User Guide

CloudMesh Hybrid Gateway – NL19MESH

Doc No. UG01363

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 CloudMesh Hybrid Gateway to transmit or receive such data.

Copyright

NetComm Wireless Limited was acquired by Casa Systems in 2019.

Note – This document is subject to change without notice.

Document history

This document relates to the following product:

NetComm CloudMesh Hybrid Gateway (NL19MESH)

Ver.	Document description	Date
v1.0	First document release	3 December 2021

Table i. – Document revision history

Contents

Overview 7

Introduction 7
Prerequisites 7
Notation 7

Set up your Internet connection 8

Before you begin 8
Insert the SIM card 8
Connect to internet service 9
Ethernet WAN 9
ADSL or VDSL 10
Configure your gateway 10

Connect with Wi-Fi 11

Connect a telephone 11

CloudMesh app 12

Download the CloudMesh app 12

Interfaces 13

Front view 13
LED indicators 13
Rear view 15
Side view 16
Safety and product care 16
Transport and handling 17

Placement of your CloudMesh Gateway 17

Avoid obstacles and interference 17

Configure the CloudMesh Gateway 18

Device Info 19
Basic Setup 20
ADSL connections 20
VDSL connections 25
Ethernet WAN connections 29
Backup Basic Setup 33

Advanced setup 34

Layer2 Interface 35
ATM Interface 35
PTM Interface 37
ETH Interface 38
WAN Service 39
PPOE (PPP over Ethernet) 40
IPOE (IP over Ethernet) 41

Bridging 42
Mobile Broadband 42
Add/Edit Mobile Broadband Setup 44
PIN settings 45
Modem information 46
LAN 47
IPv4 Autoconfig 47
IPv6 LAN Auto Configuration 49
LAN VLAN Setting 50
NAT 51
Virtual Servers 51
Port Triggering 52
DMZ Host 53
ALG 54
MAC Filtering 55
Parental Control 56
Time Restriction 56
URL Filter 57
Firewall 58
Level Rule 58
Quality of Service 61
QoS Queue 62
QoS Classification 63
QoS Port Shaping 64
Routing 66
Default Gateway 66
Static Route 67
Policy Routing 68
RIP 69
DNS 70
DNS Server 70
Dynamic DNS 71
DSL 73
UPnP 74
DNS Proxy 74
DLNA 75
Storage Service 75
Storage Device Info 75
User Accounts 76
Interface Grouping 77

Wireless 79

Wi-Fi 2.4GHz / Wi-Fi 5GHz 79
Basic 80
SSID 81
Security 82
WPS 83
MAC Filter 84
Advanced 85

Voice 88

VoIP Status 88

SIP Basic Setting....89
SIP Advanced Setting....91
Configuring a VoIP dial plan....94
Dial plan syntax....94
SIP Extra Setting....96
SIP Star Code Setting....97
SIP Debug Setting....98

VoIP Functionality....99

Registering....99
Placing a Call....99
Anonymous call....99
Do Not Disturb (DND)....100
Call Return....100
Blind Transfer....101
Consultative Transfer....101
Call Forwarding No Answer....101
Call Forwarding Busy....101
Call Forwarding All....102
Three-Way Conference....102
T.38 Faxing....102
Pass-Through Faxing....102

Diagnostics....103

Diagnostics....103
Ethernet OAM....106
Ping....107
Traceroute....108
Start / Stop DSL....109

Management....110

Settings....110
Backup....110
Update Settings....111
Factory Reset....111
System Log....112
Security Log....113
SNMP Agent....114
TR-069 Client....115
Internet Time....116
Access Control....117
Passwords....117
Access List....118
Services Control....118
Update Firmware....119
Reboot....120

Appendix: Quality of Service setup example....121

Reserving IP addresses....121
QoS Configuration Settings....125

High Priority QoS Queue Configuration ... 125
Low Priority QoS Queue Configuration ... 127
High Priority QoS Classification ... 128
Low Priority QoS Classification ... 130
Limiting the upstream rate ... 132
Limiting the downstream rate ... 133

Overview

Introduction

This document provides a detailed description of the device, including instructions on setting up, configuring and using the NetComm CloudMesh Gateway.

Prerequisites

To configure your CloudMesh Gateway, you will require a computing device with a web browser and either a wired or wireless network adapter.

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.

Set 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.

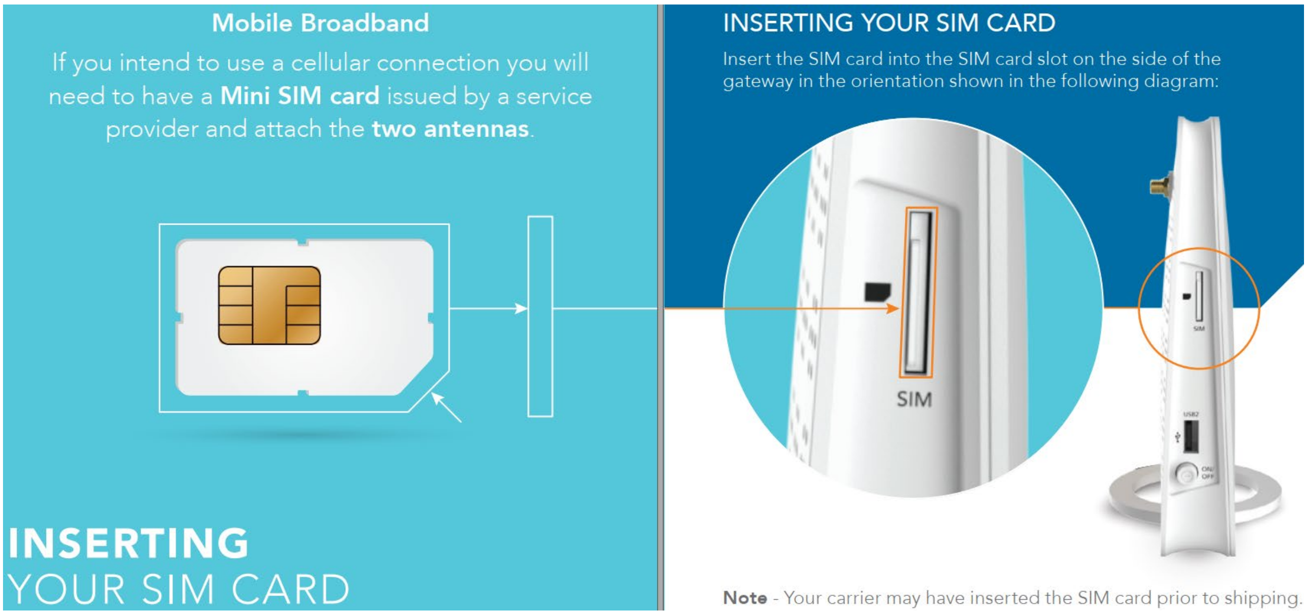
Before you begin

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.

Insert the SIM card

If your carrier has not pre-inserted a SIM card into the card slot on the side of the gateway, insert a Mini SIM card issued by a service provider into the card slot on the side of the gateway.



Mobile Broadband

If you intend to use a cellular connection you will need to have a **Mini SIM card** issued by a service provider and attach the **two antennas**.

INSERTING
YOUR SIM CARD

INSERTING YOUR SIM CARD

Insert the SIM card into the SIM card slot on the side of the gateway in the orientation shown in the following diagram:

Note - Your carrier may have inserted the SIM card prior to shipping.

Figure 1 - Ethernet WAN connection summary

If you intend to use the SIM card for a mobile cellular connection, you will also have to fit the two antennas.

Connect to internet service

There are two ways to connect your gateway to the Internet service:

Ethernet WAN

This is the most common access type in Australia and New Zealand and covers fixed line technologies such as nbn™ FTTP, HFC, FTTC as well as UFB Fixed Wireless and Sky Muster™ satellite services.

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 access network provider.

How to connect for Ethernet WAN connections

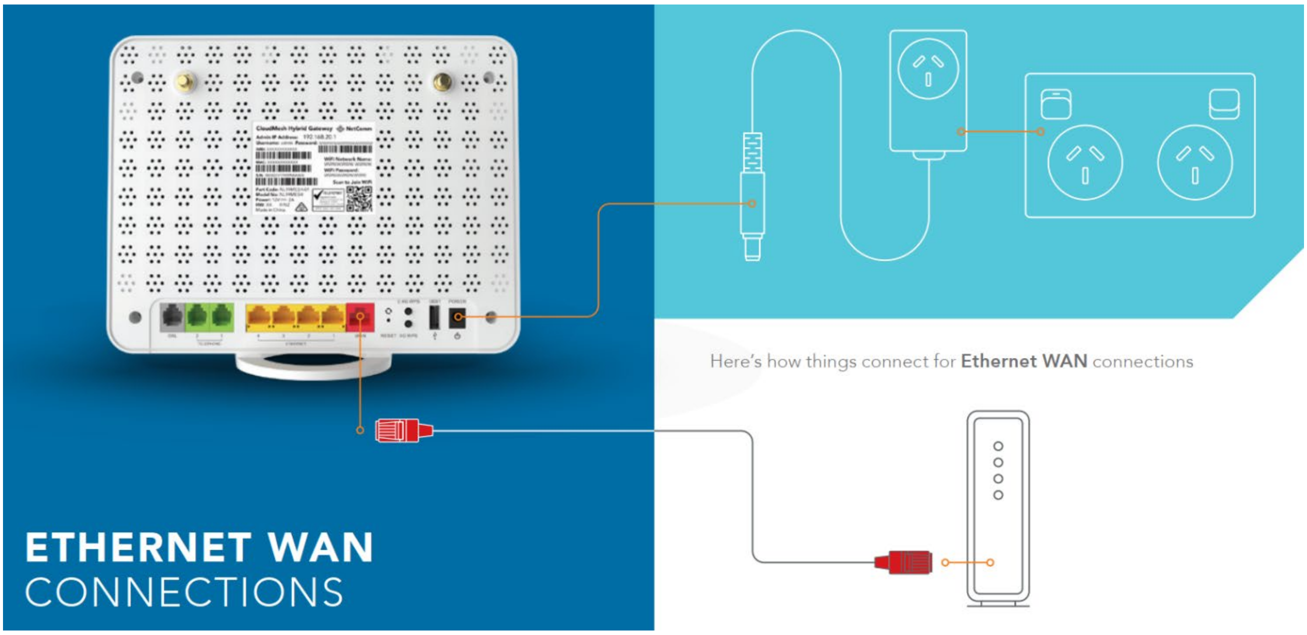


Figure 2 - Ethernet WAN connection summary

ADSL or VDSL

These access types are provided by nbn™ FTTB, FTTN or ADSL/VDSL over a traditional telephone line.

This connection uses the grey DSL port on the back of the gateway.

How to connect for ADSL/VDSL connections

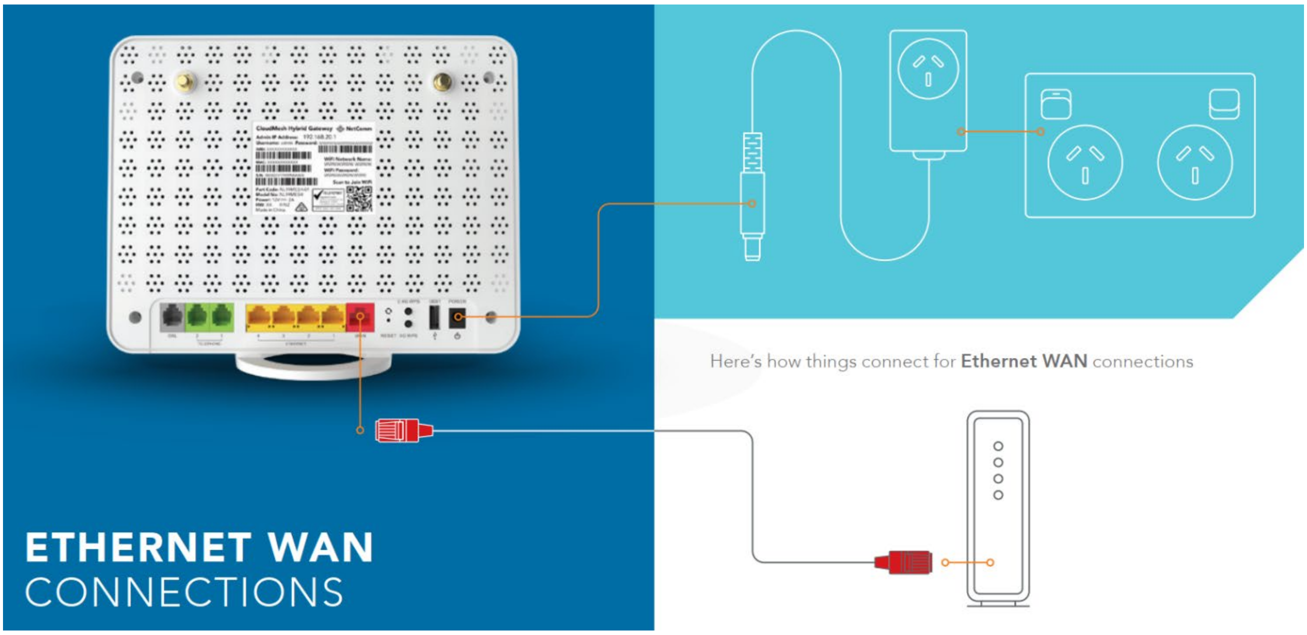


Figure 3 - ADSL/VDSL connection summary

Configure your gateway

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

- Internet service type (ADSL/VDSL/Ethernet WAN)
- Connection type (PPPoE/PPPoA/Dynamic IP/Static IP)
- 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 side of the CloudMesh Gateway to turn it on. Wait a few minutes for it to complete starting up.

2 Open a web browser and type **192.168.20.1** into the address bar, then press **Enter**.

3 At the login screen, type **admin** into the Username field. In the Password field, type the unique password printed on the label on the bottom of the gateway, then click the **Login >** button

4 Follow the Basic Setup to complete the configuration.

Connect with 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.

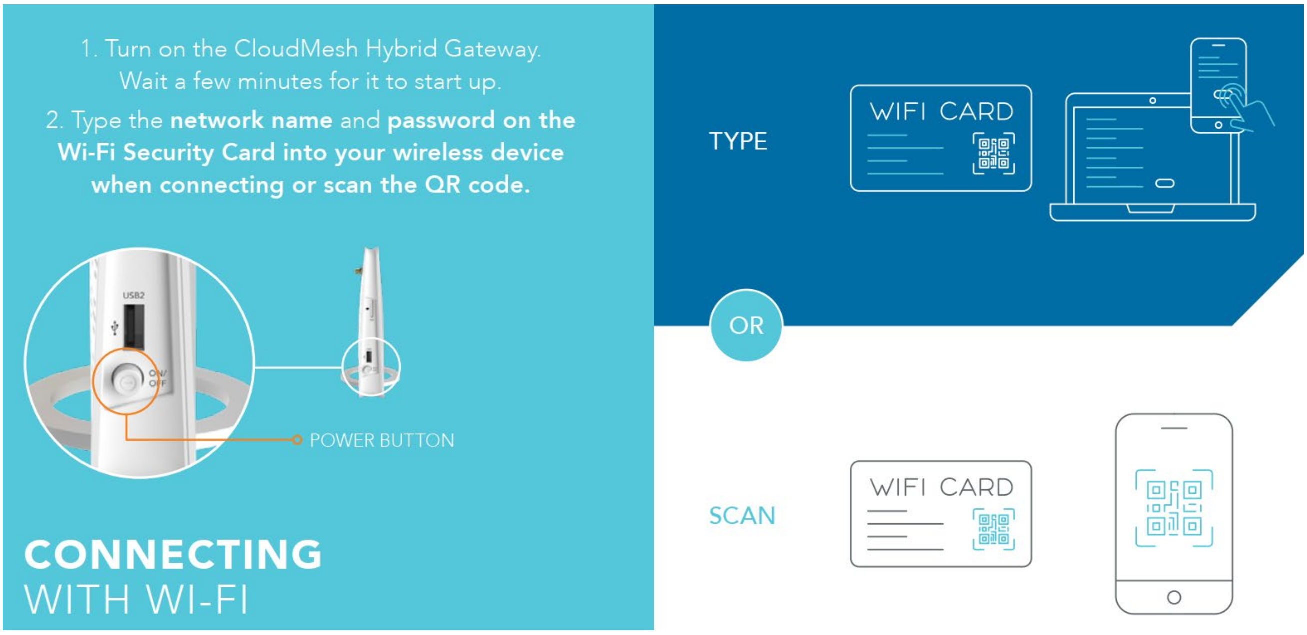

1. Turn on the CloudMesh Hybrid Gateway.
Wait a few minutes for it to start up.
2. Type the **network name** and **password on the Wi-Fi Security Card into your wireless device when connecting or scan the QR code.**
USB2
ON/OFF
POWER BUTTON
CONNECTING
WITH WI-FI
TYPE
WIFI CARD
OR
SCAN
WIFI CARD

Figure 4 - Connect with Wi-Fi

Connect a telephone

Connect a regular telephone handset to the CloudMesh 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.

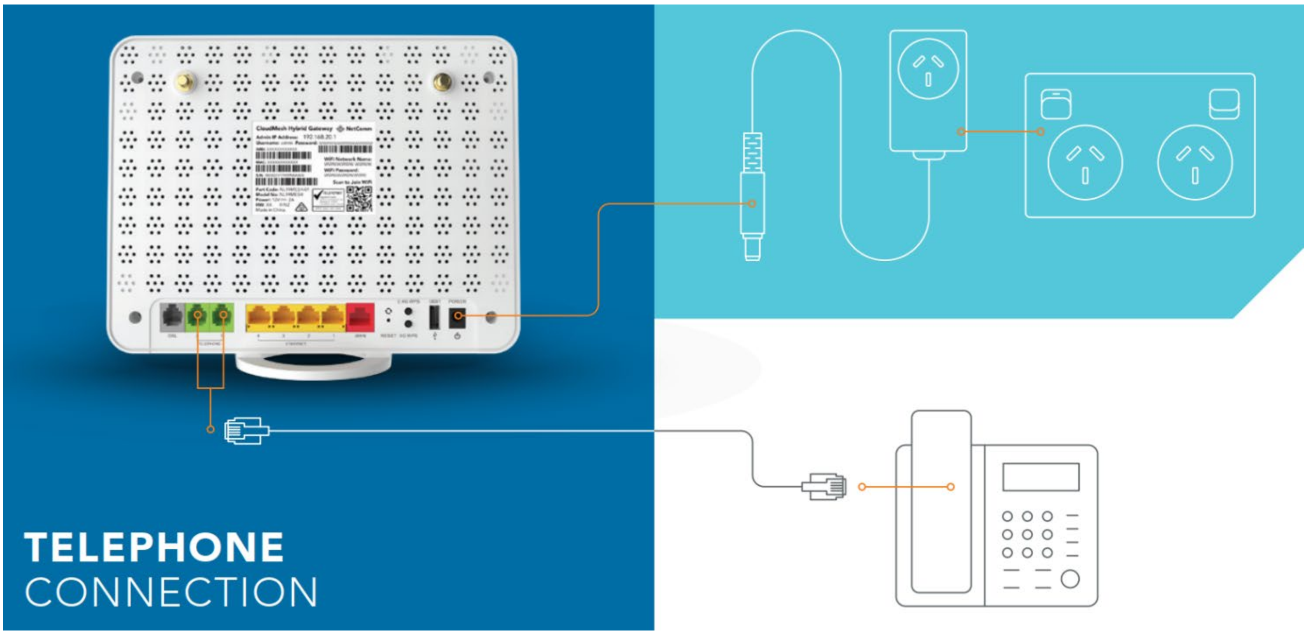


Figure 5 - Telephone connection diagram

CloudMesh app

Download the CloudMesh app

Finding the best place for your CloudMesh Satellite is easy using the CloudMesh App.

- Satellite placement assistance
- WiFi Analytics
- WiFi Troubleshooting
- Setup does not require the App

Get it on the **App Store** or **Google Play**.

Interfaces

The CloudMesh Gateway is designed to be placed on a desktop with the front facing outward.

All of the cables exit from the rear for easy organization and the SIM slot, USB2 port and power ON/OFF button are on the side.

Front view

The LED display visible on the front of the CloudMesh Gateway provides you with information about network activity and the device status.

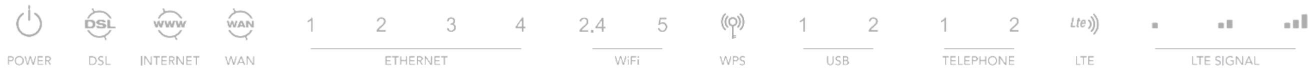


Figure 6 - LED icons

LED indicators

The following table contains an explanation of each of the indicator lights on the front of the CloudMesh Gateway.

Icon and label	Colour	Definition
POWER	Red	The CloudMesh Gateway is powered on and initialising.
	Green	The CloudMesh Gateway is powered on and operating normally.
	Off	The power is off.
DSL	Off	No DSL signal detected.
	Green Blinking	Synching
	Green	DSL synchronized.
INTERNET	Green	The CloudMesh Gateway is connected to an Internet service.
	Green Blinking	Data is being transmitted to or from the Internet. Note that this will only blink for Ethernet WAN connections. Other connection types will show a steady green status.
	Off	The CloudMesh Gateway is not connected to the Internet.
WAN	Green	A device is connected to the Ethernet WAN port.
	Green Blinking	Data is being transmitted to or from the WAN.
	Off	No device is connected to the Ethernet WAN port.

Icon and label	Colour	Definition
1 2 3 4 ETHERNET	Green	A device is connected to the Ethernet LAN port.
	Green Blinking	Data is being transmitted to or from the Ethernet LAN port.
	Off	No device is connected to the Ethernet LAN port.
2.4 5 WiFi	Green	Wi-Fi is enabled.
	Green Blinking	Data is being transmitted to or from the Wireless interface.
	Off	Wi-Fi is disabled.
	Green	Wi-Fi is enabled.
	Green Blinking	Data is being transmitted to or from the Wireless interface.
	Off	Wi-Fi is disabled.
((ᵒ)) WPS	Blue	WPS (Wi-Fi Protected Setup) is enabled.
	Blue Blinking	WPS pairing is triggered.
	Off	WPS is disabled.
1 2 USB	Green	A USB device is connected.
	Green Blinking	Data is being transmitted through the USB interface.
	Off	No USB device is connected to the USB interface.
1 2 TELEPHONE	Green	A handset is registered.
	Green Blinking	Incoming call or the handset is in use.
	Off	No handset registered
Lte)) LTE	Green	Indicates whether the LTE is registered to the Network: • Off = not registered • On = registered
▪ ▪▪ ▪▪▮ LTE SIGNAL	Green	Indicates the strength of signal for your LTE service.

Table 1 - LED icon descriptions

Rear view

The following interfaces are available on the rear panel of the CloudMesh Gateway:

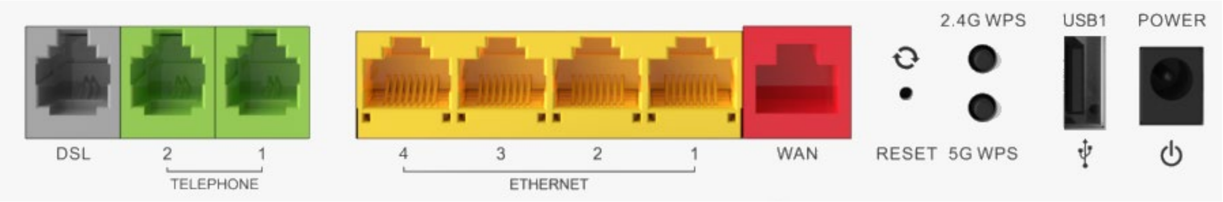


Figure 7 – CloudMesh Gateway rear view

Interface	Description
DSL	Use the provided telephone cable to connect the router to the telephone line operating your xDSL service.
TELEPHONE 1 and 2	Connect a regular analogue telephone handset here for use with a VoIP service.
ETHERNET 1–4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
WAN	Gigabit capable WAN port for connection to a WAN network. Connect to your Network Termination Device (NTD) for high-speed internet access.
RESET button	Reset unit to Default by holding the Reset button down for 10 seconds when unit is powered on.
2.4G / 5G WPS buttons	This is a multifunctional button that will trigger the Wi-Fi Protected Setup (WPS) function when held down for approximately three (3) seconds.
USB1	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the CloudMesh Gateway.
POWER supply jack	Connection point for the included power adapter. Connect the power supply here.

Table 2 – Interface descriptions

Side view

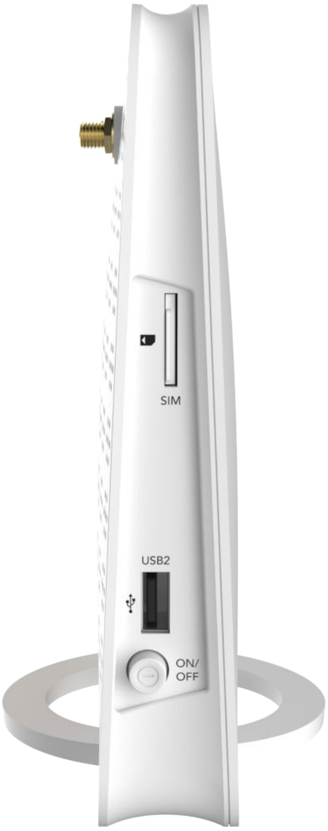


Figure 8 - Side view

Interface	Description
SIM card slot	If you want Wi-Fi connectivity or fall-back capability you must have a Mini SIM card issued by a service provider. Install the Mini SIM is this slot.
USB2	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the CloudMesh Gateway.
ON/OFF button	Toggles the power on and off.

Table 3 - Side buttons

Safety and product care

Your router 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 router. There are no user-serviceable parts.
- Do not allow the router 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 CloudMesh Gateway

The wireless connection between your CloudMesh 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 CloudMesh 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 CloudMesh 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.

Try not to place the CloudMesh Gateway near a cordless telephone that operates at the same radio frequency as the CloudMesh Gateway (2.4GHz/5GHz).

Avoid obstacles and interference

Avoid placing your CloudMesh Gateway near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- 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 CloudMesh Gateway).

Configure the CloudMesh Gateway

Configure the CloudMesh Gateway via its web interface which you can access via a browser.

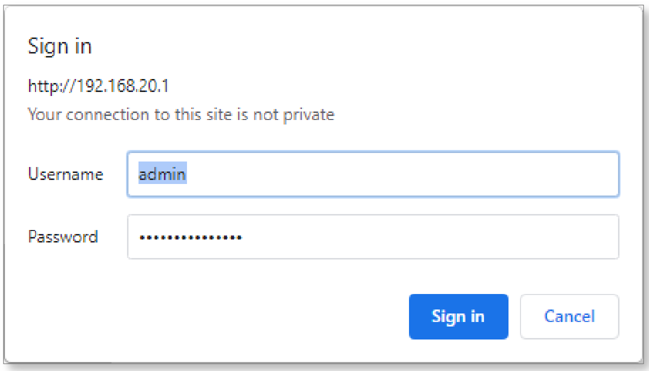
1 Push the power button on the side of the CloudMesh Gateway to turn it on. Wait a few minutes for it to complete starting up.

2 Open a web browser and type 192.168.20.1 into the address bar, then press Enter.

3 At the Sign in dialog, type **admin** into the Username field.

In the Password field, type the unique password printed on the label on the back of the gateway, then click the Sign in button.

Note – If you have changed the password, enter it into the Password field instead.



Sign in

http://192.168.20.1

Your connection to this site is not private

Username: admin

Password: ••••••••••••••••

Figure 9 – Log in dialog

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.

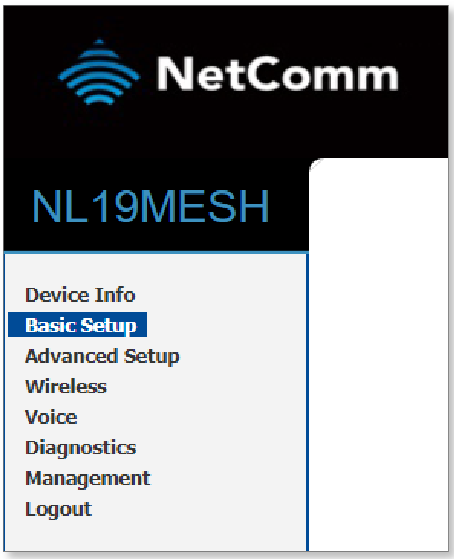


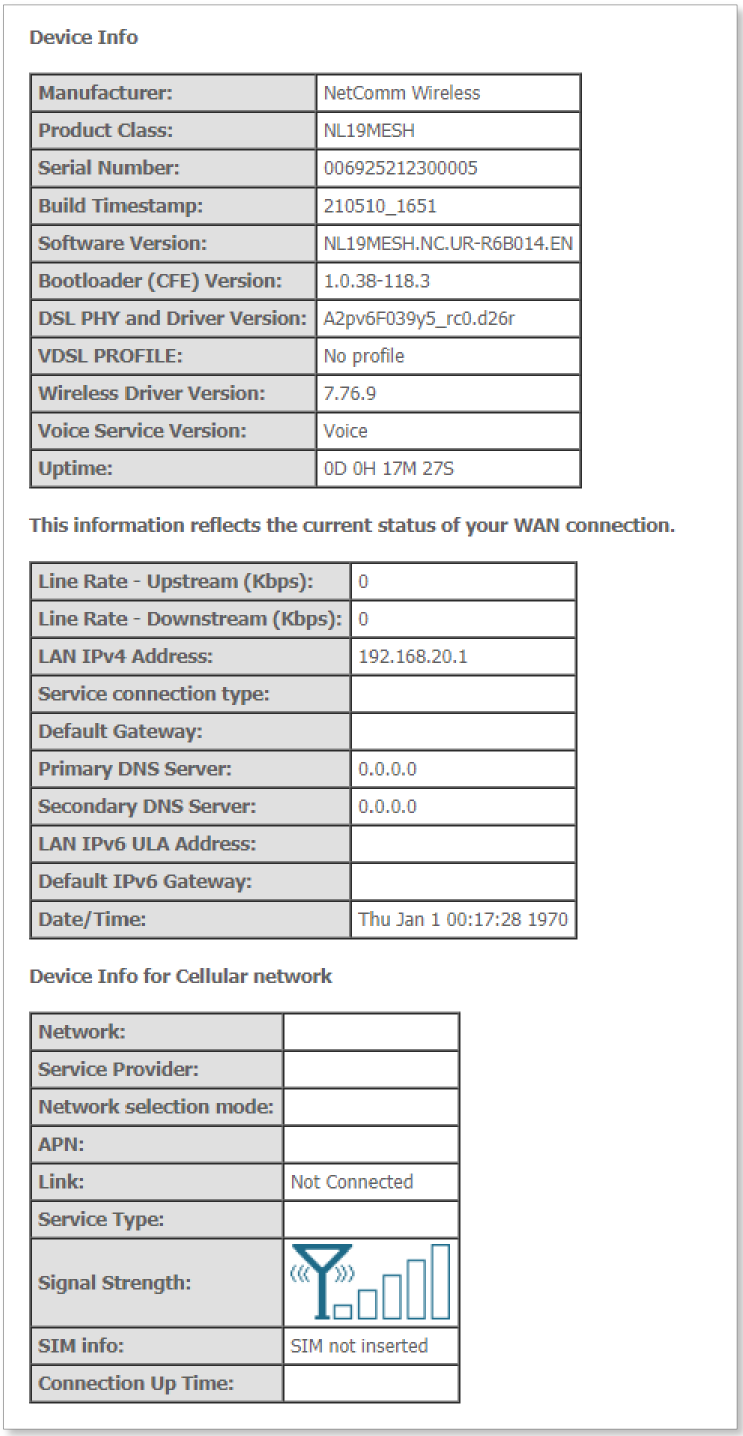
Figure 10 - Basic Setup menu item

Go to the Basic Setup section of this document for a description of the steps in the configuration wizard.

Device Info

The Device Info 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 the configuration of your WAN connection and cellular network status.



Device Info

Manufacturer:	NetComm Wireless
Product Class:	NL19MESH
Serial Number:	006925212300005
Build Timestamp:	210510_1651
Software Version:	NL19MESH.NC.UR-R6B014.EN
Bootloader (CFE) Version:	1.0.38-118.3
DSL PHY and Driver Version:	A2pv6F039y5_rc0.d26r
VDSL PROFILE:	No profile
Wireless Driver Version:	7.76.9
Voice Service Version:	Voice
Uptime:	0D 0H 17M 27S

This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.20.1
Service connection type:	
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 ULA Address:	
Default IPv6 Gateway:	
Date/Time:	Thu Jan 1 00:17:28 1970

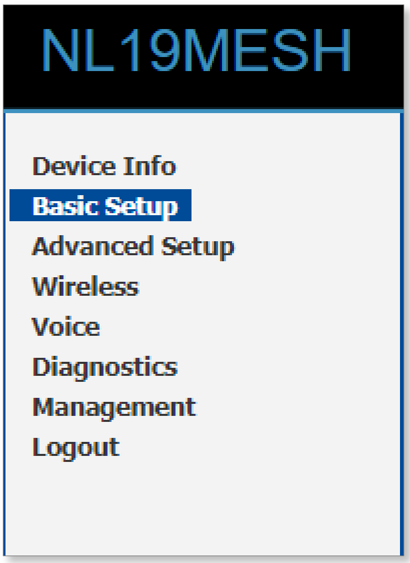
Device Info for Cellular network

Network:	
Service Provider:	
Network selection mode:	
APN:	
Link:	Not Connected
Service Type:	
Signal Strength:	📶
SIM info:	SIM not inserted
Connection Up Time:	

Figure 11 - Device Info page

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.

Basic Setup


NL19MESH

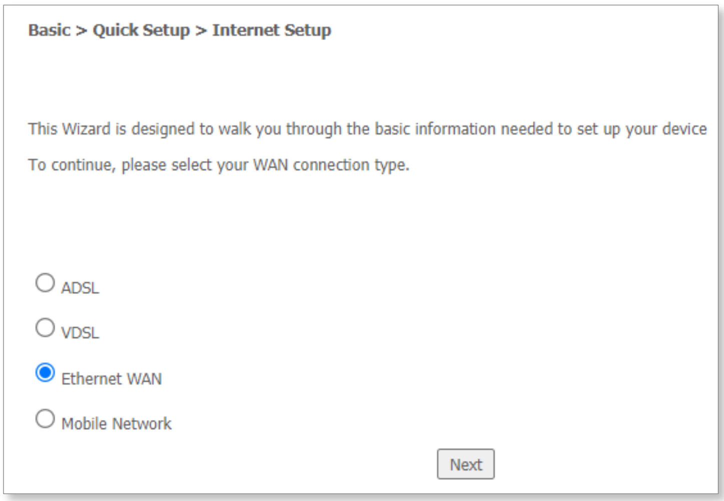
The Basic Setup configuration wizard guides you through setting up your Internet connection.

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.

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.

ADSL connections

1 Select ADSL and click the Next button.


Basic > Quick Setup > Internet Setup

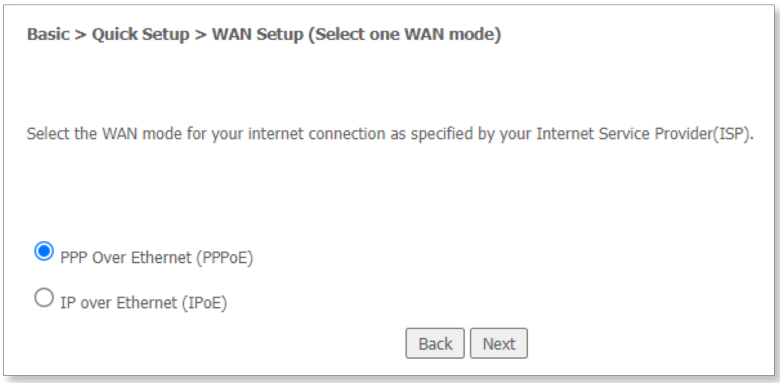
This Wizard is designed to walk you through the basic information needed to set up your device

To continue, please select your WAN connection type.

○ ADSL
○ VDSL
● Ethernet WAN
○ Mobile Network

Figure 12 –Select ADSL as WAN connection type

2 Select either the PPP over Ethernet (PPPoE), IP over Ethernet (IPoE), Bridging or PPP Over ATM (PPPoA) for your Internet connection as specified by your Internet Service Provider (ISP)



Basic > Quick Setup > WAN Setup (Select one WAN mode)

Select the WAN mode for your internet connection as specified by your Internet Service Provider(ISP).

● PPP Over Ethernet (PPPoE)

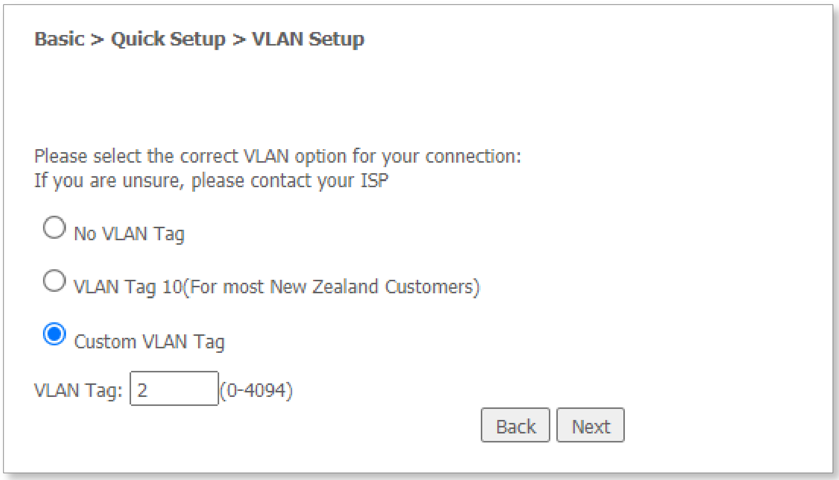
○ IP over Ethernet (IPoE)

Figure 13 – Select WAN mode

Click the Next button.

