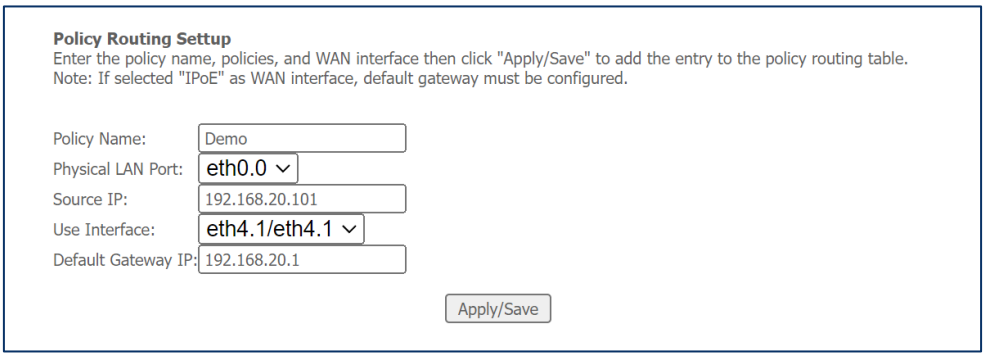


Figure 69 – Routing – Policy Routing

2 Enter the details into the provided fields, then select Apply/Save. The required parameters are listed in the table below:

Field	Description
Policy Name	A user defined name for the policy route.
Physical LAN Port	The LAN port to be used for the policy.
Source IP	The IP address of the LAN device involved with the policy.
Use Interface	Select the Interface that the policy will employ.
Default Gateway	Enter the gateway address.

Table 13 – Routing – Policy routing parameters

RIP

The Routing Information Protocol (RIP) allows gateways to exchange network topology information. This information allows the automatic creation and updating of routing tables.

Note – RIP cannot be selected for a WAN interface which is NAT enabled, such as PPPoE.
Go to **Basic Setup** and select **Ethernet WAN**, click **Next** and then select **IP over Ethernet (IPoE)**. The RIP option will now be available.

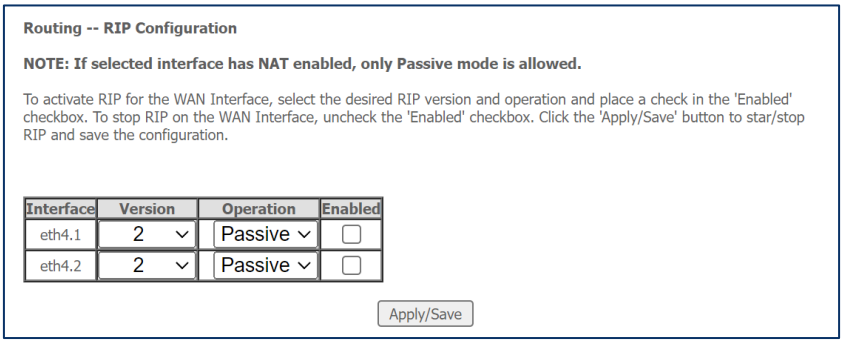


Figure 70 – Routing – RIP

The following table details the different options that can be configured for RIP:

Item	Description
Interface	The network interface that the RIP settings apply to.
Version	1 – Use RIPv1 to support classful routing. 2 – Use RIPv2 to support subnet information gathering and Classless Inter-Domain Routing. Both – RIP will use both RIPv1 & RIPv2, and will multicast and broadcast to all adjacent gateways.
Operation	Passive – RIP will only respond to "Request Message" queries on the RIP enabled interface. Active – RIP will broadcast and respond to "Request Message" queries on the RIP enabled interface.
Enabled	Select ☑ Enabled to activate the RIP routing service on the selected Interface.
Apply/Save button	Click the Apply/Save button to initiate the change.

DNS

The DNS option found in the Advanced Setup drop-down menu configures access related parameters for the following:

- DNS Server
- Dynamic DNS (DynDNS)

DNS Server

A DNS server is a server that contains a database of hostnames and their associated public IP addresses. A hostname is the address that most users would commonly recognise as a URL, such as www.netcomm.com. The DNS server is used to resolve hostnames to a unique public IP address when requested.

When a user enters a URL e.g., www.netcomm.com into their browser, your gateway is contacting the DNS server and requesting the webserver IP address.

Hostname URLs are easier for humans to understand and remember than IP address numbers. A host's IP addresses can change from time to time hence a DNS server is required to locate and translate a hostname.

DNS Servers can be used to block unwanted content, such as explicit material. By using a filtered DNS server, the hostname of these materials will not be resolved, allowing parental control to accessible content.

Parental Control DNS are available as a free service or customizable paid service. For example: OpenDNS FamilyShield, Norton ConnectSafe, Yandex.DNS, Comodo Secured, etc.

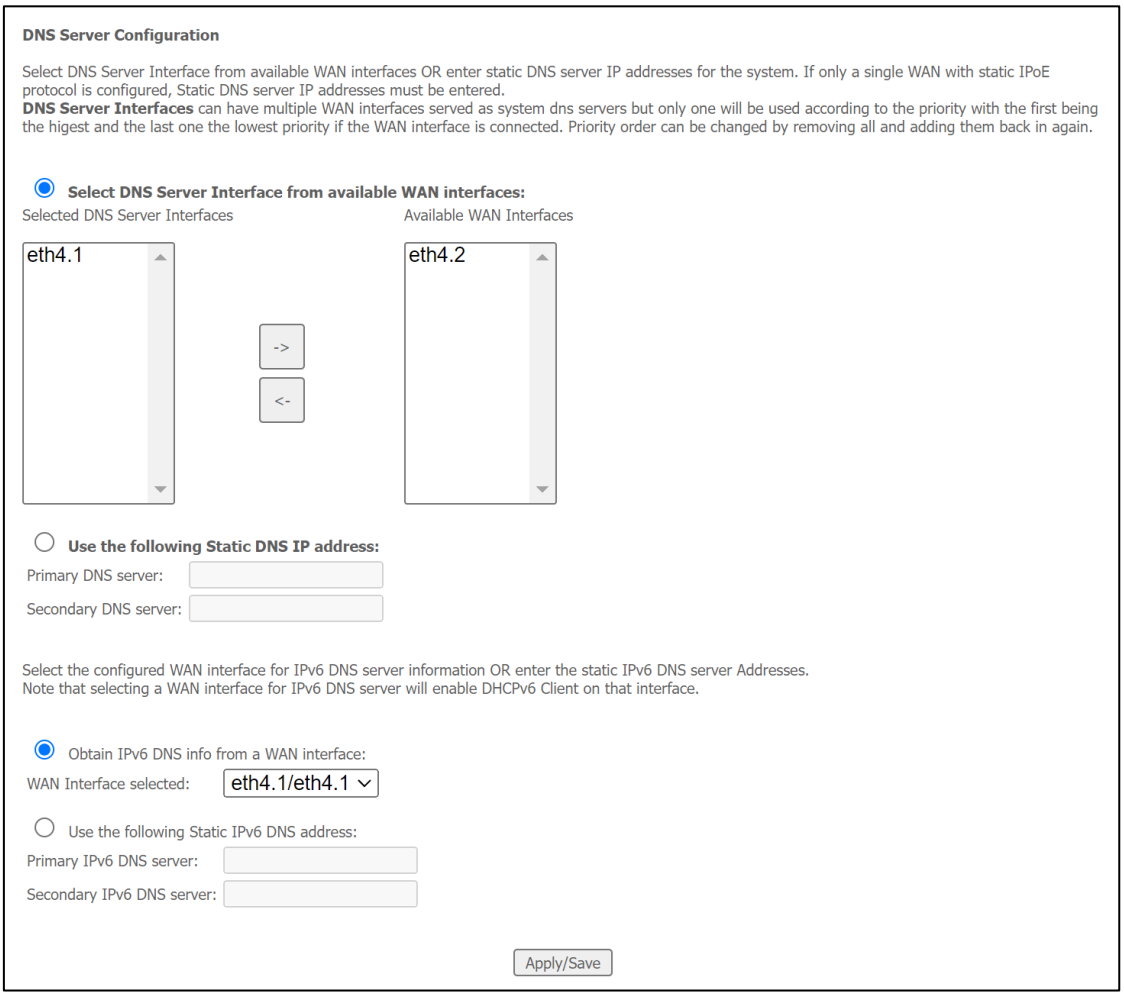


Figure 71 – DNS – DNS Server

Update the following parameters to configure the DNS server to be used by the Gateway, and by extension the users on the local network.

Field	Description
DNS server via interface	Use DNS server provided from your ISP automatically from the assigned interface. Use the arrow to select the WAN interface to request DNS server, with the first being the highest priority.
Static DNS IP Address	Specify your own Primary and Secondary DNS server.

IPv6 DNS info from WAN interface	Use IPv6 DNS server provided from your ISP automatically from the assigned interface.
Static IPv6 DNS IP Address	Specify your own Primary and Secondary IPv6 DNS server.
Apply/Save Button	Click the Apply/Save button to initiate the change.

Table 14 – DNS – DNS Server Configuration

Dynamic DNS

Dynamic DNS (DDNS) allows your Gateway to associate an easy-to-remember domain name, such as [yourdomainname].com with the regularly changing IP address assigned by your ISP. This feature allows you to connect remotely more easily to your home network.

Note – DDNS is one component of connecting remotely to your home network. For complete connectivity, you will need to add port forwarding rules for the relevant application in the firewall. Some ISPs block common ports, such as 80 and 443, so you may need to contact your internet provider to allow traffic from your ISP to your gateway. Refer to your ISP documentation for further information.

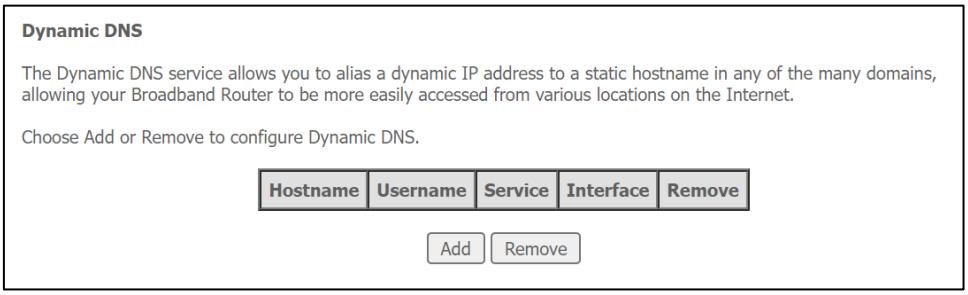


Figure 72 – DNS – Dynamic DNS

To add a new Dynamic DNS profile:

1 Select the **Add** button. The Add Dynamic DNS screen is displayed.

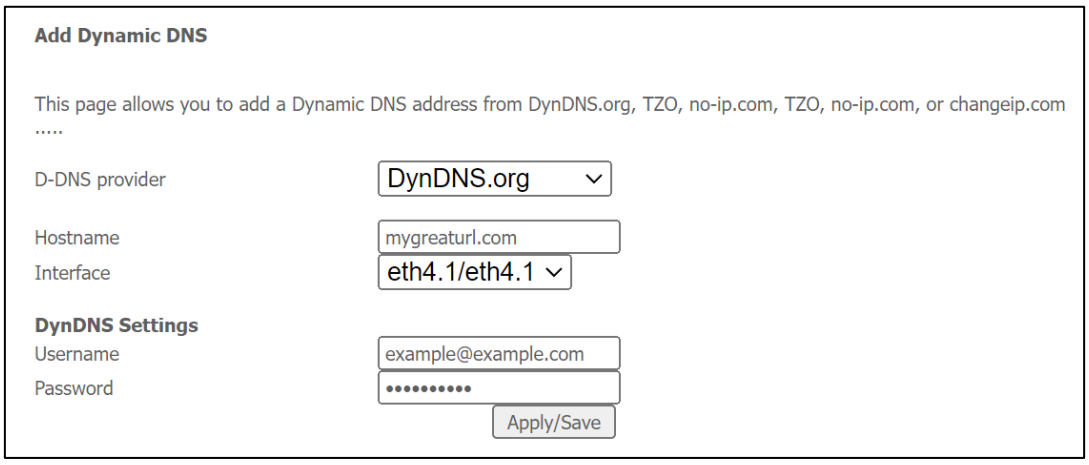


Figure 73 – DNS – Dynamic DNS – Add Dynamic DNS page

2 From the D-DNS provider drop-down list, select your Dynamic DNS provider.

3 In the **Hostname** field, enter the dynamic DNS hostname.

4 Use the **Interface** drop-down list to select the interface that the service should operate on.

5 Enter the username and password for your dynamic DNS account.

6 Select **Apply / Save**.

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, gaming console, Wi-Fi access points and mobile phones to automatically detect each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

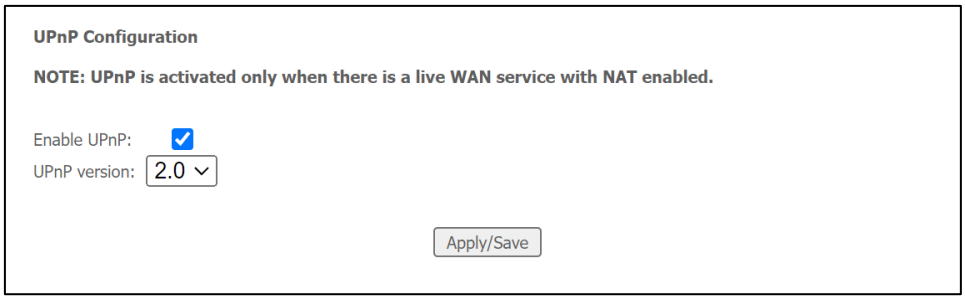


Figure 74 – UPnP

Select ☑ **Enable UPnP** and then click the **Apply/Save** button to allow automatic port forwarding configuration detection for your UPnP devices.

Note – The **UPnP** functionality is only available when there is a live **WAN** service with **NAT** enabled.

DNS Proxy

You can define an easy to remember proxy name for the standard URL of the Gateway (192.168.20.1) to provide more convenient access the gateway's Web UI.

Select ☑ **Enable DNS Proxy** and then enter the proxy **Host name of the Broadband Router** and the proxy **Domain name of the LAN network**, as in the example shown below. Select **Apply / Save** to continue.