PPPoE (PPP over Ethernet)

a Enter the VPI and VCI settings.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

○ No VLAN Tag

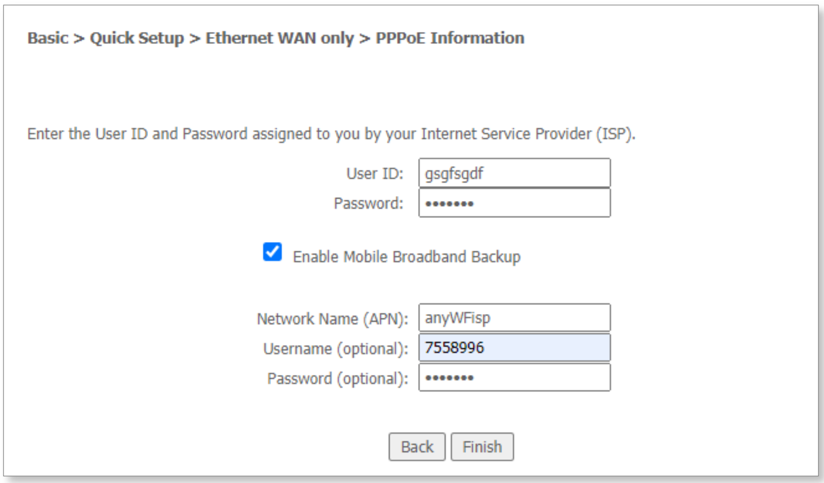
○ VLAN Tag 10(For most New Zealand Customers)

● Custom VLAN Tag

VLAN Tag: 2 (0-4094)

Figure 14 - ADSL VPI/VCI settings

b In the User ID and Password fields, enter the PPPoE authentication username and password assigned to you by your Internet Service Provider (ISP).



Basic > Quick Setup > Ethernet WAN only > PPPoE Information

Enter the User ID and Password assigned to you by your Internet Service Provider (ISP).

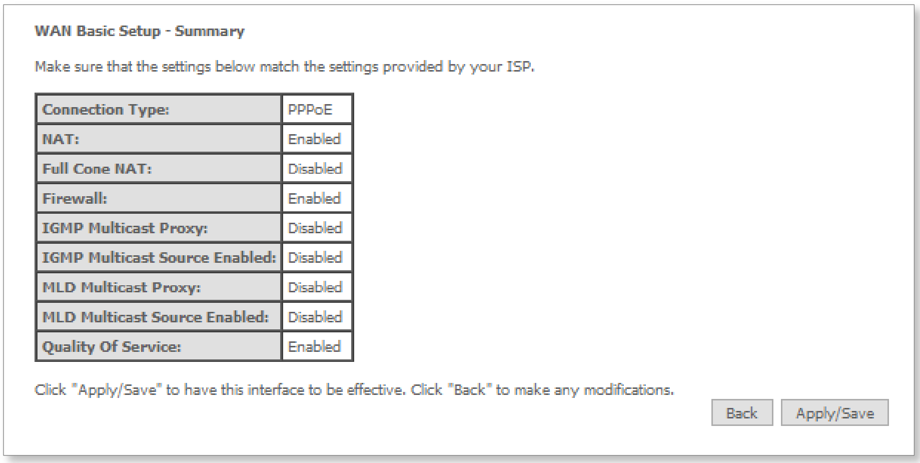
User ID:	gsgfsgdf
Password:	•••••••

☑ Enable Mobile Broadband Backup

Network Name (APN):	anyWFisp
Username (optional):	7558996
Password (optional):	•••••••

Figure 15 - PPPoE User ID and password

c A summary of the settings is displayed. Click the Apply/Save button to complete the wizard.



WAN Basic Setup - Summary

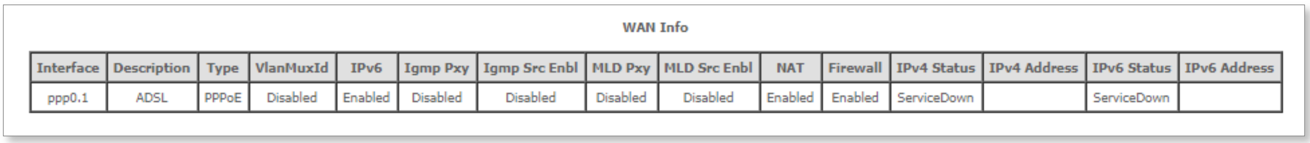
Make sure that the settings below match the settings provided by your ISP.

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

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

Figure 16 - ADSL WAN Setup Summary

A WAN information table is displayed.



WAN Info

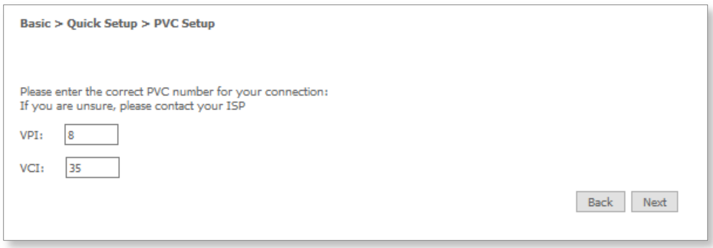
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ppp0.1	ADSL	PPPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

Figure 17 – PPPoE WAN Info table

The setup is complete.

IPoE (IP over Ethernet)

a Enter the **VPI** and **VCI** settings.



Basic > Quick Setup > PVC Setup

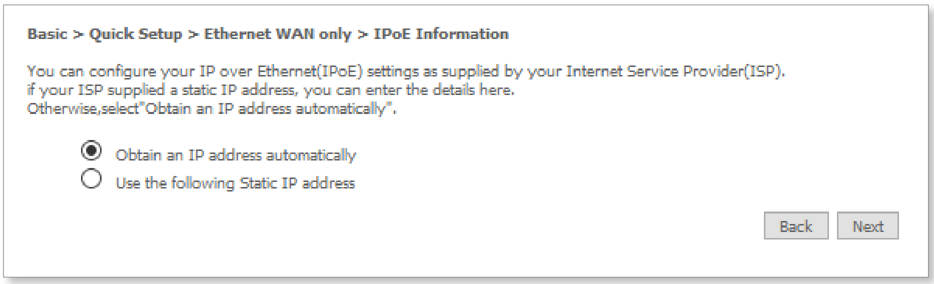
Please enter the correct PVC number for your connection:
If you are unsure, please contact your ISP

VPI: 8

VCI: 35

Figure 18 - ADSL VPI/VCI settings

b Select whether to obtain an **IP address automatically** or **Use the following Static IP address**.



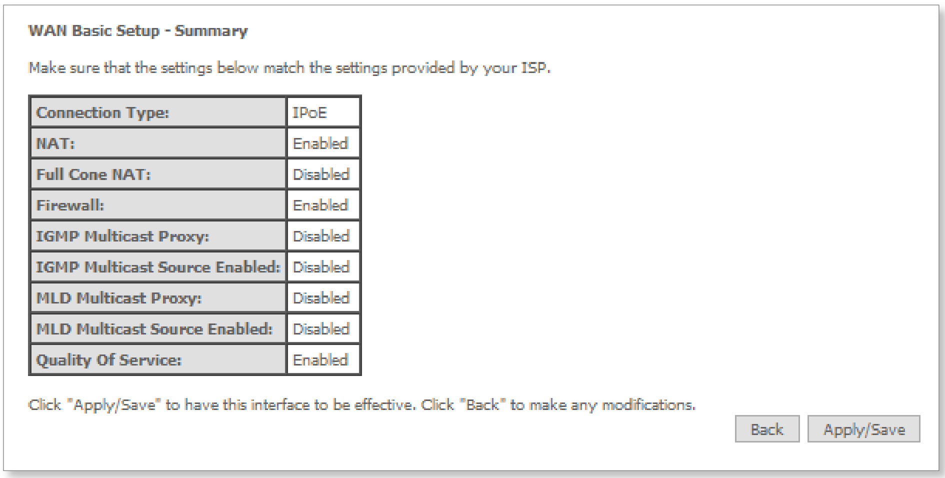
Basic > Quick Setup > Ethernet WAN only > IPoE Information

You can configure your IP over Ethernet(IPoE) settings as supplied by your Internet Service Provider(ISP).
if your ISP supplied a static IP address, you can enter the details here.
Otherwise,select"Obtain an IP address automatically".

● Obtain an IP address automatically
○ Use the following Static IP address

Figure 19 - IPoE information

c A summary of the settings is displayed. Click the **Apply/Save** button to complete the wizard.



WAN Basic Setup - Summary

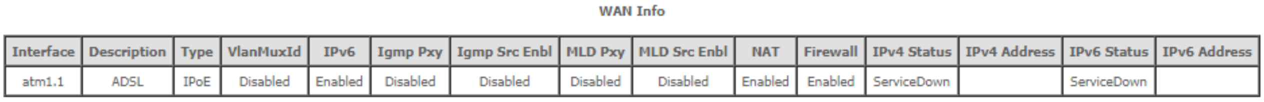
Make sure that the settings below match the settings provided by your ISP.

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

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

Figure 20 - WAN Setup summary

A WAN information table is displayed.



WAN Info

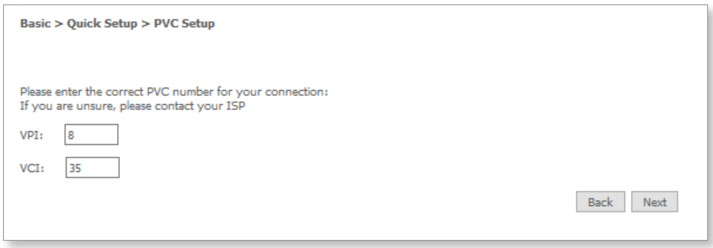
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
atm1.1	ADSL	IPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

The setup is complete.

Figure 21 – IPoE WAN info table

Bridging

a Enter the **VPI** and **VCI** settings.



Basic > Quick Setup > PVC Setup

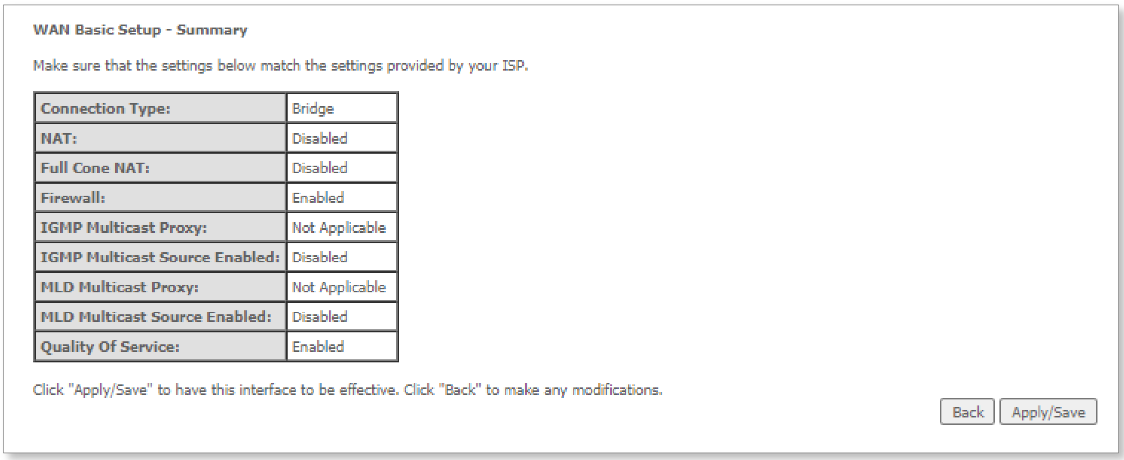
Please enter the correct PVC number for your connection:
If you are unsure, please contact your ISP

VPI: 8

VCI: 35

Figure 22 - ADSL VPI/VCI settings

b A summary of the settings is displayed. Click the **Apply/Save** button to complete the wizard.



WAN Basic Setup - Summary

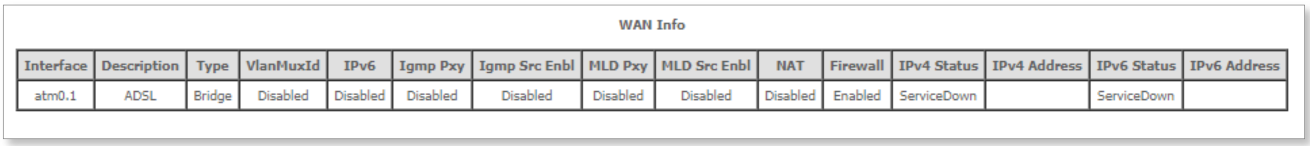
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

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

Figure 23 - WAN Setup summary

A WAN information table is displayed.



WAN Info

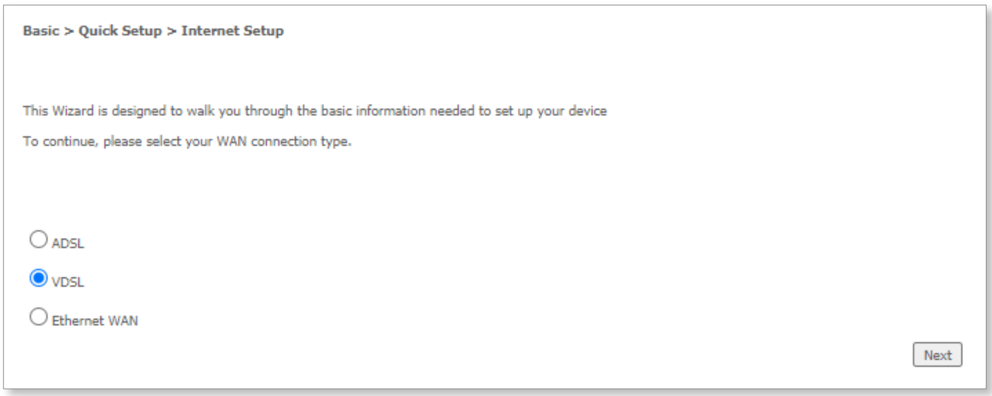
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
atm0.1	ADSL	Bridge	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	ServiceDown		ServiceDown	

Figure 24 - Bridging WAN information table

The setup is complete.

VDSL connections

1 Select **VDSL** and click the **Next** button.



Basic > Quick Setup > Internet Setup

This Wizard is designed to walk you through the basic information needed to set up your device

To continue, please select your WAN connection type.

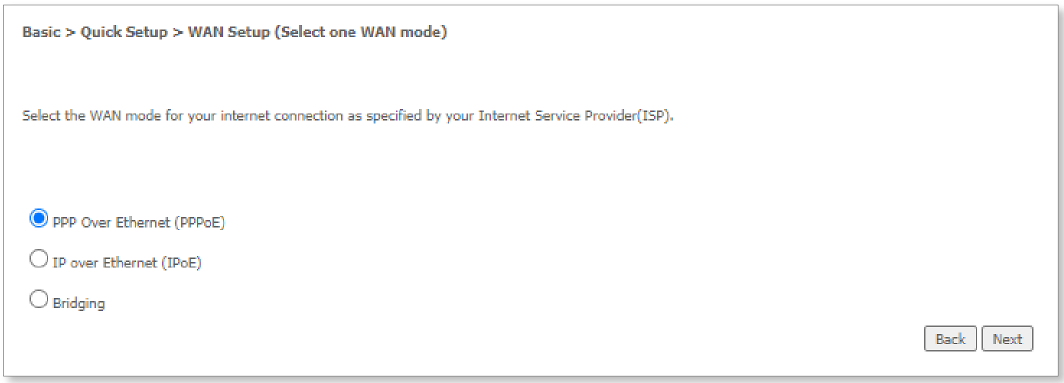
○ ADSL

● VDSL

○ Ethernet WAN

Figure 25 – VDSL Internet setup

2 Select either the **PPP over Ethernet (PPPoE)**, **IP over Ethernet (IPoE)**, or **Bridging** for your Internet connection as specified by your Internet Service Provider (ISP)



Basic > Quick Setup > WAN Setup (Select one WAN mode)

Select the WAN mode for your internet connection as specified by your Internet Service Provider(ISP).

● PPP Over Ethernet (PPPoE)

○ IP over Ethernet (IPoE)

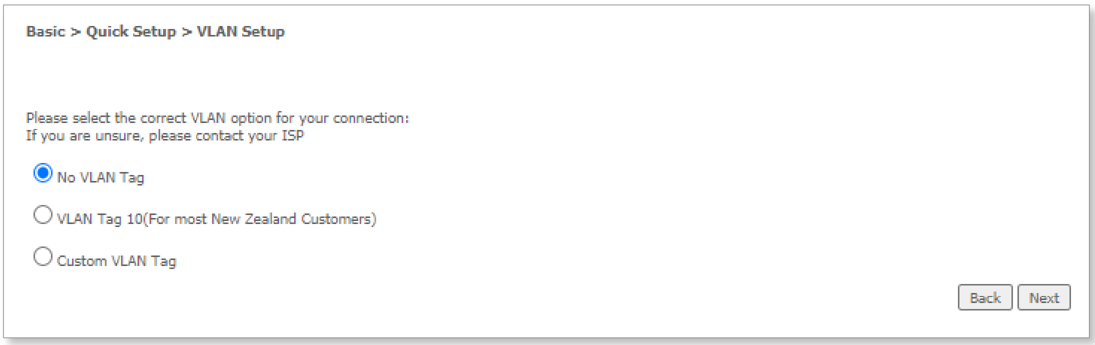
○ Bridging

Figure 26 – Select WAN mode

Click the **Next** button.

PPPoE (PPP over Ethernet)

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for VDSL is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

● No VLAN Tag

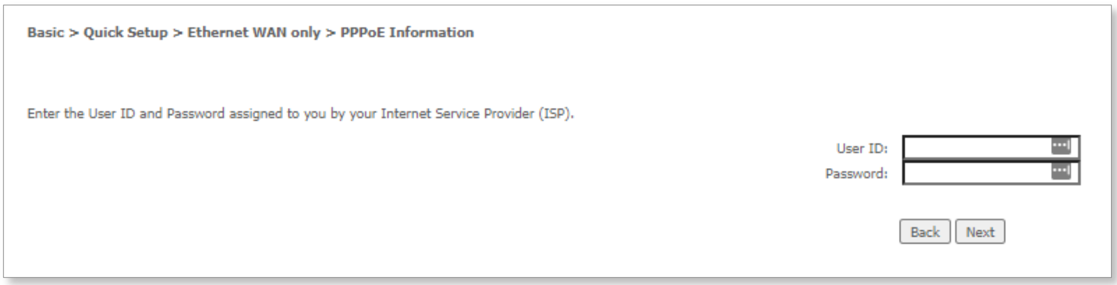
○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 27 – Select VLAN option for VDSL connection

Click the **Next** button.

b Enter the **User ID** and **Password** for the connection.



Basic > Quick Setup > Ethernet WAN only > PPPoE Information

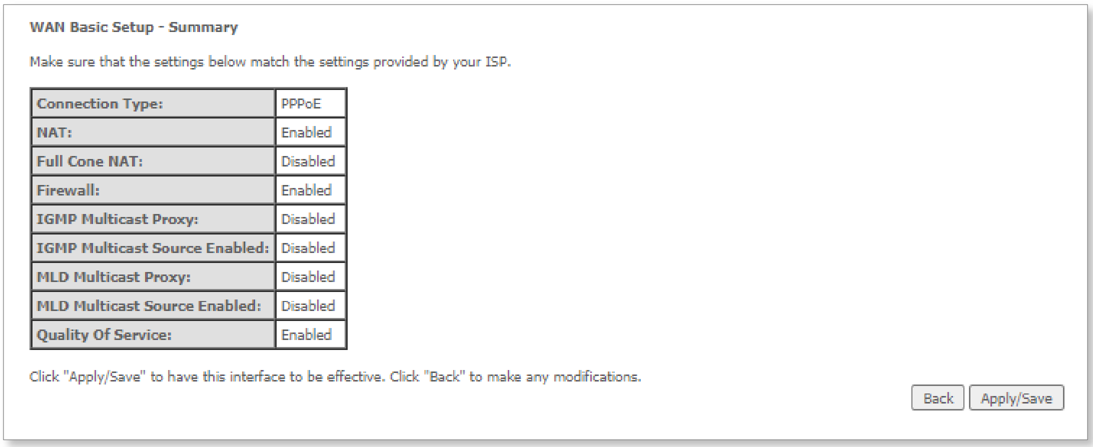
Enter the User ID and Password assigned to you by your Internet Service Provider (ISP).

User ID:

Password:

Figure 28 - PPPoE User ID and Password

c Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

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

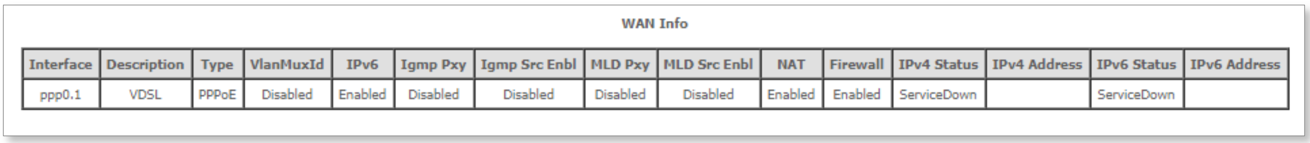
Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

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

Figure 29 - WAN setup summary

d Click the **Apply/Save** button when you have entered the required details.

A WAN information table is displayed.



WAN Info

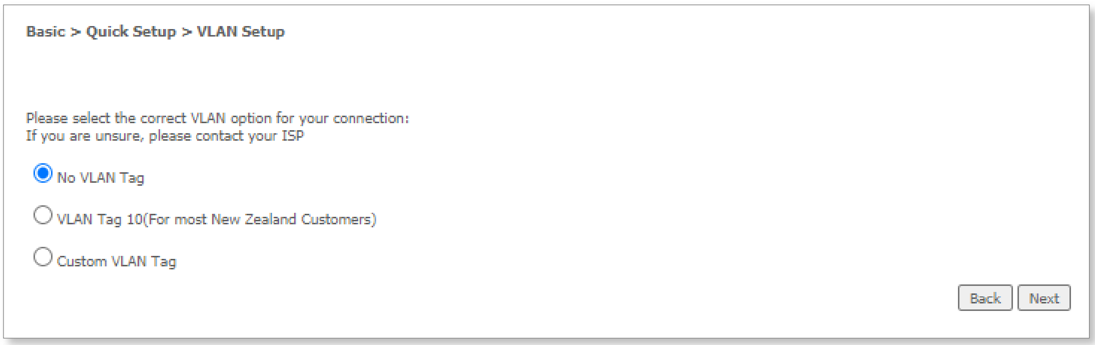
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ppp0.1	VDSL	PPPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

Figure 30 - WAN info table

The setup is complete.

IPoE (IP over Ethernet)

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for VDSL is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

● No VLAN Tag

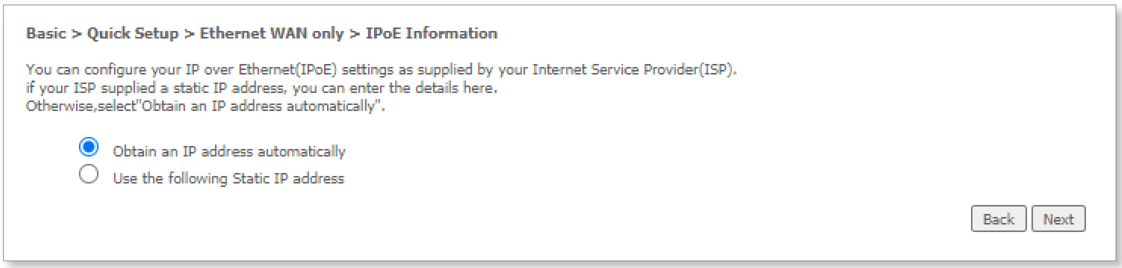
○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 31 – Select VLAN option for VDSL connection

Click the **Next** button.

b Select whether to obtain an **IP address automatically** or **Use the following Static IP address**.



Basic > Quick Setup > Ethernet WAN only > IPoE Information

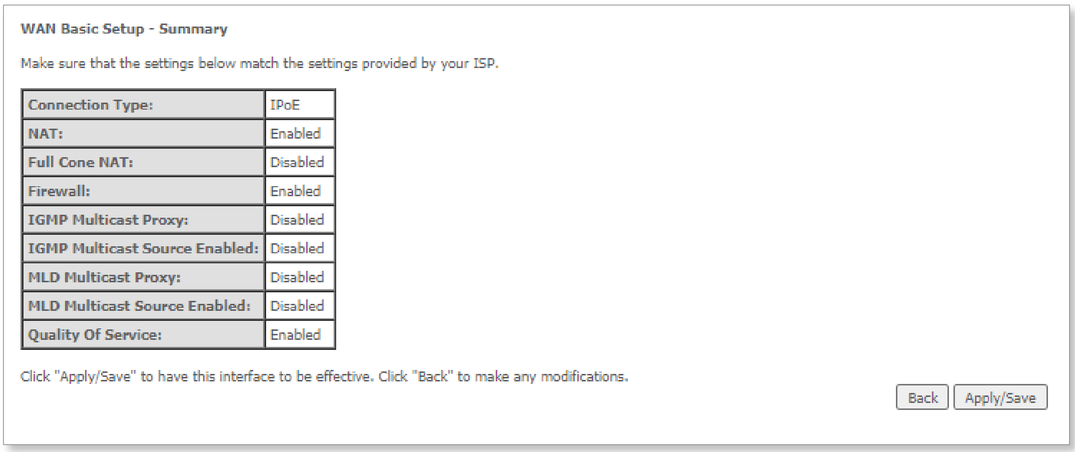
You can configure your IP over Ethernet(IPoE) settings as supplied by your Internet Service Provider(ISP).
if your ISP supplied a static IP address, you can enter the details here.
Otherwise,select"Obtain an IP address automatically".

● Obtain an IP address automatically

○ Use the following Static IP address

Figure 32 – IPoE information

c Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

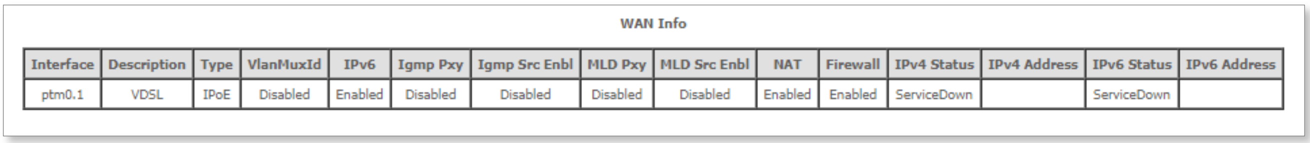
Make sure that the settings below match the settings provided by your ISP.

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

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

Figure 33 - WAN setup summary

d Click the **Apply/Save** button when you have entered the required details. A WAN information table is displayed.



WAN Info

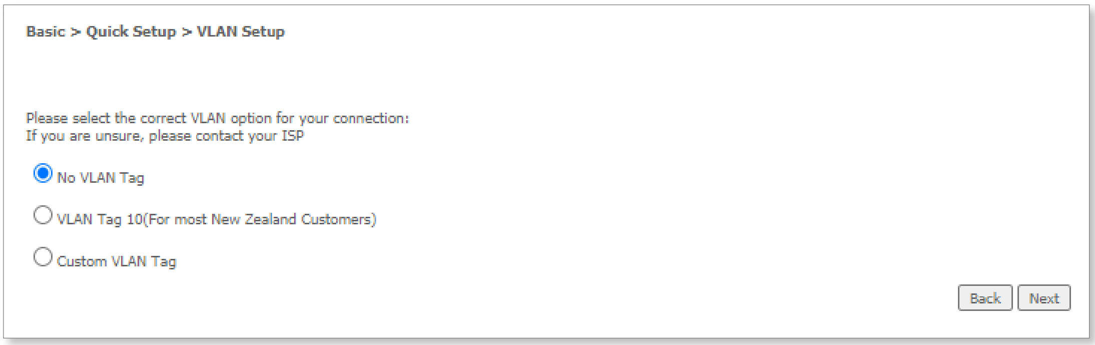
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ptm0.1	VDSL	IPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

Figure 34 - WAN info table

The setup is complete.

Bridging

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for VDSL is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

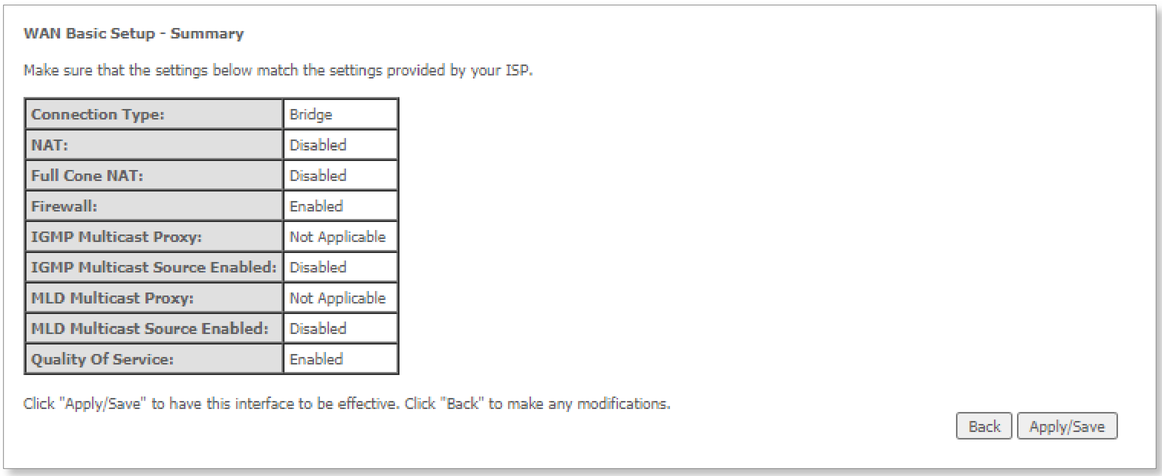
● No VLAN Tag

○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 35 – Select VLAN option for VDSL connection

b Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

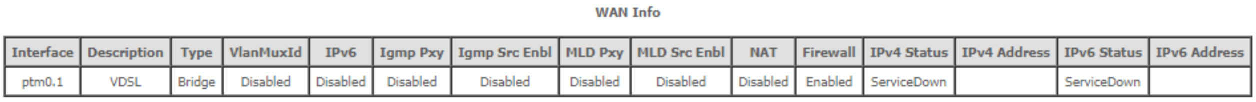
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

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

Figure 36 - WAN setup summary

c Click the **Apply/Save** button when you have entered the required details. A WAN information table is displayed.



WAN Info

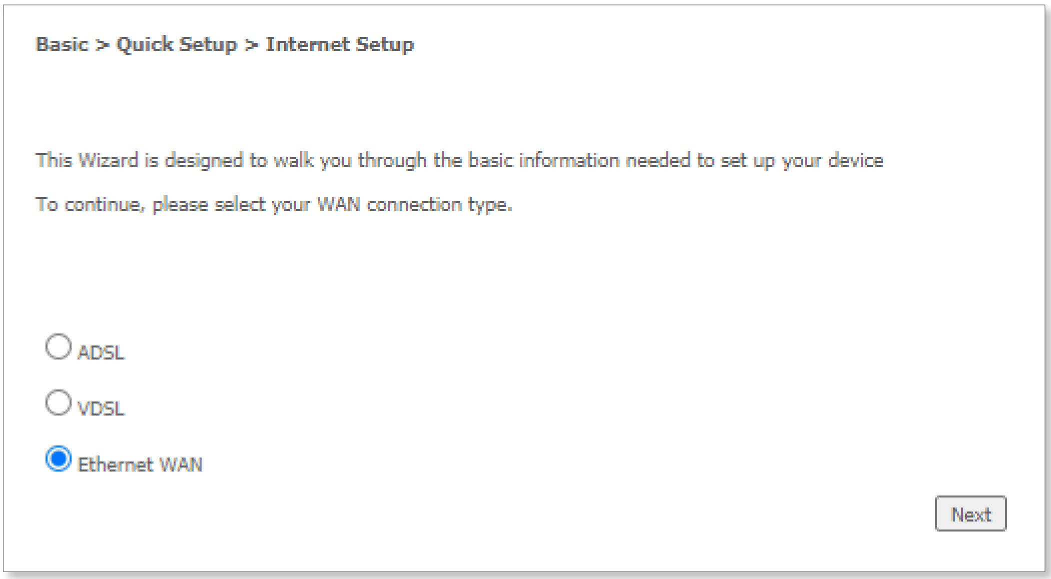
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ptm0.1	VDSL	Bridge	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	ServiceDown		ServiceDown	

Figure 37 - WAN info table

The setup is complete.

Ethernet WAN connections

1 Select **Ethernet WAN** then click the **Next** button.



Basic > Quick Setup > Internet Setup

This Wizard is designed to walk you through the basic information needed to set up your device

To continue, please select your WAN connection type.

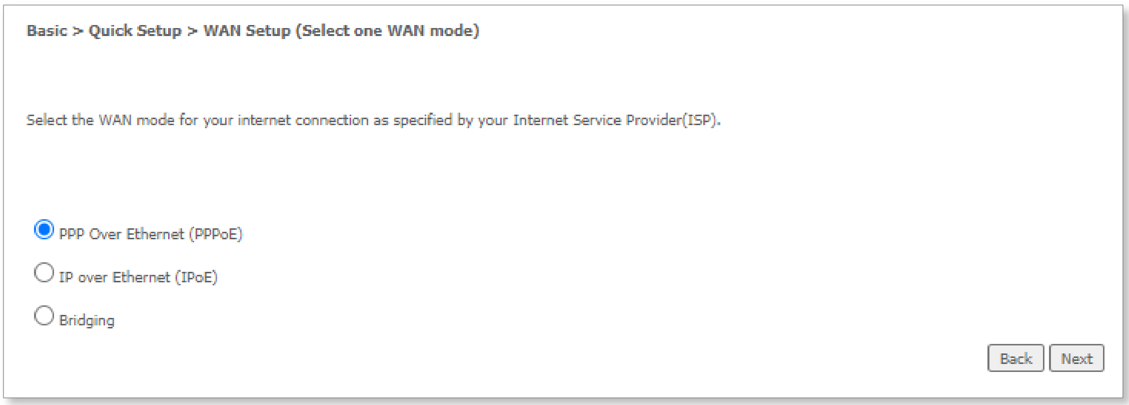
○ ADSL

○ VDSL

● Ethernet WAN

Figure 38 –Select Ethernet WAN as WAN connection type

2 Select the WAN mode for your Internet connection as specified by your Internet Service Provider (ISP).



Basic > Quick Setup > WAN Setup (Select one WAN mode)

Select the WAN mode for your internet connection as specified by your Internet Service Provider(ISP).

● PPP Over Ethernet (PPPoE)

○ IP over Ethernet (IPoE)

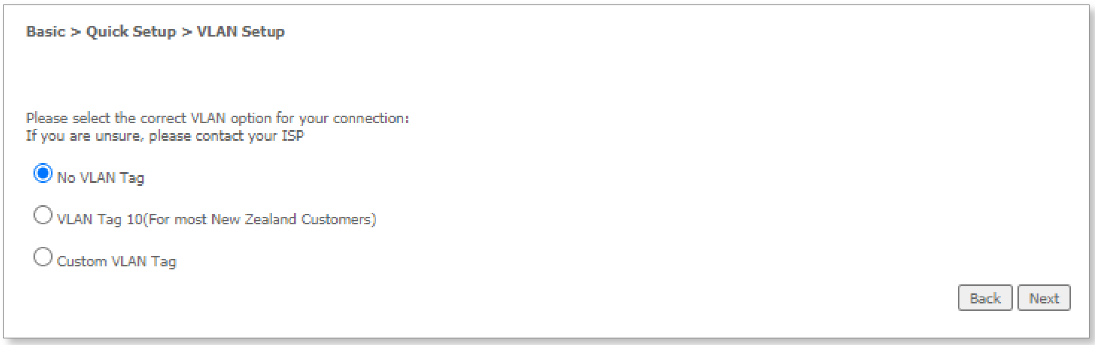
○ Bridging

Figure 39 – Select WAN mode for Ethernet WAN connection

Click the **Next** button.

PPPoE

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for most ISPs fibre connections is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

● No VLAN Tag

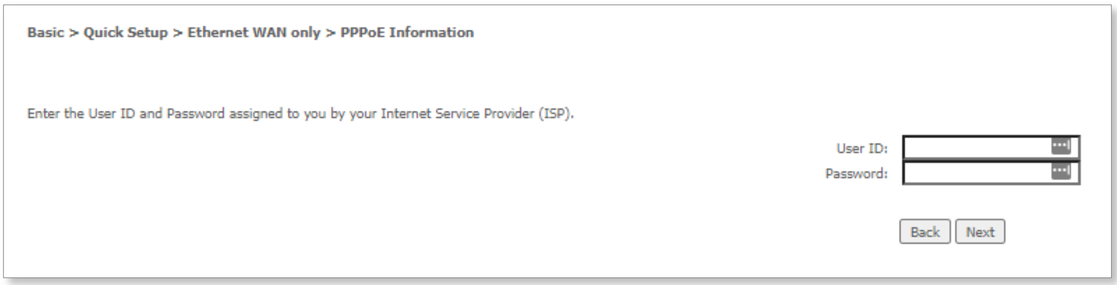
○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 40 – Select VLAN option for VDSL connection

Click the **Next** button.

b Enter the **User ID** and **Password** for the connection.