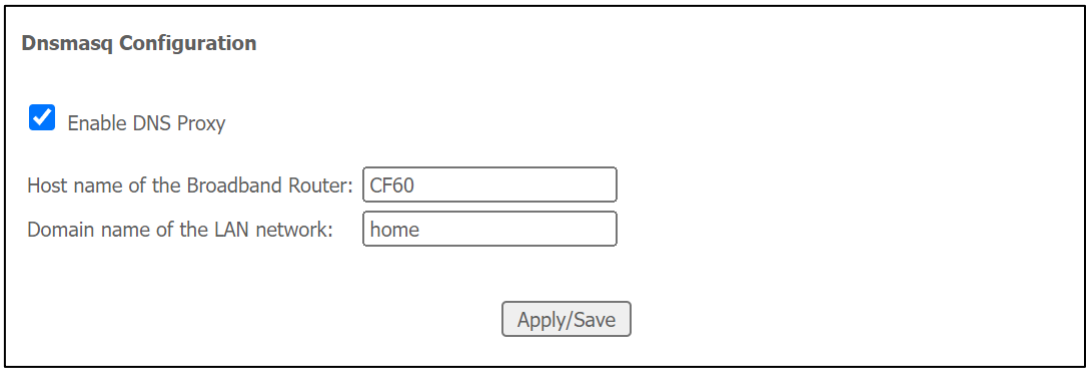


Figure 75 – DNS Proxy

The **Host name** and **Domain name** are combined to form a unique label that is mapped to the gateway IP address. This can be used to access the user interface of the gateway with a local name rather than by using the gateway IP address. In the example above you will now be able to access your gateway by entering the proxy name **http://cf60.home** into your web browser.

Proxy names can also be custom: quick.uiaccess, goto.gatewayui, etc.

DLNA

The DLNA page allows you to enable or disable and configure the DLNA digital media server. DLNA allows you to stream digital media that is stored on an external storage device that is connected via USB to the Gateway.

Select ☑ Enable on-board digital media server and then use the drop-down list to select the Interface. In the Media Library Path field, enter the path to the media and then enter a period between media library updates in seconds.

Storage Service

The Storage Service options enable you to manage attached USB Storage devices and create accounts to access the data stored on an attached USB storage device.

Storage Device Info

The storage device info page displays information about the attached USB Storage device.

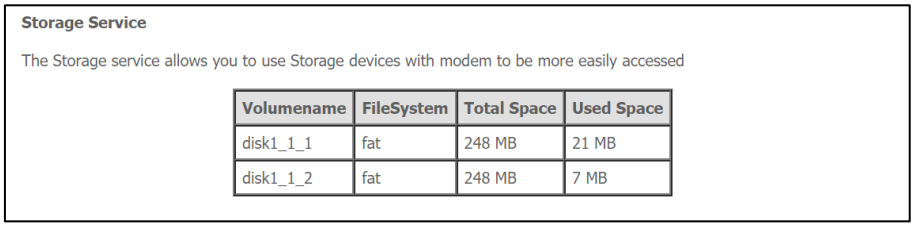


Figure 76 – Storage Service – Storage Device Info

User Accounts

User accounts are used to manage access to the attached USB storage device.

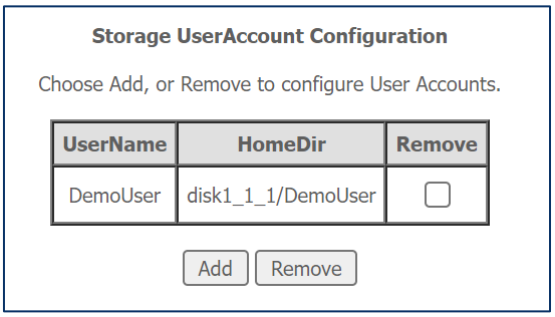


Figure 77 – Storage Service – User Accounts

Adding an account allows the creation of specific user accounts with a password to further control access permissions. To add an account, select the Add button and then enter the desired username and password for the account. In the Volume Name field, enter the Volume Name of the device, which can be found on the Storage Device Info page.

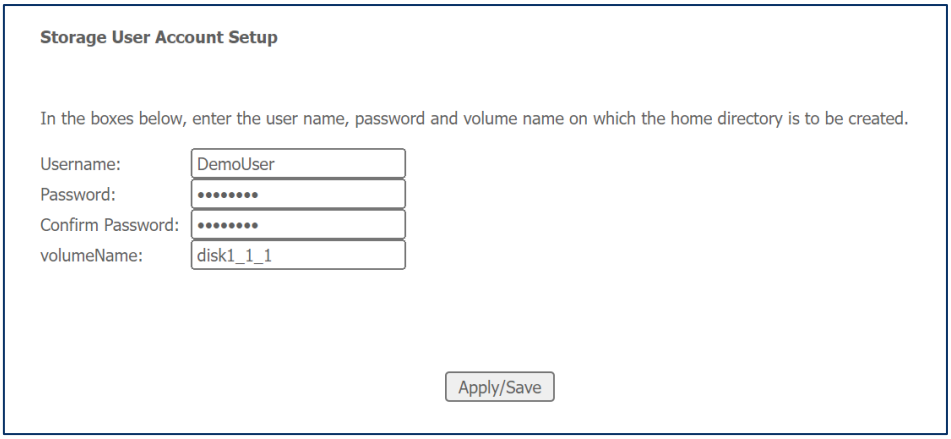


Figure 78 – Storage Service – User Account configuration

Interface Grouping

Port Mapping allows you to create groups composed of the various interfaces available on your gateway. These groups then act as separate networks.

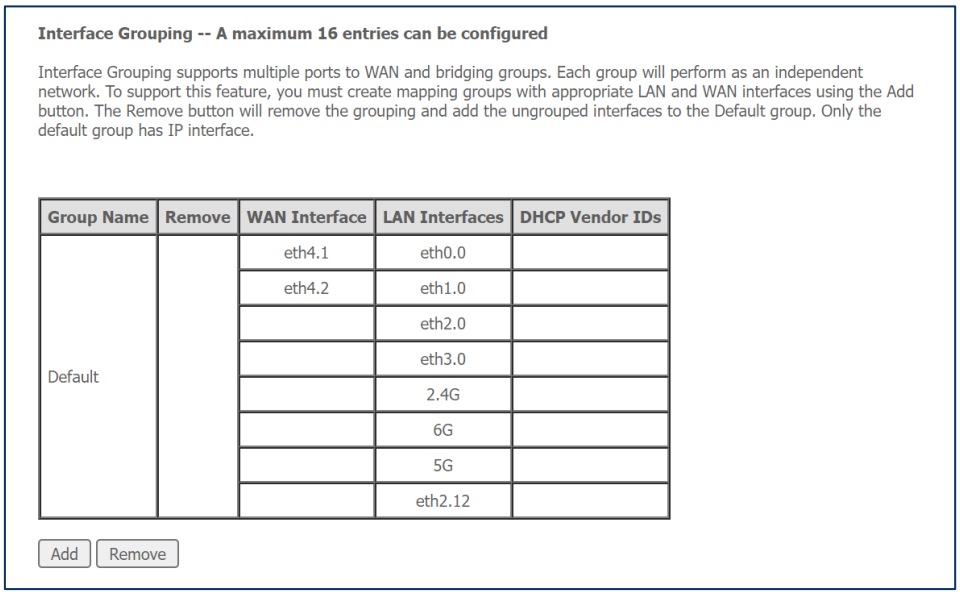


Figure 79 – Interface grouping

Select **Add** to create an Interface Group.

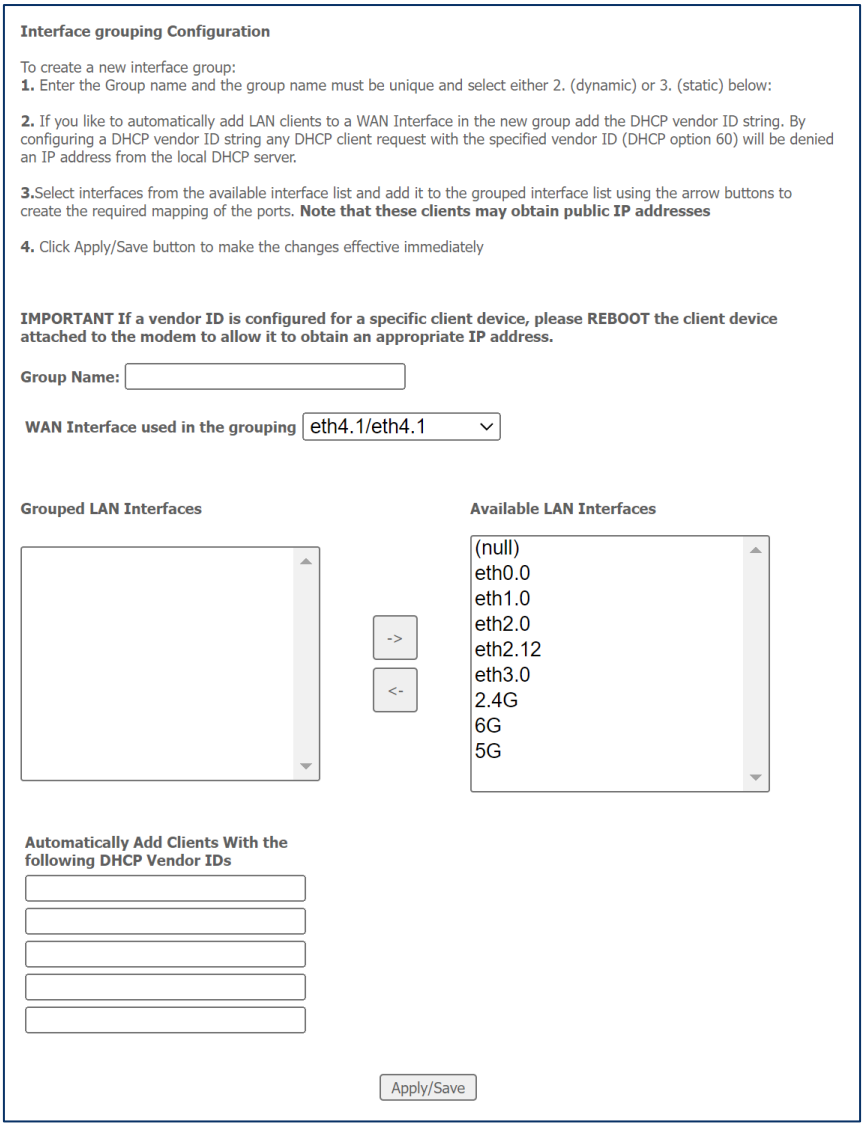


Figure 80 – Interface grouping – Create interface group

Enter a group name and then use the arrow buttons to select which interfaces you wish to group. If applicable, enter a DHCP Vendor ID to automatically place those devices in the group (for example IP telephones or network switches).

Select **Apply/Save** to save the Interface grouping configuration settings.

Wireless

Your Gateway is configured with three Wi-Fi bands, 2.4GHz, 5GHz and 6GHz. Each can be configured independently of the other. All pages contain the same configuration settings, aside from 6GHz, which does not include the WPS page. Select the appropriate band you want to configure from the navigation bar to the left of the page.

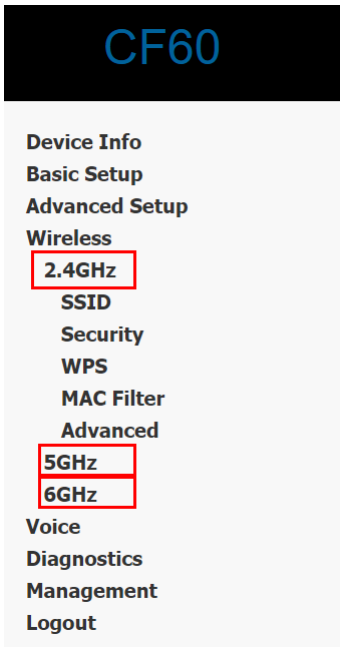


Figure 81 – Wireless – Wireless navigation

SSID

The SSID configuration page allows you to enable the wireless network and configure general settings, such as name, country and the maximum number of clients that can connect.

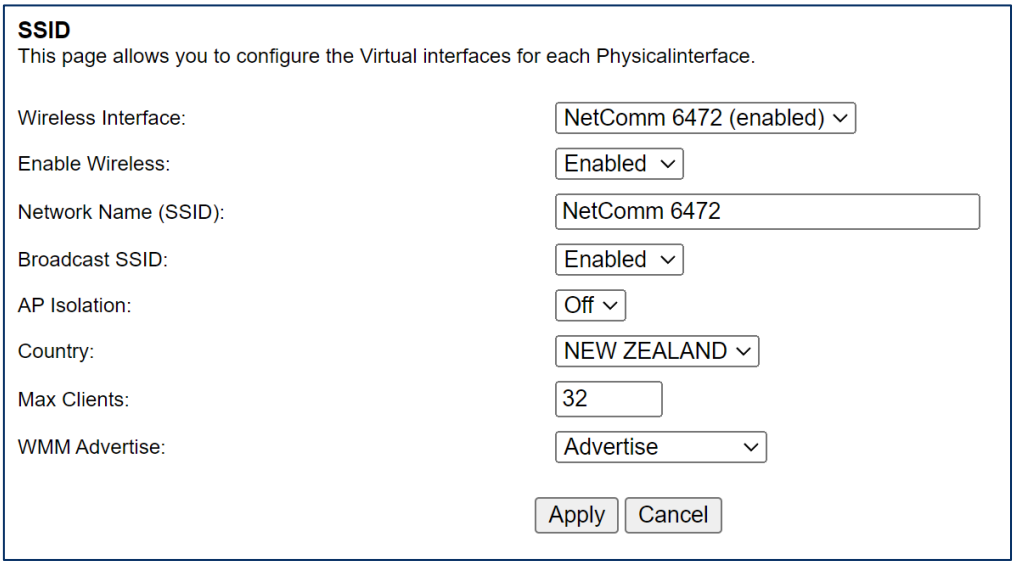


Figure 82 – Wireless - SSID

The following settings can be configured on this page:

Parameter	Definition
Wireless Interface	Select the wireless interface to configure.
Mode	Allows you to select the mode that the wireless radio operates in.
Enable Wireless	Select Enabled to activate the wireless network function.
Network Name (SSID)	Allows you to configure the network name displayed when a client scans for wireless networks.
Broadcast SSID	Select Enabled to hide the wireless network when an SSID scan is performed.
AP Isolation	Select On to prevent clients on the wireless network being able to access each other.
Country	Set the country to apply specific Wi-Fi conditions for that region.
Max Clients	Set the maximum number of clients. The default value is 32.
WMM Advertise	Select Do Not Advertise to prevent the Gateway advertising its WMM QoS function.

Table 15 – Basic Wireless settings table

Select Apply/Save to save the new wireless configuration settings.

Note – Hiding the network may leads to potential connection problems, a non-broadcast network is not undetectable, so is not recommended as a security feature.

Security

The Security Page allows configuration of the security functionality of the Wi-Fi network, such as encryption types and the Wi-Fi passphrase (Wi-Fi password).

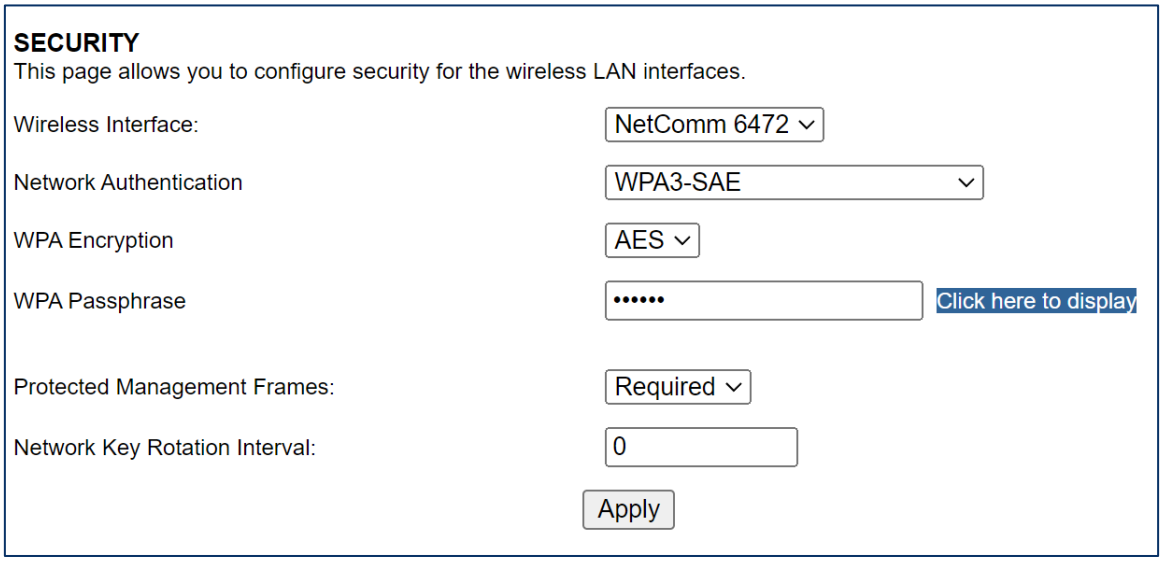


Figure 83 – Wireless - Security

The following security settings can be configured on this page:

Parameter	Definition
Wireless Interface	Select the SSID to apply the security settings to.
Network Authentication	Select the Wireless security type to use with the wireless network. The Gateway supports the following encryption types: WPA2-PSK, WPA3-PSK, Mixed WPA2/WPA-PSK, Mixed WPA2-PSK/WPA3-SAE and WPA3-SAE.
WPA Encryption	Select the type of encryption to use on the wireless network.
WPA passphrase	Enter the security key to use with the wireless network.
Protected Management Frames	Select whether the protected management frames should be Off, Capable or Required.
Network Key Rotation Interval	Enter the group rekey interval. This should not need to change.

Table 16 – Wireless security settings

WPS

WPS (Wi-Fi Protected Setup) is a network security standard that can be used to create a secure wireless home network. WPS on the Gateway is activated by pressing the WPS button on the top of the Gateway for three seconds, or by selecting the Add Enrollee button on the WPS page.

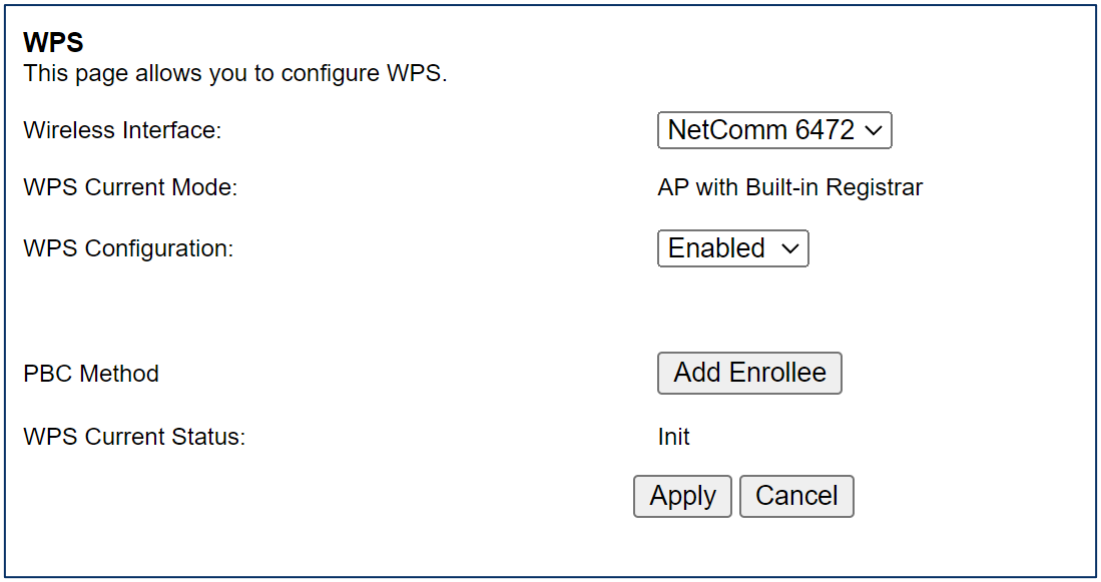


Figure 84 – Wireless – WPS

MAC filter

The MAC Filter page allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network. First use the Wireless Interface drop-down list to select the wireless network you wish to configure, then change the MAC Restrict Mode setting from Disabled, then select to either Allow or Deny access to the MAC addresses listed.

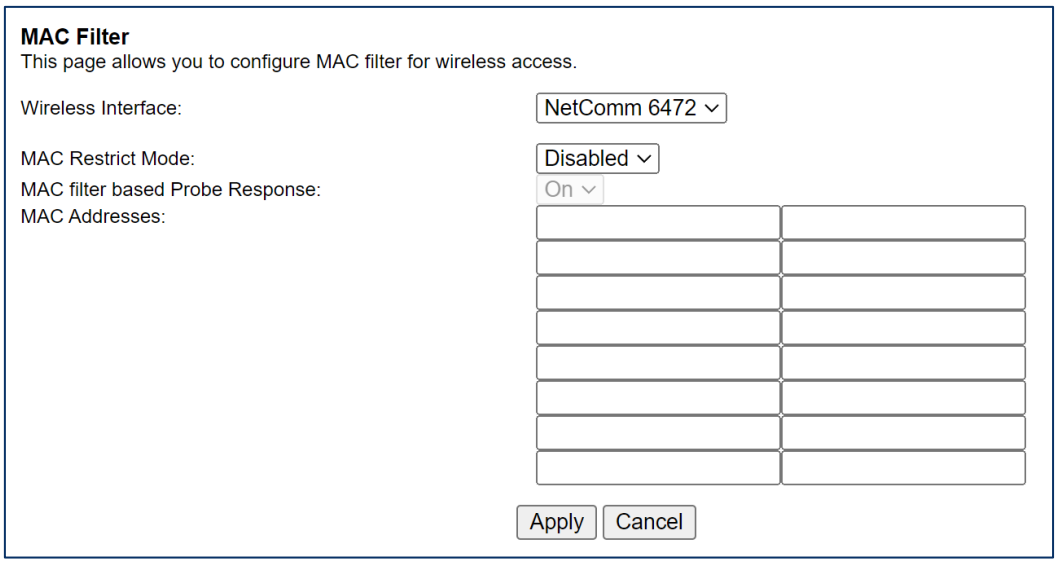


Figure 85 – Wireless – MAC Filter list

Enter a MAC address in the MAC Addresses fields provided then select Apply to add a MAC Address Filter. Enter the MAC address in the format of aa:bb:cc:11:22:33

To delete a MAC filter entry, select the MAC address and delete the entry, then select Apply to confirm the deletion.

Note – While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC and then spoofing one's own MAC into a validated on. Some devices even do this natively, so MAC Filtering should be used alongside other security measures to prevent unauthorised access to the Wi-Fi network.

Advanced

The **Advanced** wireless page allows you to configure detailed wireless network settings such as the band, channel, bandwidth, transmit power, and preamble settings.

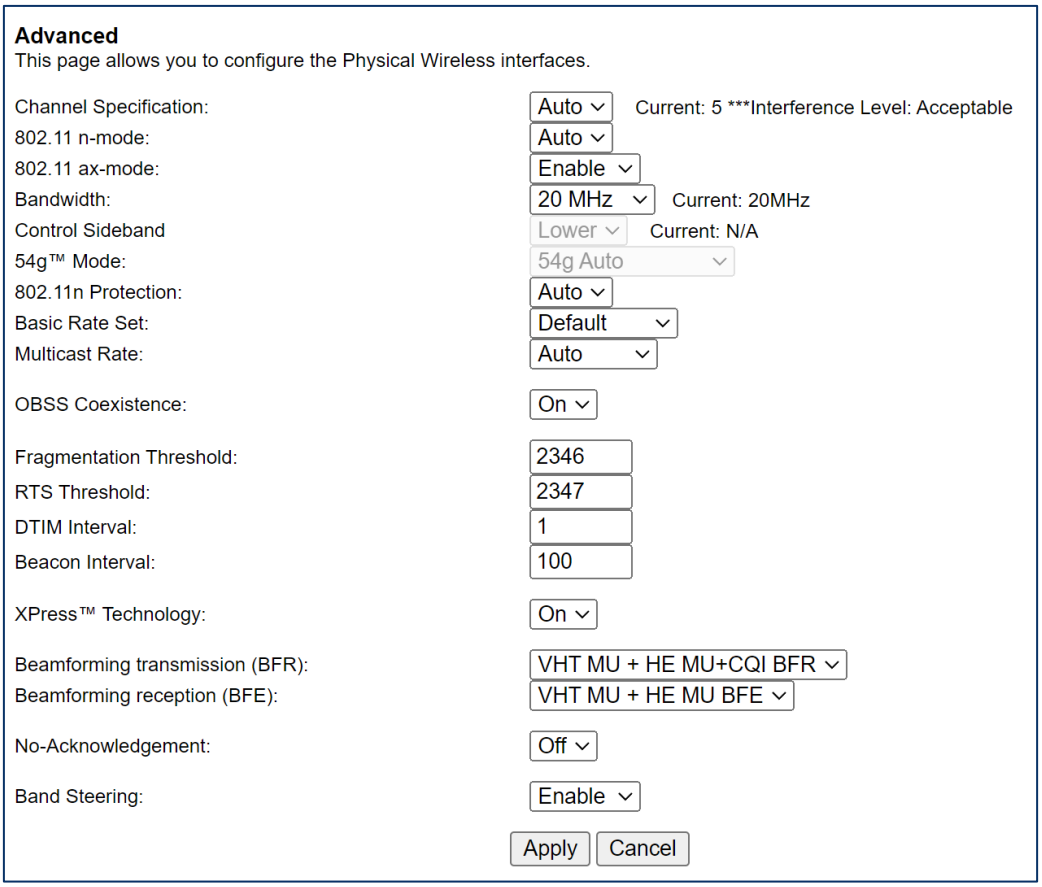


Figure 86 – Wireless – Advanced

The following advanced configuration options are available:

Parameter	Definition
Channel Specification	Select the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This gateway supports Auto channelling functionality (default setting). The Current: channel number, together with the current level of detected interference, will be displayed on the right.
802.11 n-mode	Select 802.11n functionality to be either: Auto or Off
802.11 ax-mode (2.4GHz only)	Select 802.11ax functionality to be either Enabled or Disabled.
Bandwidth	Select the bandwidth for the network: For 2.4GHz this may be 20MHz or 40MHz. For 5GHz and 6GHz this may be 20MHz, 40MHz, 80MHz or 160MHz.
54g™ Mode	For 54g mode, you can select **54g Auto**, **54g Performance**, **54g LRS** or **802.11b Only**.

(2.4 GHz and 802.11n disabled only)	This option is only visible when **802.11n mode** is set as **Disabled**.
802.11n Protection	The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.
Basic Rate Set	Select the basic transmission rate ability for the AP.
Multicast Rate	Select the multicast transmission rate in Mbps for the network. The rate of data transmission should be set depending on the speed of your wireless network. Available settings are: Auto, 6, 9, 12, 18, 24, 36, 48, 54 Select Auto to have the Gateway automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Gateway and a wireless client. The default value is Auto.
OBSS Co-Existence	With OBSS (Overlapping BSS) set to On the Gateway automatically changes the channel width from 40MHz to 20MHz to avoid interference with other APs and then back to 40MHz, if possible.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance. The default setting is: 2346
RTS Threshold	The RTS Threshold is the minimum size in bytes for which the Request to Send/Clear to Send (RTS/CTS) channel contention mechanism is used. The Gateway sends RTS frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default setting (which is the maximum value): 2347 In a network with significant radio interference or large number of wireless devices on the same channel, reducing the RTS Threshold might help in reducing frame loss.
DTIM Interval	A DTIM (Delivery Traffic Indication Message) interval is the length in seconds of a countdown informing clients of the next window for listening to broadcast and multicast messages. Enter a value between 1 and 255 seconds for the DTIM interval between messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is the period of time (sent with the beacon) which will elapse before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). The default (100 ms) is recommended.