Basic > Quick Setup > Ethernet WAN only > PPPoE Information

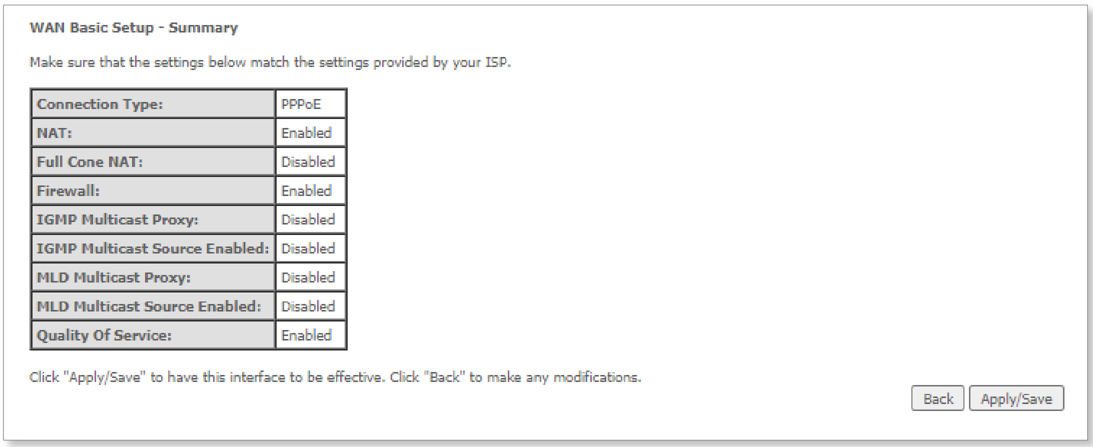
Enter the User ID and Password assigned to you by your Internet Service Provider (ISP).

User ID:

Password:

Figure 41 - PPPoE User ID and Password

c Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

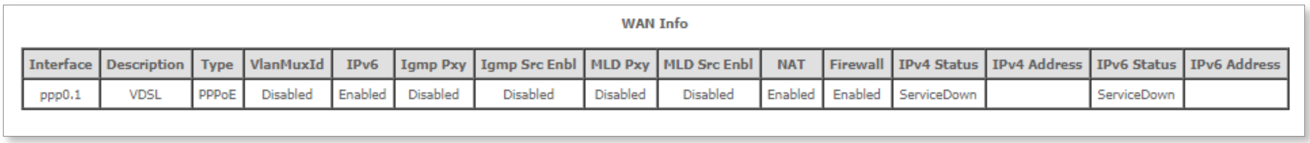
Make sure that the settings below match the settings provided by your ISP.

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

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

Figure 42 - WAN setup summary

d Click the **Apply/Save** button when you have entered the required details. A WAN information table is displayed.



WAN Info

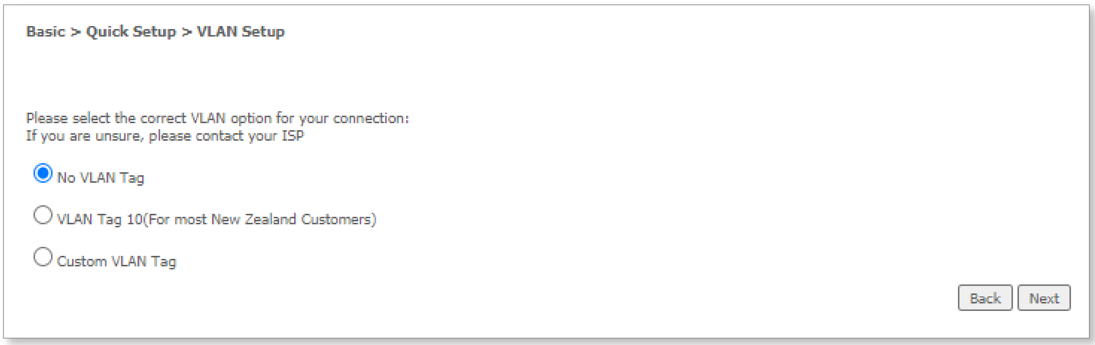
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ppp0.1	VDSL	PPPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

Figure 43 - WAN info table

The setup is complete.

IPoE

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for most ISPs fibre connections is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

● No VLAN Tag

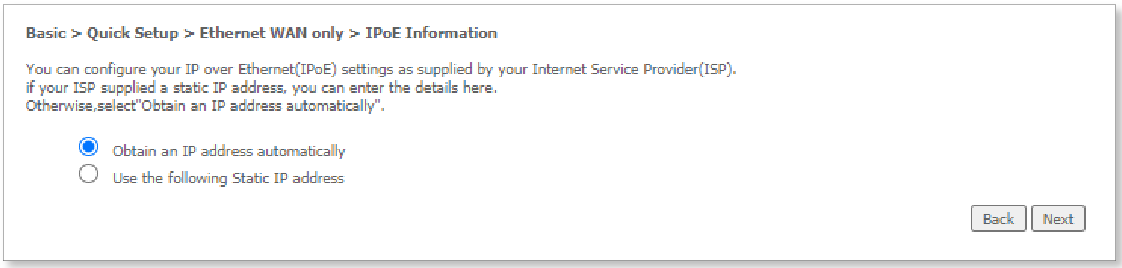
○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 44 – Select VLAN option for VDSL connection

Click the **Next** button.

b Select whether to obtain an **IP address automatically** or **Use the following Static IP address**.



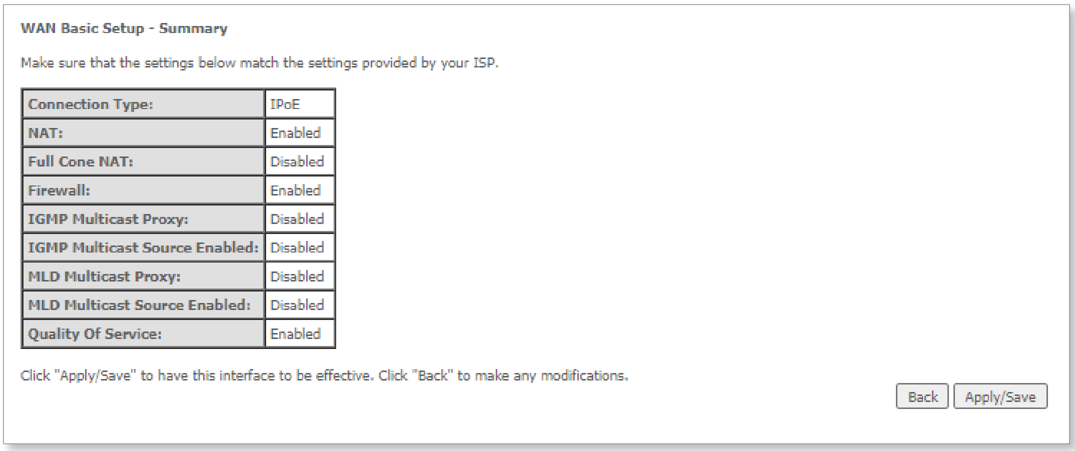
Basic > Quick Setup > Ethernet WAN only > IPoE Information

You can configure your IP over Ethernet(IPoE) settings as supplied by your Internet Service Provider(ISP).
if your ISP supplied a static IP address, you can enter the details here.
Otherwise,select"Obtain an IP address automatically".

● Obtain an IP address automatically
○ Use the following Static IP address

Figure 45 – IPoE information

c Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

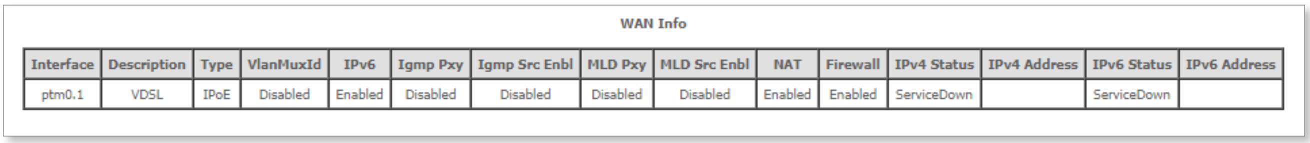
Make sure that the settings below match the settings provided by your ISP.

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

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

Figure 46 - WAN setup summary

d Click the **Apply/Save** button when you have entered the required details. A WAN information table is displayed.



WAN Info

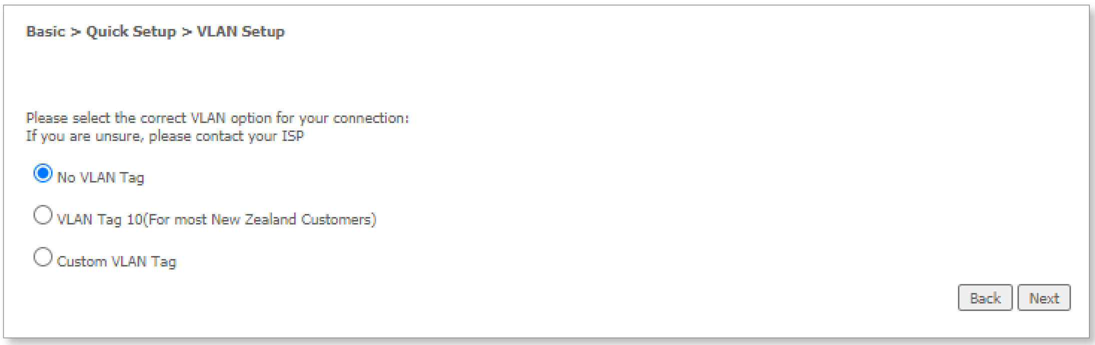
Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ptm0.1	VDSL	IPoE	Disabled	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown	

Figure 47 - WAN info table

The setup is complete.

Bridging

a Select the correct VLAN option for your connection.
For New Zealand customers, the requirement for most ISPs fibre connections is VLAN tag 10.
If you are not sure of the tagging requirement for your connection, please contact your ISP.



Basic > Quick Setup > VLAN Setup

Please select the correct VLAN option for your connection:
If you are unsure, please contact your ISP

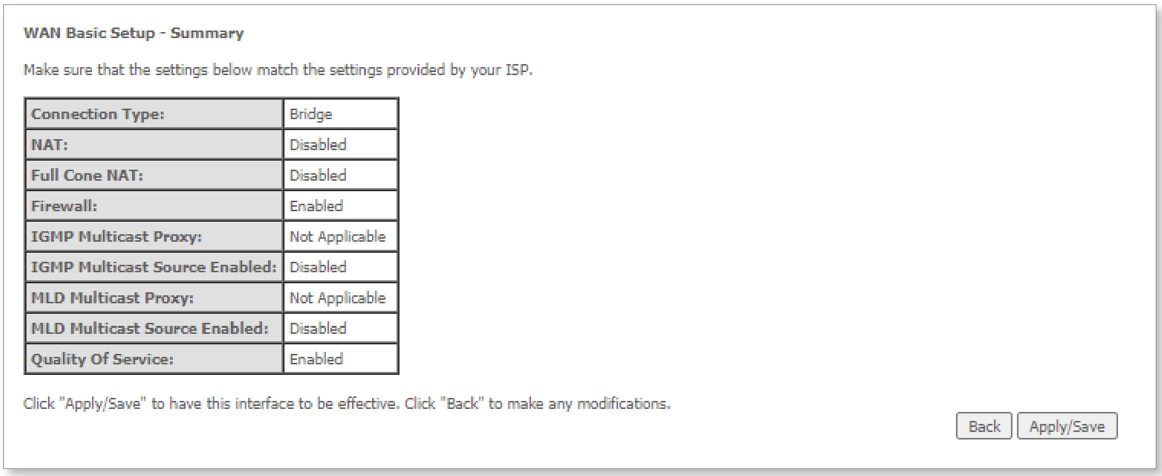
● No VLAN Tag

○ VLAN Tag 10(For most New Zealand Customers)

○ Custom VLAN Tag

Figure 48 – Select VLAN option for VDSL connection

b Click the **Next** button. A summary of the settings is displayed.



WAN Basic Setup - Summary

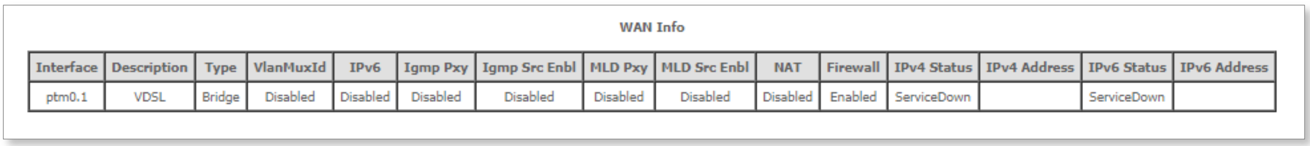
Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Enabled

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

Figure 49 - WAN setup summary

c Click the **Apply/Save** button when you have entered the required details. A WAN information table is displayed.



WAN Info

Interface	Description	Type	VlanMuxId	IPv6	Igmp Pxy	Igmp Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status	IPv6 Address
ptm0.1	VDSL	Bridge	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	ServiceDown		ServiceDown	

Figure 50 - WAN info table

The setup is complete.

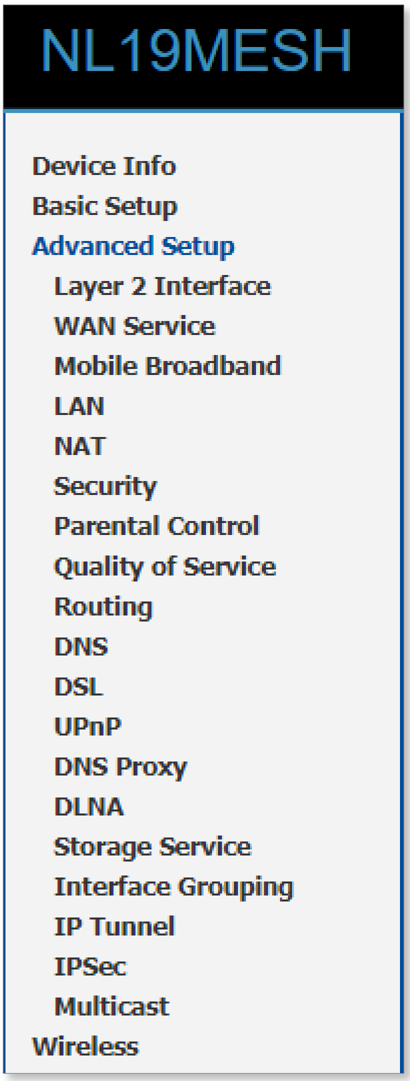
Backup Basic Setup

To make a backup file of your current configuration which you can use to restore those settings, go to **Management> Settings > Backup** to create a backup file.

Go to **Management > Settings > Update** to retrieve the backup file and reapply its settings.

For more information on backing up and restoring your current settings, go to the Management > Settings section of this guide on page **Error! Bookmark not defined.**.

Advanced setup


NL19MESH

The Advanced Setup menu provides a variety of options for configuring the gateway for advanced functions.

These include settings related to the WAN service, Mobile Broadband, 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 under the Advanced Setup menu and we recommend that you do not change many of the settings unless you are sure of the effect that the changes will have, and have a backup of your current working configuration, see next.

Backup settings

To make a backup file of your current configuration which you can use to restore those settings, go to Management> Settings > Backup to create a backup file.

Go to Management > Settings > Update to retrieve the backup file and reapply its settings.

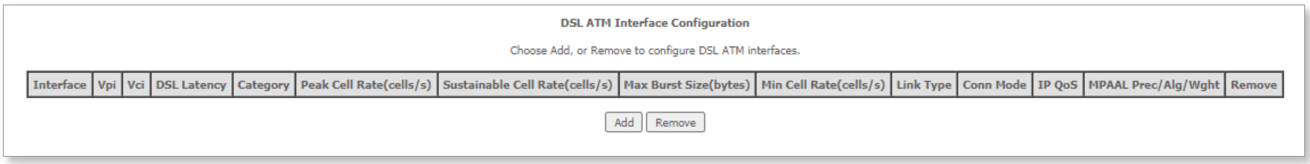
For more information on backing up and restoring your current settings, go to the Management > Settings section of this guide on page Error! Bookmark not defined..

Layer2 Interface

ATM Interface

The **DSL ATM Interface Configuration** page shows the settings of all available DSL ATM interfaces.

The ATM interface is used for ADSL connections.



DSL ATM Interface Configuration

Choose Add, or Remove to configure DSL ATM interfaces.

Interface	Vpi	Vci	DSL Latency	Category	Peak Cell Rate(cells/s)	Sustainable Cell Rate(cells/s)	Max Burst Size(bytes)	Min Cell Rate(cells/s)	Link Type	Conn Mode	IP QoS	MPAAL Prec/Alg/Wght	Remove

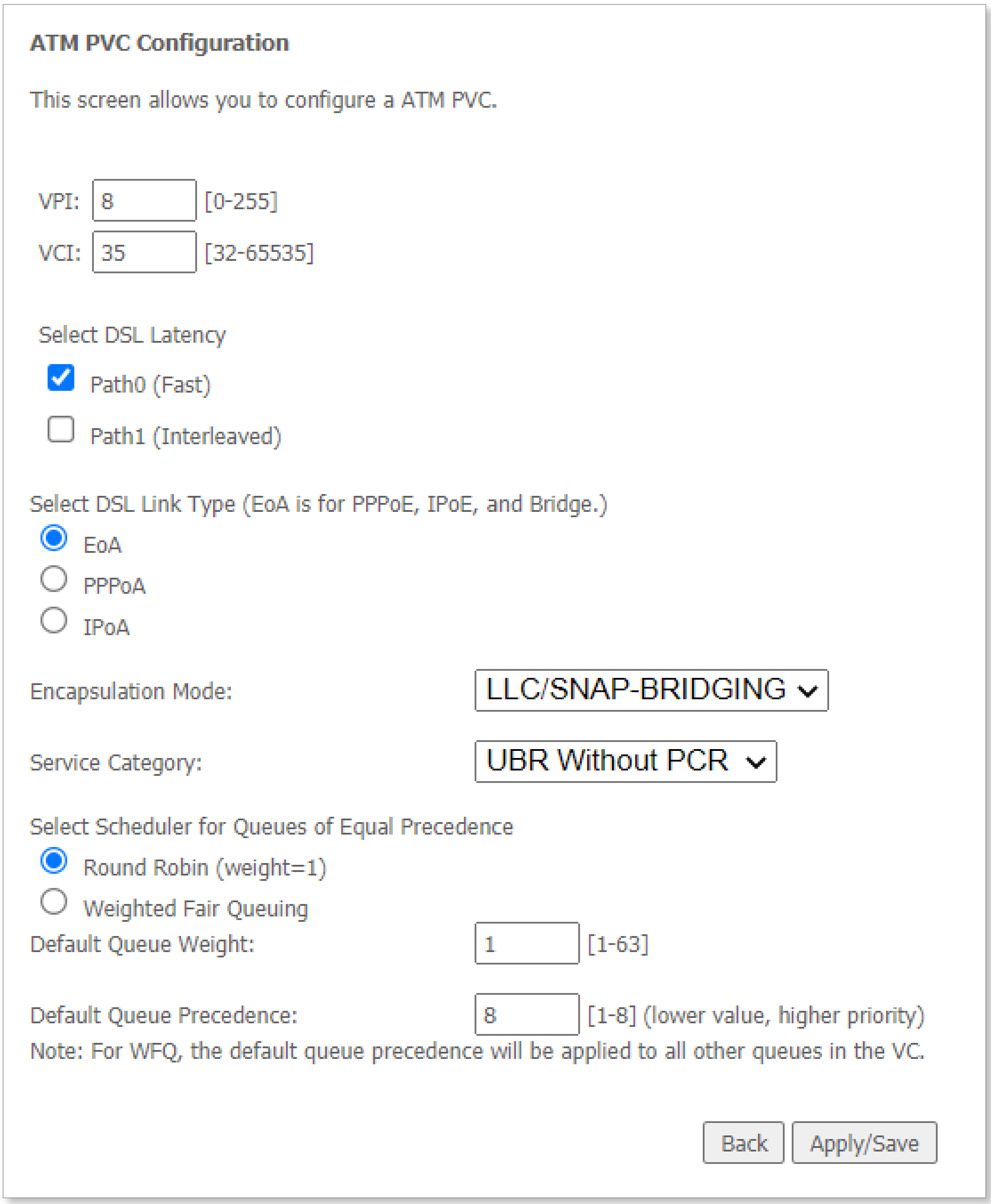
Figure 51 – DSL ATM Interface list

Field	Description
Interface	This field shows the interface name.
VPI	This field shows the Virtual Path Identifier (VPI) value. For most Australian connections the VPI is 8, for most New Zealand connections the VPI is 0. Please refer to your ISP for correct value.
VCI	This field shows the Virtual Channel Identifier (VCI) value. For most Australian connections the VCI is 35, for most New Zealand connections the VCI is 100. Please refer to your ISP for correct value.
DSL Latency	The value of the DSL Latency.
Category	This field shows the ATM service classes.
Peak Cell Rate (cell/s)	The maximum number of cells that may be transferred per second over the ATM interface.
Sustainable Cell Rate (cell/s)	An average, long-term cell transfer rate on the ATM interface.
Max Burst Size (bytes)	The maximum allowable burst size of cells that can be transmitted contiguously on the ATM interface.
Min Cell Rate (cell/s)	The minimum allowable rate at which cells may be transferred on the ATM interface.
Link Type	This field shows the type of link in use.
Connection Mode	This field shows the selected mode of connection.
IP QoS	This field shows the status of the Quality of Service (QoS) function.
MPAAL Prec/Alg/Wght	This displays data related to QoS Queue priority and algorithm.
Remove button	Check ☑ the box in this field and click the **Remove** button below the table to permanently delete the ATM configuration.

Table 4 – DSL ATM Interface Configuration settings table

To add an ATM interface, click the **Add** button.

The ATM PVC Configuration page will display.



ATM PVC Configuration

This screen allows you to configure a ATM PVC.

VPI: 8 [0-255]

VCI: 35 [32-65535]

Select DSL Latency

☑ Path0 (Fast)

□ Path1 (Interleaved)

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)

● EoA

○ PPPoA

○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Select Scheduler for Queues of Equal Precedence

● Round Robin (weight=1)

○ Weighted Fair Queuing

Default Queue Weight: 1 [1-63]

Default Queue Precedence: 8 [1-8] (lower value, higher priority)

Note: For WFQ, the default queue precedence will be applied to all other queues in the VC.

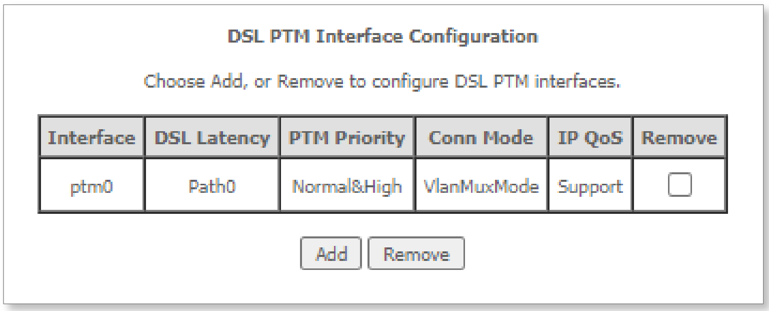
Figure 52 – ATM PVC Configuration page

Enter the details as required by your Internet Service Provider and click the Apply/Save button.

The newly defined configuration will be added to the table on the DSL ATM Interface Configuration page.

PTM Interface

The router can also establish DSL connections using PTM (Packet Transfer Mode). This page shows you an overview of the PTM interfaces and allows you to add or remove them. PTM interface is used for VDSL connections.



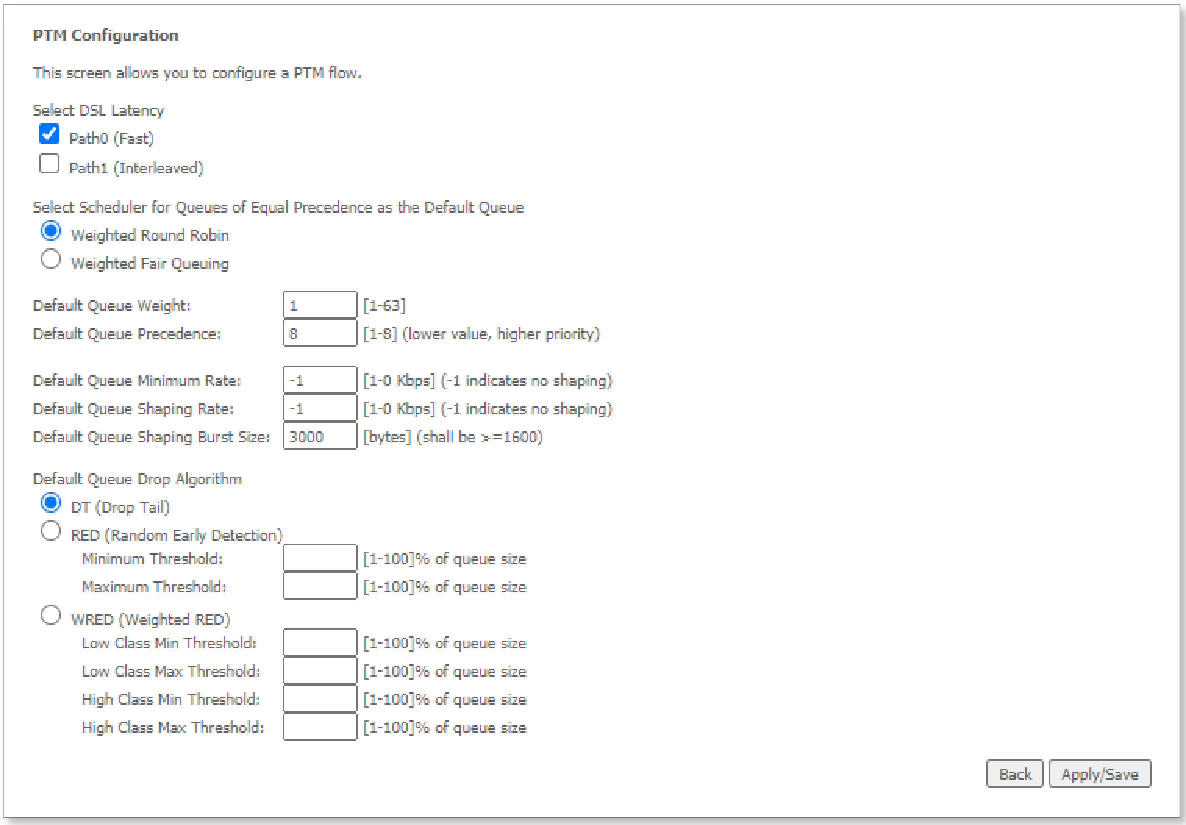
DSL PTM Interface Configuration

Choose Add, or Remove to configure DSL PTM interfaces.

Interface	DSL Latency	PTM Priority	Conn Mode	IP QoS	Remove
ptm0	Path0	Normal&High	VlanMuxMode	Support	□

Figure 53 – DSL PTM Interface list

Click the **Add** button to create a new PTM interface. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.



PTM Configuration

This screen allows you to configure a PTM flow.

Select DSL Latency
☑ Path0 (Fast)
□ Path1 (Interleaved)

Select Scheduler for Queues of Equal Precedence as the Default Queue
● Weighted Round Robin
○ Weighted Fair Queuing

Default Queue Weight:	1	[1-63]
Default Queue Precedence:	8	[1-8] (lower value, higher priority)
Default Queue Minimum Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Rate:	-1	[1-0 Kbps] (-1 indicates no shaping)
Default Queue Shaping Burst Size:	3000	[bytes] (shall be >=1600)

Default Queue Drop Algorithm
● DT (Drop Tail)
○ RED (Random Early Detection)

Minimum Threshold:		[1-100]% of queue size
Maximum Threshold:		[1-100]% of queue size

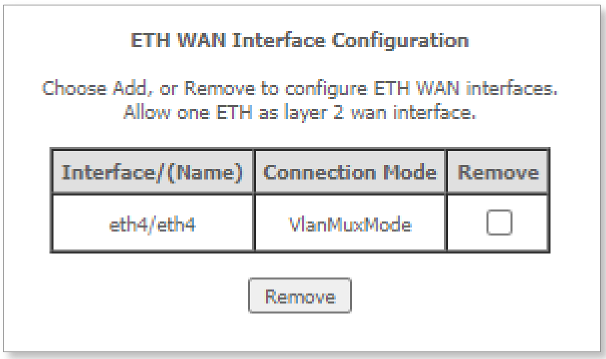
○ WRED (Weighted RED)

Low Class Min Threshold:		[1-100]% of queue size
Low Class Max Threshold:		[1-100]% of queue size
High Class Min Threshold:		[1-100]% of queue size
High Class Max Threshold:		[1-100]% of queue size

Figure 54 – PTM Configuration page

ETH Interface

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



ETH WAN Interface Configuration

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

Interface/(Name)	Connection Mode	Remove
eth4/eth4	VlanMuxMode	□

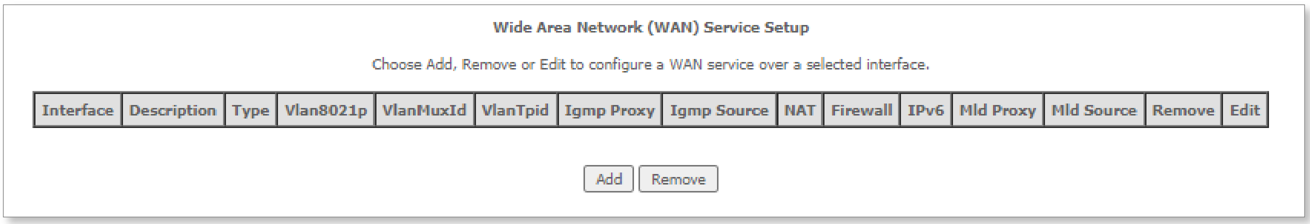
Figure 55 – ETH WAN interface list WAN Service

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 router to connect to a larger network for Internet access.

Attention – WAN service requires a preconfigured Layer 2 interface, be it ATM/PTM or Ethernet WAN.



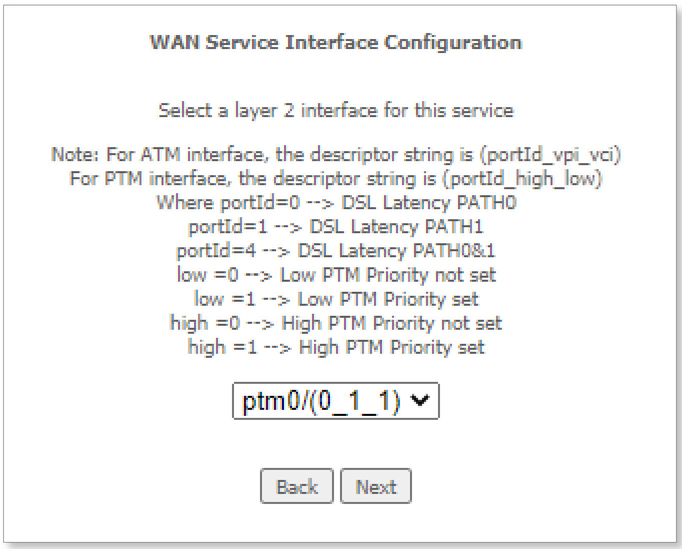
Wide Area Network (WAN) Service Setup

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

Interface	Description	Type	Vlan8021p	VlanMuxId	VlanTpid	Igmp Proxy	Igmp Source	NAT	Firewall	IPv6	Mld Proxy	Mld Source	Remove	Edit

Figure 56 – WAN Service setup

To add a WAN service, click the Add button. Use the drop-down list to select the layer 2 interface to use for the WAN service and click the Next button.



WAN Service Interface Configuration

Select a layer 2 interface for this service

Note: For ATM interface, the descriptor string is (portId_vpi_vci)
For PTM interface, the descriptor string is (portId_high_low)
Where portId=0 --> DSL Latency PATH0
portId=1 --> DSL Latency PATH1
portId=4 --> DSL Latency PATH0&1
low =0 --> Low PTM Priority not set
low =1 --> Low PTM Priority set
high =0 --> High PTM Priority not set
high =1 --> High PTM Priority set

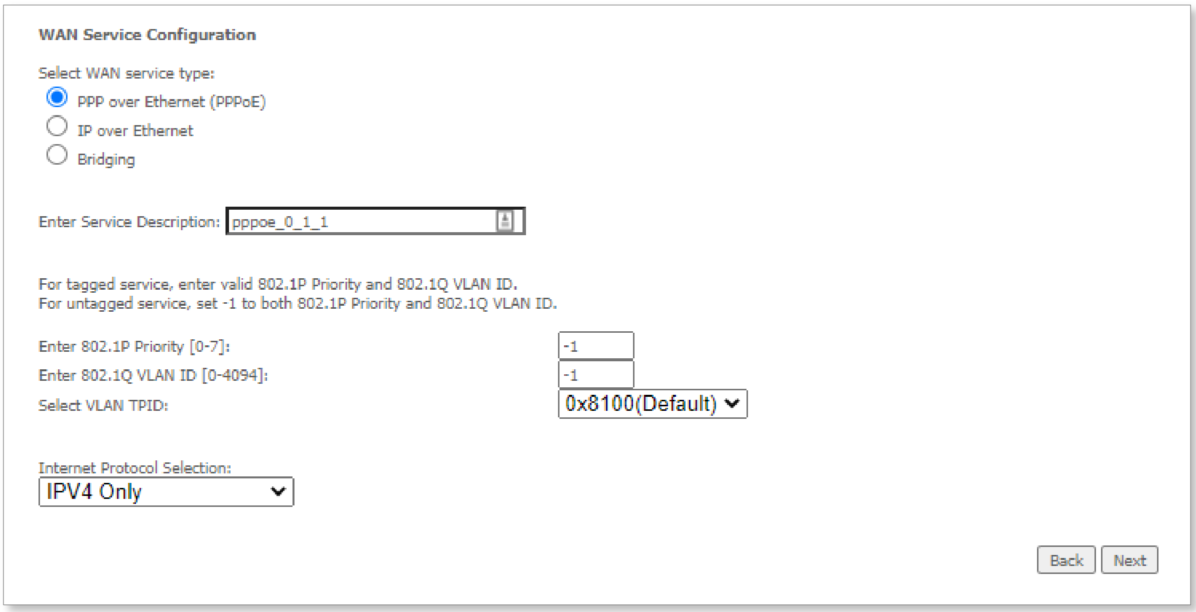
ptm0/(0_1_1)

Figure 57 – WAN Service – Select layer 2 interface

Select a WAN service type, enter a Service Description, enter the 802.1P Priority and 802.1Q VLAN ID if required, then click the Next button.

To disable VLAN tagging, place input value of -1.

Refer to your ISP for VLAN information as required by your Internet Service Provider.



WAN Service Configuration

Select WAN service type:

● PPP over Ethernet (PPPoE)
○ IP over Ethernet
○ Bridging

Enter Service Description: pppoe_0_1_1

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

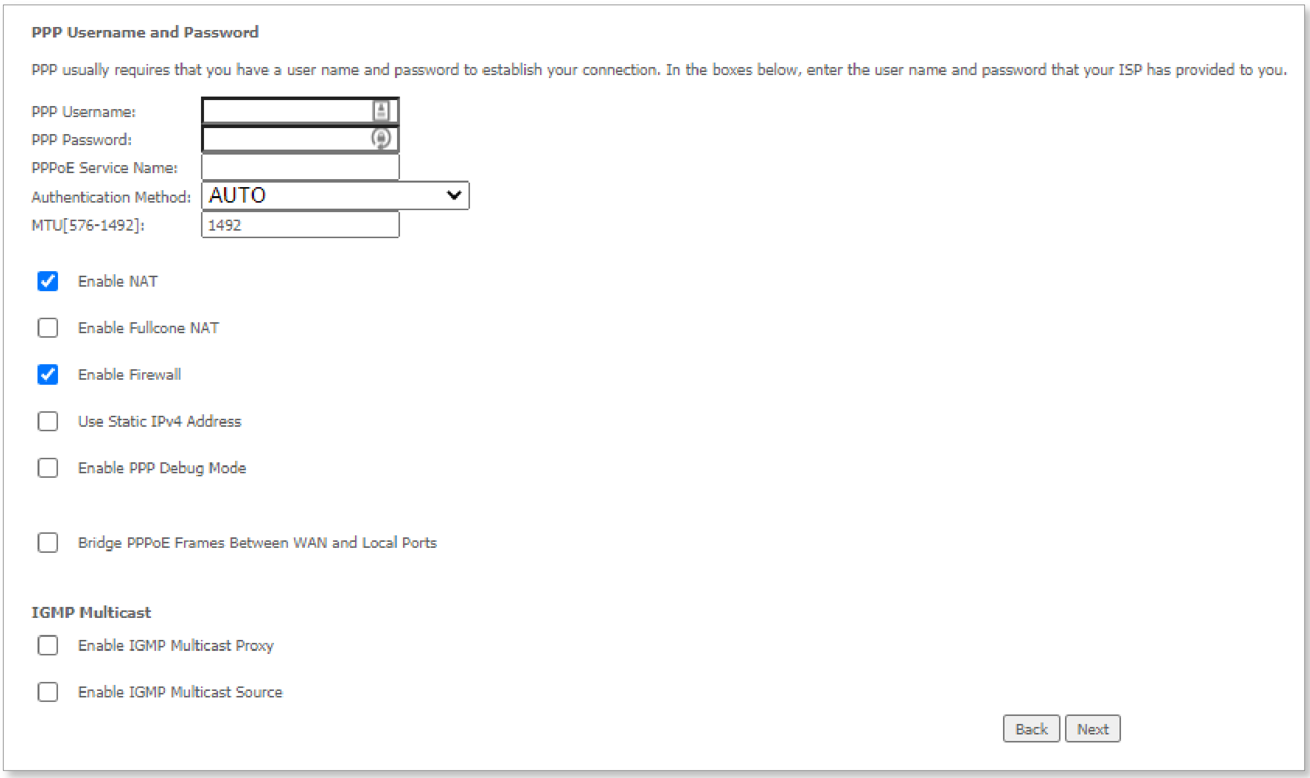
Enter 802.1P Priority [0-7]: -1
Enter 802.1Q VLAN ID [0-4094]: -1
Select VLAN TPID: 0x8100(Default)

Internet Protocol Selection: IPV4 Only

Figure 58 – WAN Service – Select WAN Service Type

PPOE (PPP over Ethernet)

Enter the PPPoE authentication details as required by your Internet Service Provider and click the Next button.