XPress Technology	Select On to enable this is special frame-bursting accelerating technology for IEEE802.11g. The default is: On
Beamforming Transmission (BFR)	Changes the Beamforming Transmission type. The default transmission type is VHT MU + HE MU + CQI BFR. This is the recommended transmission type.
Beamforming Reception (BFE)	Select SU (Single-User) BFE to concentrate the transmission signal at the Gateway location. Changes the Beamforming Reception type. The default reception type is VHT MU + HE MU BFE. This is the recommended reception type.
No-Acknowledgement	This setting is only available when WMM Support is set to Auto or On. By default, the 'Ack Policy' for each access category is set to Off, meaning that an acknowledgement packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. Select On to turn off the acknowledgement request. This can be useful for Voice transmissions where speed of transmission is important and packet loss is tolerable to a certain degree.
Band Steering	Select Enable to detect if the client has the ability to use three bands. When enabled, the less congested 5GHz network is selected (by blocking the client's 2.4GHz network).

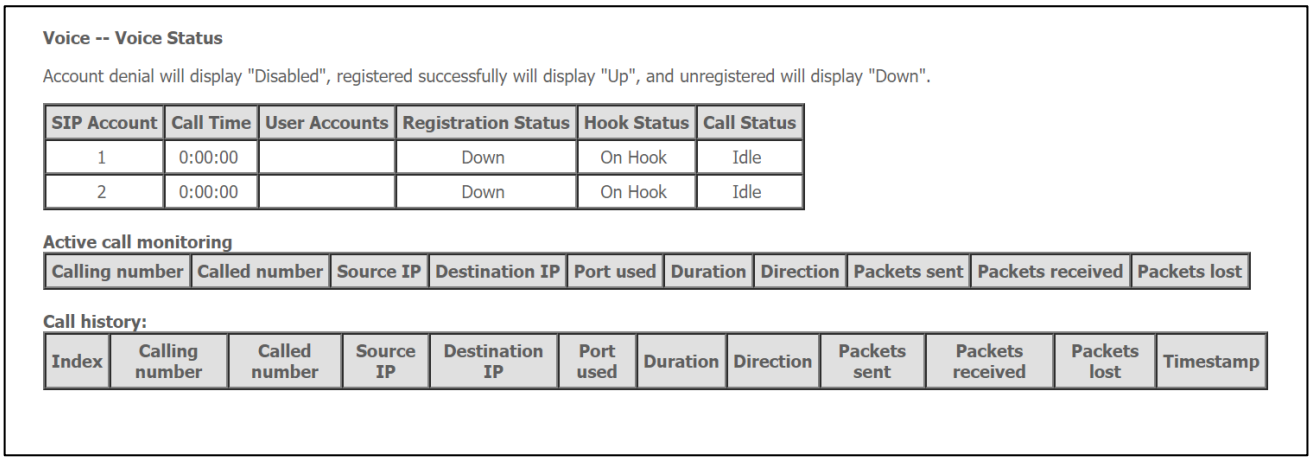
Table 17 – Advanced Wireless settings

Voice

This section explains how to configure the VoIP settings of the Gateway. VoIP allows you to use a traditional landline handset with your broadband connection, with calls routed over the internet. To configure VoIP, you will require a VoIP account, usually bundled alongside your internet connection as an add on. Contact your ISP for further information.

VoIP Status

The Voice Status page displays the registration status of your SIP accounts and the total call time of each account.



Voice -- Voice Status

Account denial will display "Disabled", registered successfully will display "Up", and unregistered will display "Down".

SIP Account	Call Time	User Accounts	Registration Status	Hook Status	Call Status
1	0:00:00		Down	On Hook	Idle
2	0:00:00		Down	On Hook	Idle

Active call monitoring

Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost

Call history:

Index	Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost	Timestamp

Figure 87 – VoIP – Voice status

SIP Basic Setting

The SIP Settings page is where you enter your VoIP service settings as supplied by your VoIP service provider (VSP). If you are unsure about a specific setting or have not been supplied information for a particular field, please contact your VoIP service provider to verify if this setting is needed or not.

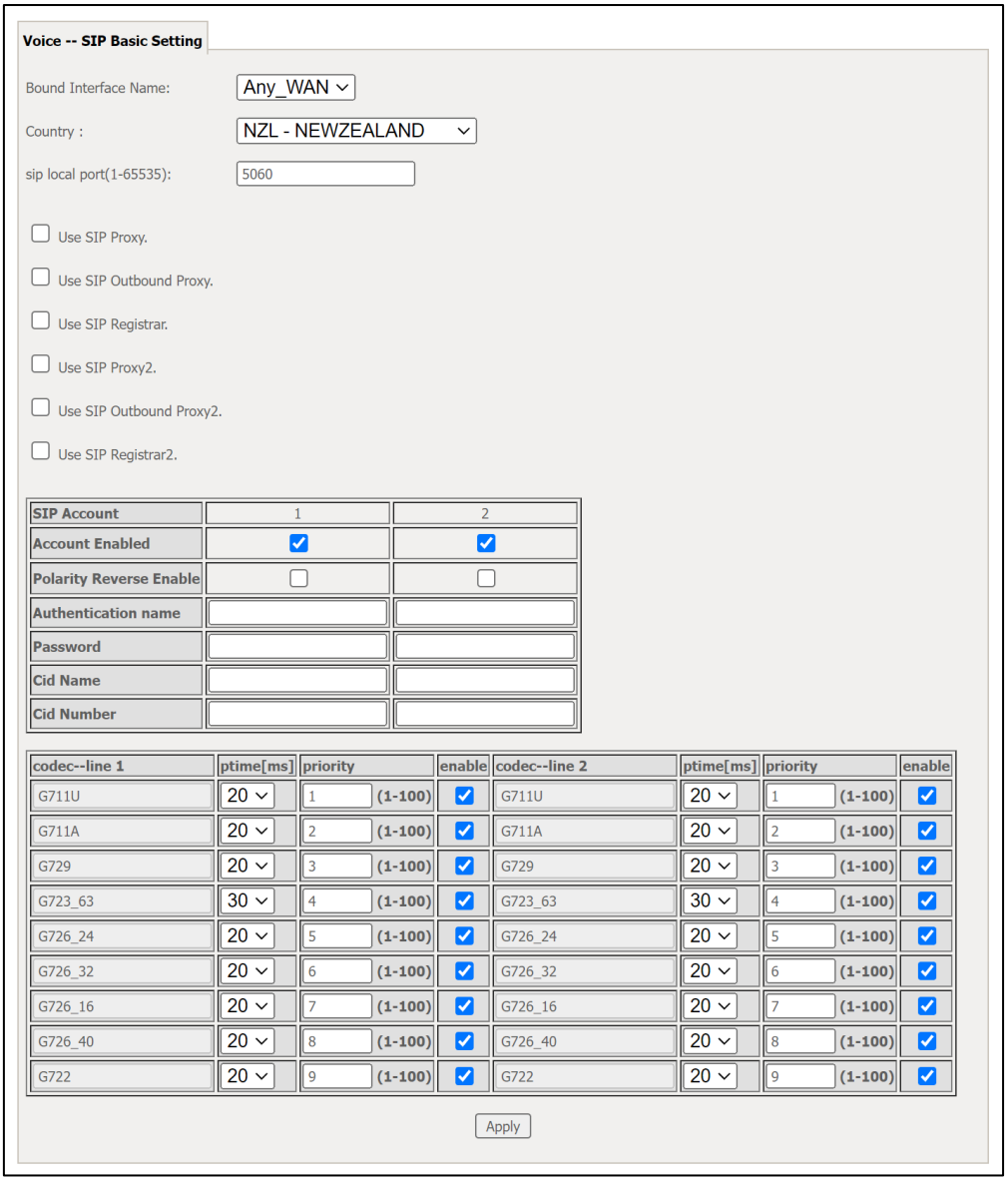


Figure 88 – VoIP – SIP basic setting

The individual fields shown above on the SIP Basic Settings page are explained in the following table.

Option	Definition
Bound Interface Name	Select the Interface that the VoIP account will use to make a connection to the VoIP Service Provider.
Country	Set the country where your SIP provider is located.
SIP Local Port	Set the SIP local port of the gateway, the default value is 5060. SIP local port is the SIP UA (user agent) port.
Use SIP Proxy	Select the checkbox of Use SIP Proxy, if your router uses a SIP proxy. SIP proxy allows other parties to call DSL router through it. When it is selected, the following fields appear.
SIP Proxy	The IP address of the proxy.
SIP Proxy port	The port that this proxy is listening on. By default, the port value is 5060.

Use SIP Outbound Proxy	Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet. When it is selected, the following fields appear.
SIP Outbound Proxy	The IP address of the outbound proxy.
SIP Outbound Proxy port	The port that the outbound proxy is listening on. By default, the port value is 5060.
Use SIP Registrar	Select this option if required by your VoIP Service Provider. Enter the SIP Proxy Domain Name and SIP Proxy Port which is typically 5060.
SIP Registrar	The IP address of the SIP registrar.
SIP Registrar port	The port that SIP registrar is listening on. By default, the port value is 5060.
Account Enabled	If it is unselected, the corresponding account is disabled, you cannot use the account to initiate or accept any call.
Polarity Reverse Enable	Enable or disable Polarity Reverse.
Authentication name	Set the username of authentication.
Password	Set the password of authentication.
Cid Name	Username. It is the Display Name.
Cid Number	Set the caller number. It must be a number of 0~9.
ptime	You can use it to set the packetization time (PT). The PT is the length of the digital voice segment that each packet holds. The default is 20 millisecond packets. Changing this setting to 10 milliseconds improves the voice quality, but leads to increased network traffic.
Priority	The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the router chooses the codec automatically.

Table 18 – Voice – SIP Basic Setting parameters

After entering your VoIP settings select the Apply button, then select Management > Save/Reboot and select the Reboot button. After the gateway restarts and an internet connection is established, the VoIP service will start. If the service does not work as expected, recheck the above settings with your VoIP provider to ensure they are correct.

SIP Advanced Setting

The SIP Advanced page allows you to configure settings that your VoIP service provider has enabled on your SIP account and if you have the appropriate call features and other functionality on your cordless or corded phone handsets.

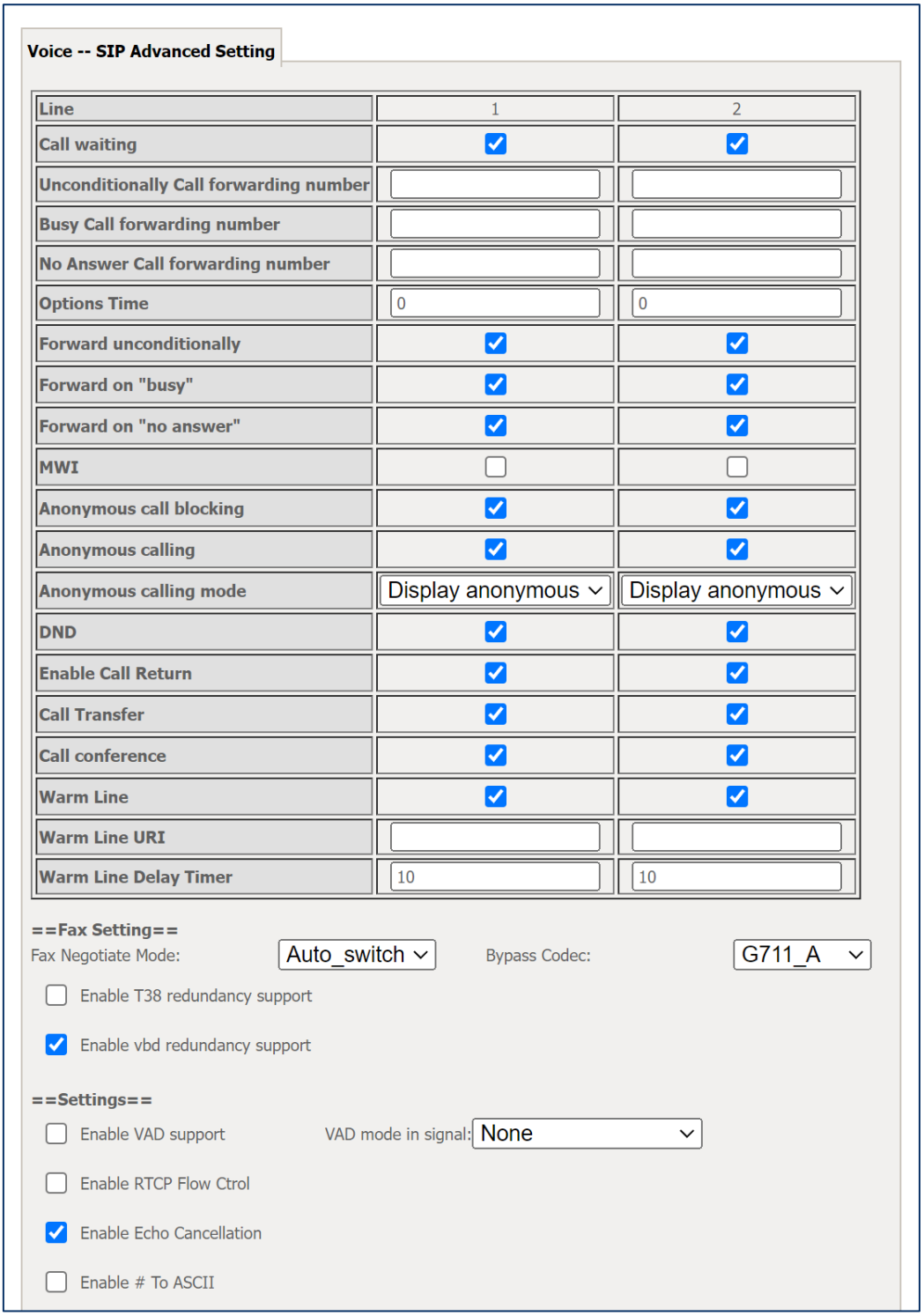


Figure 89 – VoIP – SIP Advanced Setting

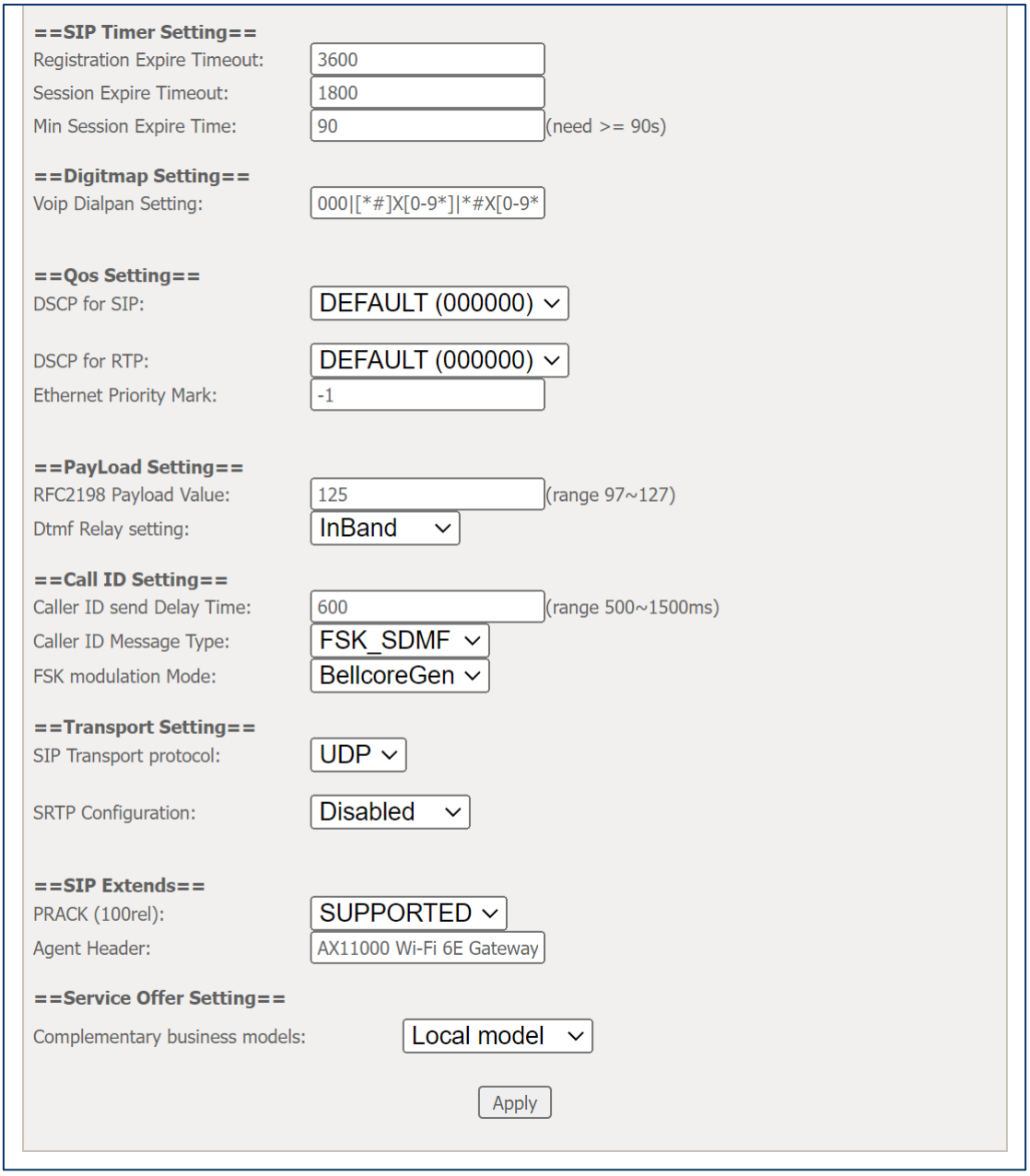


Figure 90 – VoIP – SIP Advanced Setting Continued

To configure the SIP advanced settings, the following parameters are configurable:

Parameter	Definition
Line	Displays the phone port you want to configure
Call Waiting	Select this option for your phone if your VoIP Service Provider has enabled Call Waiting on your SIP account.
Unconditionally Call forwarding number	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Busy Call Forwarding Number	Enter the phone number to forward a call to if it arrives while the line is busy.
No Answer Call forwarding number	Enter the phone number to forward a call to if the call is not answered.

Forward Unconditionally	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Forward On “busy”	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Forward On “No Answer”	Select this option if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
MWI (Message Waiting Indicator)	Select this option if your VoIP Service Provider has enabled MWI (Message Waiting Indicator) on your SIP account and you wish to use this feature.
Anonymous Call Blocking	Select this option if your VoIP Service Provider has enabled Anonymous Call Blocking on your SIP account and you wish to use this feature.
Anonymous Calling	Select this option if your VoIP Service Provider has enabled Anonymous Calling on your SIP account and you wish to use this feature.
Anonymous calling mode	When set to Display anonymous, the modem hides your caller ID. When set to All anonymous, the modem hides both caller ID and the SIP URL of the originating call.
DND (Do Not Disturb)	Select this option if your VoIP Service Provider has enabled DND (Do Not Disturb) on your SIP account and you wish to use this feature.
Enable T38 Redundancy Support	Select this function if you wish to send or receive faxes via VoIP and have a fax machine capable of using the T38 fax over VoIP protocol.
Enable VBD redundancy support	Select this checkbox to use the feature.
Enable VAD support	Enables the Voice Activated Detection function of the modem. When enabled, no data is transmitted during periods of silence or low volume, reducing the data usage.
Enable RTCP Flow Control	Select this checkbox to use the feature.
Enable Echo Cancellation	Select this checkbox to use the feature.
Enable # To ASCII	Select this checkbox to use the feature.
Enable Reinjection Function	Select this checkbox to use the feature.
RFC2198 Payload Value (range 97-127)	Enter the RFC2198 payload value that the valid range is 96 ~ 127.
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	The interval of dialog refreshing time.
Min Session Expire Time	The minimum interval of dialog refreshing time.
VoIP DialPlan Setting	Set the VoIP dial plan. If user-dialled number matches it, the number is processed by the VoIP router immediately.
DSCP for SIP	Set the DSCP QoS tagging for Session Initiation Protocol. You can select it from the drop-down list.
DSCP for RTP	Set the DSCP QoS tagging for Real-time Transport Protocol. You can select it from the drop-down list.

Dtmf Relay Setting	Set DTMF transmit method, which can be following values: SIP Info: Use SIP INFO message to transmit DTMF digits. RFC2833: Use RTP packet to encapsulate DTMF events, as specified in RFC 2833. InBand: DTMF events are mixed with user voice in RTP packet.
SIP Transport Protocol	Select the transport protocol to use for SIP signalling. Note that your SIP proxy and registrar will need to support the protocol you select.
Enable Local Supplementary Service	Select the checkbox to enable the supplementary service settings by the telephone set. If you deselect the checkbox, the supplementary service cannot be set by the telephone set.

Table 19 – Voice – SIP Advanced Parameters

Configuring a VoIP dial plan

The gateway comes with a default dial plan suitable for use in New Zealand. The dial plan tells the router to dial a number immediately when a string of numbers entered on a connected handset matches a string in the dial plan. For example, the string `13[1-9]XXX` allows the router to recognize six digit "13 numbers" allowing customers to call a business for the price of a local call anywhere in Australia. The reason it is configured as 13[1-9]XXX is because 13 numbers cannot begin with a 0 after the 13 while the last 3 digits may be any numeric digit.

You can configure the dial plan to match any string you like. Below are some rules for configuring a dial plan:

- Separate strings with a | (pipe) character.
- Use the letter X to define any single numeric digit.
- Use square brackets to specify ranges or subsets, for example:
  - `[1-9]` allows any digit from 1 to 9.
  - `[247]` allows either 2 or 4 or 7.
  - Combine ranges with other keys, for example, `[247-9*#]` means 2 or 4 or 7 or 8 or 9 or * or #.

Dial plan syntax

Dial Plan Syntax

To specify a...	Enter	Result
New dial string	| (Pipe)	Separates dial strings
Digit	0 1 2 3 4 5 6 7 8 9	Identifies a specific digit (do not use #)
Range	[digit-digit]	Identifies any digit dialled that is included in the range
Wild card	X	X matches any single digit that is dialled
Timer	.t (dot t)	Indicates that an additional time out period of 4 seconds should take place before automatic dialling starts

Table 20 – Dial Plan Syntax table

Dial plan example: Australia Dial Plan

000|[*#]x[0-9*]|*#x[0-9*]|00[1-9]xx.t|014xxxxxxx|016xxxxxx|0192x|0198xxxxxx|0[23478]xxxxxxxx|0500xxxxxx|11xx|123x|124xx|1251xx|1252xxx|1255x|1258xxx|1271x|130xxxxxxx|13[1-9]xxx|1802xxx|189xx|1[8-9]xxxxxxxx|[2-9]xxxxxxx

---

000 = Australia Emergency Call Service

0011*t = International number (After 0011 the router allows entry of arbitrary digits then and dials out after 4 seconds from the entry of the last digit.)(Note: Please ensure your VoIP provider supports international numbers for the country you are dialling.)

0[23478]XXXXXXXX = Landline numbers with area code 02,03,04,07,08 +XXXX XXXX and Mobile numbers with 04XXXXXXXX)

1[8-9]XXXXXXXX = 1800 and 1900 free call numbers

130XXXXXXX = 1300 business numbers

13[1-9]XXX = 13 business numbers

[2-9]XXXXXXX = Landline numbers without area code

SIP Star Code Setting

The SIP Star Code Setting page provides you with the ability to configure the codes used to active and deactivate call features such as call forwarding and call waiting.

Please consult your VoIP provider if SIP Star Code is supported on SIP side.

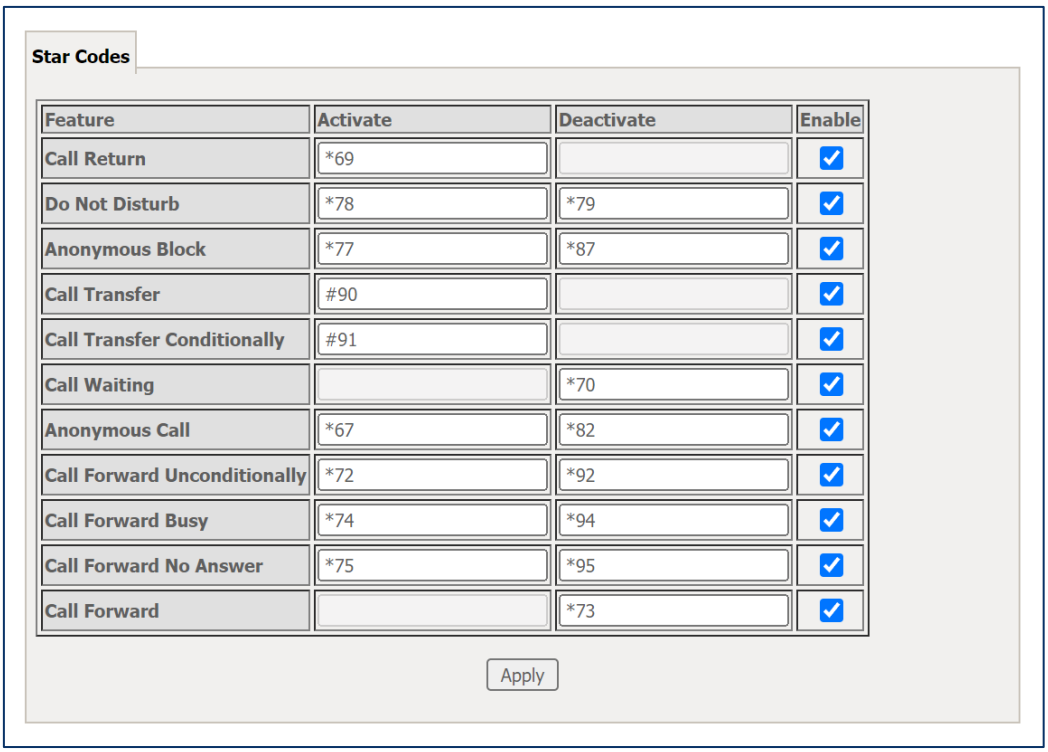


Figure 91 – VoIP – SIP Star Code Setting

SIP Extra Setting

The SIP Extra Setting page displays additional settings related to the SIP service.

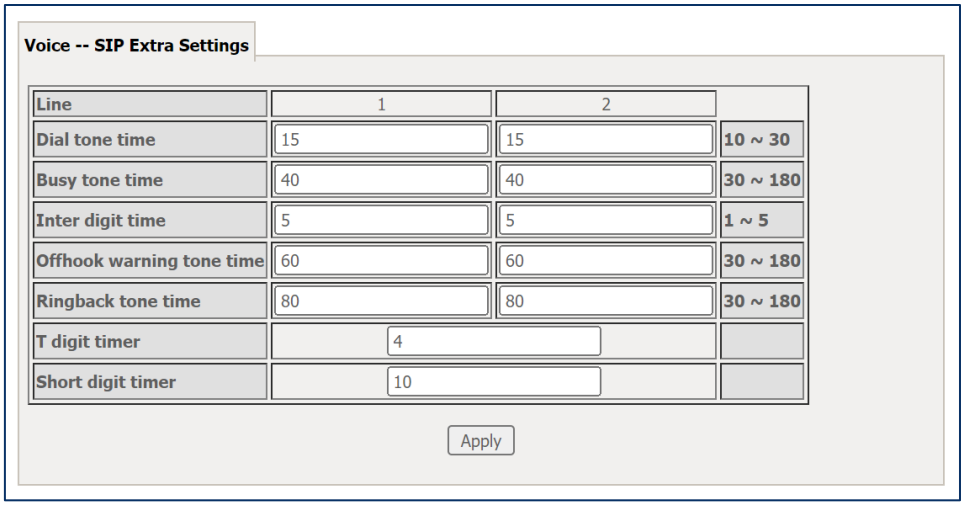


Figure 92 – VoIP – SIP Extra Settings

The following parameters are configurable on this page:

Parameter	Definition
Dial tone time	Set the Dial tone duration.
Busy tone time	Set the Busy tone duration.
Inter digit time	Set the timing between digits. The valid range is 1 ~ 5.
Off hook warning tone time	Set the Off-hook warning tone duration.
Ringback tone time	Set the Ring back tone duration.

Table 21 – Voice – SIP Extra parameters

SIP Error Information

The SIP Error Information page displays a log of any voice-related errors that occur.