PPP Username and Password

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

PPP Username:
PPP Password:
PPPoE Service Name:
Authentication Method: AUTO
MTU[576-1492]: 1492

☑ Enable NAT
☐ Enable Fullcone NAT
☑ Enable Firewall
☐ Use Static IPv4 Address
☐ Enable PPP Debug Mode

☐ Bridge PPPoE Frames Between WAN and Local Ports

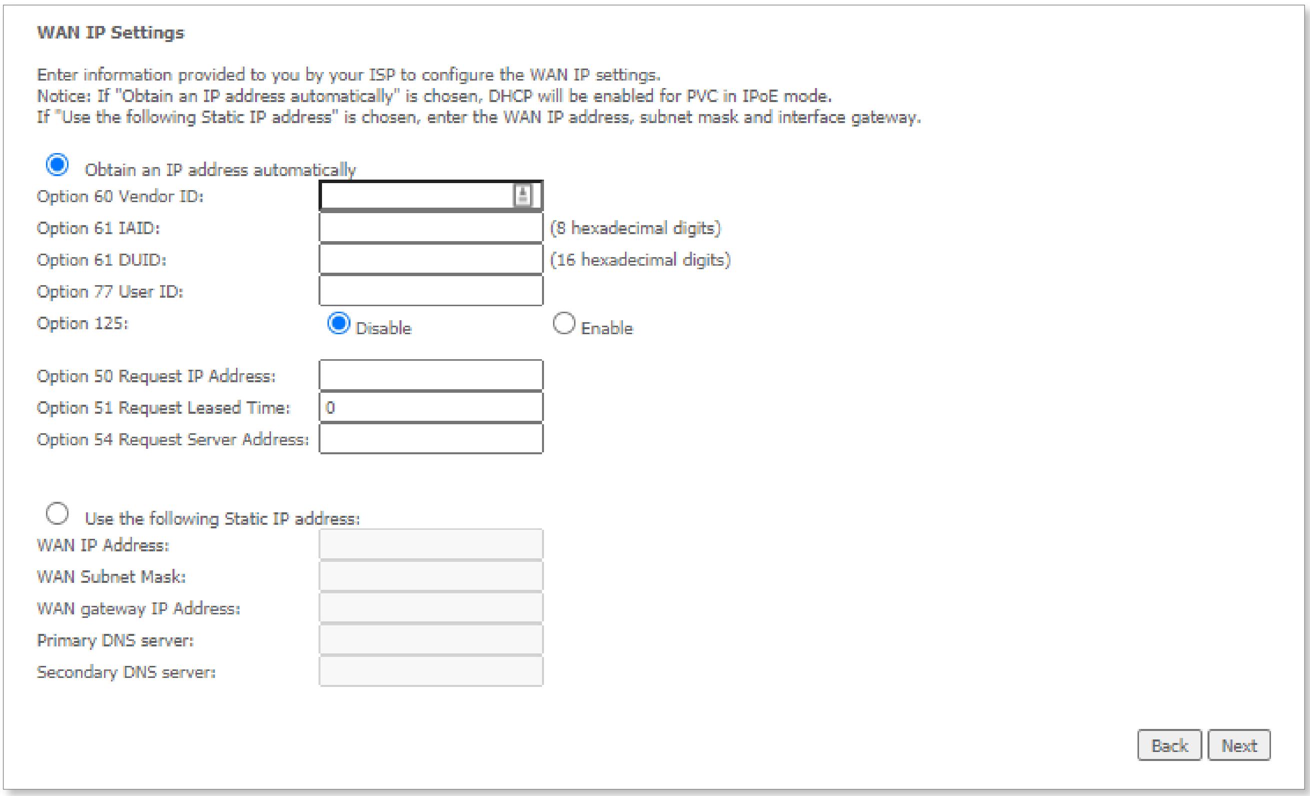
IGMP Multicast

☐ Enable IGMP Multicast Proxy
☐ Enable IGMP Multicast Source

Figure 59 – Enter PPP over Ethernet details

IPOE (IP over Ethernet)

Enter the details as required by your Internet Service Provider and click the **Next** button.



WAN IP Settings

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

● Obtain an IP address automatically

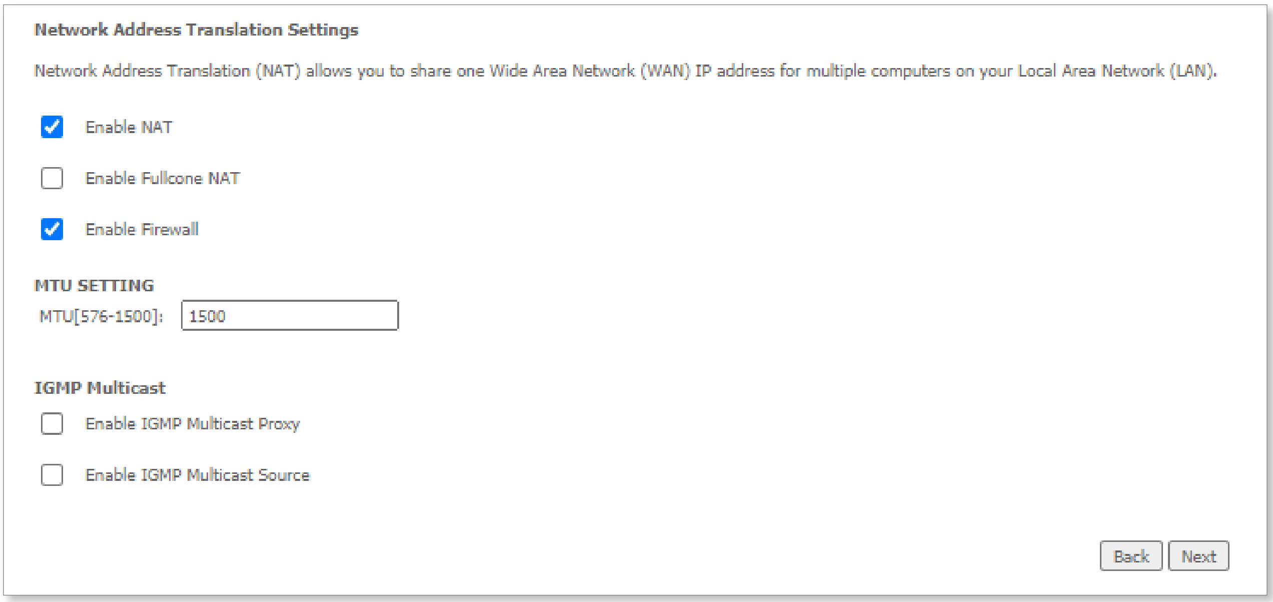
Option 60 Vendor ID:		
Option 61 IAID:		(8 hexadecimal digits)
Option 61 DUID:		(16 hexadecimal digits)
Option 77 User ID:		
Option 125:	● Disable	○ Enable
Option 50 Request IP Address:		
Option 51 Request Leased Time:	0	
Option 54 Request Server Address:		

○ Use the following Static IP address:

WAN IP Address:	
WAN Subnet Mask:	
WAN gateway IP Address:	
Primary DNS server:	
Secondary DNS server:	

Figure 60 – Enter IP over Ethernet details

Select the NAT Translation settings as desired and click the **Next** button.



Network Address Translation Settings

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

☑ Enable NAT

☐ Enable Fullcone NAT

☑ Enable Firewall

MTU SETTING

MTU[576-1500]: 1500

IGMP Multicast

☐ Enable IGMP Multicast Proxy

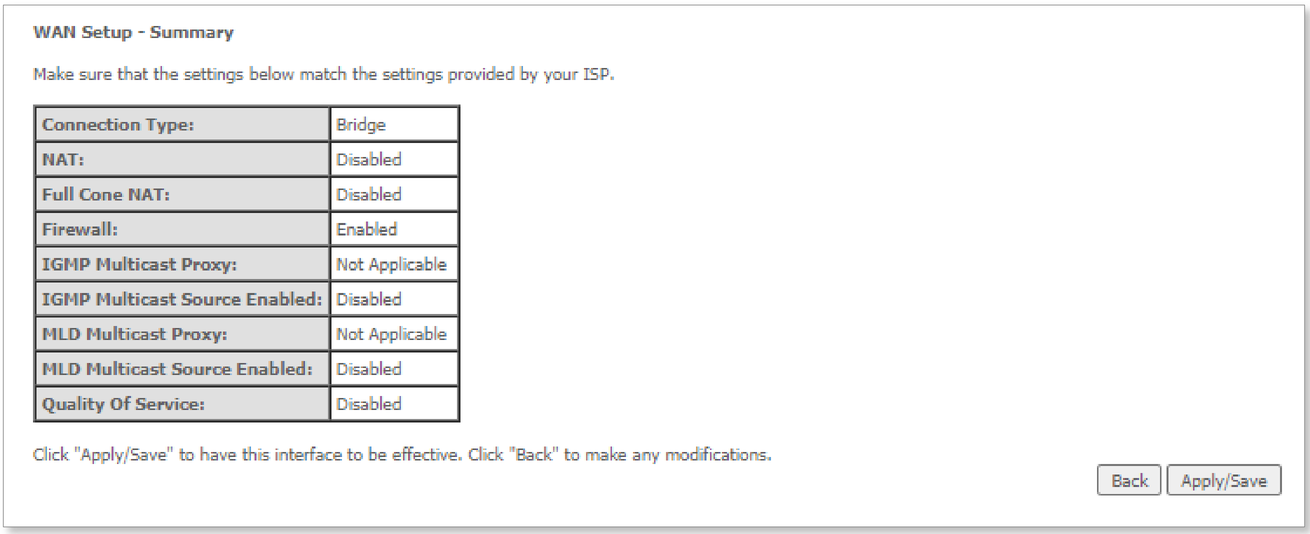
☐ Enable IGMP Multicast Source

Figure 61 – Enter IPoE NAT Translation settings

Bridging

When you select ⦿ Bridging mode, a summary of the settings is displayed.

Click Apply/Save to commit the settings.



WAN Setup - Summary

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

Connection Type:	Bridge
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

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

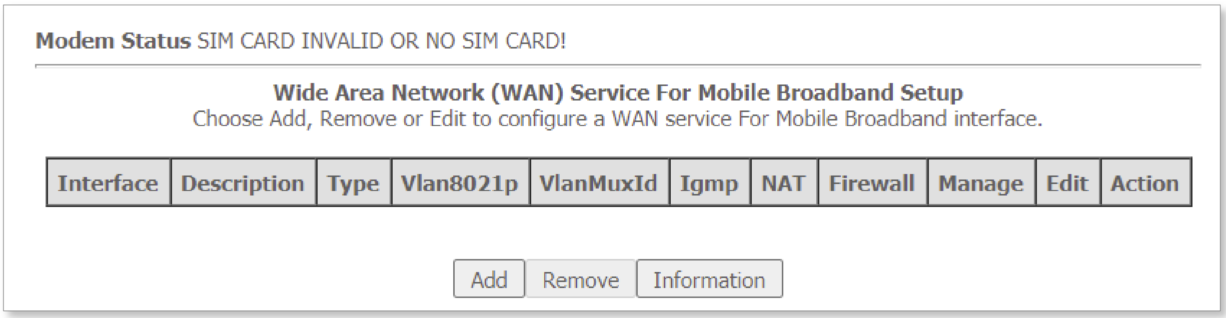
Figure 62 – Enter Bridging WAN service summary

Mobile Broadband

The Mobile Broadband page displays the current Wide Area Network service setup and allows you to configure the gateway to connect to a mobile (cellular) network for primary Internet access.

Only one Mobile Broadband can be set up at a time. You can alter the setup by clicking the Edit button, or Remove the setup and Add a new service.

Note – After a Factory Reset there will be no Mobile Broadband by default.
Insert a Standard Size SIM card into the device's SIM Card Slot and click the Add button to configure the Mobile Broadband service.



Modem Status SIM CARD INVALID OR NO SIM CARD!

Wide Area Network (WAN) Service For Mobile Broadband Setup
Choose Add, Remove or Edit to configure a WAN service For Mobile Broadband interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	Manage	Edit	Action

Figure 63 – Mobile Broadband setup

Field	Description
Modem status indicator	In the top left corner above the start of the table is the Modem status indicator: dialling..., CONNECTED, Manual Dialled, undialing..., DISCONNECT, SIM CARD INVALID OR NOT SIM CARD!, etc.

Field	Description
Interface	The interface of the mobile connection.
Description	The description of the mobile connection.
Type	The type of WAN connection.
Vlan802.1p	N/A for mobile interface.
VlanMuxId	N/A for mobile interface.
IGMP	Internet Group Management Protocol (IGMP) is used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.
NAT	**NAT (Network Address Translation)** status of the mobile WAN connection: **Enabled** or **Disabled**
Firewall	The status of the gateway firewall across the mobile WAN connection.
Manage PIN button	Click to open the **PIN settings** page where you can enable, disable and change the PIN on the SIM.
Edit details button	Click the **Edit** button to modify the details of the current Mobile Broadband service parameters.
Action Connect button	Click the **Connect** button to manually connect and register to the Mobile network. When connected this button changes to **Disconnect** and allows the user to manually disconnect and deregister register from the Mobile network.
Add button	Click open the **Mobile Broadband Setup** page, see next section.
Remove button	You can only have one **Mobile Broadband** service at a time. To replace it click the **Remove** button and then click the **Add** button.
Information button	Click to see details of the mobile broadband connection.

Table 5 – Mobile configuration settings table

Add/Edit Mobile Broadband Setup

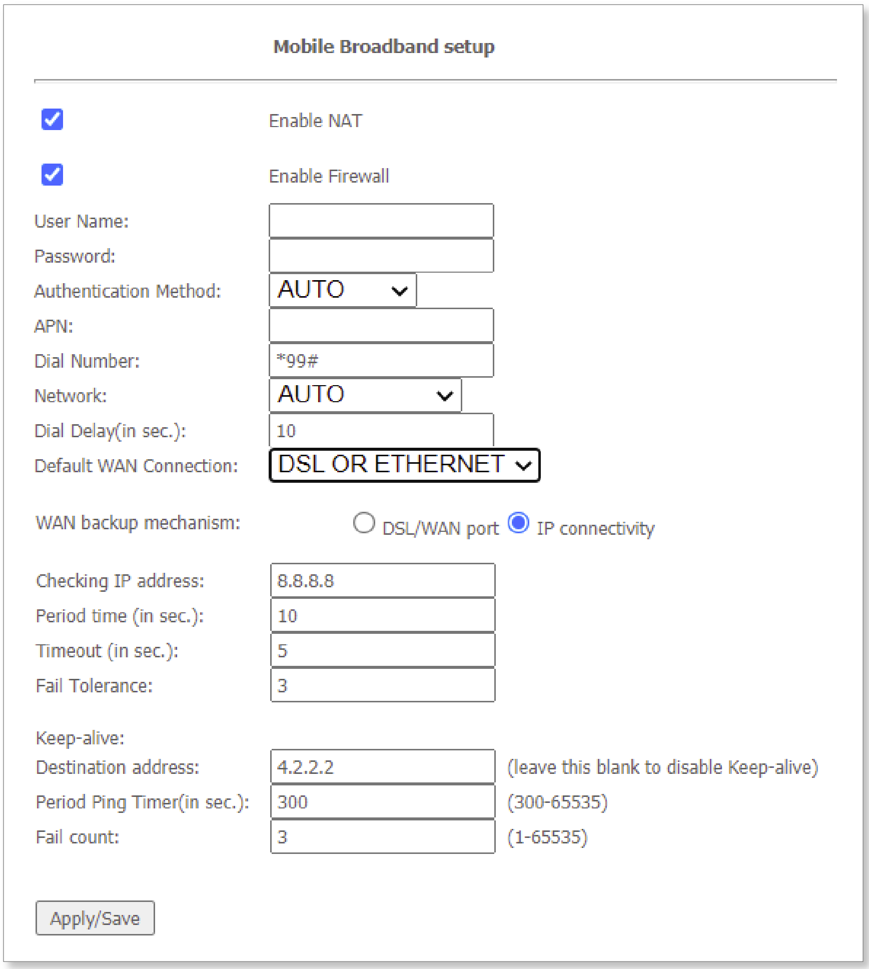
Only one mobile cellular service can be defined at one time.

If one is not currently defined, click the **Add** button.

If one already exists, either click the **Edit** button or click the **Remove** button and then click the **Add** button.

Note – If the service is currently connected, before you can edit it you must click the **Action/Disconnect** button and then click the **Edit** or **Remove/Add** button(s).

Both the **Add** and the **Edit** buttons on the **Mobile Status** page open the **Mobile Broadband modem setup** dialog.



Mobile Broadband setup

☑ Enable NAT

☑ Enable Firewall

User Name:
Password:
Authentication Method: AUTO
APN:
Dial Number: *99#
Network: AUTO
Dial Delay(in sec.): 10
Default WAN Connection: DSL OR ETHERNET

WAN backup mechanism: ○ DSL/WAN port ● IP connectivity

Checking IP address: 8.8.8.8
Period time (in sec.): 10
Timeout (in sec.): 5
Fail Tolerance: 3

Keep-alive:
Destination address: 4.2.2.2 (leave this blank to disable Keep-alive)
Period Ping Timer(in sec.): 300 (300-65535)
Fail count: 3 (1-65535)

Figure 64 – Mobile Broadband setup interface (from NL19MESH)

Field	Description
Enable NAT	☑ Enable NAT (Network Address Translation) is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the router modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the router originated from the WAN IP address of the router's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.

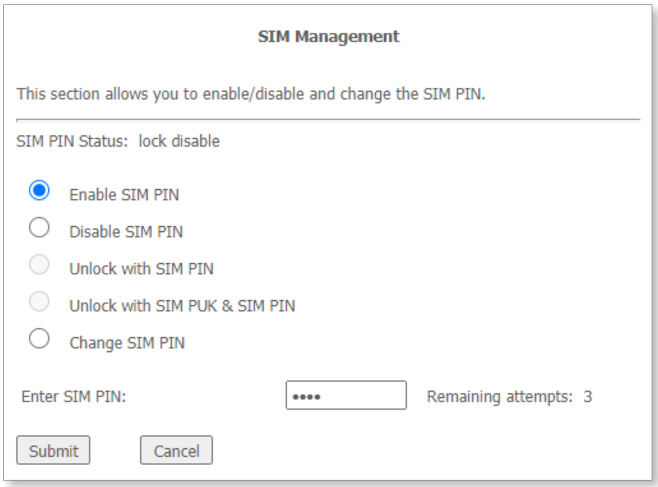
Field	Description	
Enable Firewall	☑ Enable Firewall to prevent attack from the lte0 interface.	
User Name	The Username for your broadband service provided by your broadband ISP.	
Password	The Password for your broadband service provided by your broadband ISP.	
Authentication Method	Choose: AUTO, PAP, CHAP or MSCHAP	
APN	Enter the APN (Access Point Name) provided by your broadband ISP.	
Dial Number	Enter the number to dial to get data connectivity provided by your broadband ISP.	
Dial Delay (in secs.)	Enter the time delay in seconds that must elapse before re-connecting to the mobile connection when primary connection dropped, and mobile broadband is configured as backup.	
Default WAN Connection	Select either Mobile Broadband or DSL OR ETHERNET from the drop-down menu.	
WAN backup mechanism	DSL	Select to use DSL/Ethernet WAN physical status.
	IP connectivity	Select to use a specified IP address connectivity check.
Apply/Save button	Click to save and apply your changes.	

Table 6 – DSL ATM Interface Configuration settings table

Note – Mobile Broadband service requires an unlocked SIM card in the 2FF format. See PIN settings section on the next page.

PIN settings

When the Action button Connect is displayed (click Disconnect to disconnect) click the PIN button in the Manage column to open the SIM Management page:



SIM Management

This section allows you to enable/disable and change the SIM PIN.

SIM PIN Status: lock disable

● Enable SIM PIN
○ Disable SIM PIN
○ Unlock with SIM PIN
○ Unlock with SIM PUK & SIM PIN
○ Change SIM PIN

Enter SIM PIN: •••• Remaining attempts: 3

Figure 65 – SIM – PIN settings

The following fields are found on this page.

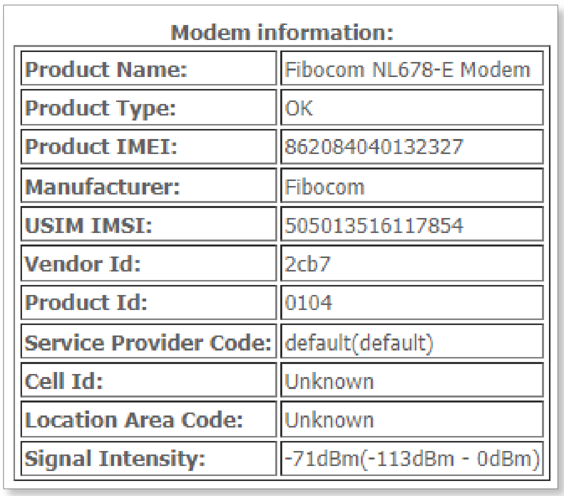
Field	Description
SIM PIN Status	Current status of the SIM card's PIN.

Field	Description
Enable SIM PIN	When ◉ Enable SIM PIN is selected, the current PIN must be entered.
Disable SIM PIN	When ◉ Disable SIM PIN is selected, PIN entry not required. By default PIN protection is disabled.
Change SIM PIN	When ◉ Change SIM PIN is selected you can change the PIN to something easier to remember or more secure. The next two fields display for you to make the change.
Enter current SIM PIN	Enter current PIN to unlock it.
Enter new SIM PIN	Enter the new SIM PIN number.
Confirm new PIN	Re-enter the new SIM PIN number.
Remaining attempts	Enter the number of tries allowed before the system PUK locks the SIM card. The default is three (3) attempts.
Submit button	Click to save and apply the changes.
Cancel button	Click to close without saving and return to the broadband setup page.

Table 7 – USB mobile PIN Configuration page

Modem information

Click the Information button to display details of the gateway (Modem) and its mobile service.



Modem information:

Product Name:	Fibocom NL678-E Modem
Product Type:	OK
Product IMEI:	862084040132327
Manufacturer:	Fibocom
USIM IMSI:	505013516117854
Vendor Id:	2cb7
Product Id:	0104
Service Provider Code:	default(default)
Cell Id:	Unknown
Location Area Code:	Unknown
Signal Intensity:	-71dBm(-113dBm - 0dBm)

Figure 66 – Modem information display

The following fields are found on this page.

Field	Description
Product Name	The Mobile Broadband module's product name.
Product IMEI	The Mobile Broadband module's International Mobile Equipment Identity.
Manufacturer	The Manufacturer of the Mobile Broadband module.
USIM IMSI	The SIM card's International Mobile Subscriber Identity.
Vendor Id	The Mobile Broadband Module's Vendor ID

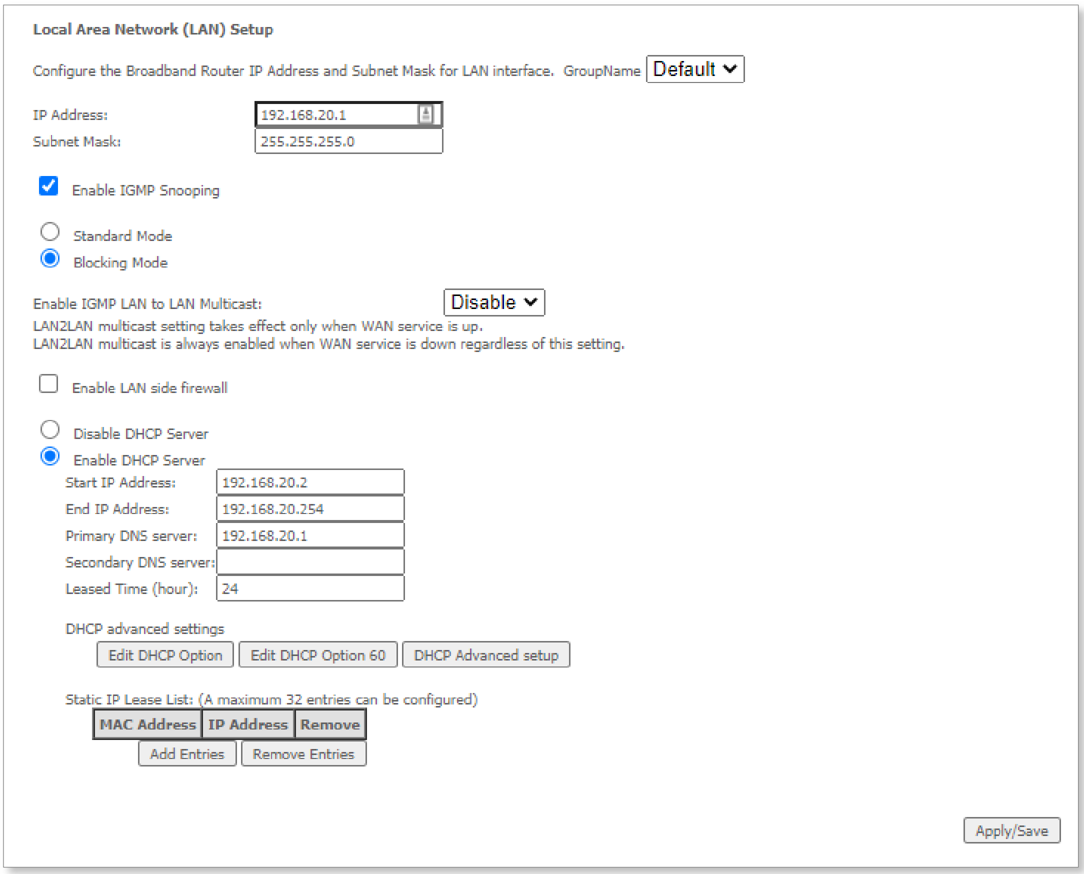
Field	Description
Product Id	The Mobile Broadband Module's Product ID.
Service Provide Code	The Mobile Network Service Provider Code.
Cell Id	The current Mobile station Cell ID.
Location Area Code	The current Mobile station Location/Tracking Area Code.
Signal Intensity	The current Receive Signal Strength Indicator (RSSI) detected by the Mobile Broadband Module.
Apply/Save button	Press the **Apply/Save** button to save the changes to the Modem information.

Table 8 – Modem information page

LAN

IPv4 Autoconfig

The LAN window allows you to modify the settings for your local area network (LAN).



Local Area Network (LAN) Setup

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

IP Address: 192.168.20.1
Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode
● Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable
LAN2LAN multicast setting takes effect only when WAN service is up.
LAN2LAN multicast is always enabled when WAN service is down regardless of this setting.

□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server
Start IP Address: 192.168.20.2
End IP Address: 192.168.20.254
Primary DNS server: 192.168.20.1
Secondary DNS server:
Leased Time (hour): 24

DHCP advanced settings

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

MAC Address	IP Address	Remove

Figure 67 – LAN setup -- IPv4 Autoconfig settings

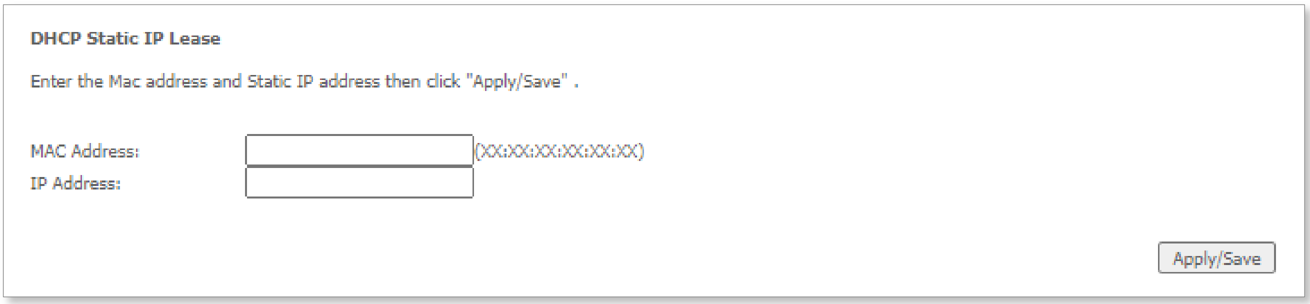
The following options are available to configure:

Parameter	Definition
IP Address	Enter the Local IP Address to use for the CloudMesh Gateway.

Parameter	Definition
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 traffic between LAN host-LAN hosts and WiFi Clients.
Enable DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
Apply/Save button	Press the **Apply/Save** button to save the IPv4 Autoconfig settings.

Table 9 – IPv4 Autoconfig settings table

You can also reserve DHCP Addresses for specific hosts as shown below:



DHCP Static IP Lease

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

MAC Address: (XX:XX:XX:XX:XX:XX)

IP Address:

Figure 68 – Enter DHCP Static IP Addresses

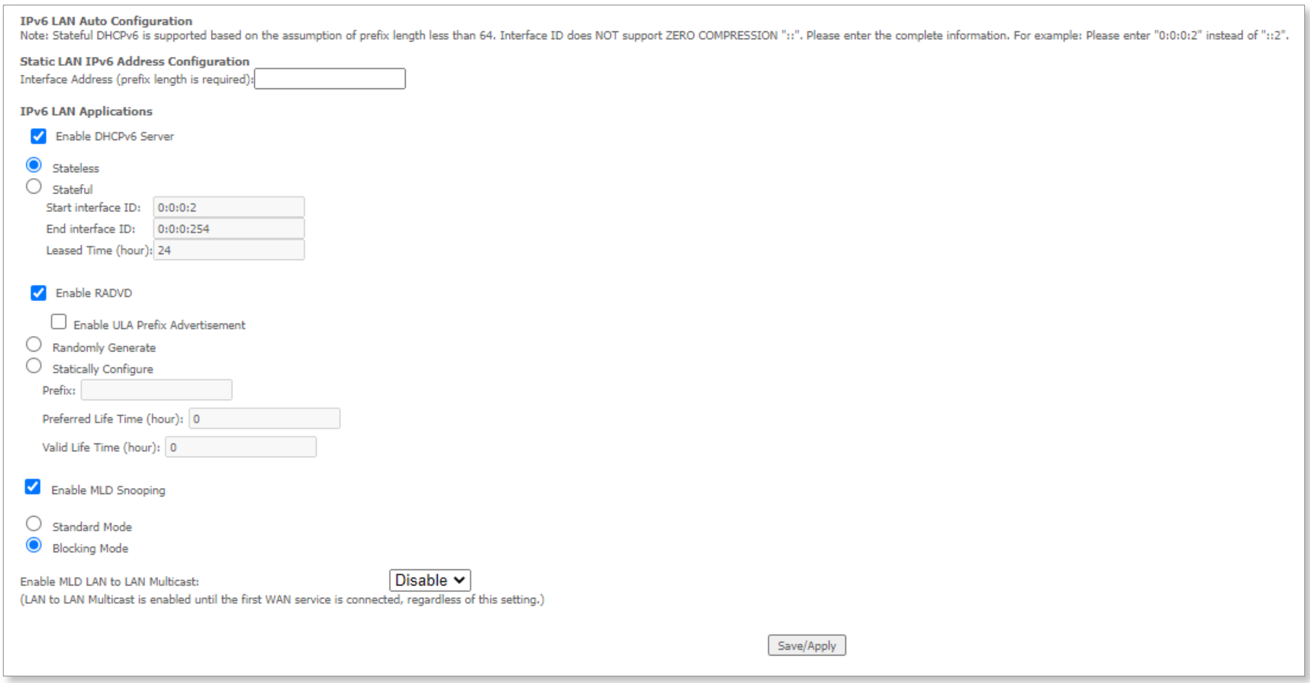
To set a DHCP reservation, enter the MAC Address of the chosen host and IP to use and then click **Apply/Save**.

The CloudMesh Gateway enables you to set the DHCP options which are provided to hosts attempting to connect to the DHCP server.

These options should not normally need to be set or changed. Click **Apply/Save** to save the new LAN configuration settings.

IPv6 LAN Auto Configuration

The IPv6 LAN Auto Configuration page allows you to configure settings pertaining to the IPv6 service.



IPv6 LAN Auto Configuration

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

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

☑ Enable DHCPv6 Server

● Stateless
○ Stateful

Start interface ID: 0:0:0:2
End interface ID: 0:0:0:254
Leased Time (hour): 24

☑ Enable RADVD

☐ Enable ULA Prefix Advertisement
○ Randomly Generate
○ Statically Configure

Prefix:
Preferred Life Time (hour): 0
Valid Life Time (hour): 0

☑ Enable MLD Snooping

○ Standard Mode
● Blocking Mode

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

Figure 69 – IPv6 LAN Auto Configuration page

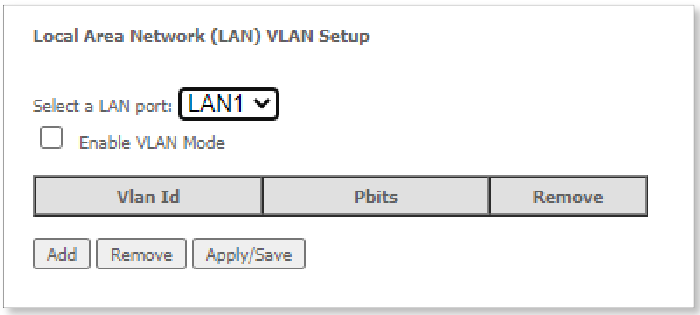
Option	Definition
Enable Unique Local Addresses and Prefix Advertisement	Enable the use of unique local addresses. The router will advertise the IPv6 /64 prefix to new devices on the network.
Randomly Generate	Randomly generates the unique local addresses and the prefix.
Statically Configure	Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider (ISP).
IPv6 LAN Applications	Enable IPv6 DHCP server
Enable DHCPv6 Server or 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.

Option	Definition
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 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.
Apply/Save button	Press the Apply/Save button to save the IPv6 Autoconfig settings.

Table 10 – IPv6 LAN Auto Configuration settings

LAN VLAN Setting

This page allows you to specify a LAN port to apply VLAN tagging to.



Local Area Network (LAN) VLAN Setup

Select a LAN port: LAN1

☐ Enable VLAN Mode

Vlan Id	Pbits	Remove

Figure 70 – Specify a LAN port for VLAN tagging

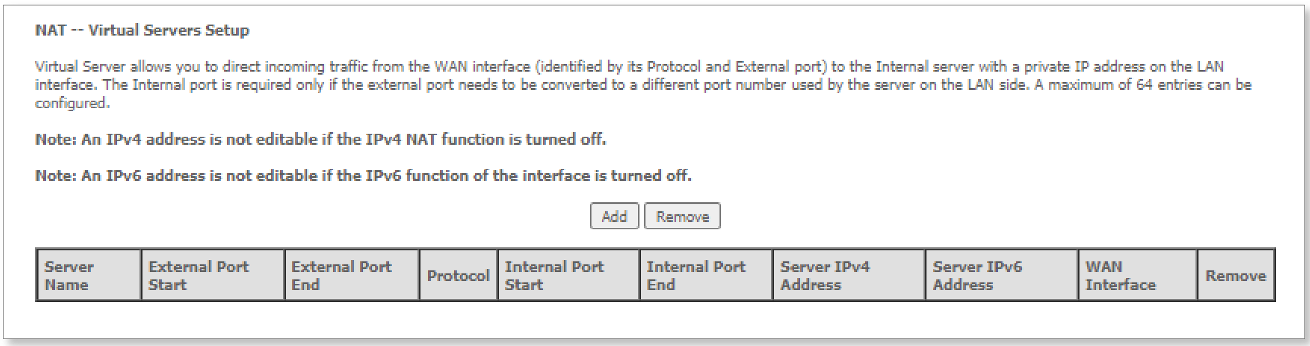
Select the LAN port using the drop-down menu, then click the **Add** button. Enter the **VLAN ID** and in the Pbits field, enter a value from 0-7 indicating the priority bits that dictates the priority of the VLAN.

Click **Apply/Save** when you have finished.

NAT

Virtual Servers

Virtual Servers (also commonly referred to as port forwarding) allow you to direct incoming traffic from the WAN side to the Internal network host with a private IP address on the LAN side.



NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from the WAN interface (identified by its Protocol and External port) to the Internal server with a private IP address on the LAN interface. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 64 entries can be configured.