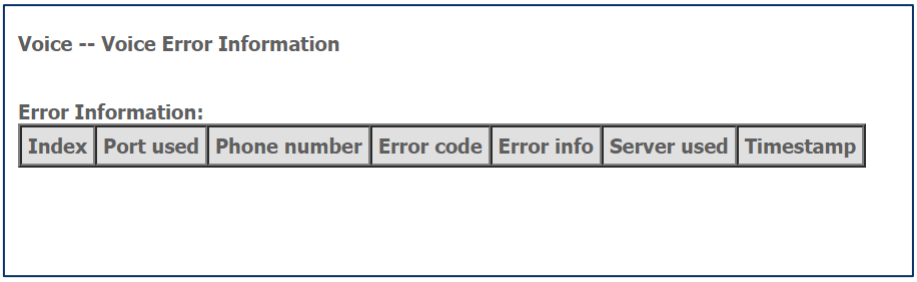


Figure 93 – VoIP – SIP Error Information

Diagnostics

Ping

The Ping page allows you to ping a remote IP address or hostname to test the internet connection.

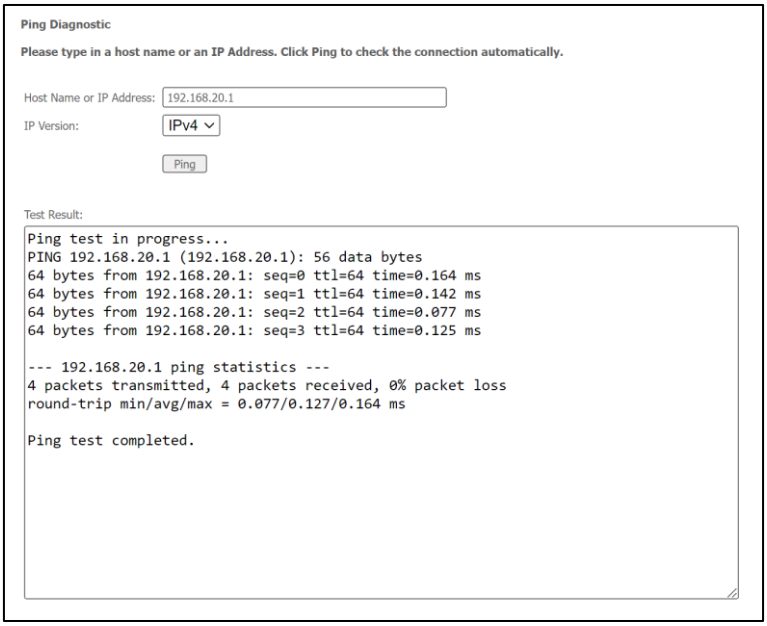


Figure 94 – Diagnostics – Ping

Traceroute

The Traceroute page allows you to perform a traceroute to a remote IP or hostname. A traceroute works by sending Internet Control Message Protocol (ICMP) packets, and every router involved in transferring the data gets these packets. The ICMP packets provide information about whether the routers used in the transmission can effectively transfer the data.

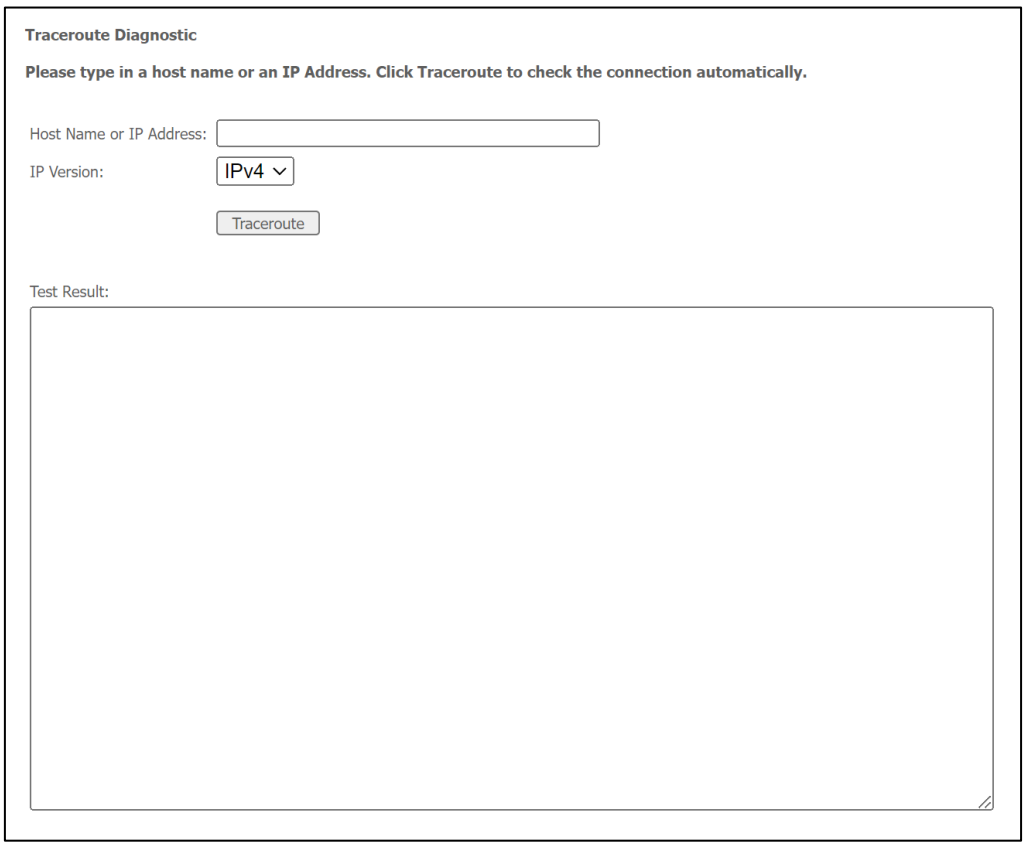


Figure 95 – Diagnostics – Traceroute

Diagnostics

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a FAIL status:

1 Select the Help link and follow the troubleshooting procedures in the Help screen that appears.

2 After following the troubleshooting procedures, select Rerun Diagnostic Tests at the bottom of the screen to re-test and confirm the error.

3 If the test continues to fail, contact Technical Support.

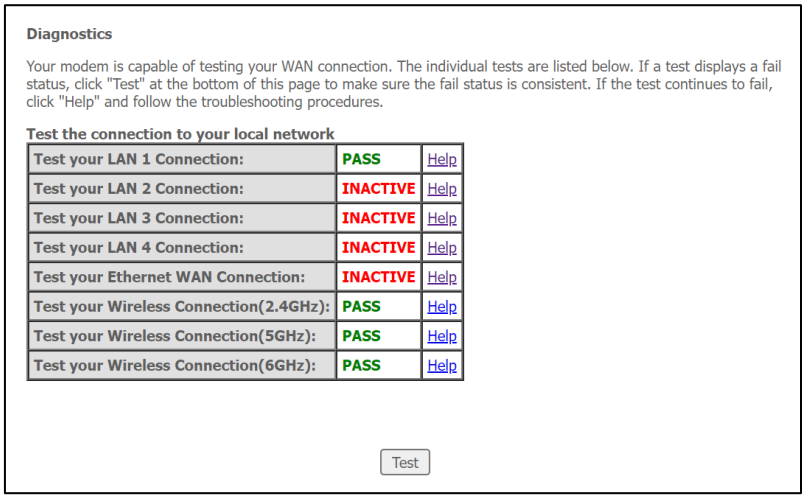


Figure 96 – Diagnostics – Diagnostics page

Management

Settings

The Settings section allows you to back up and restore your Gateway configuration and restore the Gateway to factory defaults.

Backup

The Backup feature allows you to take a snapshot of the current configuration of your gateway so that you can roll back to the current configuration if you plan to make changes.

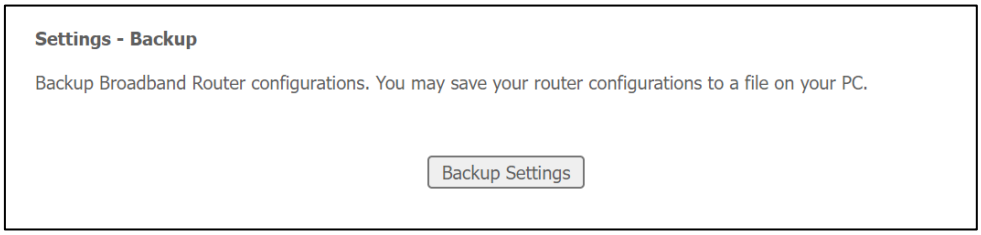


Figure 97 – Management – Settings - Backup

Select the Backup Settings button to save the current configuration settings. The configuration file is saved via your browser to the download folder configured in your browser. To restore the configuration on your Gateway, see the Update section below.

Update

Use the Update page to restore a previously saved configuration from the Backup page.

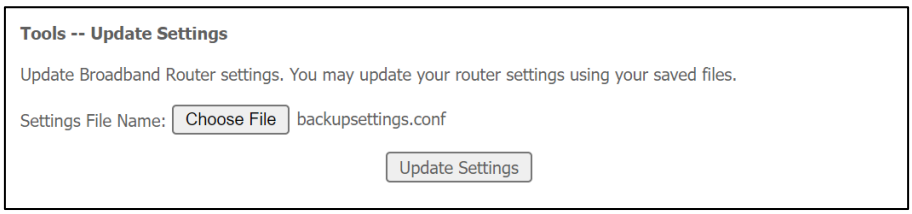


Figure 98 – Management – Settings - Update

To restore a previous configuration:

1. Select the Choose File button, and locate the file on your computer. The selected file appears next to the Choose File button.
2. Select the Update Settings button to begin the configuration update. The configuration restore takes up to five minutes to complete.
3. The gateway restarts when the configuration update is complete.

Restore defaults

The **Restore defaults** page allows you to factory reset the gateway. All settings will be erased and reset to the gateway will be reset to its default configuration. Select the **Restore Default Settings** button to perform the reset. The factory reset may take up to five minutes to complete, and the Gateway will reboot during this time.

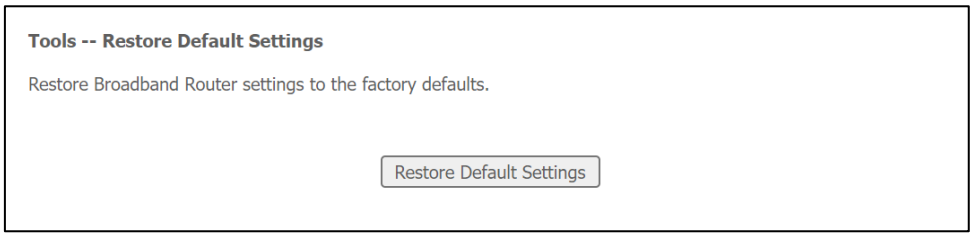


Figure 99 – Management – Settings – Restore defaults

System Log

The **System Log** page allows you to view a log of the Gateway, as well as configure the types of log the Gateway should collect.

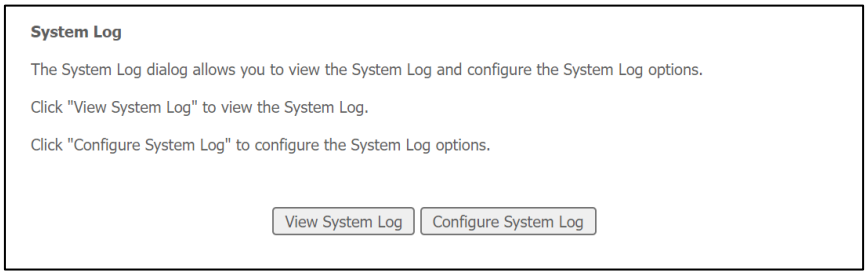
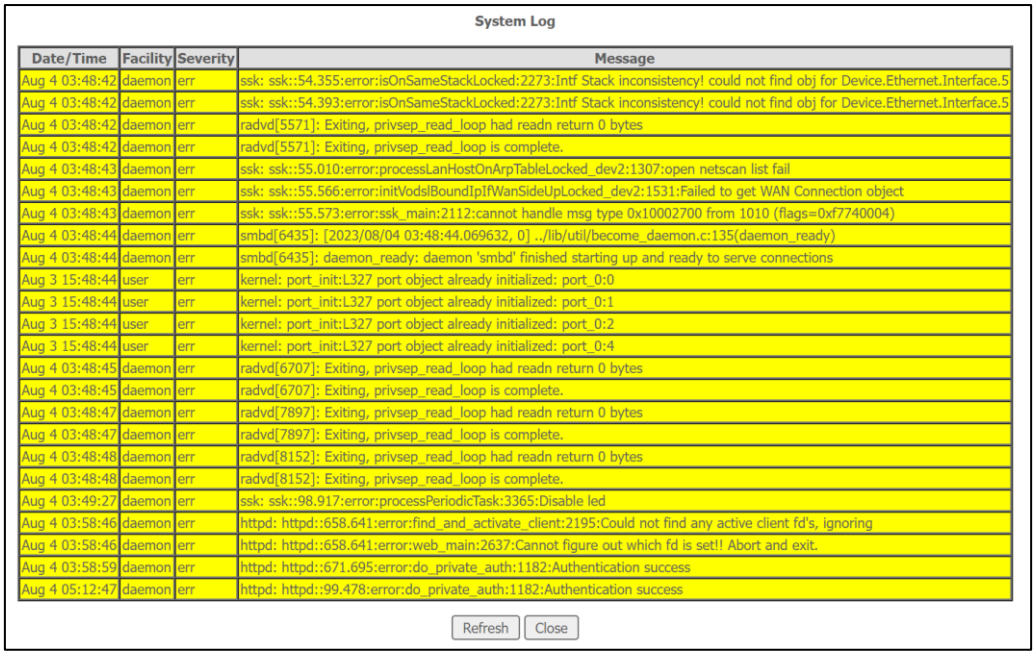


Figure 100 – Management – System Log

To view the System Log, select the **View System Log** button. Select the **Refresh** button to refresh the log. Select the **Close** button to close the log.


System Log

Date/Time	Facility	Severity	Message
Aug 4 03:48:42	daemon	err	ssk: ssk::54.355:error:isOnSameStackLocked:2273:Intf Stack inconsistency! could not find obj for Device.Ethernet.Interface.5
Aug 4 03:48:42	daemon	err	ssk: ssk::54.393:error:isOnSameStackLocked:2273:Intf Stack inconsistency! could not find obj for Device.Ethernet.Interface.5
Aug 4 03:48:42	daemon	err	radvd[5571]: Exiting, privsep_read_loop had readn return 0 bytes
Aug 4 03:48:42	daemon	err	radvd[5571]: Exiting, privsep_read_loop is complete.
Aug 4 03:48:43	daemon	err	ssk: ssk::55.010:error:processLanHostOnArpTableLocked_dev2:1307:open netscan list fail
Aug 4 03:48:43	daemon	err	ssk: ssk::55.566:error:initVodslBoundIpIfWanSideUpLocked_dev2:1531:Failed to get WAN Connection object
Aug 4 03:48:43	daemon	err	ssk: ssk::55.573:error:ssk_main:2112:cannot handle msg type 0x10002700 from 1010 (flags=0xf7740004)
Aug 4 03:48:44	daemon	err	smbd[6435]: [2023/08/04 03:48:44.069632, 0] ../lib/util/become_daemon.c:135(daemon_ready)
Aug 4 03:48:44	daemon	err	smbd[6435]: daemon_ready: daemon 'smbd' finished starting up and ready to serve connections
Aug 3 15:48:44	user	err	kernel: port_init:L327 port object already initialized: port_0:0
Aug 3 15:48:44	user	err	kernel: port_init:L327 port object already initialized: port_0:1
Aug 3 15:48:44	user	err	kernel: port_init:L327 port object already initialized: port_0:2
Aug 3 15:48:44	user	err	kernel: port_init:L327 port object already initialized: port_0:4
Aug 4 03:48:45	daemon	err	radvd[6707]: Exiting, privsep_read_loop had readn return 0 bytes
Aug 4 03:48:45	daemon	err	radvd[6707]: Exiting, privsep_read_loop is complete.
Aug 4 03:48:47	daemon	err	radvd[7897]: Exiting, privsep_read_loop had readn return 0 bytes
Aug 4 03:48:47	daemon	err	radvd[7897]: Exiting, privsep_read_loop is complete.
Aug 4 03:48:48	daemon	err	radvd[8152]: Exiting, privsep_read_loop had readn return 0 bytes
Aug 4 03:48:48	daemon	err	radvd[8152]: Exiting, privsep_read_loop is complete.
Aug 4 03:49:27	daemon	err	ssk: ssk::98.917:error:processPeriodicTask:3365:Disable led
Aug 4 03:58:46	daemon	err	httpd: httpd::658.641:error:find_and_activate_client:2195:Could not find any active client fd's, ignoring
Aug 4 03:58:46	daemon	err	httpd: httpd::658.641:error:web_main:2637:Cannot figure out which fd is set!! Abort and exit.
Aug 4 03:58:59	daemon	err	httpd: httpd::671.695:error:do_private_auth:1182:Authentication success
Aug 4 05:12:47	daemon	err	httpd: httpd::99.478:error:do_private_auth:1182:Authentication success

Figure 101 – Management – System Log – View System Log

To configure the **System Log**, select the **Configure System Log** button.

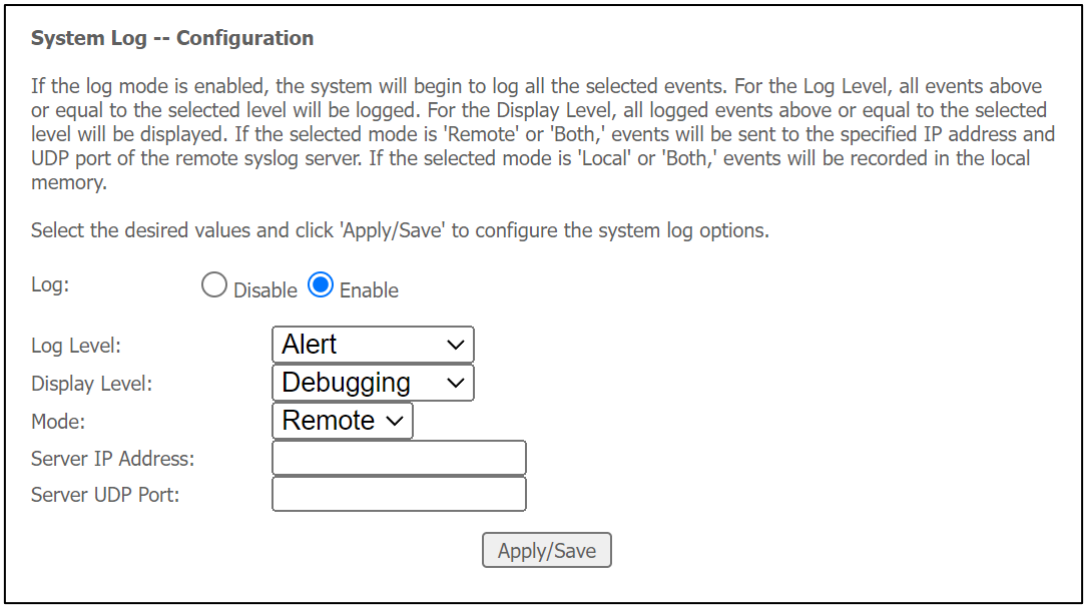


Figure 102 – Management – System Log – Configure System Log

To configure the **System Log,** update the following parameters:

Option	Definition
Log	Enables or disables the logging function.
Log Level	Set the level of detail that should be collected by the log. The following log levels are available: - Emergency - Alert - Critical - Error - Warning - Notice - Informational - Debugging
Display Level	Set the level of detail that should be shown by the log on the **View Log** screen. Note that even if you set the Display Level lower than the **Log Level,** the log will not show those items unless they are collected in the **Log Level** setting.
Mode	Where the logs should be collected. The mode can be set to **Local**, where the logs are stored on the Gateway, **Remote** where the logs are sent to a remote server, or **Both**. If using remote or both, enter the details of your remote syslog server.
Apply / Save	Select the **Apply / Save** button to apply the configuration.

Table 22 – Management – System Log – Log Configuration

Security Log

The Security Log page allows you to view a log of security events which have occurred on the Gateway, such as user log ins.

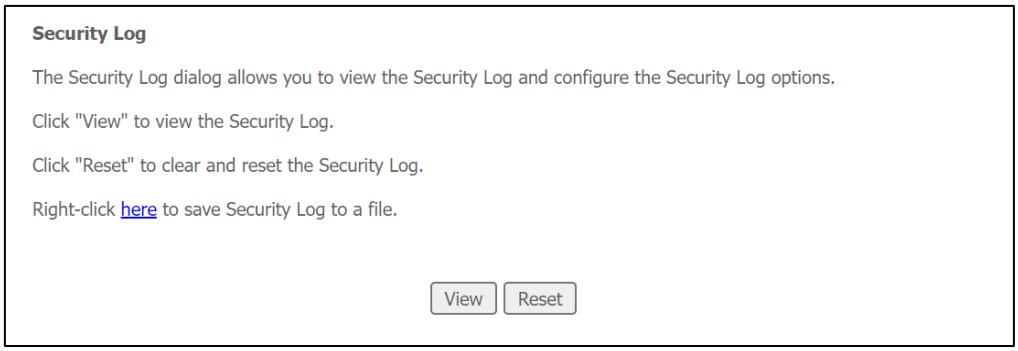


Figure 103 – Management – Security Log

To view the Security Log, select the View button. The Security Log opens in a new window.

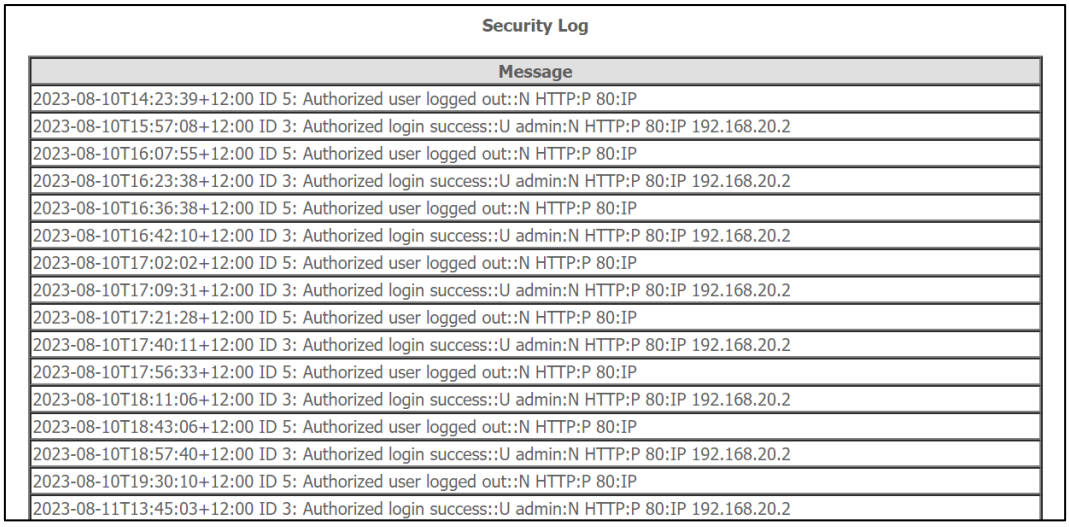


Figure 104 – Management – Security Log – View Security Log

To save a copy of the Security Log to your computer, right click on the 'here' hyperlink in the browser, and select, Save Link As. The file downloads to your default download folder.

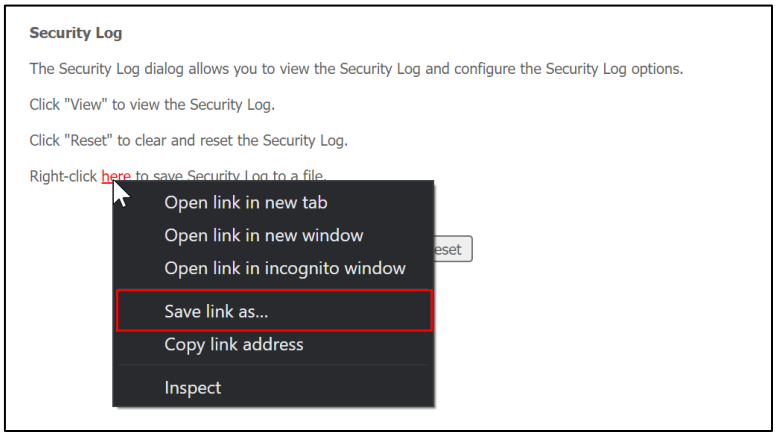


Figure 105 – Management – Security Log – Save Security Log

SNMP Agent

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the Gateway (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

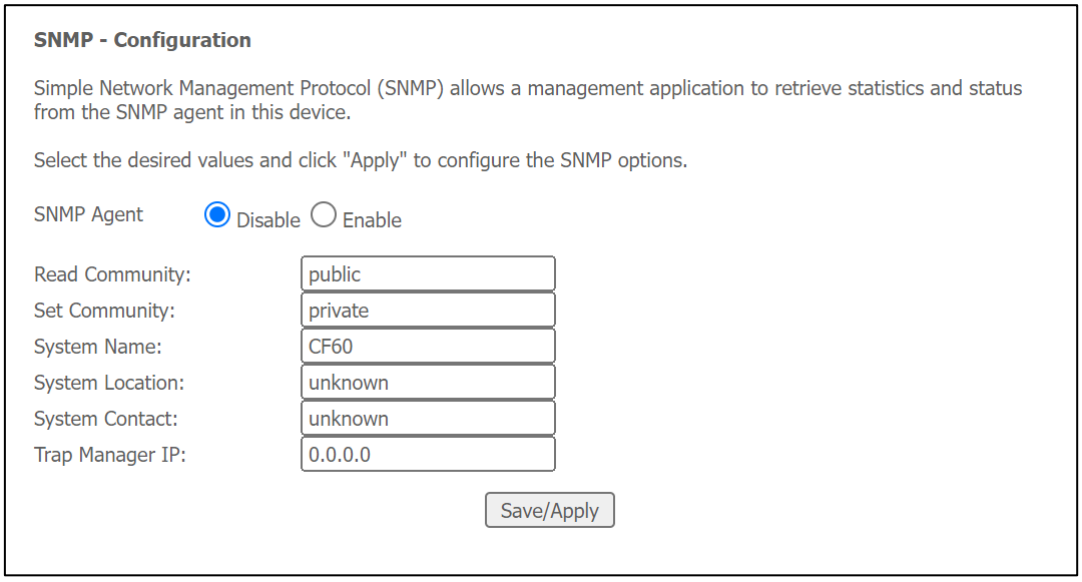


Figure 106 – Management – SNMP

The following parameters are available on the SNMP configuration page:

Option	Definition
SNMP Agent	Enables or disables the SNMP functionality.
Read Community	The read only name of the community.
Set Community	The read write name of the community.
System Name	The name which this device should appear as in the SNMP management software.
System Location	Text field which can be set to the location of the Gateway. Optional.
System Contact	Text field which can be set to the contact detail for the Gateway. Optional.
Trap Manager IP	The IP of the Trap Manager.
Apply / Save	Select the Apply / Save button to apply the configuration.

Table 23 – Management – SNMP – SNMP Parameters

TR-069 Client - Configuration

TR-069 enables provisioning, configuration, or diagnostics to be automatically performed on your router by your Internet Service Provider (ISP). Generally, TR-069 will be preconfigured, and you will not be required to updated these settings.