Note: An IPv4 address is not editable if the IPv4 NAT function is turned off.

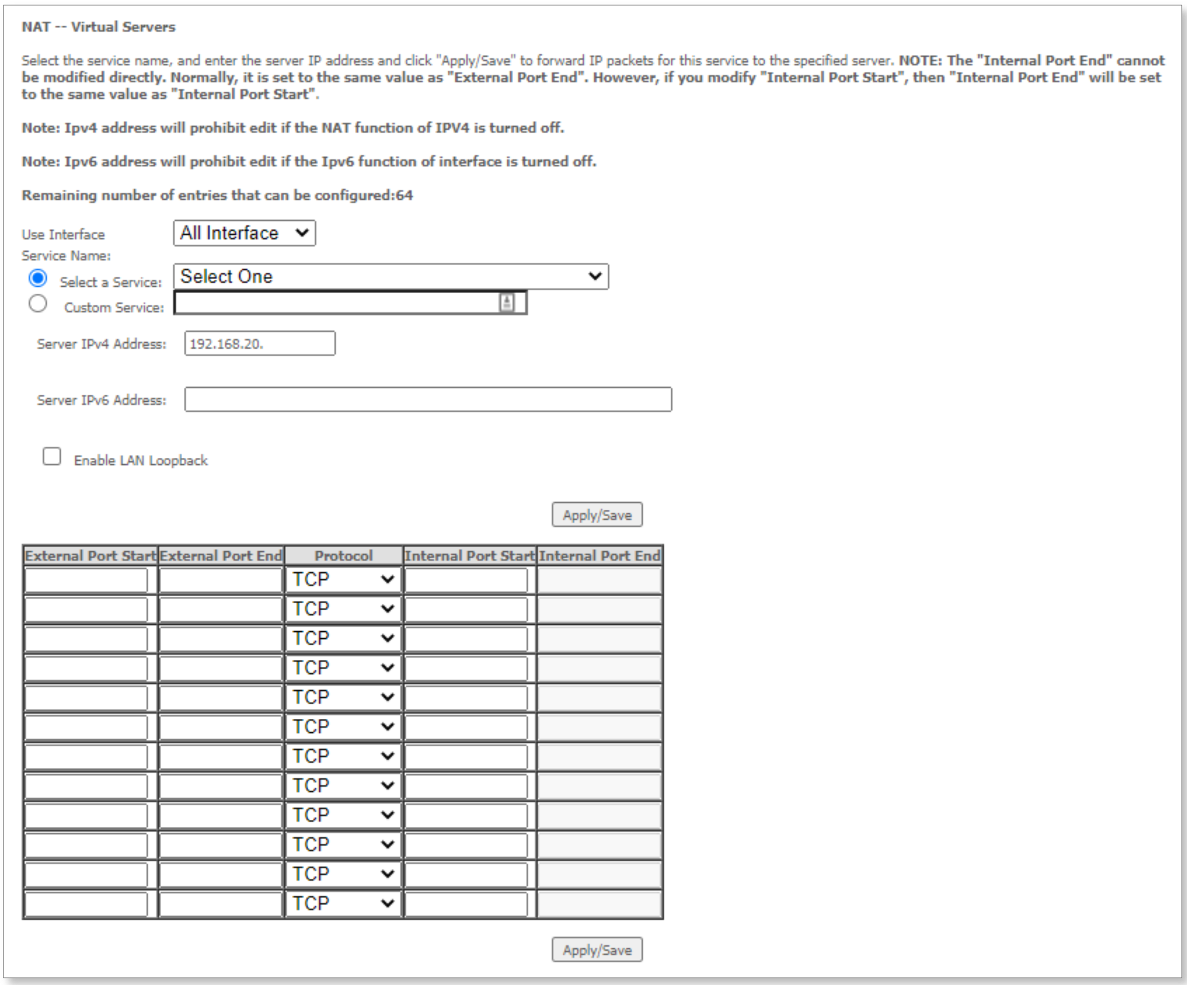
Note: An IPv6 address is not editable if the IPv6 function of the interface is turned off.

Add | Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IPv4 Address	Server IPv6 Address	WAN Interface	Remove

Figure 71 – NAT -- Virtual Server list

Click the Add button to add a virtual server.



NAT -- Virtual Servers

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

Note: Ipv4 address will prohibit edit if the NAT function of IPV4 is turned off.

Note: Ipv6 address will prohibit edit if the Ipv6 function of interface is turned off.

Remaining number of entries that can be configured:64

Use Interface: All Interface

Service Name:

● Select a Service: Select One

○ Custom Service:

Server IPv4 Address: 192.168.20.

Server IPv6 Address:

□ Enable LAN Loopback

Apply/Save

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

Apply/Save

Figure 72 – NAT -- Virtual Server Configuration page

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.
Apply/Save button	Press the Apply/Save button to save the virtual server configuration details.

Table 11 – NAT -- Virtual Server settings table

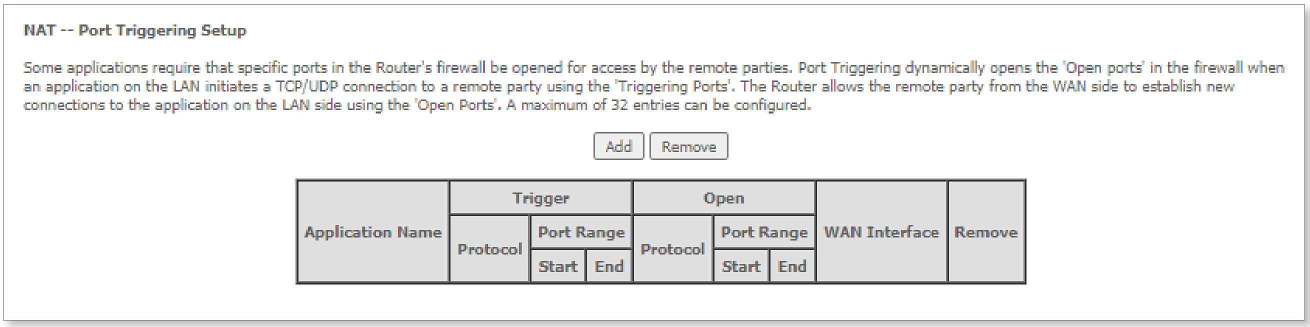
Click Save/Apply to save your settings when you have finished creating virtual servers.

Port Triggering

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

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 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.



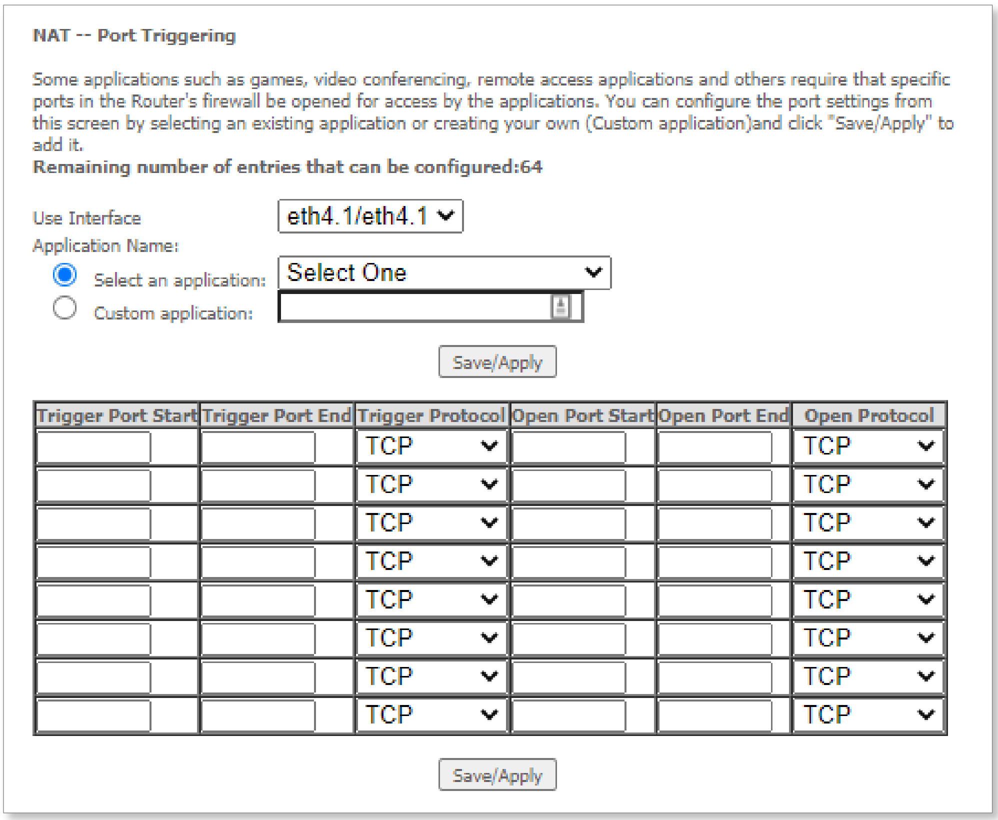
NAT -- Port Triggering Setup

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

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

Figure 73 – NAT -- Port Triggering list

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



NAT -- Port Triggering

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

Remaining number of entries that can be configured:64

Use Interface: eth4.1/eth4.1

Application Name:

● Select an application: Select One

○ Custom application:

Save/Apply

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

Save/Apply

Figure 74 – NAT -- Port Trigger Configuration page

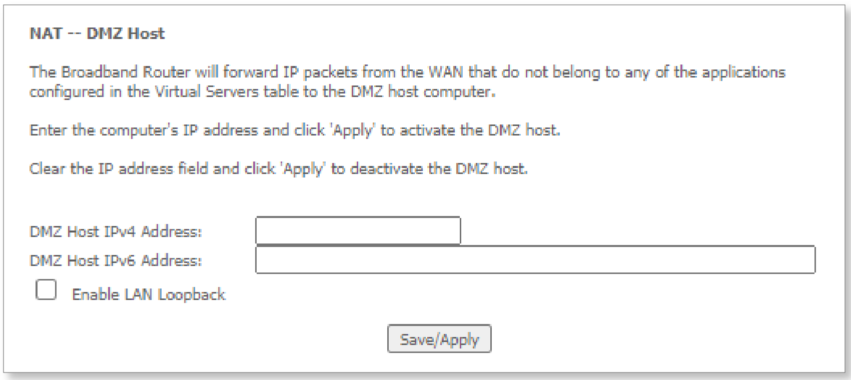
Field	Description
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When 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
Apply/Save button	Press the Apply/Save button to save the port triggering rule.

Table 12 – NAT -- Port Trigger Configuration settings

DMZ Host

The CloudMesh 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 **Host's IP address** and click **Apply** to activate the DMZ host. To deactivate the DMZ Host function, clear the IP address field and press the **Save/Apply** button.



NAT -- DMZ Host

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

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

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

DMZ Host IPv4 Address:

DMZ Host IPv6 Address:

☐ Enable LAN Loopback

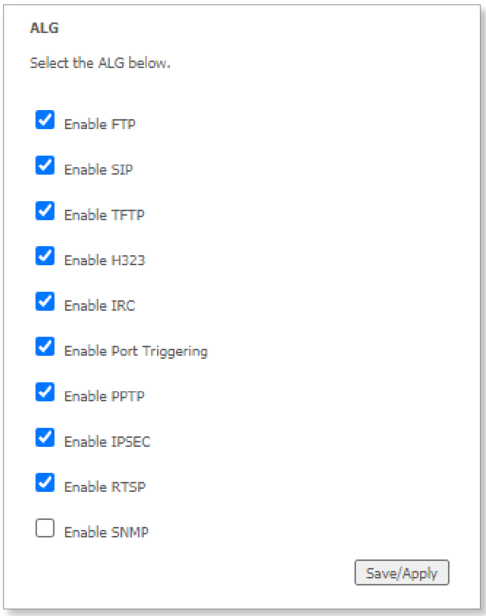
Figure 75 – NAT – DMZ Host settings

Note that **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 router 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.



ALG

Select the ALG below.

☑ Enable FTP

☑ Enable SIP

☑ Enable TFTP

☑ Enable H323

☑ Enable IRC

☑ Enable Port Triggering

☑ Enable PPTP

☑ Enable IPSEC

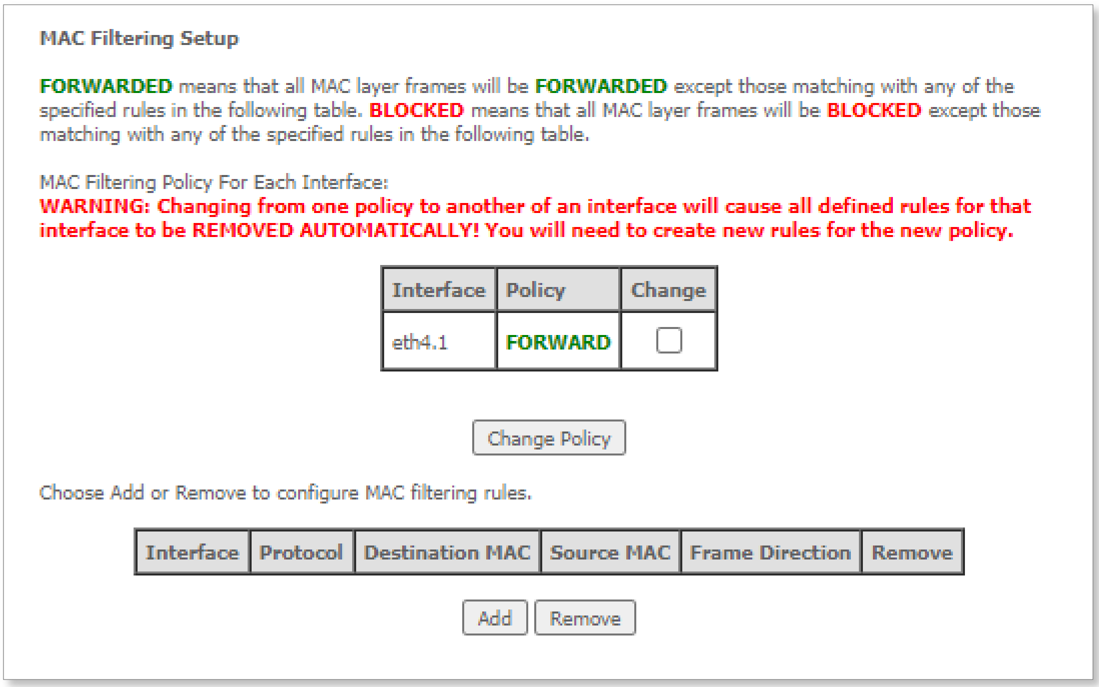
☑ Enable RTSP

☐ Enable SNMP

Figure 76 – NAT – Application Layer Gateway (ALG) settings

MAC Filtering

The CloudMesh Gateway offers the ability to use MAC Address filtering on ATM PVCs. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow all connections.



MAC Filtering Setup

FORWARDED means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface:
WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

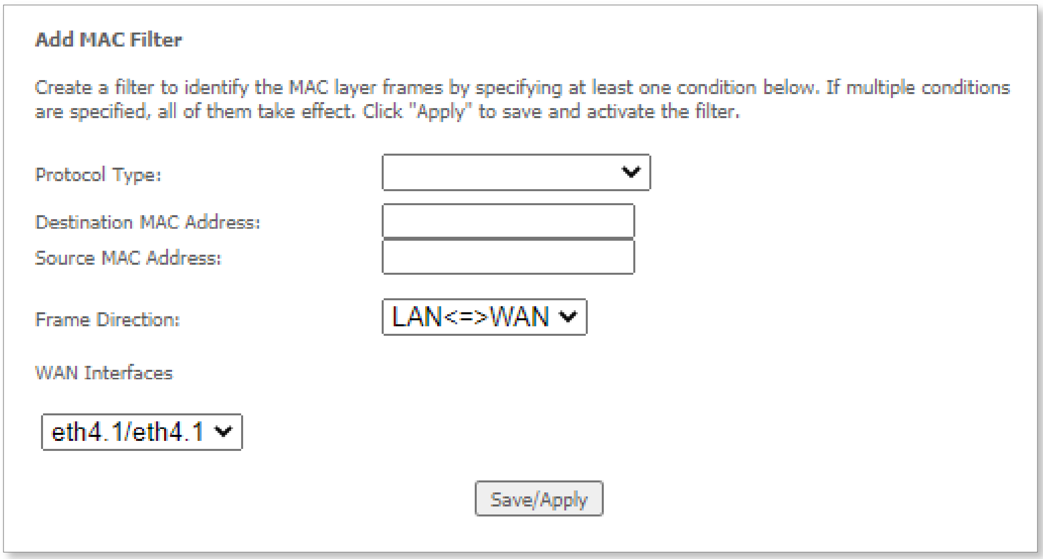
Interface	Policy	Change
eth4.1	FORWARD	□

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	Remove

Figure 77 – Security – MAC Filter list

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



Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction: LAN<=>WAN

WAN Interfaces

eth4.1/eth4.1

Figure 78 – Security – MAC Filter settings

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.

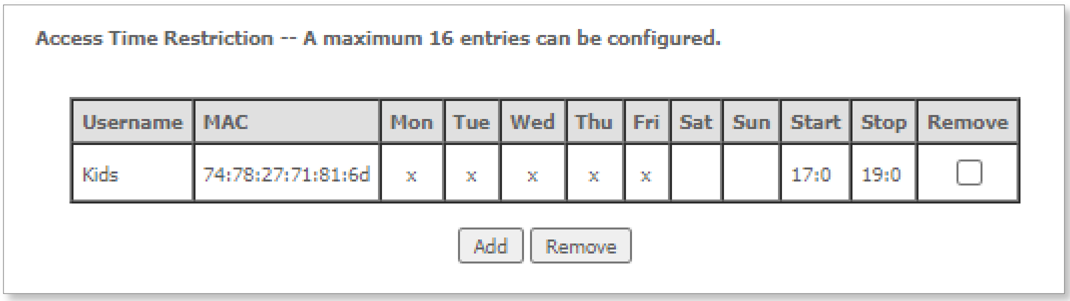
Click **Apply/Save** to save the new MAC filtering configuration.

Parental Control

The Parental Control feature allows you to take advanced measures to ensure the computers connected to the LAN are used only 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.

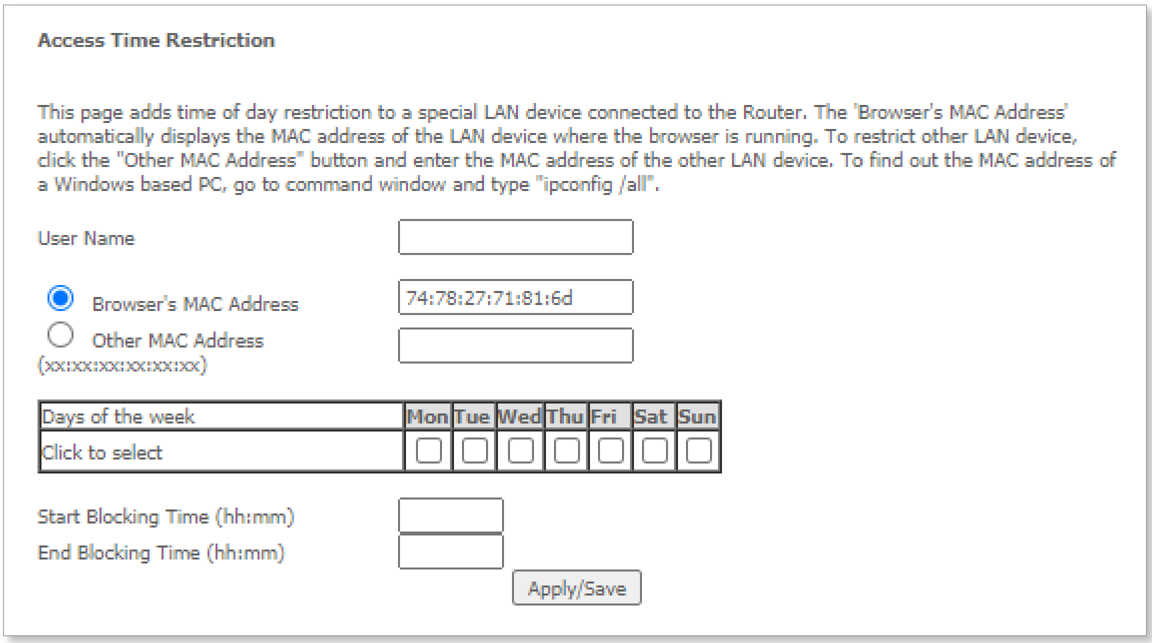


Access Time Restriction -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
Kids	74:78:27:71:81:6d	x	x	x	x	x			17:0	19:0	□

Figure 79 – Advanced – Parental Control – Time Restriction

To add a time restriction rule, press the **Add** button. The following screen appears.



Access Time Restriction

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

User Name

● Browser's MAC Address 74:78:27:71:81:6d

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

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

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 80 – Advanced – Parental Control – Add Time Restriction

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 LAN device or network card.
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	Press the Apply/Save button to save a time restriction rule.

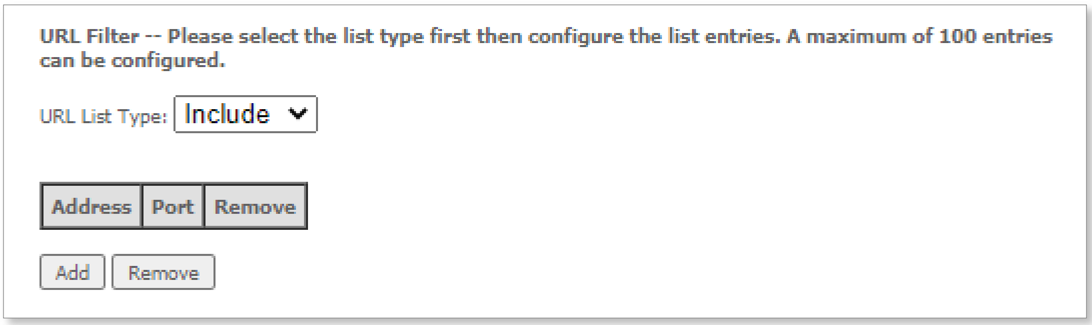
Table 13 – Advanced – Parental Control – Add Time Restriction Settings

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 CloudMesh Gateway.

⚠ Important – Parental Control URL blocking will not block apps used on smartphones such as Twitter or Facebook.
The Parental control URL blocking feature may not work with all browsers via HTTPS, or support certain TLS versions.

Select the Exclude (to block) or Include (to allow) option and then click Add to enter the URL you wish to add to the URL Filter list. Please note that the Include/Exclude function will not work on sites that use the HTTPS protocol.



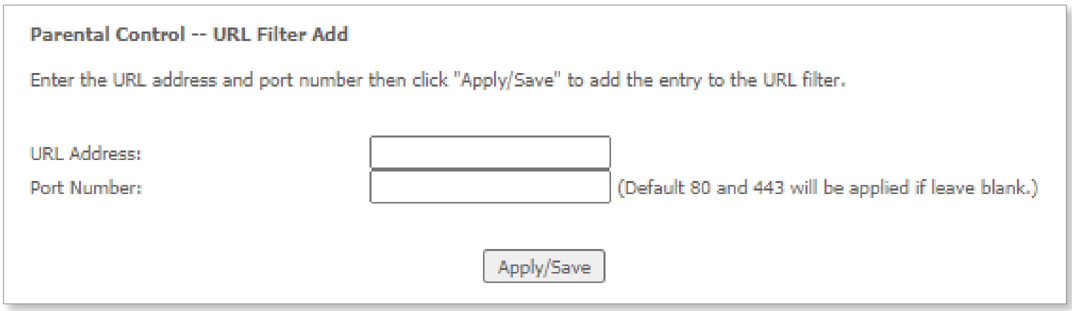
URL Filter -- Please select the list type first then configure the list entries. A maximum of 100 entries can be configured.

URL List Type: Include

Address	Port	Remove

Figure 81 – Advanced – Parental Control – URL Filter

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select the Apply/Save button.



Parental Control -- URL Filter Add

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

URL Address:
Port Number: (Default 80 and 443 will be applied if leave blank.)

Figure 82 – Advanced – Parental Control – Add URL Filter

Field	Description
URL Address	The URL address of the device you want to black list or white list.
Port Number	The Port Number (Default is 80).
Days of the Week	The days of the week for which the rules apply.
Start Time	The time of day when the restriction starts. (24 hour time: 00:00–23:59)
End time	The time of day when the restriction ends. (24 hour time: 00:00–23:59)
Apply/Save button	Press the Apply/Save button to save a time restriction rule.

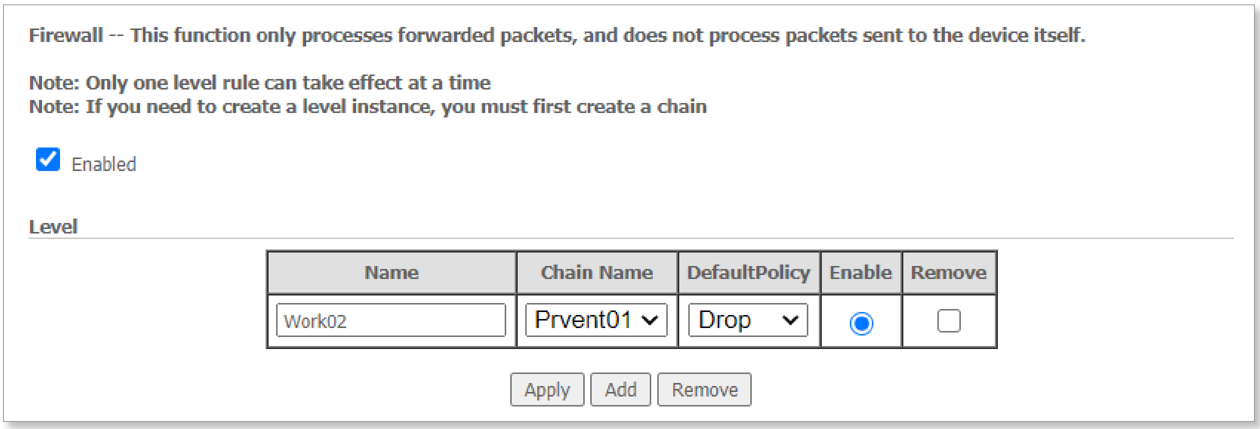
Table 14 – Advanced – Parental Control – Add URL Restriction Settings

Firewall

The **Firewall** feature should be ☑ **Enabled** in order to allow connections to specified internet addresses or to prevent connections.

Level Rule

Use the chains you have defined in the **Firewall - Add** page, see below, to apply to the **Level** rule to your firewall. Only one level rule can be applied at a time.



Firewall -- This function only processes forwarded packets, and does not process packets sent to the device itself.

Note: Only one level rule can take effect at a time
Note: If you need to create a level instance, you must first create a chain

☑ Enabled

Level

Name	Chain Name	DefaultPolicy	Enable	Remove
Work02	Prvent01	Drop	●	□

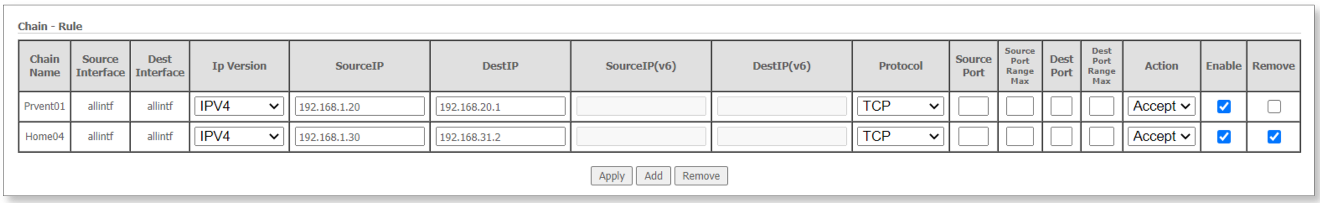
Figure 83 – Advanced – Firewall – Level Rule

The rules available for selection are listed in the **Chain – Rule** table, see next.

Chain – Rule

You can define a number of Chain Rules and retain them in the **Chain Rule** list.

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**).



Chain - Rule

Chain Name	Source Interface	Dest Interface	Ip Version	SourceIP	DestIP	SourceIP(v6)	DestIP(v6)	Protocol	Source Port	Source Port Range Max	Dest Port	Dest Port Range Max	Action	Enable	Remove
Prvent01	allintf	allintf	IPV4	192.168.1.20	192.168.20.1			TCP					Accept	☑	□
Home04	allintf	allintf	IPV4	192.168.1.30	192.168.31.2			TCP					Accept	☑	☑

Figure 84 – Advanced – Firewall – Chain – Rules table

Check ☑ **Enable** to use the Chain Rule to define a new Firewall, see next.

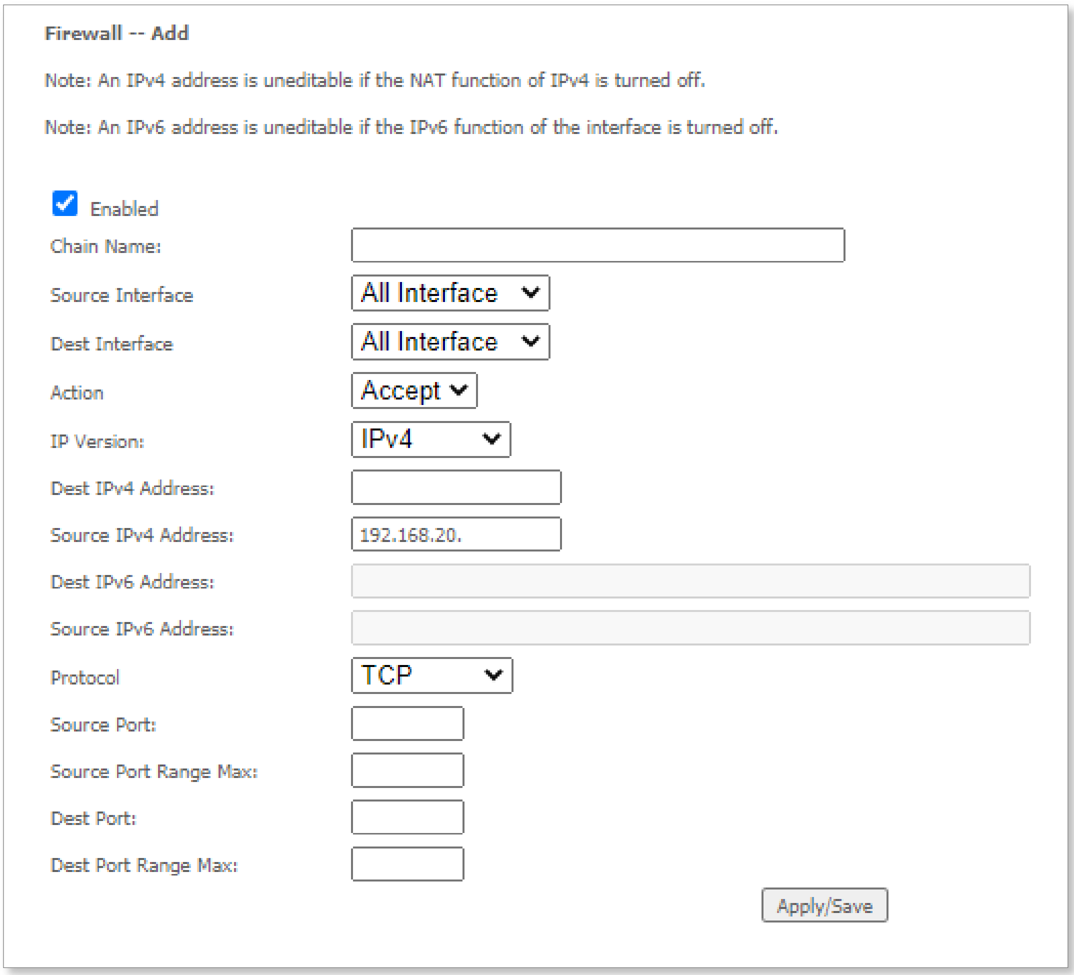
To permanently remove a Chain Rule from the list, select ☑ in the rule's **Remove** column and then click the **Remove** button to delete the rule from the list. Multiple rules can be selected and deleted at the same time.

Click the **Add** button to create a new Firewall rule, see next section.

Firewall – Add

Create individual rules for inclusion in the **Chain Rules** table.

Select ☑ **Enabled** to create a rule that can be used for a firewall.



Firewall -- Add

Note: An IPv4 address is uneditable if the NAT function of IPv4 is turned off.

Note: An IPv6 address is uneditable if the IPv6 function of the interface is turned off.

☑ Enabled

Chain Name:	
Source Interface	All Interface
Dest Interface	All Interface
Action	Accept
IP Version:	IPv4
Dest IPv4 Address:	
Source IPv4 Address:	192.168.20.
Dest IPv6 Address:	
Source IPv6 Address:	
Protocol	TCP
Source Port:	
Source Port Range Max:	
Dest Port:	
Dest Port Range Max:	

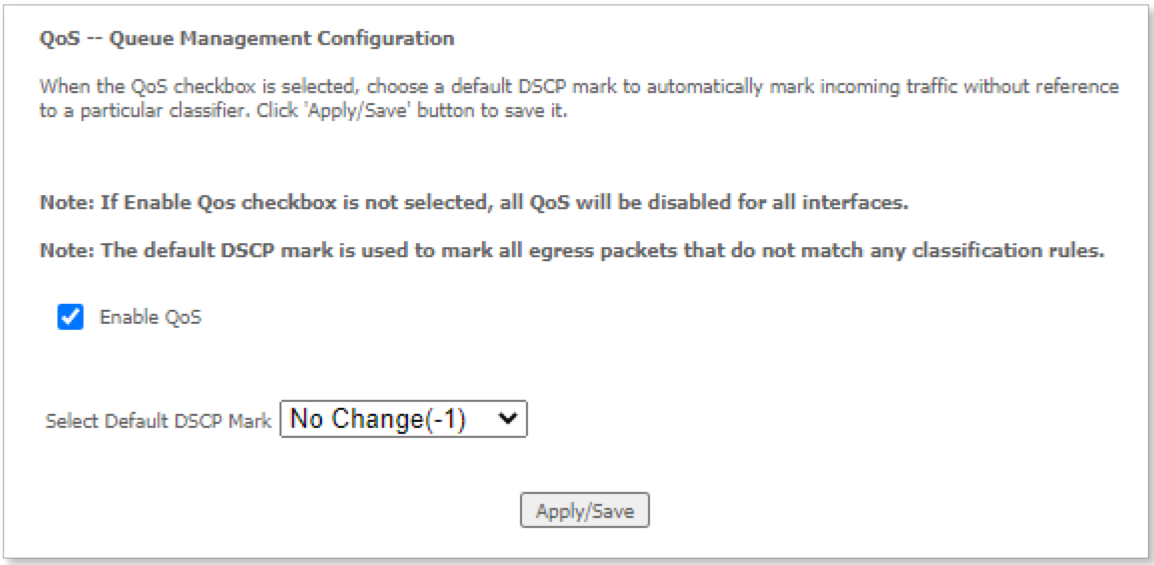
Figure 85 – Advanced – Firewall – Add

Field	Description
Chain Name	Add a meaningful name.
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	Press the Apply/Save button to save the firewall rule and add it to the Chain Rule table, see previous.

Table 15 – Advanced – Firewall – Add Firewall rule

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network traffic. This means that if you are streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video traffic.



QoS -- Queue Management Configuration

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

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

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

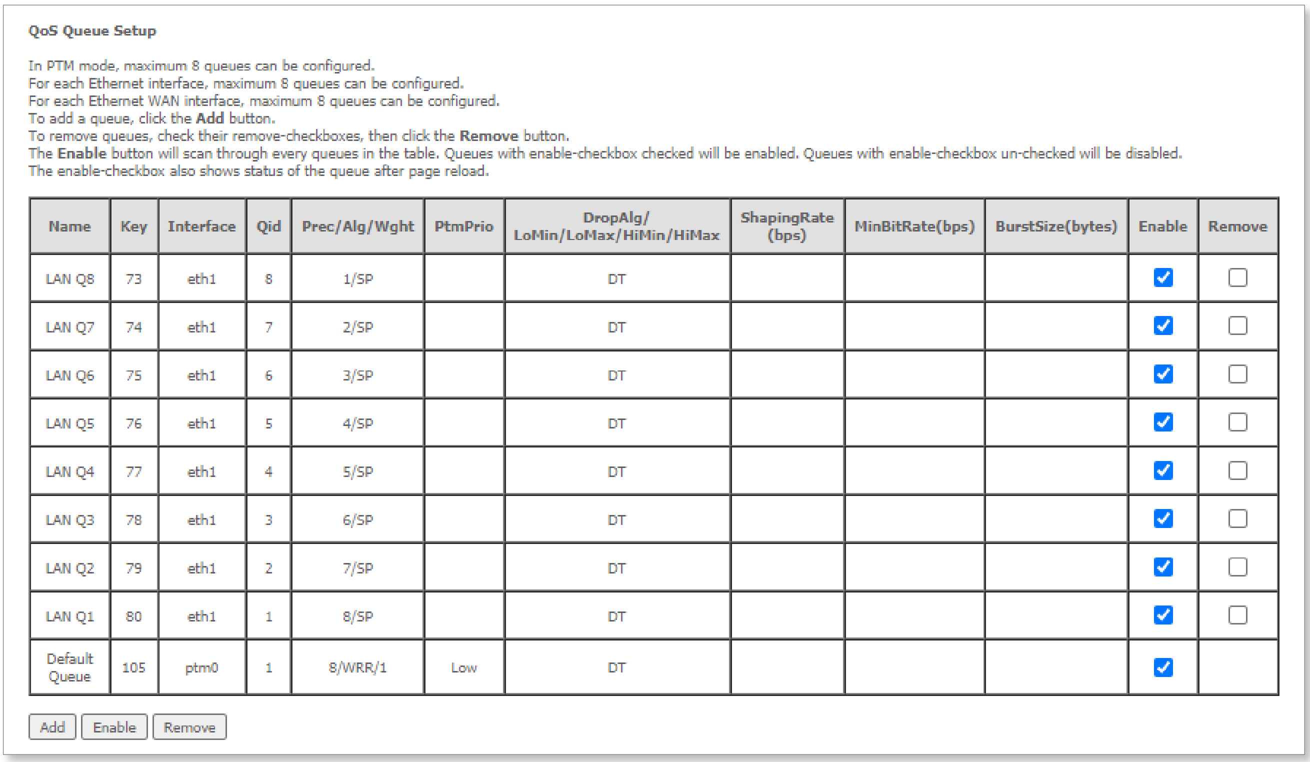
☑ Enable QoS

Select Default DSCP Mark: No Change(-1)

Figure 86 – Advanced – Enable QoS

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

QoS Queue



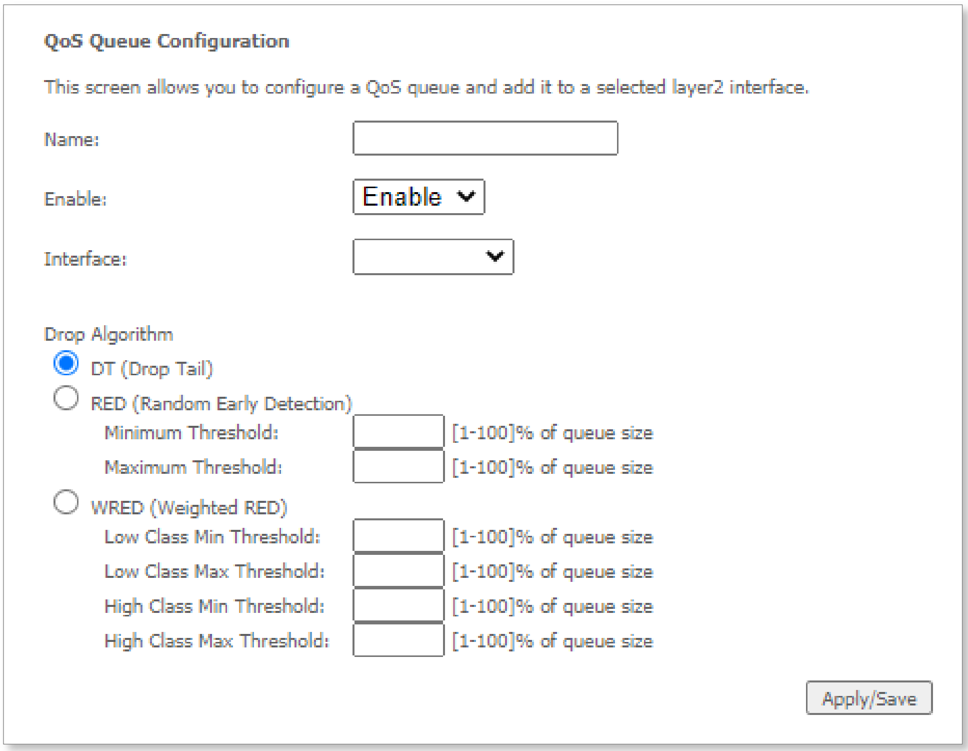
QoS Queue Setup

In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 8 queues can be configured.
For each Ethernet WAN interface, maximum 8 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.

Name	Key	Interface	Qid	Prec/Alg/Wght	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
LAN Q8	73	eth1	8	1/SP		DT				☑	☐
LAN Q7	74	eth1	7	2/SP		DT				☑	☐
LAN Q6	75	eth1	6	3/SP		DT				☑	☐
LAN Q5	76	eth1	5	4/SP		DT				☑	☐
LAN Q4	77	eth1	4	5/SP		DT				☑	☐
LAN Q3	78	eth1	3	6/SP		DT				☑	☐
LAN Q2	79	eth1	2	7/SP		DT				☑	☐
LAN Q1	80	eth1	1	8/SP		DT				☑	☐
Default Queue	105	ptm0	1	8/WRR/1	Low	DT				☑	

Figure 87 – Advanced – QoS Queue Setup

Click the Add button to add a QoS Queue. The following screen is displayed.



QoS Queue Configuration

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

Name:	
Enable:	Enable
Interface:	

Drop Algorithm

● DT (Drop Tail)

○ RED (Random Early Detection)

Minimum Threshold:		[1-100]% of queue size
Maximum Threshold:		[1-100]% of queue size

○ WRED (Weighted RED)

Low Class Min Threshold:		[1-100]% of queue size
Low Class Max Threshold:		[1-100]% of queue size
High Class Min Threshold:		[1-100]% of queue size
High Class Max Threshold:		[1-100]% of queue size

Figure 88 – Advanced – QoS – Add QoS Queue

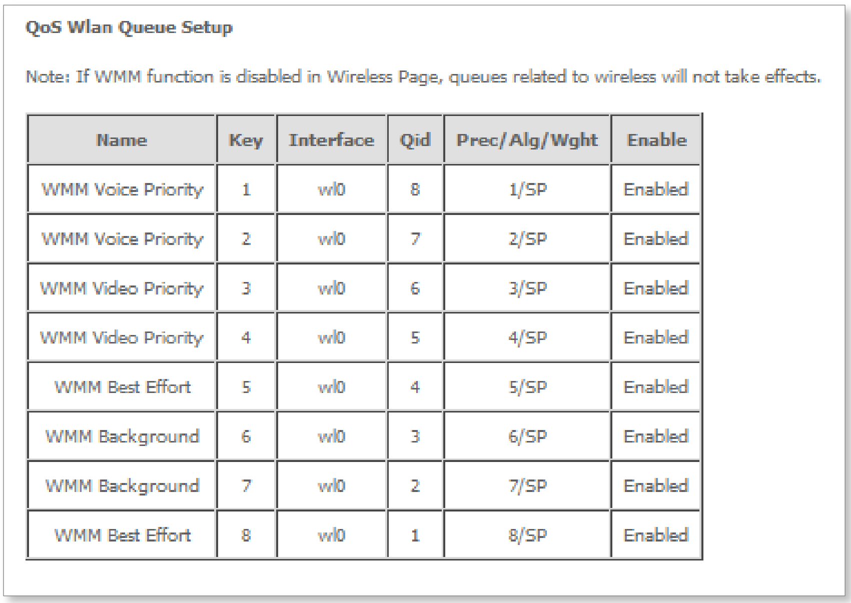
The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence.

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.



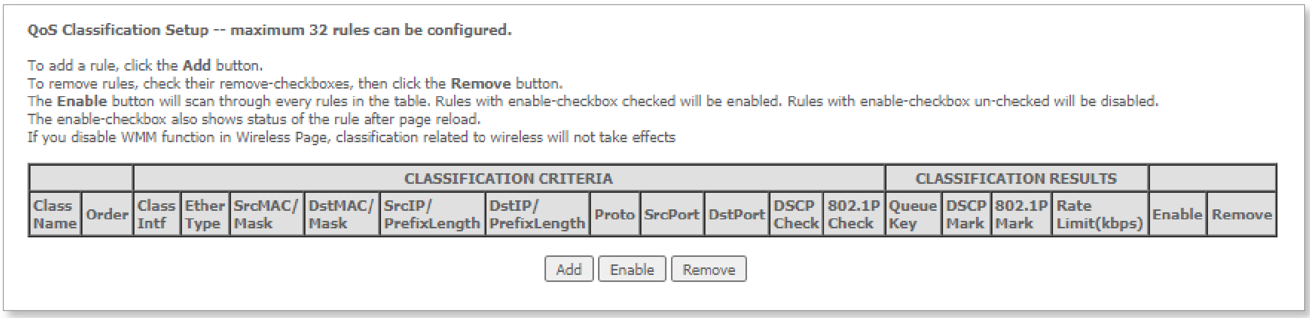
QoS Wlan Queue Setup

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 Voice Priority	1	wl0	8	1/SP	Enabled
WMM Voice Priority	2	wl0	7	2/SP	Enabled
WMM Video Priority	3	wl0	6	3/SP	Enabled
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled

Figure 89 – Advanced – QoS – WLAN Queue

QoS Classification



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

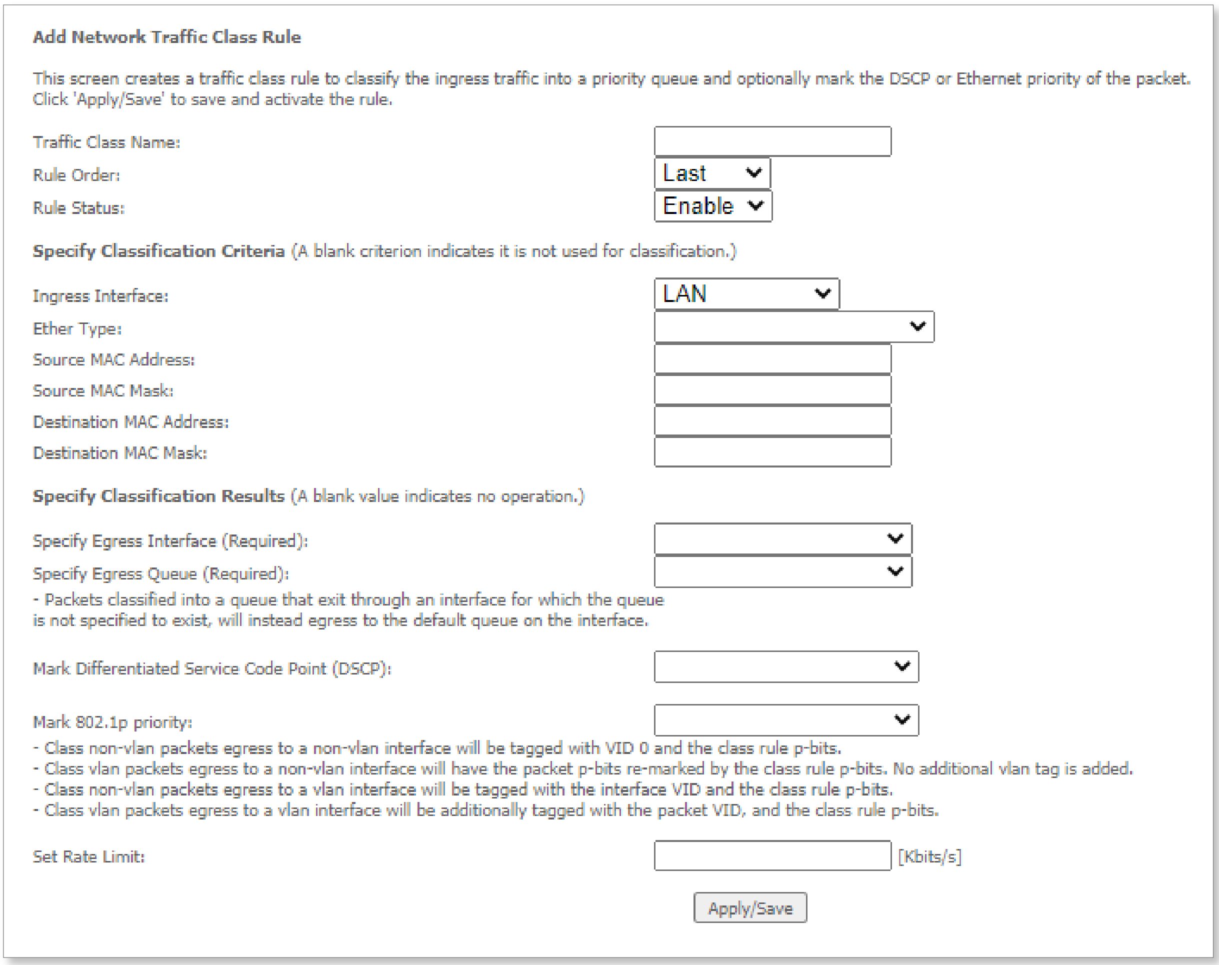
To add a rule, click the **Add** button.
To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The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

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

Figure 90 – Advanced – QoS Classification list

Click the **Add** button to configure network traffic classes.

The Add Network Traffic Class Rule page will display.



Add Network Traffic Class Rule

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

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

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

Ingress Interface:	LAN
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

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

Specify Egress Interface (Required):

Specify Egress Queue (Required):

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

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

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

Set Rate Limit: [Kbits/s]

Figure 91 – Advanced – QoS – Network Traffic Class settings

The above screen 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.

Click 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.

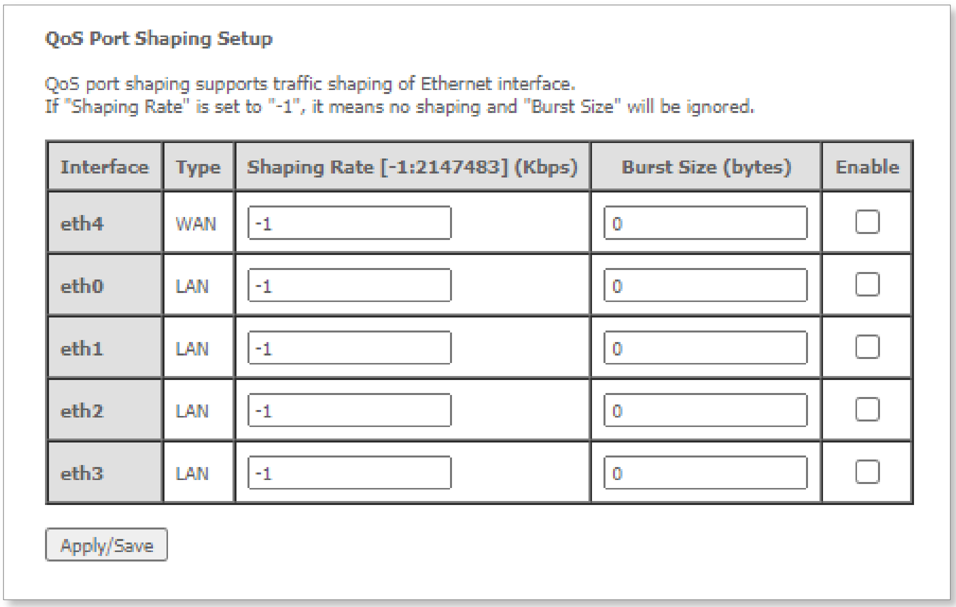
By configuring QoS Port Shaping with a Burst size, web pages are allowed to load using the burst speed, while continuous traffic such as file downloads will be shaped at a lower rate.

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 = 1 ms at the Gigabit Ethernet line rate.

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



QoS Port Shaping Setup

QoS port shaping supports traffic shaping of Ethernet interface.
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate [-1:2147483] (Kbps)	Burst Size (bytes)	Enable
eth4	WAN	-1	0	□
eth0	LAN	-1	0	□
eth1	LAN	-1	0	□
eth2	LAN	-1	0	□
eth3	LAN	-1	0	□

Figure 92 – QoS Port Shaping settings

Item	Description
Interface	Identifies the interface type.
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

Figure 93 – Advanced – QoS – Port Shaping settings

Note – 1 byte = 8 bits

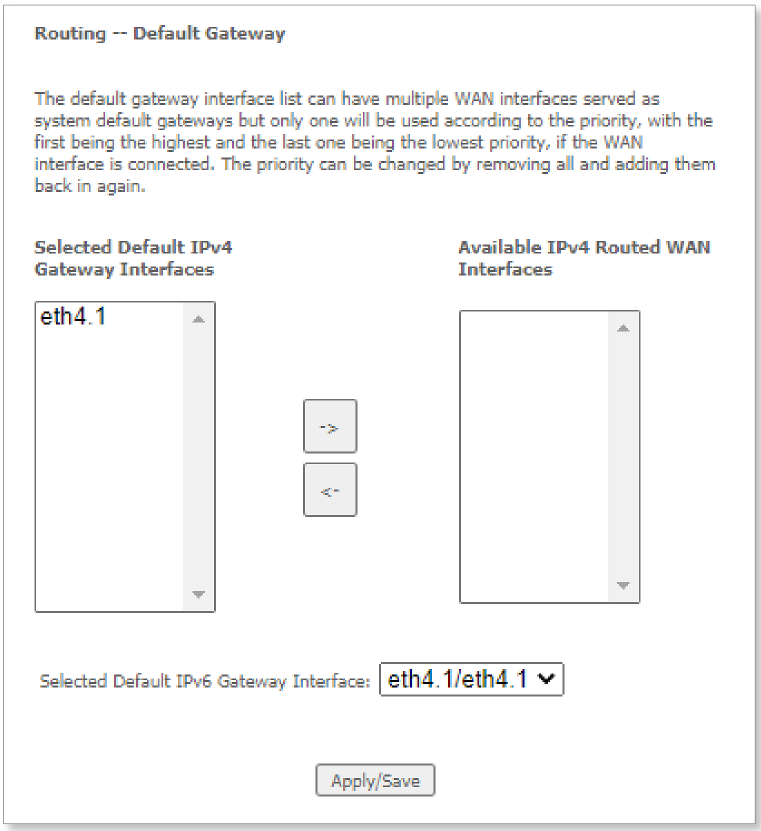
Routing

The Default Gateway, Static Route, Policy Routing and Dynamic Route settings can be found in the Routing option of the Advanced menu.

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.



Routing -- Default Gateway

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

Selected Default IPv4 Gateway Interfaces: eth4.1

Available IPv4 Routed WAN Interfaces

Selected Default IPv6 Gateway Interface: eth4.1/eth4.1

Figure 94 – Routing – Set Default Gateway

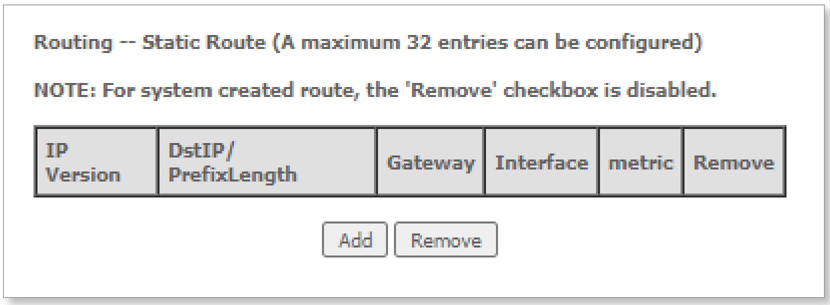
Use the arrow buttons to move the interfaces required as DNS Server interfaces to the left.

The interface highest on the list has the highest priority as a DNS server.

Click Apply/Save to commit your settings to the gateway.

Static Route

The Static Route screen displays the configured static routes. Click the Add or Remove buttons to change settings.



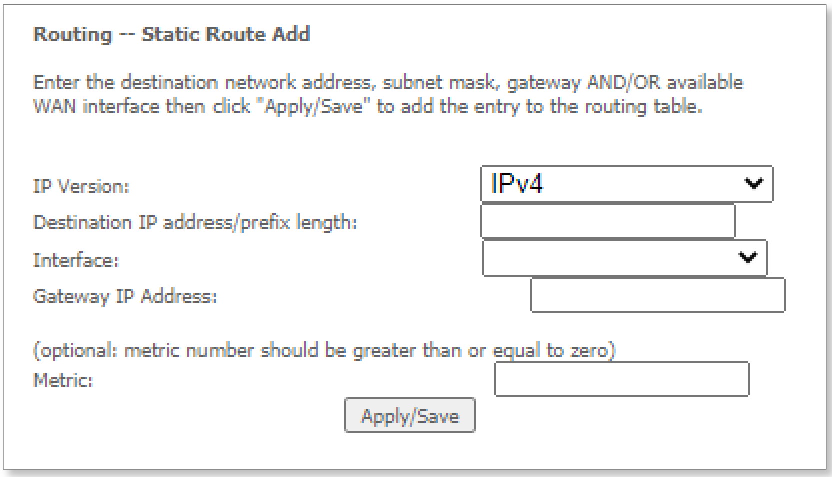
Routing -- Static Route (A maximum 32 entries can be configured)

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

IP Version	DstIP/ PrefixLength	Gateway	Interface	metric	Remove

Figure 95 – Routing – Static Route list

To add a static route rule click the Add button. The following screen is displayed.



Routing -- Static Route Add

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

IP Version: IPv4

Destination IP address/prefix length:

Interface:

Gateway IP Address:

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

Metric:

Figure 96 – Routing – Static Route configuration

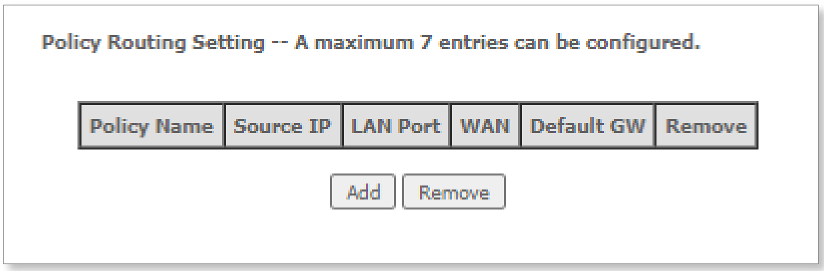
Select the IP Version from the drop-down menu, enter the Destination Network Address, select an Interface, and enter the Gateway IP Address.

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.

Then click Apply/Save to add the entry to the routing table.

Policy Routing

This function allows you to add policy rules to certain situations.

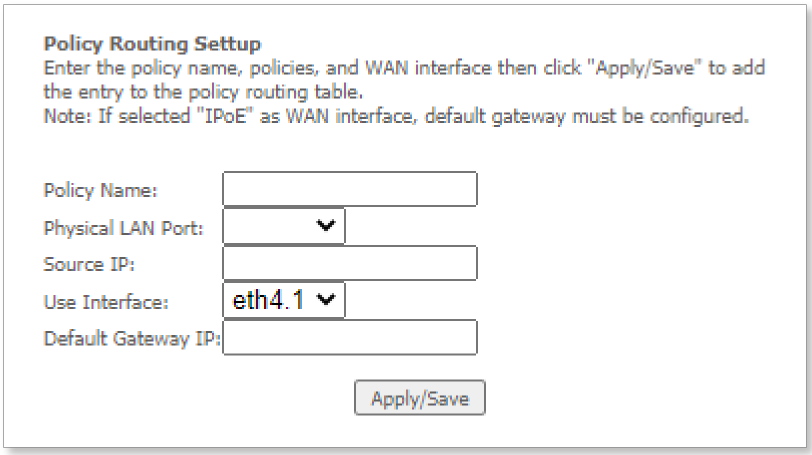


Policy Routing Setting -- A maximum 7 entries can be configured.

Policy Name	Source IP	LAN Port	WAN	Default GW	Remove

Figure 97 – Routing – Policy Routing list

Click the Add button to add a policy rule. The following screen is displayed.



Policy Routing Settup
Enter the policy name, policies, and WAN interface then click "Apply/Save" to add the entry to the policy routing table.
Note: If selected "IPoE" as WAN interface, default gateway must be configured.

Policy Name:	
Physical LAN Port:	
Source IP:	
Use Interface:	eth4.1
Default Gateway IP:	

Figure 98 – Advanced – Routing – Policy Route configuration

Enter the details into the provided fields. The table below describes each field.

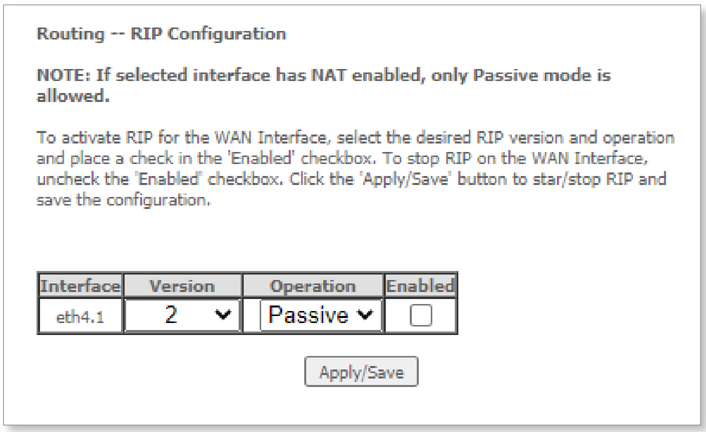
Field	Description
Policy Name	A user defined name for the policy route.
Physical LAN Port	The LAN port to be used for the policy.
Source IP	The IP address of the LAN device involved with the policy.
Use Interface	Select the Interface that the policy will employ.
Default Gateway IP	Enter the gateway address.
Apply/Save button	Click to save and apply your changes

Table 16 – Routing – Policy Route settings table

RIP

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

Attention – 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.



Routing -- RIP Configuration

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

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

Interface	Version	Operation	Enabled
eth4.1	2	Passive	□

Figure 99 – Routing – RIP list

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.

Table 17 – Routing – RIP settings

DNS

DNS Server

A DNS server is a server that contains a database of hostnames and their associated public IP addresses.

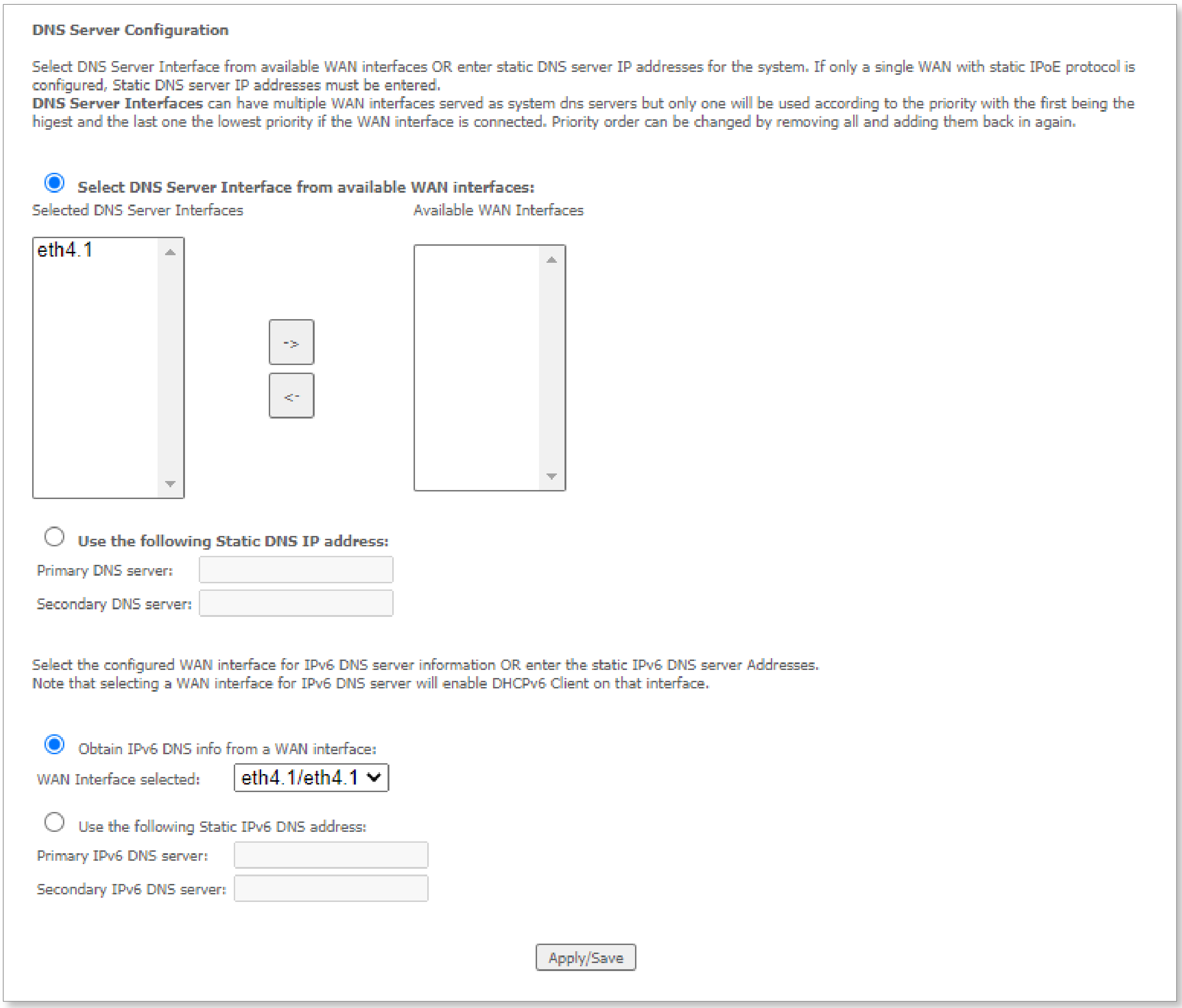
This server is used to resolve hostnames to a unique public IP address when requested.

When a user enters a URL e.g., www.casa-systems.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.



DNS Server Configuration

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

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

Selected DNS Server Interfaces: eth4.1

Available WAN Interfaces:

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

Primary DNS server:

Secondary DNS server:

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

● Obtain IPv6 DNS info from a WAN interface:

WAN Interface selected: eth4.1/eth4.1

○ Use the following Static IPv6 DNS address:

Primary IPv6 DNS server:

Secondary IPv6 DNS server:

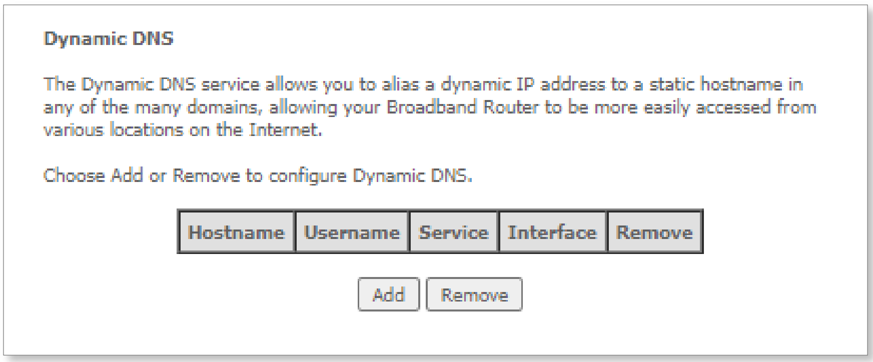
Figure 100 - DNS Server Configuration

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 18 – Routing – RIP settings

Dynamic DNS

When you have an Internet plan that provides a dynamic IP address, that is, an address which is dynamically assigned and changes each time you connect, an easy way to provide a permanent address is to use a Dynamic DNS service. There are both free and paid DDNS services available.



Dynamic DNS

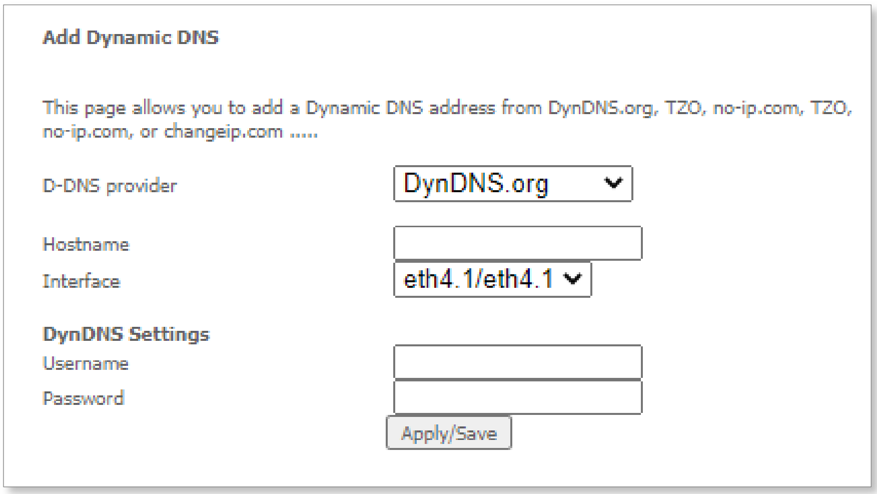
The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Broadband Router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure 101 – Dynamic DNS list

To add a new Dynamic DNS profile, click the **Add** button. The Add Dynamic DNS screen is displayed.



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org, TZO, no-ip.com, TZO, no-ip.com, or changeip.com .....

D-DNS provider: DynDNS.org

Hostname:

Interface: eth4.1/eth4.1

DynDNS Settings

Username:

Password:

Figure 102 – Add Dynamic DNS

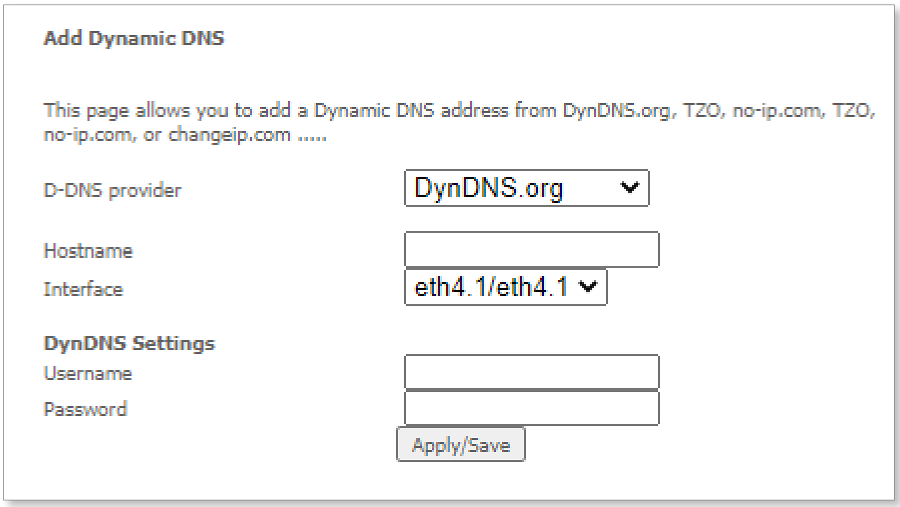
1 From the **D-DNS provider** drop-down list, select your Dynamic DNS provider.

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

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

4 Enter the **Username** and **Password** for your dynamic DNS account.

5 Click **Apply/Save**.



Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org, TZO, no-ip.com, TZO, no-ip.com, or changeip.com .....

D-DNS provider: DynDNS.org

Hostname:

Interface: eth4.1/eth4.1

DynDNS Settings

Username:

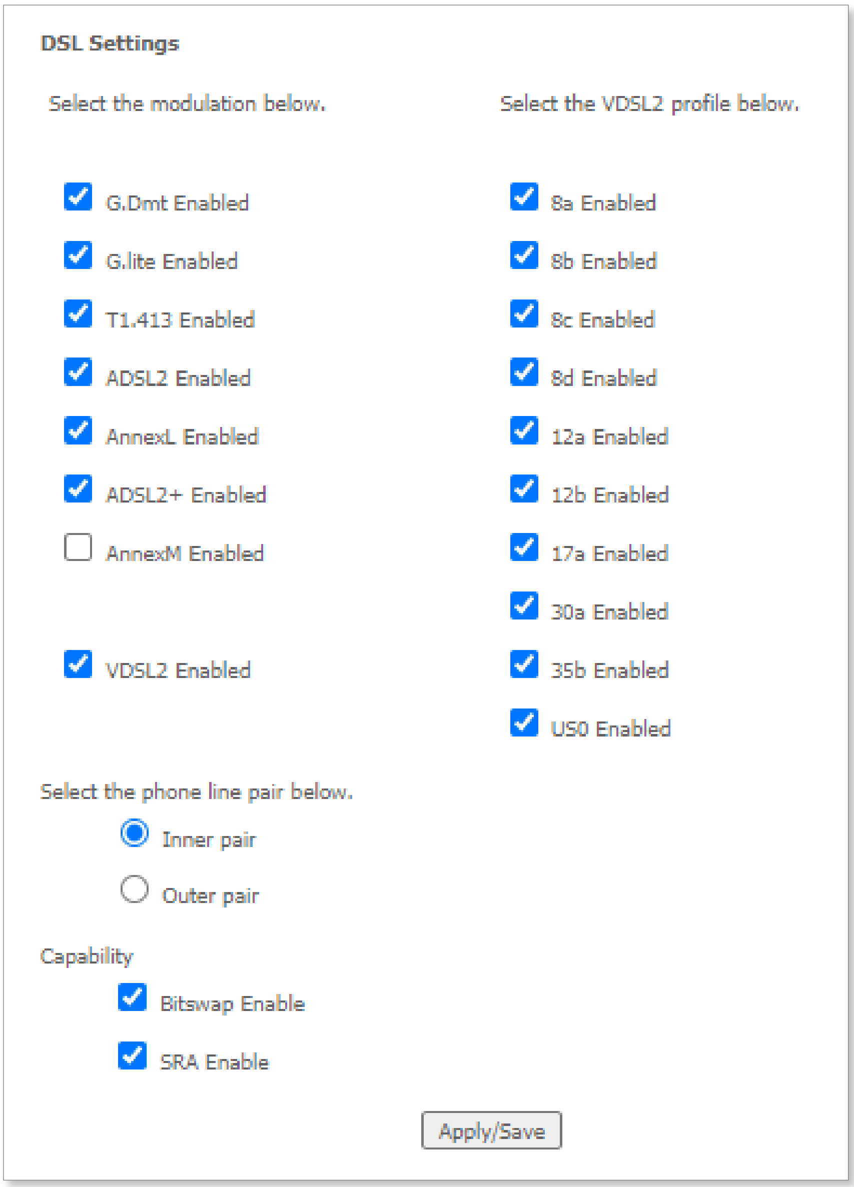
Password:

Figure 103 – Add Dynamic DNS

DSL

This page allows you to modify the DSL modulation settings on the unit. By changing the settings, you can specify which DSL modulation that the gateway will use.