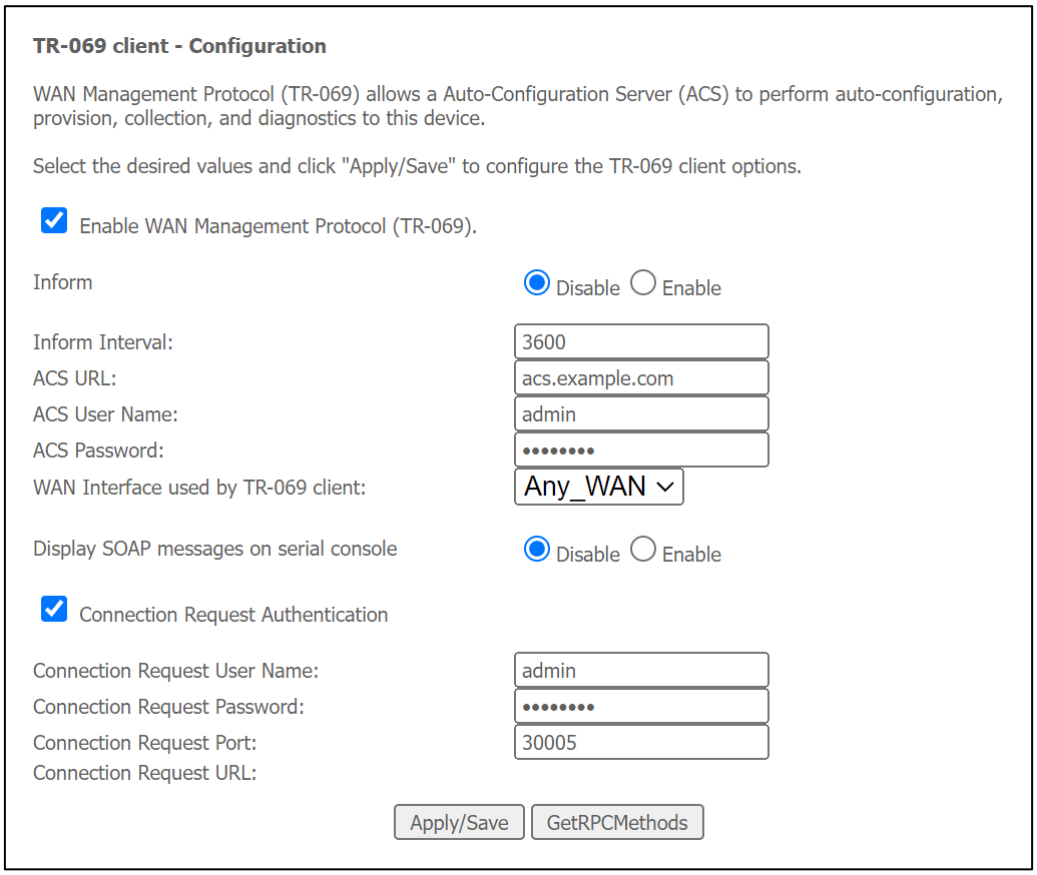


Figure 107 – Management – TR-069

The following parameters are available on the TR-069 page:

Field	Description
Inform	Set to enable to TR-069 client inform session initialization.
Inform interval	Time in seconds that inform session data is sent to the Auto-Configuration Server (ACS).
ACS URL	The address of the ACS server.
ACS User Name	The username to access the ACS server.
ACS Password	The password to access the ACS server.
WAN Interface used by TR-069 Client	The interface connection used to send and receive data to the ACS server.
Connection Request Authentication	Enter the username, password, port and URL if the TR-069 connection request requires authentication.
Apply / Save	Select the **Apply / Save** button to apply the configuration.

Table 24 – Management – TR-069 – TR-069 Parameters

Internet Time

The tools on the Internet Time page allow you to use the Network Time Protocol (NTP) to configure specific time servers to synchronise time, set local time zones, etc. for the modem. The time servers are correct to within a few milliseconds of Coordinated Universal Time (UTC).

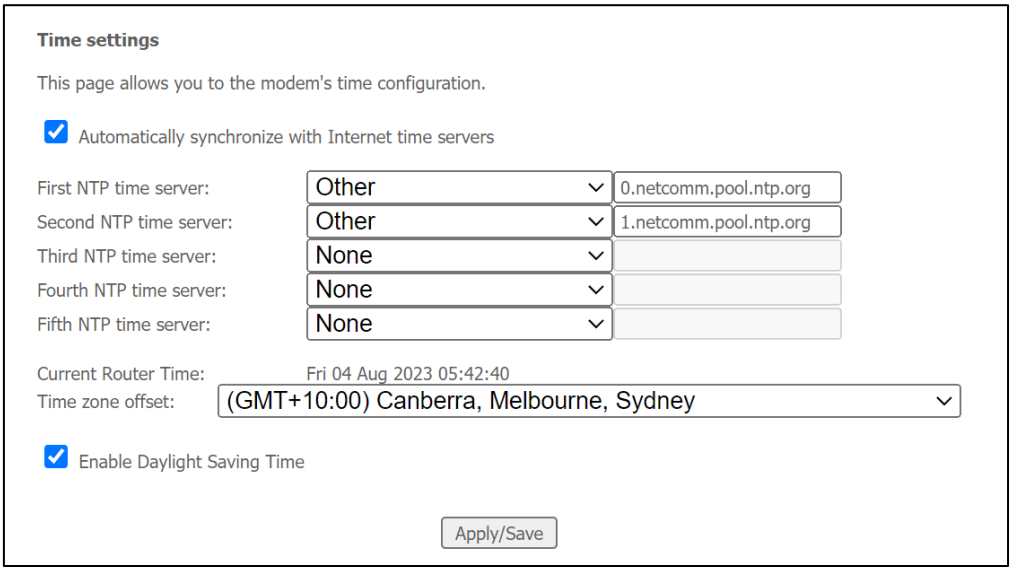


Figure 108 – Management – Internet time

Up to five NTP time servers can be configured for redundancy, in case the preceding time server cannot be reached, although configuring all five is not required. To update each time server, select the dropdown to choose a pre-configured time server. Else select Other to enter your own time server. Set the time zone offset by using the drop-down and selecting your local time zone. Select Enable Daylight Saving Time if you would like the router to automatically adjust itself when daylight savings begins and ends in your time zone.

Access Control

The Access Control option found in the Management drop-down menu configures access related parameters for the following:

- Passwords
- Timeout
- Access list
- Services Control

Passwords

The **Passwords** page allows you to configure the password for your Gateway.

Note – If you forget the password to your Gateway after changing it, you can reinstate the default password by performing a reset using the **Reset** button.

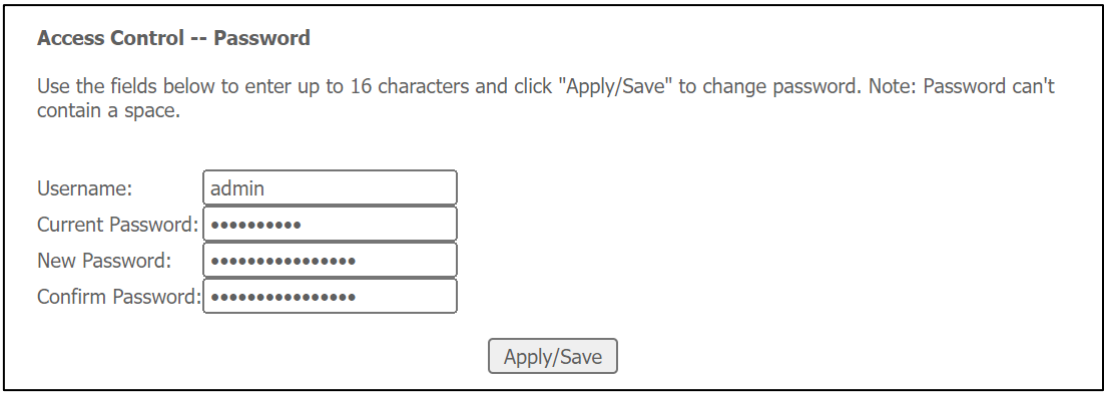


Figure 109 – Management – Access Control - Password

To update the password:

1. Enter the username if required. Generally the username is **admin.**
2. Enter the current password, which was used to log into the Gateway.
3. Enter a new password for the Gateway. Passwords must be 16 characters or less with no spaces.
4. Enter the password again to confirm.
5. Select the **Apply / Save** button.

Timeout

The **Timeout** page allows you to configure the amount of inactive / idle time before the web interface is logged out. To update, enter the amount of time, in seconds, then select the **Save / Apply** button.

Figure 110 – Management – Access Control - Timeout

Access List

The Access List page is used to restrict access to the web interface by IP. When the Access List functionality is enabled, only those IP addresses in the list can access management services on the Gateway.

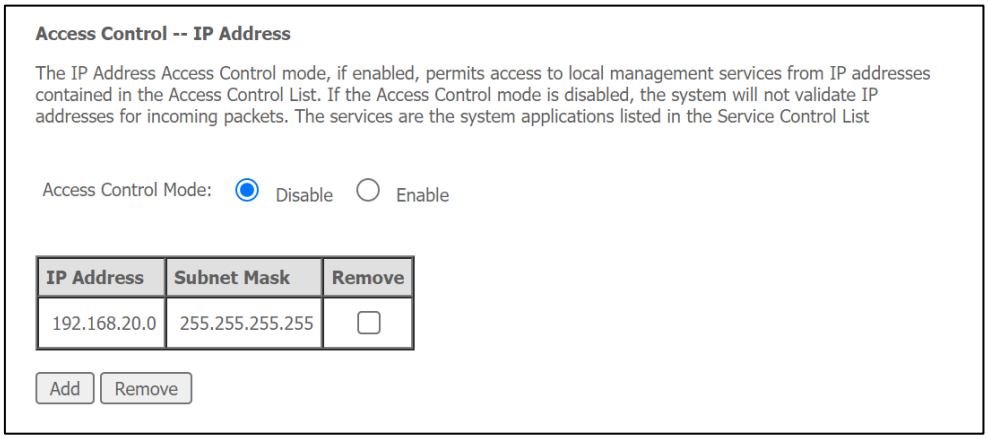


Figure 111 – Management – Access Control – Access List

To add a device to the list, select the Add button, then enter the IP address and subnet mask using CIDR slash notation. For example:

```
192.168.20.1/32
```

To permanently delete an IP Address from the list, select ☑ in the Remove column and then select the Remove button.

Services Control

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by selecting the LAN or WAN checkbox and specifying the service port assigned to the service.

The following access services are available: HTTP, HTTPS, SSH, FTP, TFTP, ICMP, SNMP and SAMBA. Select the Apply / Save button to enable or disable the services after updating.

Note – You should change your default password before enabling a WAN service. You should also consider carefully if the service needs to be exposed on the WAN port, as it may allow unauthorised access to the Gateway and by extension, your home network.

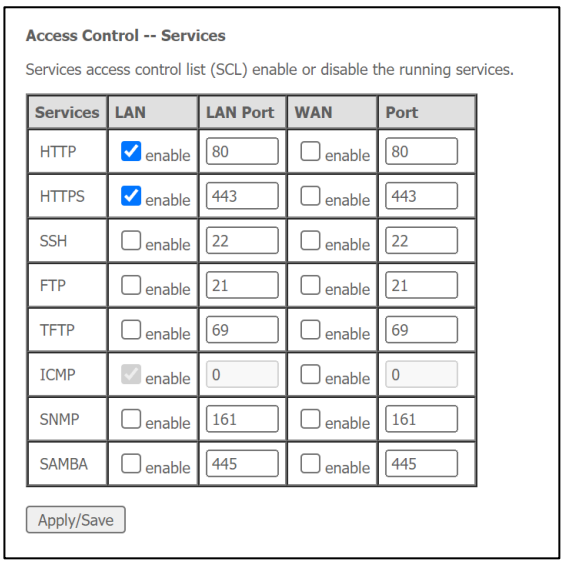


Figure 112 – Management – Access Control – Services Control

LED Control

The LED control page allows you to turn the LED indicators on the front panel of the Gateway On or Off. The lights update automatically when the option is chosen. When the LED settings toggle is set to Enable the LED indicators are On. When the LED settings toggle is set to Disable the LED indicators are off.

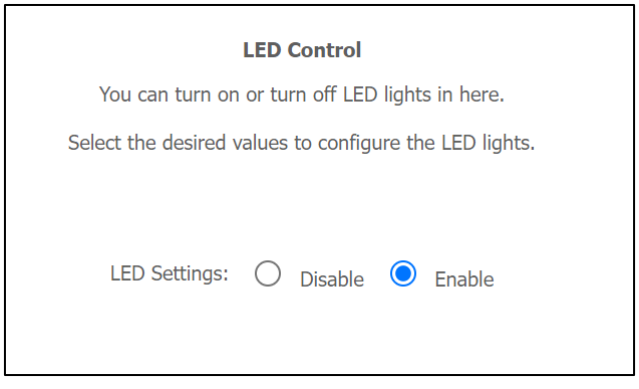


Figure 113 – Management – LED Control

Update Software

The Update Software page is used to manually update your Gateway's firmware.

Important – Some ISPs may have their own custom firmware for the Gateway and manage this for you remotely. In this situation, manually updating the firmware yourself could cause issues with your router, so we recommend that you consult with your ISP before installing any software updates manually.

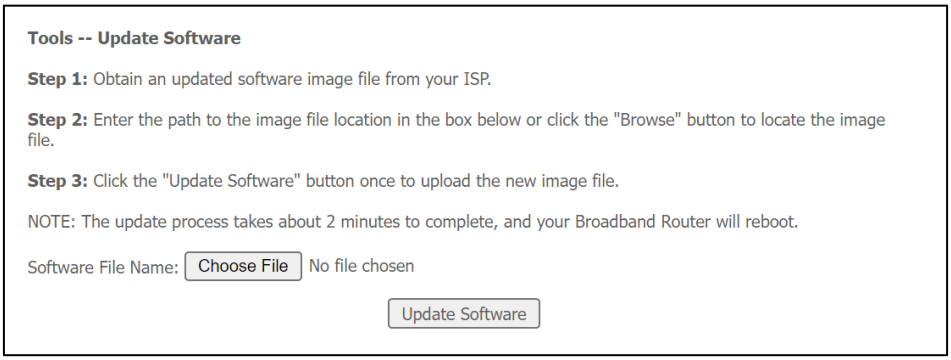


Figure 114 – Management – Update Software

To perform a firmware upgrade:

1. Check for a firmware upgrade file from the NetComm Support Page for the CF60 - https://support.netcommwireless.com/products/CF60 . If a file is available, download it to your computer.
2. Select the Choose File button, and locate the file on your computer.
3. Select the Update Software button to perform the firmware upgrade. The Gateway reboots on completion.
4. Log into the Gateway and verify that the Software Version on the Device Info page matches the firmware file which was installed.

Figure 115 – Management – Update Software – Software Version

Reboot

The Reboot page allows you to restart the Gateway. Allow five minutes for the Gateway to reboot.

Figure 116 – Management – Reboot