Not all modulation types are support by your local DSLAM equipment, check with your ISP for supported modulation types.



DSL Settings

Select the modulation below.

☑ G.Dmt Enabled
☑ G.lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled
☑ VDSL2 Enabled

Select the VDSL2 profile below.

☑ 8a Enabled
☑ 8b Enabled
☑ 8c Enabled
☑ 8d Enabled
☑ 12a Enabled
☑ 12b Enabled
☑ 17a Enabled
☑ 30a Enabled
☑ 35b Enabled
☑ US0 Enabled

Select the phone line pair below.

● Inner pair
○ Outer pair

Capability

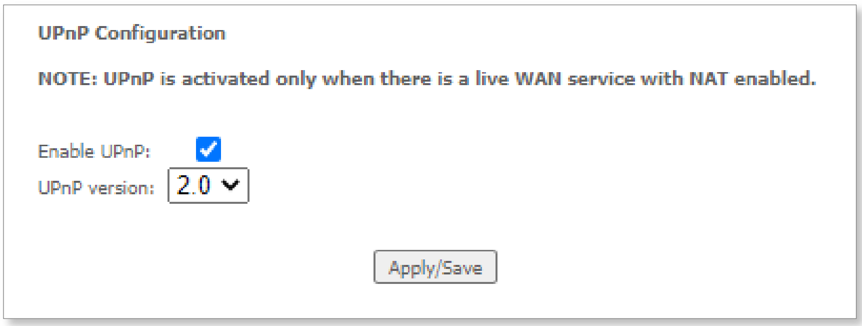
☑ Bitswap Enable
☑ SRA Enable

Figure 104 – DSL settings page

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.

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



UPnP Configuration

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

Enable UPnP: ☑

UPnP version: 2.0

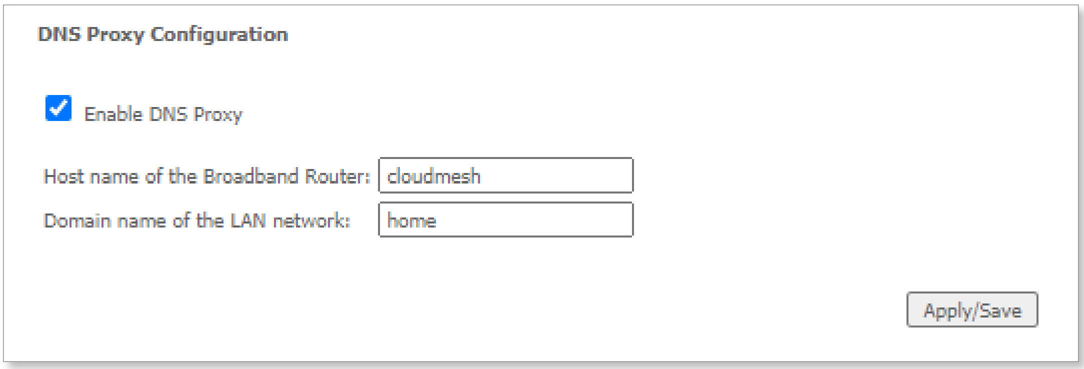
Figure 105 – UPnP activation page

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

DNS Proxy

You can define a personnalised, 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. Click Apply/Save to continue.



DNS Proxy Configuration

☑ Enable DNS Proxy

Host name of the Broadband Router: cloudmesh

Domain name of the LAN network: home

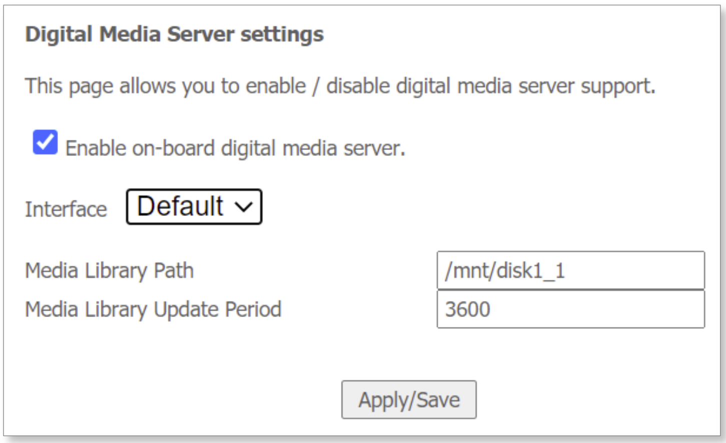
Figure 106 – DNS Proxy activation page

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://cloudmesh.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 digital media server. This means you can have digital media stored on an external USB hard drive connected to the CloudMesh Gateway and the gateway will make it accessible to other devices on your network.



Digital Media Server settings

This page allows you to enable / disable digital media server support.

☑ Enable on-board digital media server.

Interface: Default

Media Library Path: /mnt/disk1_1

Media Library Update Period: 3600

Figure 107 – DLNA setting page

1 Select ☑ Enable on-board digital media server

2 use the drop-down list to select the Interface.

3 In the Media Library Path field, enter the path to the media.

4 In the Media Library Update Period field a time period in seconds between media library updates. The default is 3600 seconds (60 hours).

5 Click the Apply/Save button when you have finished.

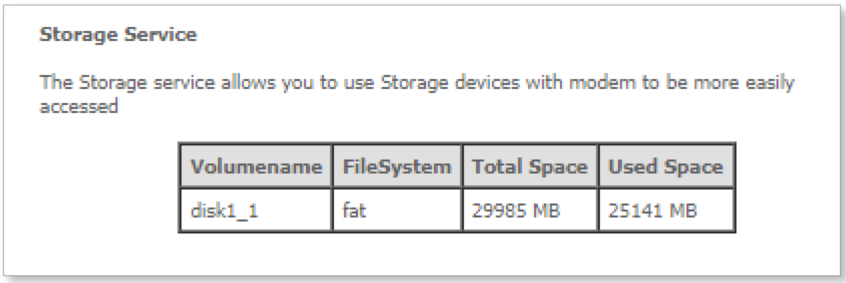
Storage Service

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

⚠ Important – Due to heightened security concerns, the most recent versions of some operating systems have disabled SAMBA (SMB) v1 by default. If this applies to your operating system, you may have to enable SAMBA (SMB) v1 on your operating system and then restart before this service will work.

Storage Device Info

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



Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed

Volumename	FileSystem	Total Space	Used Space
disk1_1	fat	29985 MB	25141 MB

Figure 108 – Storage Device Info list

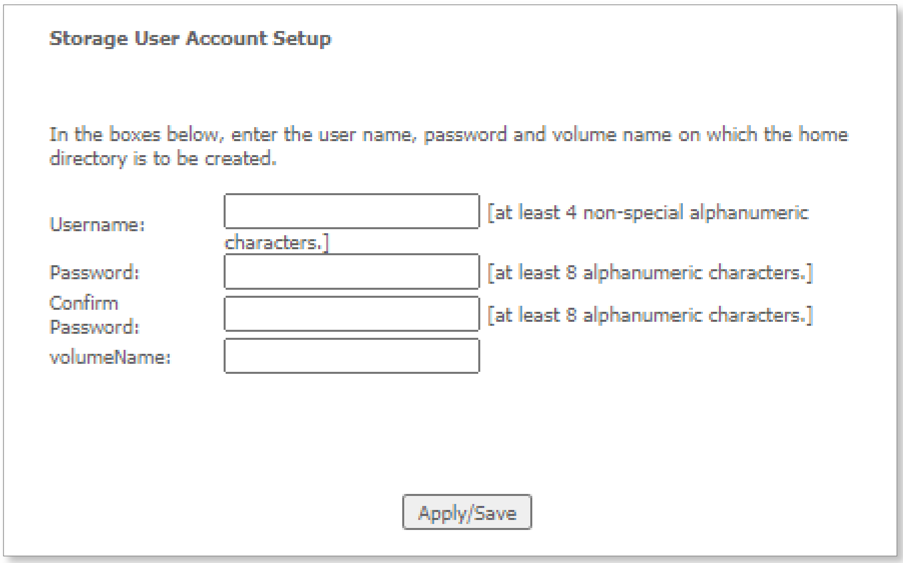
User Accounts

User accounts are used to restrict access to the attached USB Storage device.

To delete a User account entry, click the Remove checkbox next to the selected account entry and click Remove.

Click Add to create a user account.

Adding an account allows the creation of specific user accounts with a password to further control access permissions. To add an account, click the Add button and then enter the desired username and password for the account.



Storage User Account Setup

In the boxes below, enter the user name, password and volume name on which the home directory is to be created.

Username: [at least 4 non-special alphanumeric characters.]

Password: [at least 8 alphanumeric characters.]

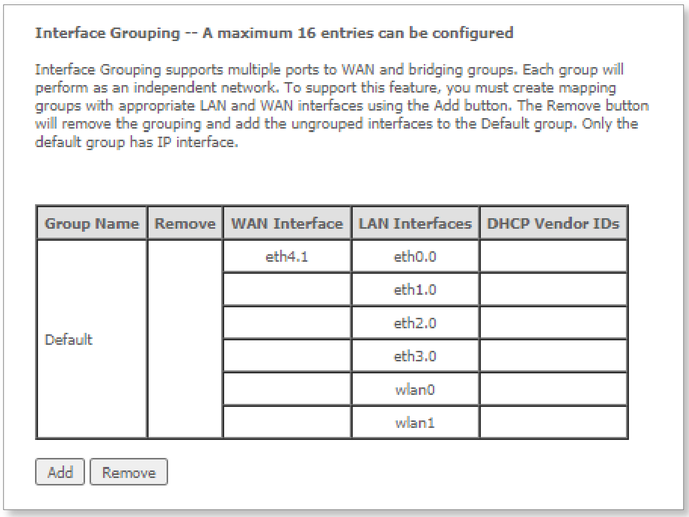
Confirm Password: [at least 8 alphanumeric characters.]

volumeName:

Figure 109 – Storage User Account Setup page

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.



Interface Grouping -- A maximum 16 entries can be configured

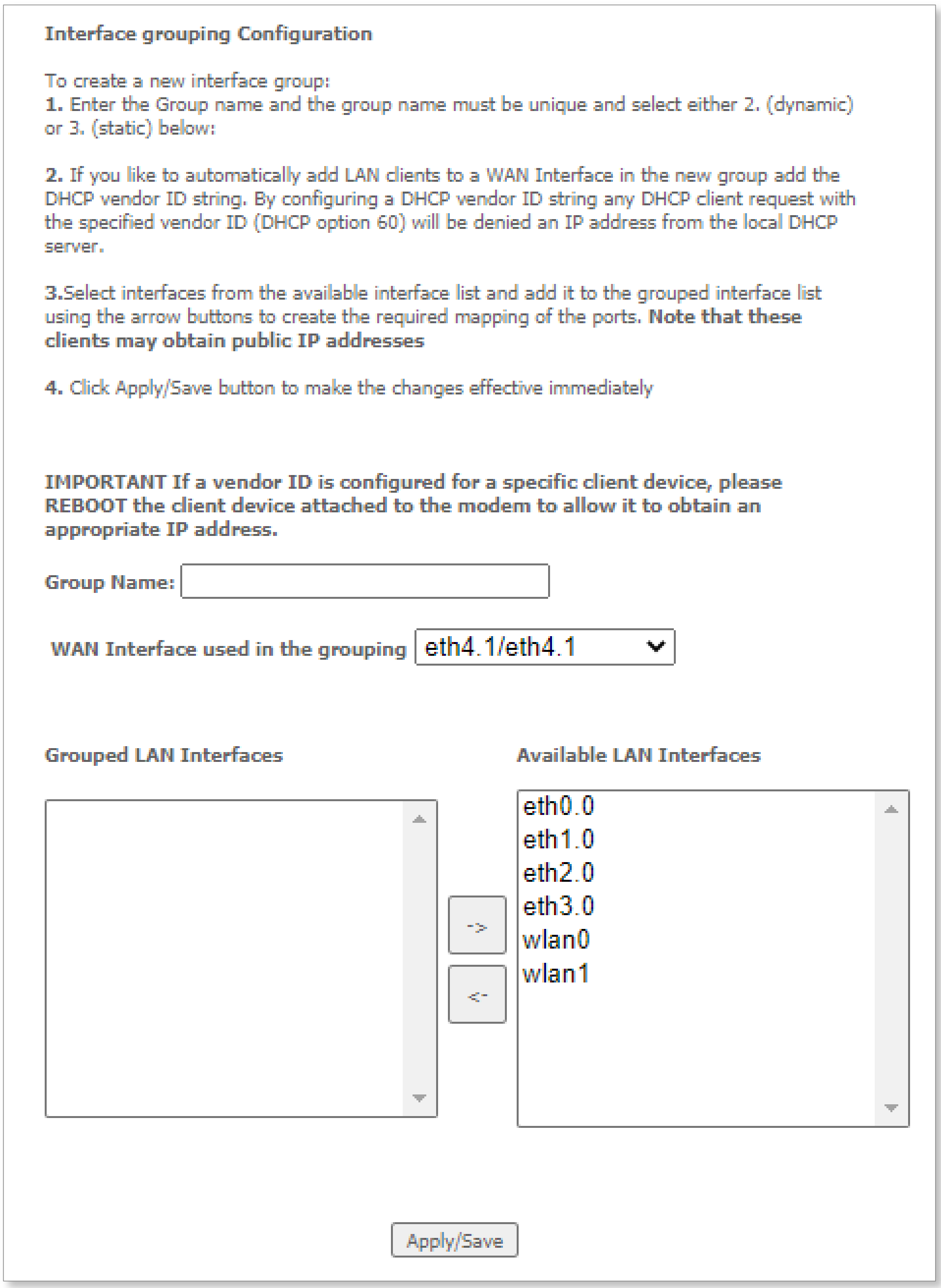
Interface Grouping supports multiple ports to WAN and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped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

Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Default		eth4.1	eth0.0	
			eth1.0	
			eth2.0	
			eth3.0	
			wlan0	
			wlan1	

Figure 110 – Interface Grouping list

Click **Add** to create an Interface group, see next section.

To delete an Interface group entry, select the ☑ **Enable** checkbox next to the selected group entry and click the **Remove** button.



Interface grouping Configuration

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

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

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

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

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

Group Name:

WAN Interface used in the grouping eth4.1/eth4.1

Grouped LAN Interfaces

Available LAN Interfaces

eth0.0
eth1.0
eth2.0
eth3.0
wlan0
wlan1

Figure 111 – Interface Grouping configuration

Enter a group name and then use the arrow buttons to select which interfaces you wish to group.

Click Apply/Save to save the Interface grouping configuration settings.

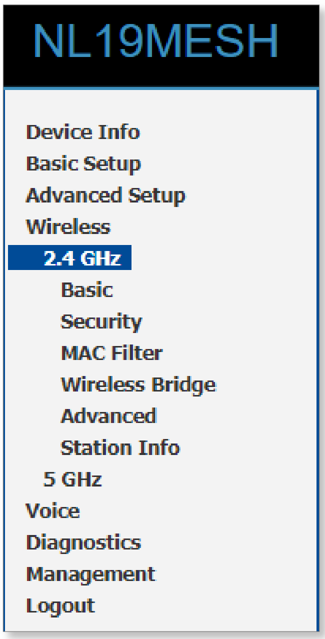
Wireless

Wi-Fi 2.4GHz / Wi-Fi 5GHz

The CloudMesh Gateway allows you to maintain separate wireless settings for both 2.4GHz and 5GHz wireless services.

Select the service you will use (or both) and separately configure them using nearly identical configuration pages:

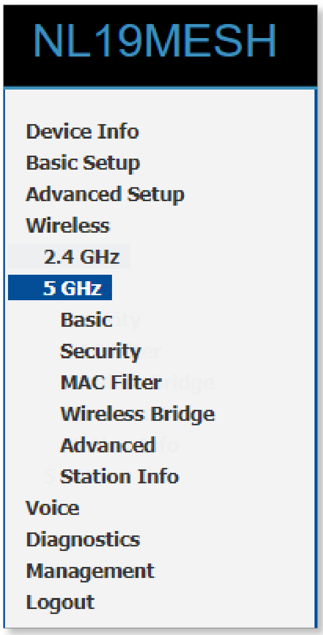
2.4 GHz Wireless Configuration pages



NL19MESH

- Device Info
- Basic Setup
- Advanced Setup
- Wireless
  - 2.4 GHz
    - Basic
    - Security
    - MAC Filter
    - Wireless Bridge
    - Advanced
    - Station Info
  - 5 GHz
- Voice
- Diagnostics
- Management
- Logout

5 GHz Wireless Configuration pages



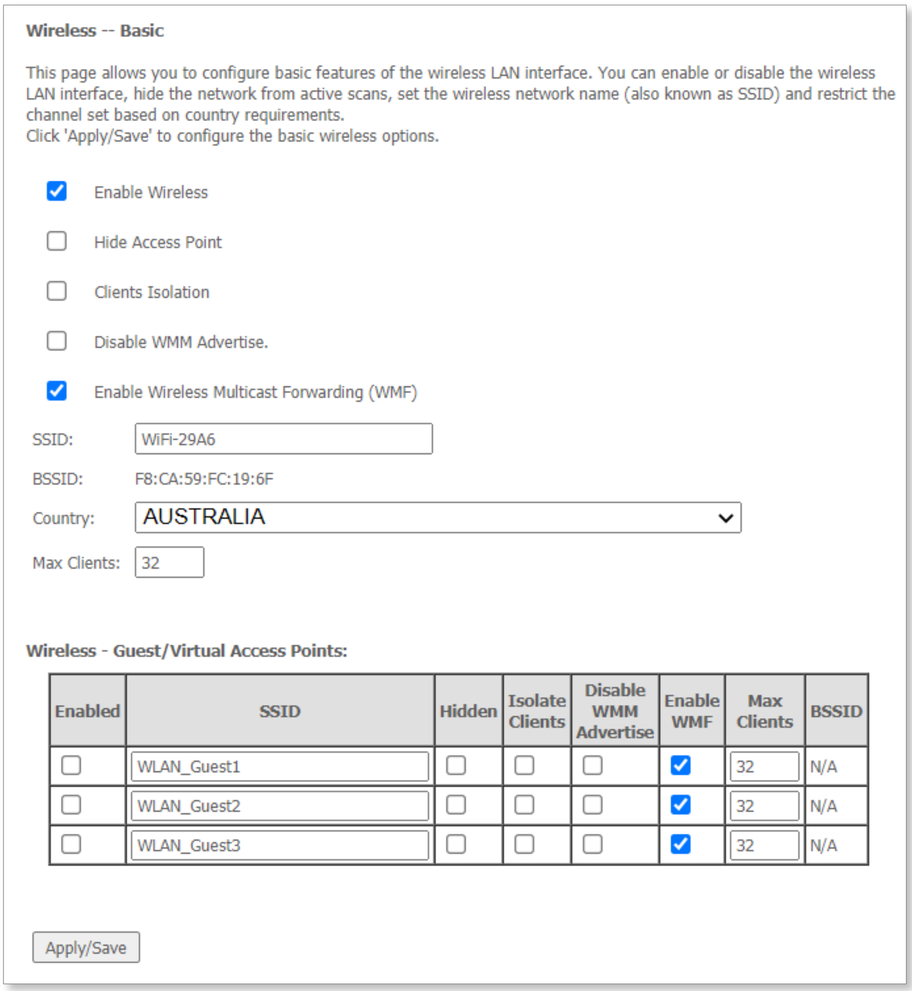
NL19MESH

- Device Info
- Basic Setup
- Advanced Setup
- Wireless
  - 2.4 GHz
  - 5 GHz
    - Basic
    - Security
    - MAC Filter
    - Wireless Bridge
    - Advanced
    - Station Info
- Voice
- Diagnostics
- Management
- Logout

Only the Advanced configuration page contains settings that are different for 5GHz wireless services.

Basic

The **Basic** configuration page allows you to enable the wireless network and configure its basic settings.



Wireless -- Basic

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

☑ Enable Wireless

□ Hide Access Point

□ Clients Isolation

□ Disable WMM Advertise.

☑ Enable Wireless Multicast Forwarding (WMF)

SSID:	WiFi-29A6
BSSID:	F8:CA:59:FC:19:6F
Country:	AUSTRALIA
Max Clients:	32

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Disable WMM Advertise	Enable WMF	Max Clients	BSSID
□	WLAN_Guest1	□	□	□	☑	32	N/A
□	WLAN_Guest2	□	□	□	☑	32	N/A
□	WLAN_Guest3	□	□	□	☑	32	N/A

Figure 112 – Wireless - Basic Configuration

The following parameters are available:

Parameter	Definition
Enable Wireless	Select ☑ to activate the wireless network function.
Hide Access Point	Select ☑ to hide the wireless network when an SSID scan is performed.
Clients Isolation	Select ☑ to prevent clients on the wireless network being able to access each other.
Disable WMM Advertise	Select ☑ to prevent the NL1901ACV advertising its WMM QoS function
Enable Multicast Forwarding (WMF)	Wireless Multicast Forwarding can reduce latency and improve throughput for wireless clients.
Max Clients	Enter the maximum number of wireless clients able to connect to the wireless network

Parameter	Definition
Wireless Guest / Virtual Access Points	Select ☑ to enable a separate Wireless Guest network. For each Guest network enter the same options as are available in the top of this page for the main system wireless network.

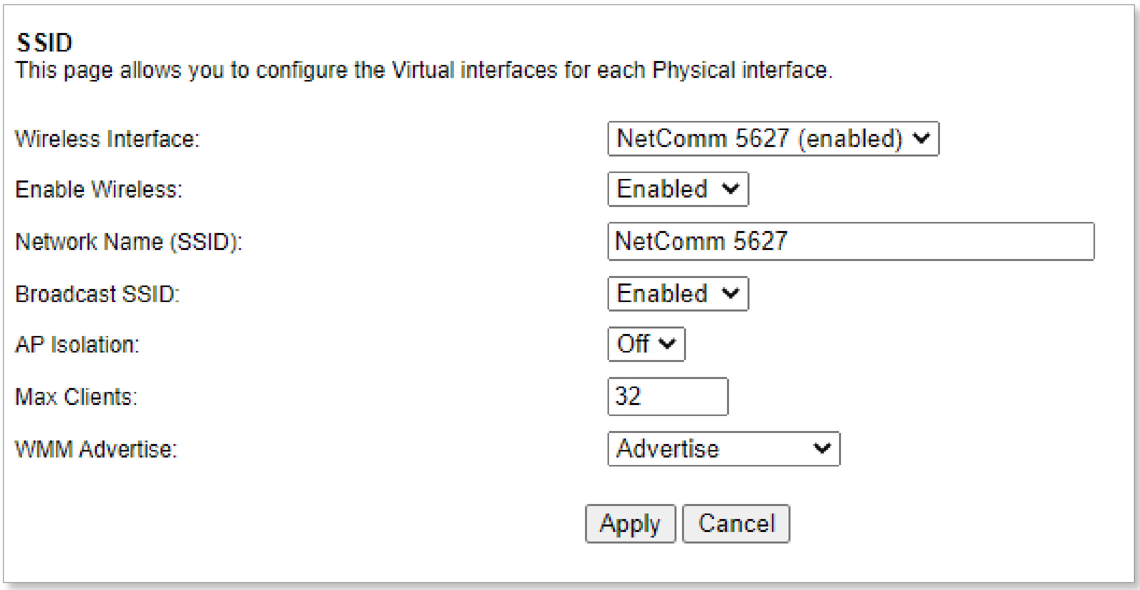
Table 19 – Basic Wireless settings table

Click the Apply/Save button to save the new wireless configuration settings.

Note – Hiding the network may lead to connection problems, a non-broadcast network not undetectable, and hiding a SSID is Security through obscurity.

SSID

The SSID configuration page allows you to enable the wireless network and configure its basic settings.



SSID
This page allows you to configure the Virtual interfaces for each Physical interface.

Wireless Interface:	NetComm 5627 (enabled)
Enable Wireless:	Enabled
Network Name (SSID):	NetComm 5627
Broadcast SSID:	Enabled
AP Isolation:	Off
Max Clients:	32
WMM Advertise:	Advertise

Figure 113 – Wireless – SSID Configuration

The following parameters are available:

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.
Max Clients	Set the maximum number of clients. The default value is 32.
AP Isolation	Select On to prevent clients on the wireless network being able to access each other.

Parameter	Definition
WMM Advertise	Select Do Not Advertise to prevent the CloudMesh Gateway advertising its WMM QoS function.

Table 20 – Basic Wireless settings table

Click **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, and hiding a SSID is Security through obscurity

Set same network name (SSID) and password for 2.4GHz/5GHz bands

The CloudMesh Gateway comes with identical settings for the SSID and password on the 2.4GHz and 5GHz bands. This allows the WiFi AutoPilot to intelligently steer your client devices to the best band. When changing the SSID of one of the bands, it is ideal to set the other band to have the same SSID and password for this reason.

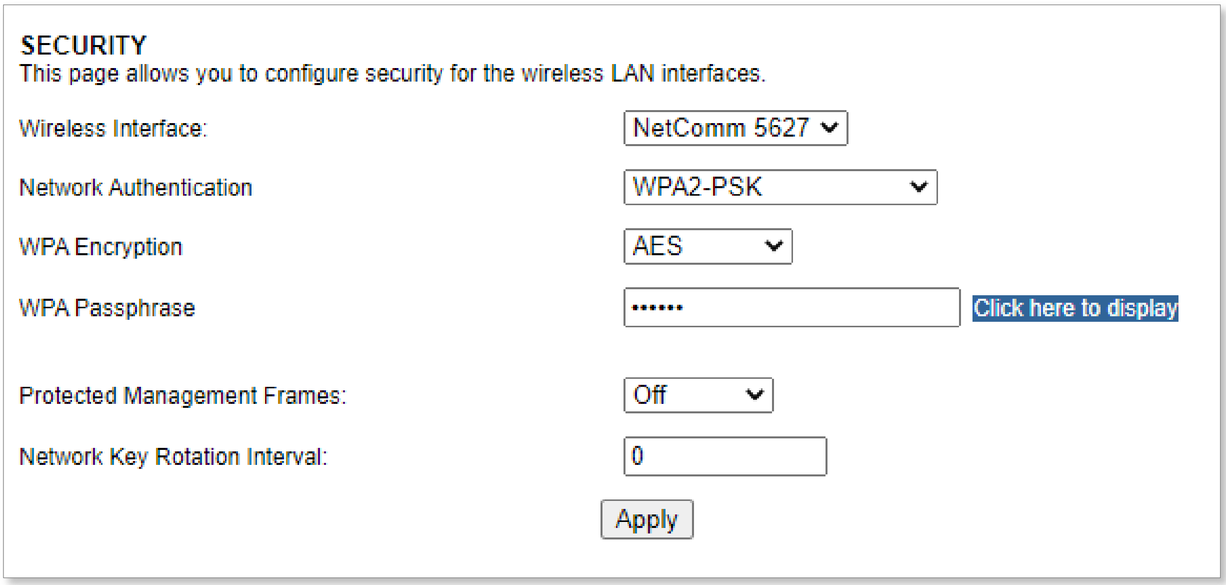
If you experience issues when both networks have the same name, consider setting separate names for the 2.4GHz and 5GHz bands.

Important – Changing the SSID and password names so that they are different for each band will stop the WiFi AutoPilot from being able to steer your clients between bands.

Security

The CloudMesh Gateway supports all encryptions within the 802.11 standard. The factory default is **WPA2-PSK**. The CloudMesh Gateway also supports: **WPA, WPA-PSK, WPA2-PSK, or WPA3-SAE**

You can also select to disable WPS mode.



SECURITY
This page allows you to configure security for the wireless LAN interfaces.

Wireless Interface:	NetComm 5627
Network Authentication	WPA2-PSK
WPA Encryption	AES
WPA Passphrase	••••••
Protected Management Frames:	Off
Network Key Rotation Interval:	0

Figure 114 – Wireless Security

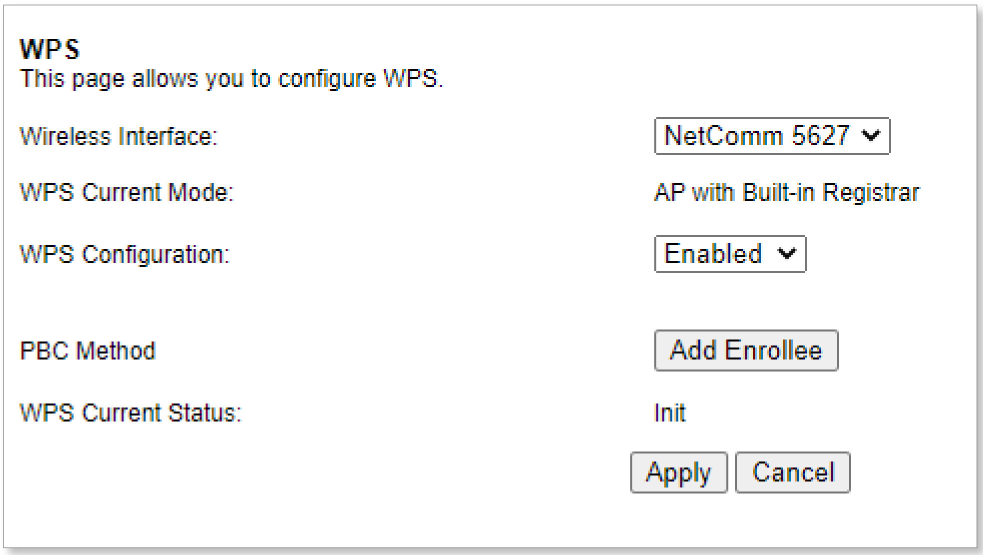
The following parameters are available:

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 default is: WPA2-PSK. The CloudMesh Gateway also supports: WPA, WPA-PSK, WPA2-PSK, or 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.
Apply/Save button	Click to save the new wireless security configuration settings \.

Table 21 – Wireless security settings table

WPS

WPS (Wi-Fi Protected Setup) is a network security standard that can be used to create a secure wireless home network.



WPS
This page allows you to configure WPS.

Wireless Interface: NetComm 5627

WPS Current Mode: AP with Built-in Registrar

WPS Configuration: Enabled

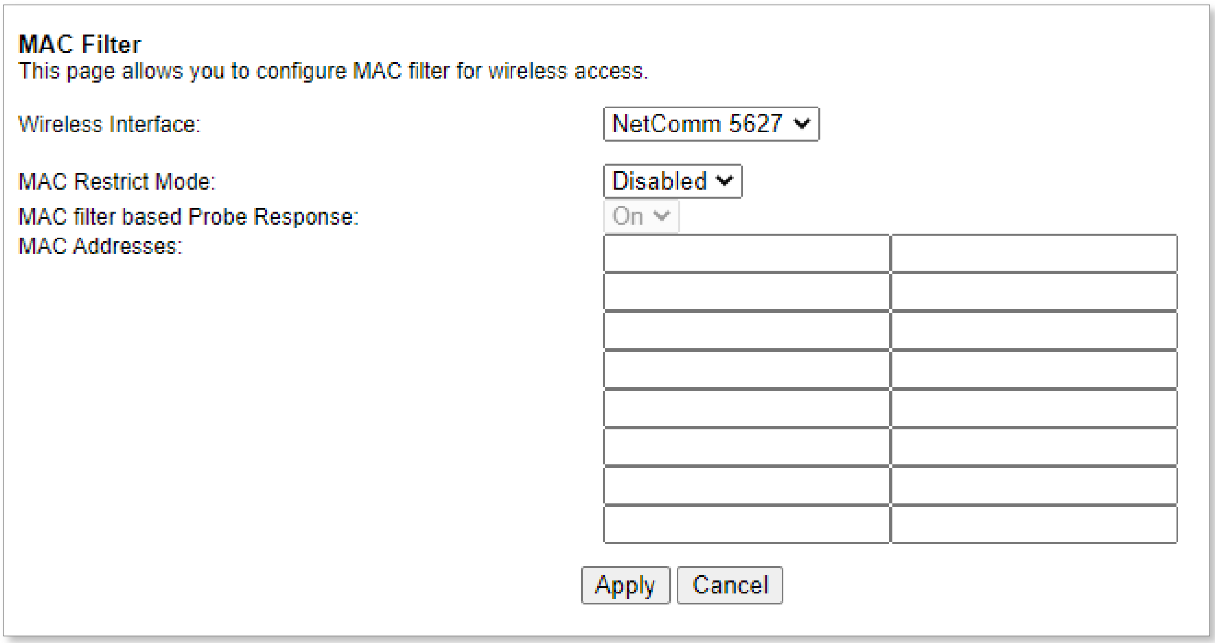
PBC Method

WPS Current Status: Init

Figure 115 - WPS configuration page

MAC Filter

MAC Filter 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 and select to either Allow or Deny access to the MAC addresses listed.



MAC Filter

This page allows you to configure MAC filter for wireless access.

Wireless Interface: NetComm 5627

MAC Restrict Mode: Disabled

MAC filter based Probe Response: On

MAC Addresses:

Figure 116 – Wireless – MAC Filter list

Enter a MAC address in the MAC Addresses fields provided then click Apply to add a MAC Address Filter.

To delete a MAC filter entry, click the Remove checkbox next to the selected filter entry and click Remove.

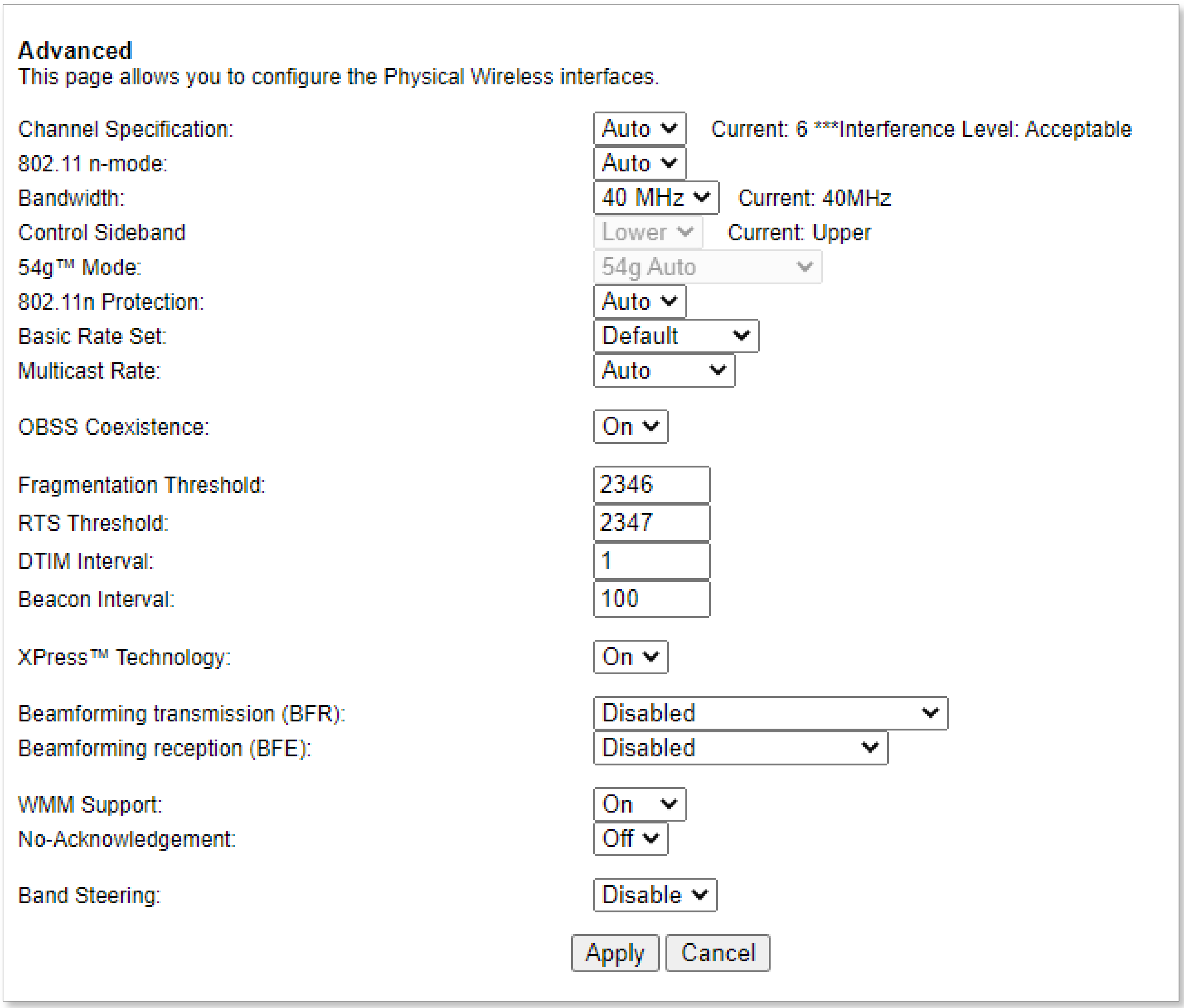
Enter MAC address in the format of aa:bb:cc:11:22:33

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 one, using MAC Filtering may lead to a false sense of security.

Advanced

⚠ Important – Changes to some of these settings may be overridden by the WiFi AutoPilot. WiFi AutoPilot constantly monitors the quality of your wireless network and adjusts settings as required to reduce wireless problems and improve your experience.

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



Advanced

This page allows you to configure the Physical Wireless interfaces.

Channel Specification:	Auto	Current: 6 ***Interference Level: Acceptable
802.11 n-mode:	Auto	
Bandwidth:	40 MHz	Current: 40MHz
Control Sideband	Lower	Current: Upper
54g™ Mode:	54g Auto	
802.11n Protection:	Auto	
Basic Rate Set:	Default	
Multicast Rate:	Auto	
OBSS Coexistence:	On	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
XPress™ Technology:	On	
Beamforming transmission (BFR):	Disabled	
Beamforming reception (BFE):	Disabled	
WMM Support:	On	
No-Acknowledgement:	Off	
Band Steering:	Disable	

Figure 117 – Wireless – Advanced configuration page

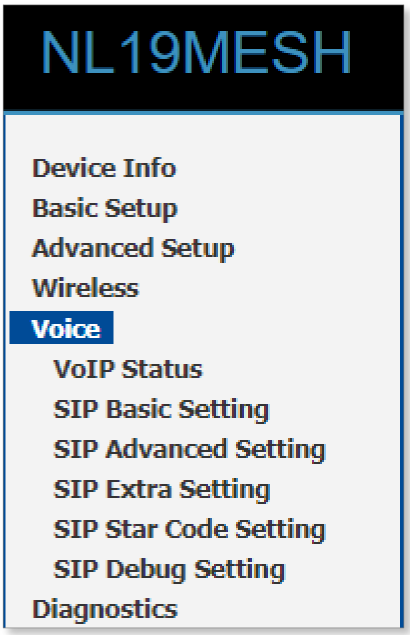
Click **Apply/Save** to save any changes to the wireless network settings configuration.

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
Bandwidth	Select the bandwidth for the network: 20MHz, 40MHz or 80MHz (available for 5G) In high wireless activity/interference environment, reduce the bandwidth to 20MHz for greater stability. The Current: bandwidth will be displayed on the right.
54g™ Mode (2.4 GHz and 802.11n disabled only)	For **54g mode**, you can select **54g Auto**, **54g Performance**, **54g LRS** or **802.11b 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.

Parameter	Definition
	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)	Select SU (Single-User) BFR to concentrate the transmission signal at the Gateway location. This results in a better signal and potentially better throughput.
Beamforming Reception (BFE)	Select SU (Single-User) BFE to concentrate the transmission signal at the Gateway location.
WMM Support	WMM (Wi-Fi Multimedia) maintains the priority of audio, video and voice, over other applications which are less time critical by ensuring that data from applications that require better throughput and performance are inserted in queues with higher priority. Select whether WMM is: Auto, On or Off Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
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 Daemon	Select Enable to detect if the client has the ability to use two bands. When enabled, the less congested 5GHz network is selected (by blocking the client's 2.4GHz network).

Table 22 -Wireless – Advanced configuration settings

Voice



The **Voice** menu provides a variety of options for configuring the gateway the VoIP settings of the CloudMesh Gateway.

Backup settings

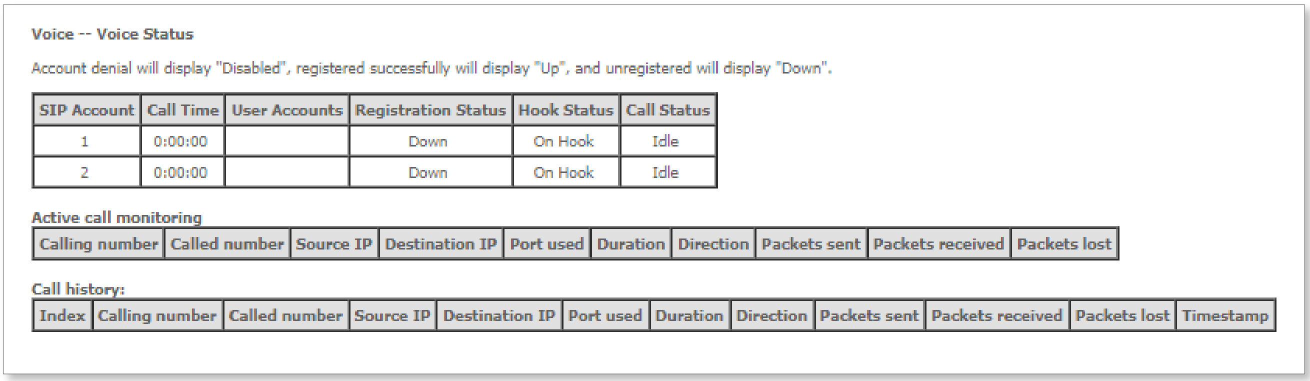
To make a backup file of your current configuration including the VoIP and SIP settings which you can use to restore those settings, go to **Management > Settings > Backup** to create a backup file.

Go to **Management > Settings > Update** to retrieve the backup file and reapply its settings.

For more information on backing up and restoring your current settings, go to the Management > Settings section of this gudie on page **Error! Bookmark not defined.**.

VoIP Status

The **VoIP 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

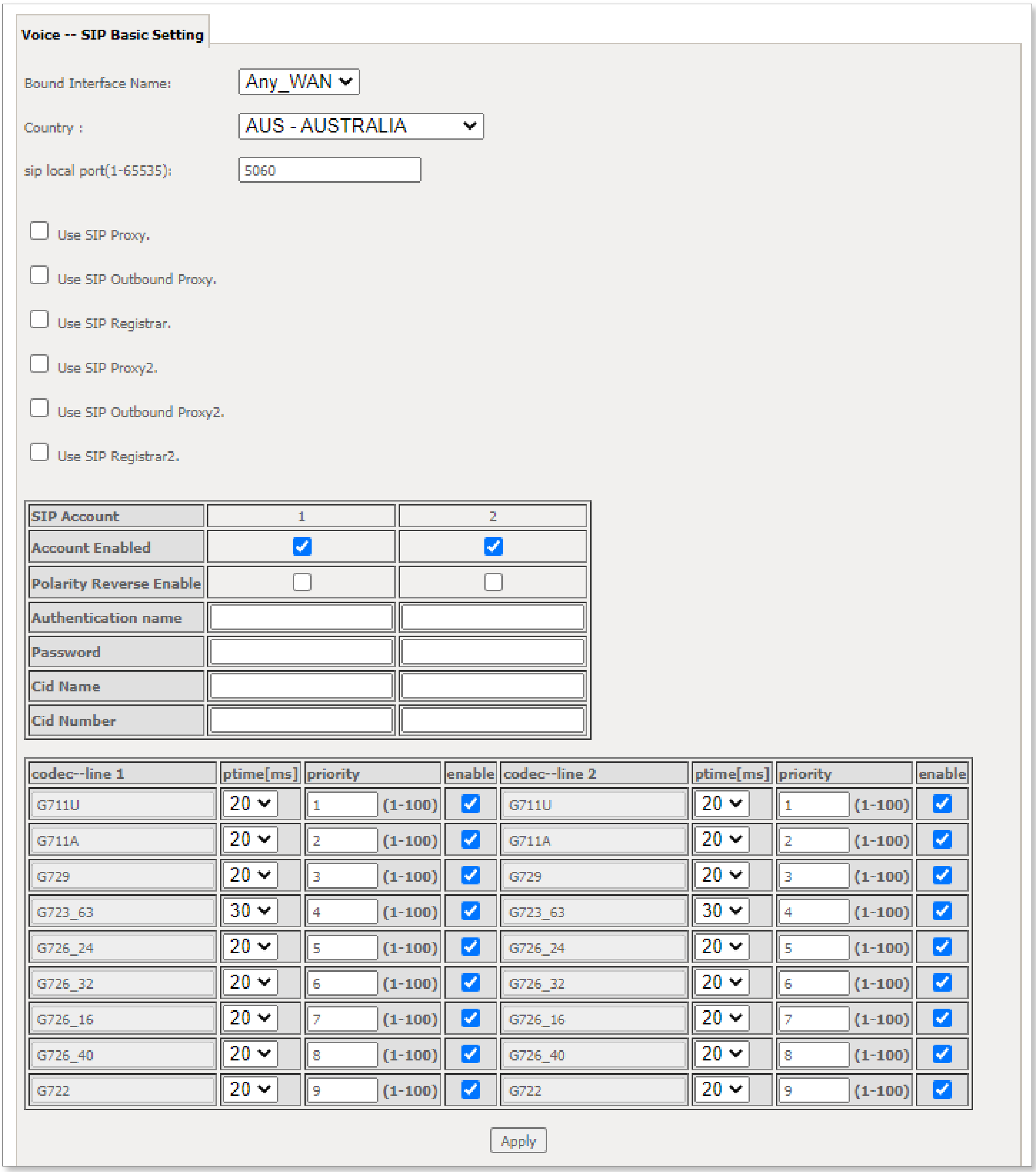
Call history:

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

Figure 118 – Voice Status page

SIP Basic Setting

The SIP Basic 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.



Voice -- SIP Basic Setting

Bound Interface Name: Any_WAN

Country : AUS - AUSTRALIA

sip local port(1-65535): 5060

☐ Use SIP Proxy.

☐ Use SIP Outbound Proxy.

☐ Use SIP Registrar.

☐ Use SIP Proxy2.

☐ Use SIP Outbound Proxy2.

☐ Use SIP Registrar2.

SIP Account	1	2
Account Enabled	☑	☑
Polarity Reverse Enable	☐	☐
Authentication name		
Password		
Cid Name		
Cid Number		

codec--line 1	ptime[ms]	priority	enable	codec--line 2	ptime[ms]	priority	enable
G711U	20	1 (1-100)	☑	G711U	20	1 (1-100)	☑
G711A	20	2 (1-100)	☑	G711A	20	2 (1-100)	☑
G729	20	3 (1-100)	☑	G729	20	3 (1-100)	☑
G723_63	30	4 (1-100)	☑	G723_63	30	4 (1-100)	☑
G726_24	20	5 (1-100)	☑	G726_24	20	5 (1-100)	☑
G726_32	20	6 (1-100)	☑	G726_32	20	6 (1-100)	☑
G726_16	20	7 (1-100)	☑	G726_16	20	7 (1-100)	☑
G726_40	20	8 (1-100)	☑	G726_40	20	8 (1-100)	☑
G722	20	9 (1-100)	☑	G722	20	9 (1-100)	☑

Figure 119 – SIP Basic Settings page

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.
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.
SIP domain name	Enter the SIP domain name or IP address of your VoIP Service Provider here.
Use SIP Proxy	Select the checkbox of Use SIP Proxy, if your DSL 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 it to initiate or accept any call.
Polarity Reverse Enable	Enable or disable this function.
Authentication name	Set the user name of authentication.
Password	Set the password of authentication.
Cid Name	User name. 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. If selecting 10 milliseconds, packets improve the voice quality. Because of the packet loss, less information is lost, but more loads on the 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.

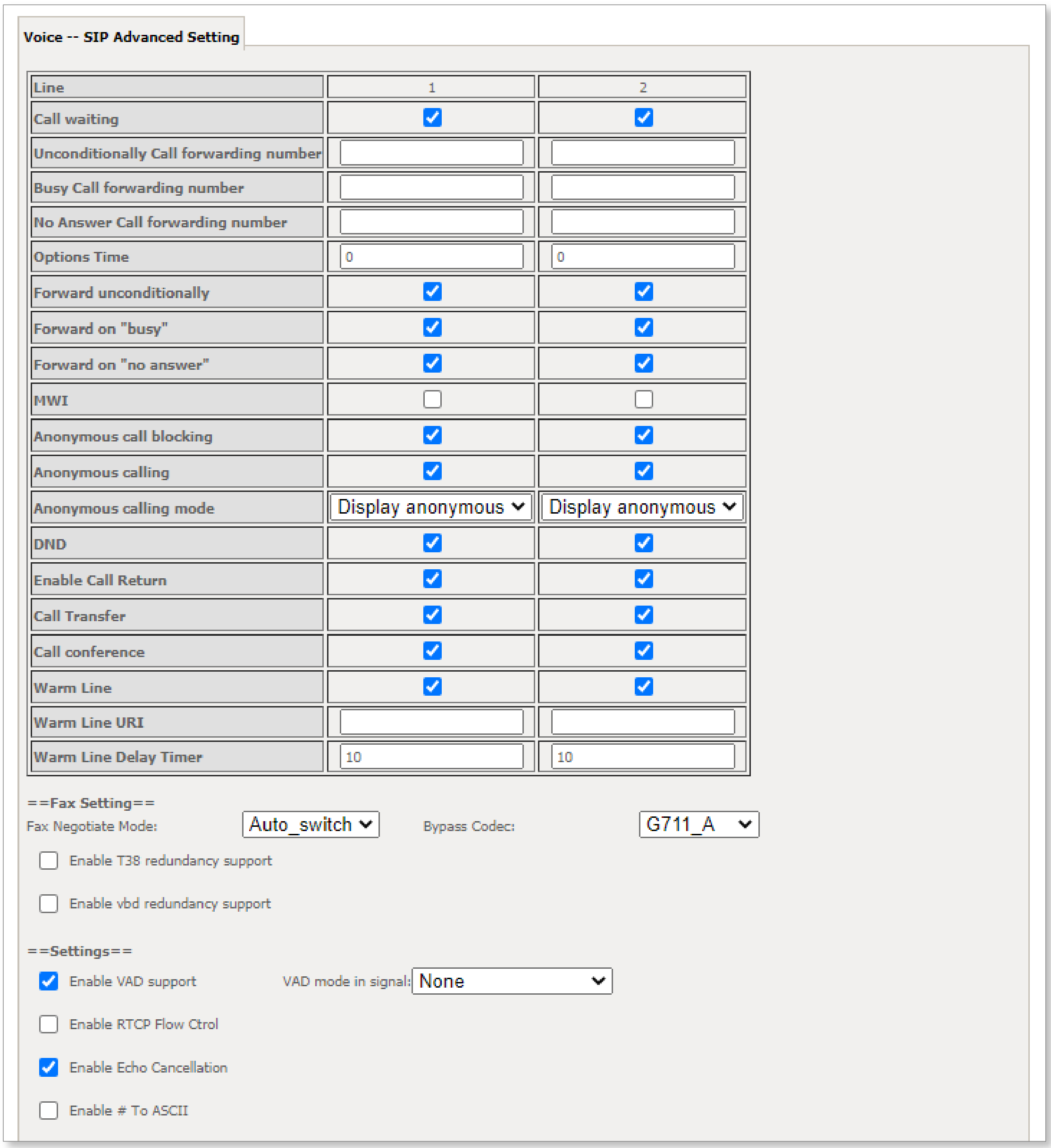
Option	Definition
	If you specify none of the codecs, using the default value showed in the above figure, the DSL router chooses the codec automatically.

Table 23 – SIP settings table

After entering your VoIP settings press the Apply button. Select Management > Save/Reboot and press the Reboot button. Once the router restarts if there is a valid internet connection and the VoIP account settings are valid the VoIP service will start.

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.



Voice -- SIP Advanced Setting

Line	1	2
Call waiting	☑	☑
Unconditionally Call forwarding number		
Busy Call forwarding number		
No Answer Call forwarding number		
Options Time	0	0
Forward unconditionally	☑	☑
Forward on "busy"	☑	☑
Forward on "no answer"	☑	☑
MWI	□	□
Anonymous call blocking	☑	☑
Anonymous calling	☑	☑
Anonymous calling mode	Display anonymous	Display anonymous
DND	☑	☑
Enable Call Return	☑	☑
Call Transfer	☑	☑
Call conference	☑	☑
Warm Line	☑	☑
Warm Line URI		
Warm Line Delay Timer	10	10

==Fax Setting==

Fax Negotiate Mode: Auto_switch   Bypass Codec: G711_A

□ Enable T38 redundancy support

□ Enable vbd redundancy support

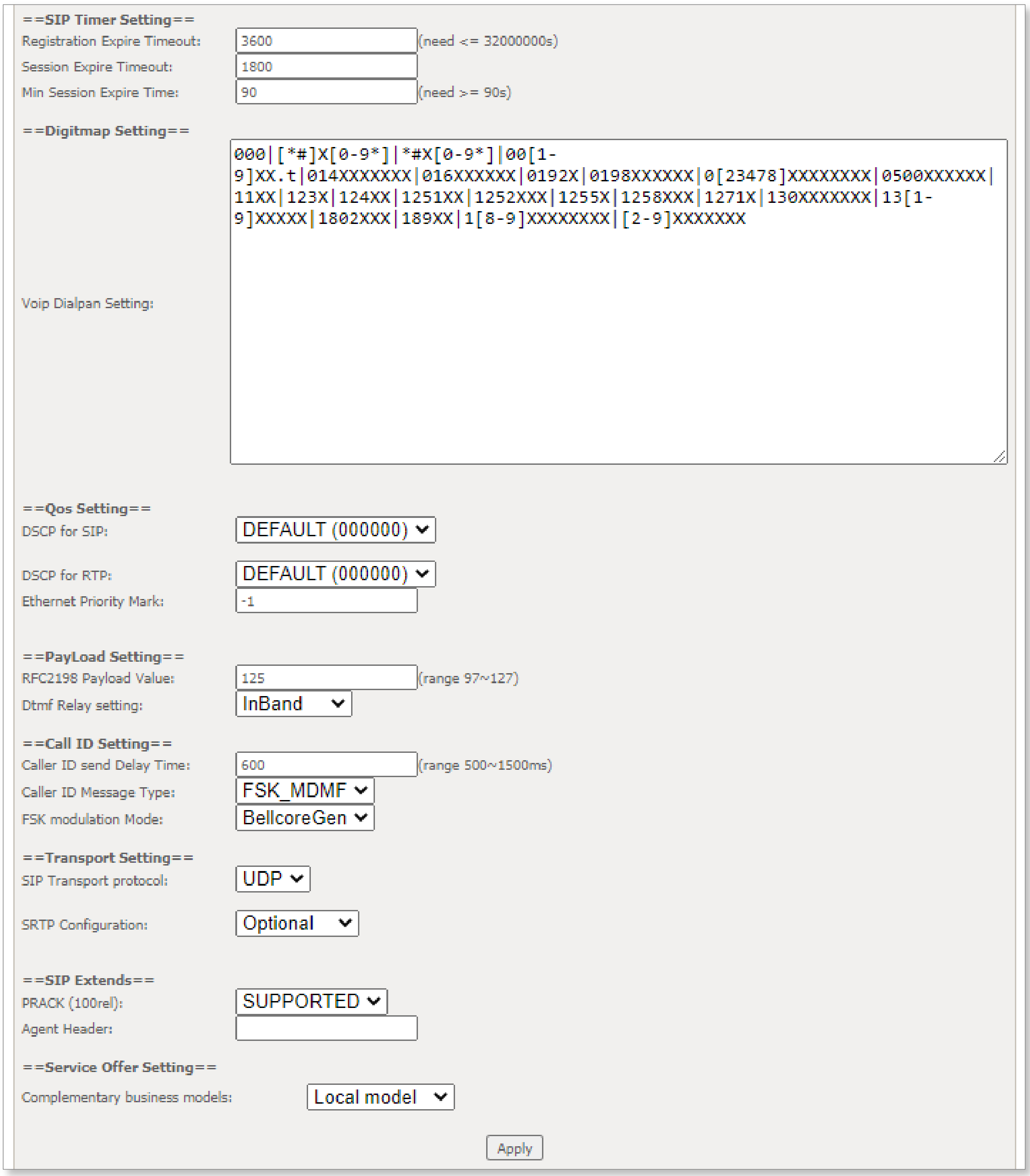
==Settings==

☑ Enable VAD support   VAD mode in signal: None

□ Enable RTCP Flow Ctrol

☑ Enable Echo Cancellation

□ Enable # To ASCII



==SIP Timer Setting==		
Registration Expire Timeout:	3600	(need <= 32000000s)
Session Expire Timeout:	1800	
Min Session Expire Time:	90	(need >= 90s)
==Digitmap Setting==		
Voip Dialpan Setting:	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]XXXXX|1802XXX|189XX|1[8-9]XXXXXXXX|[2-9]XXXXXXX	
==Qos Setting==		
DSCP for SIP:	DEFAULT (000000)	
DSCP for RTP:	DEFAULT (000000)	
Ethernet Priority Mark:	-1	
==PayLoad Setting==		
RFC2198 Payload Value:	125	(range 97~127)
Dtmf Relay setting:	InBand	
==Call ID Setting==		
Caller ID send Delay Time:	600	(range 500~1500ms)
Caller ID Message Type:	FSK_MDMF	
FSK modulation Mode:	BellcoreGen	
==Transport Setting==		
SIP Transport protocol:	UDP	
SRTP Configuration:	Optional	
==SIP Extends==		
PRACK (100rel):	SUPPORTED	
Agent Header:		
==Service Offer Setting==		
Complementary business models:	Local model	

Figure 120 – Voice- SIP Advanced settings

Option	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.

Option	Definition
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.

Option	Definition
	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 24 – VoIP – Advanced – Service Provider settings

Configuring a VoIP dial plan

The gateway comes with a default dial plan suitable for use in Australia. 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 25 – 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|12
4xx|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

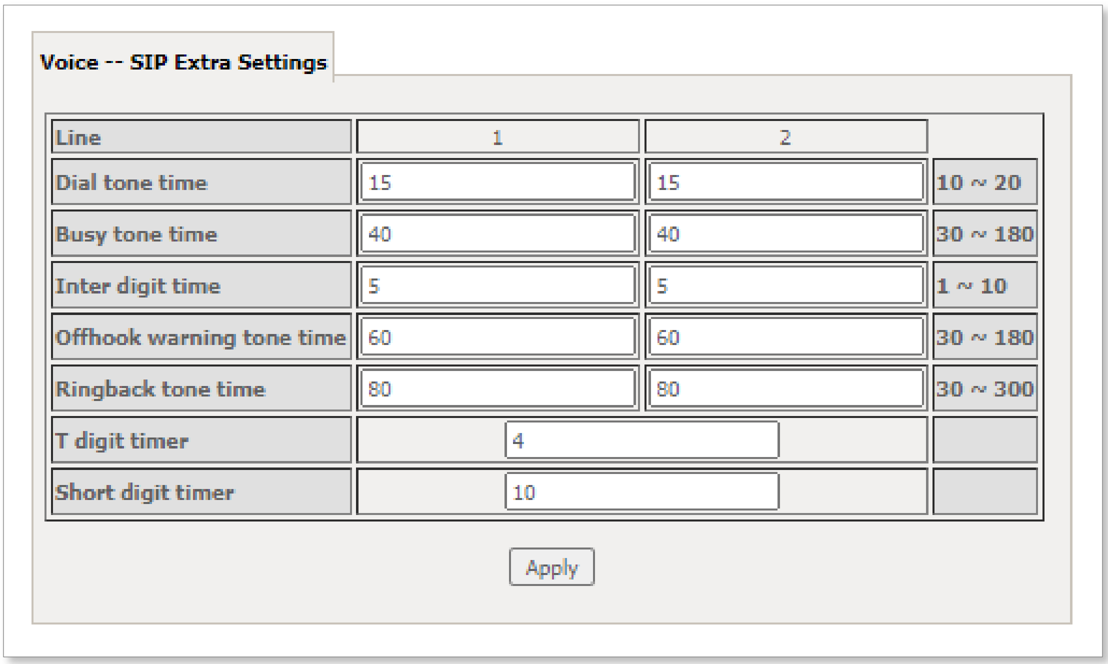
130XXXXXXX = 1300 business numbers

13[1-9]XXX = 13 business numbers

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

SIP Extra Setting

This page displays additional settings related to the SIP service.



Voice -- SIP Extra Settings

Line	1	2	
Dial tone time	15	15	10 ~ 20
Busy tone time	40	40	30 ~ 180
Inter digit time	5	5	1 ~ 10
Offhook warning tone time	60	60	30 ~ 180
Ringback tone time	80	80	30 ~ 300
T digit timer	4		
Short digit timer	10		

Figure 121 – SIP Extra Setting page

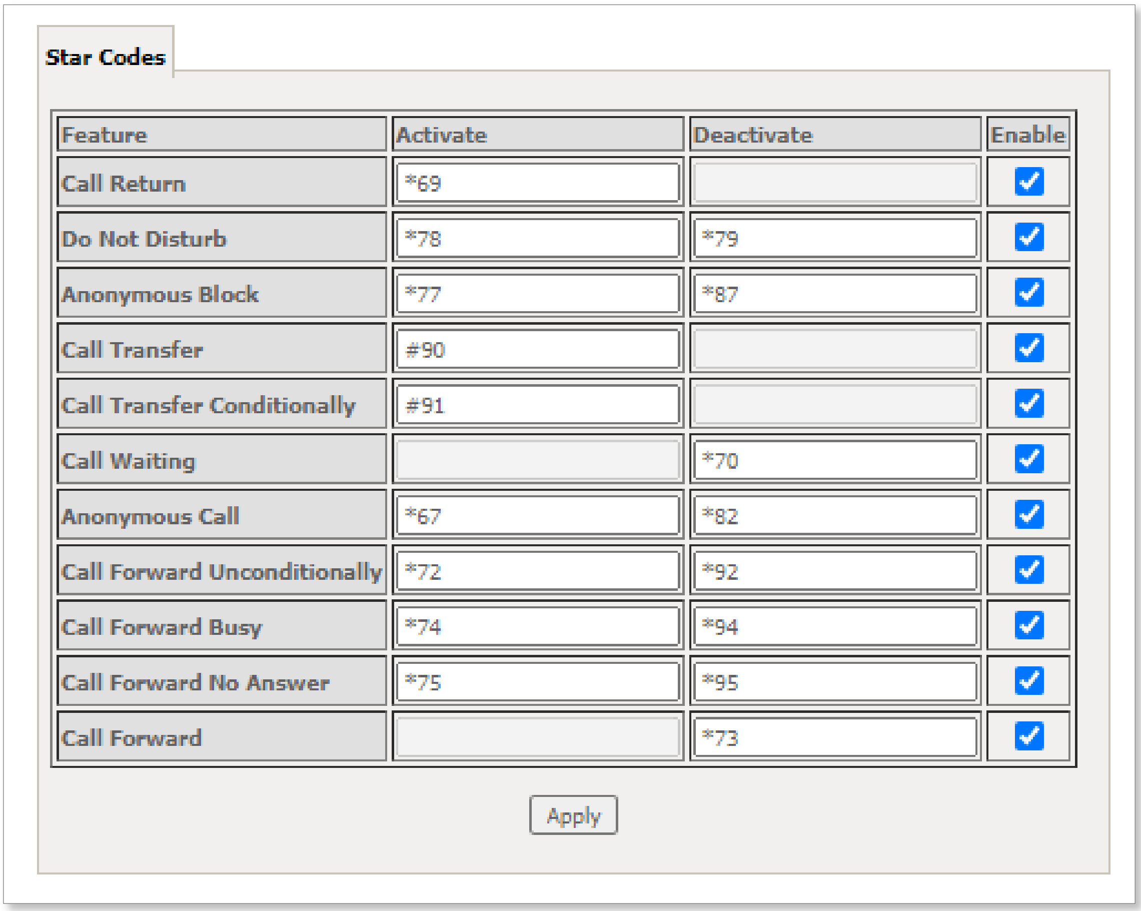
Parameter	Definition
Dial tone time	Set the Dial tone duration.
Busy tone time	Set the Busy tone duration.
Inter digit time	Set the timing between digits. The valid range is 1 ~ 5.
Off hook warning tone time	Set the Off-hook warning tone duration.
Ringback tone time	Set the Ring back tone duration.

Table 26 – SIP Extra Settings table

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.

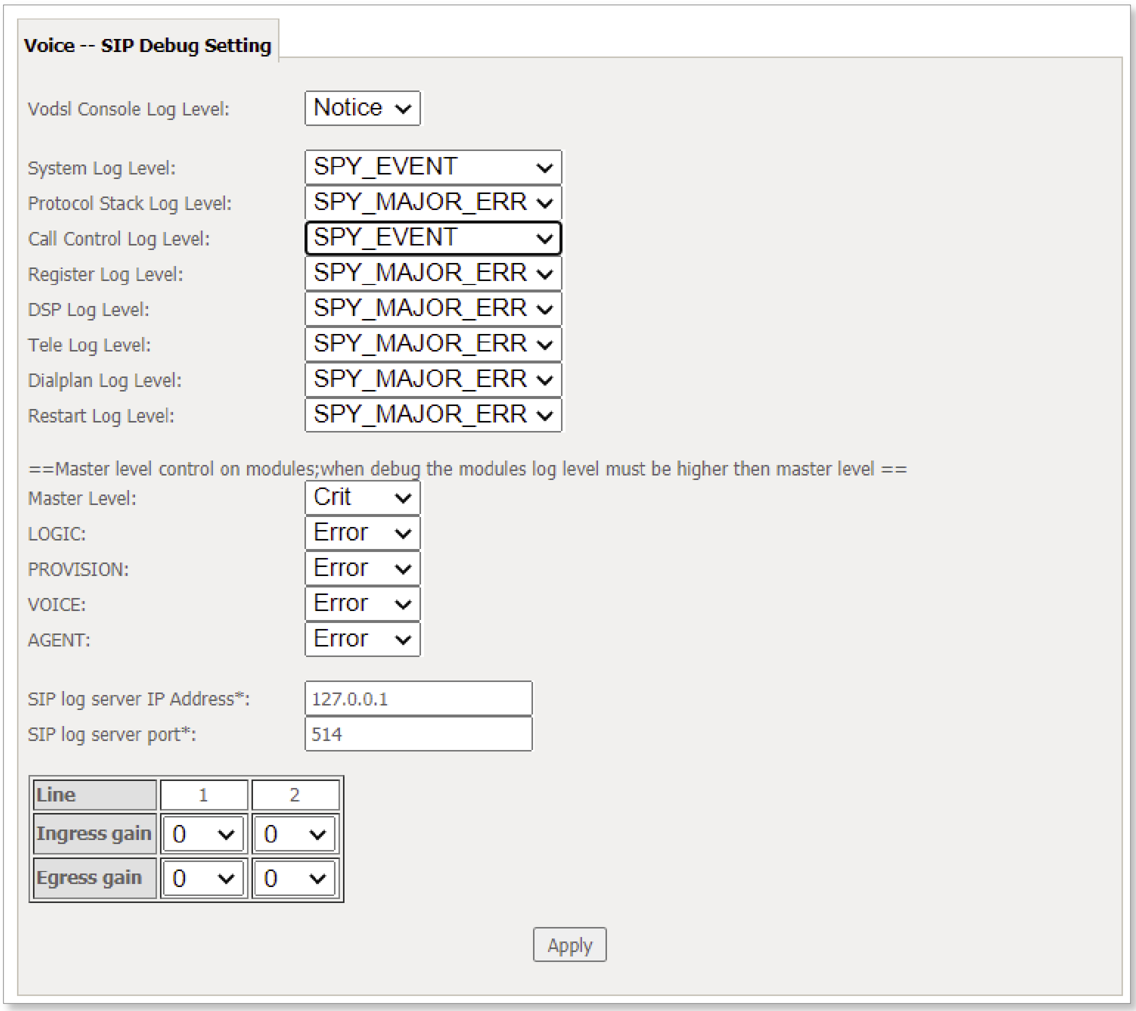


Feature	Activate	Deactivate	Enable
Call Return	*69		☑
Do Not Disturb	*78	*79	☑
Anonymous Block	*77	*87	☑
Call Transfer	#90		☑
Call Transfer Conditionally	#91		☑
Call Waiting		*70	☑
Anonymous Call	*67	*82	☑
Call Forward Unconditionally	*72	*92	☑
Call Forward Busy	*74	*94	☑
Call Forward No Answer	*75	*95	☑
Call Forward		*73	☑

Figure 122 – SIP Star Code Setting page

SIP Debug Setting

The SIP Debug Setting screen allows you to configure various settings regarding the logging levels of the SIP service.



Voice -- SIP Debug Setting

Vodsl Console Log Level: Notice

System Log Level: SPY_EVENT
Protocol Stack Log Level: SPY_MAJOR_ERR
Call Control Log Level: SPY_EVENT
Register Log Level: SPY_MAJOR_ERR
DSP Log Level: SPY_MAJOR_ERR
Tele Log Level: SPY_MAJOR_ERR
Dialplan Log Level: SPY_MAJOR_ERR
Restart Log Level: SPY_MAJOR_ERR

==Master level control on modules;when debug the modules log level must be higher then master level ==
Master Level: Crit
LOGIC: Error
PROVISION: Error
VOICE: Error
AGENT: Error

SIP log server IP Address*: 127.0.0.1
SIP log server port*: 514

Line	1	2
Ingress gain	0	0
Egress gain	0	0

Figure 123 – SIP Debug Setting page

VoIP Functionality

This section describes how to use the VoIP function of the DSL router in more detail. Some features involve 2 or 3 parties. In that case, note that all 3 parties have to be successfully registered.

Registering

Before using any VoIP functions, the DSL router has to register itself to a registrar. The DSL router also has to be configured with a proxy, which relays VoIP signalling to the next hop. In fact, many implementations integrate these two into one server, so in many case registrar and proxy refer to the same IP.

1. Select the right interface to use for registering, depending on where proxy/registrar resides. If use WAN link, ensure that it is already up.
2. Select the checkbox of Use SIP Registrar, and fill in the IP address and port with the right value.
3. Fill the extension information: Authentication name, Password, Cid Name and Cid Number.
4. Click Apply to take the settings into effect.
5. TEL indicator of VoIP service should be on, indicating that SIP client is successfully registered.

Placing a Call

This section describes how to place a basic VoIP call.

1. Pick up the receiver on the phone.
2. Hear the dial-tone. Dial the extension of remote party.
3. To end the dialling, wait for digit timeout, or just press # immediately.
4. After the remote party answers the call, you are in voice connection.

Anonymous call

Anonymous call does not send the caller ID to the remote party. This is useful if you do not want others know who you are. Check with your VoIP Provider if your service supports hidden caller ID.

1. Enable Anonymous calling in the Voice--SIP Advanced Setting web page.
2. Pick up the receiver on the phone.
3. Dial *68 to enable anonymous call.
4. Hook on the receiver, and dial another extension as you like. Now your caller ID information is blocked.

Do Not Disturb (DND)

If DND is enabled, all incoming calls are rejected. DND is useful if you do not want others to disturb you. Check with your VoIP Provider if your service supports DND.

1. Enable DND in the Voice--SIP Advanced Setting web page.
2. Pick up the receiver on the phone.
3. Dial *78 to enable DND.
4. Hook on the phone. Now your phone rejects all incoming calls.
5. Hook off again to disable the DND.

Call Return

For incoming calls, the DSL router remembers the number of calling party. Check with your VoIP Provider if your service supports Call returns. You cannot call return, if the caller has hidden caller ID.

1. Enable Call Return in the Voice--SIP Advanced Setting web page.
2. Press *69 to return a call.
3. Now you can make the call as if you have dialled the whole number.

Call Hold

Call hold enable you to put a call to a pending state, and pick it up in future. Check with your VoIP Provider if your service supports Call Hold.

1. Assuming you are in a voice connection, you can press FLASH to hold current call.
2. Now you can call another party, or press FLASH again to return to first call.

Call Waiting

Call waiting allows third party to call in when you are in a voice connection. Check with your VoIP Provider if your service supports Call Waiting.

1. Enable Call waiting in the Voice--SIP Advanced Setting web page.
2. Pick up the phone attached to the DSL router.
3. Assuming you are in a voice connection. When another call comes in, the DSL router streams a call waiting tone to your phone, indicating another call is available.
4. Press FLASH to switch to this call and the initial call put to hold automatically.
5. Press FLASH multi-times to switch between these two calls back and forth.

Blind Transfer

Blind transfer, transfers the current call to a third party blindly, regardless of whether the transfer is successfully or not. Check with your VoIP Provider if your service supports Call transfer.

1 Assume you have already been in a voice connection.

2 Press FLASH to hold the first party.

3 Dial #90 + third party number.

4 Before the third party answering the call, hook on your phone.

5 Now the first party takes over the call and he is in connection with the third party.

Consultative Transfer

Consultative transfer lets the third party answer the transferred call, and then hook on the transferring party. It' more gentle than blind transfer. Check with your VoIP Provider if your service supports Call Transfer.

1 Assume you have already been in a voice connection with a first party.

2 Press FLASH to hold the first party.

3 Dial #91 + third party number.

4 After the third party answering the call, hook on your phone.

5 Now the first party takes over the call and he is in connection with the third party.

Call Forwarding No Answer

If this feature is enabled, incoming calls are forwarded to third party when you don't answer them. It involves in two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding.

1 Enable Forward on "no answer" in the Voice--SIP Advanced Setting web page.

2 When our phone does not answer the incoming call, the call is forwarded.

Call Forwarding Busy

If this feature enabled, incoming calls will be forwarded to third party when you busy. It involves two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding.

1 Set Busy Call forwarding number and enable Forward on "busy" in the Voice--SIP Advanced Setting web page.

2 When our phone is busy, this call can be forwarded.

Call Forwarding All

If this feature enabled, incoming calls are forwarded to third party without any reason. It involves in two steps: setting the forwarding number and enable the feature. Check with your VoIP Provider if your service supports Call Forwarding.

1 Set Unconditionally Call forwarding number and Forward unconditionally in the Voice--SIP Advanced Setting web page.

2 All incoming calls are forwarded to the third party.

Three-Way Conference

Three-way conference enables you to invite a third party to a call, and every person in the conference is able to hear others' voice. Check with your VoIP Provider if your service supports Conference call.

1 Assume you are in connection with a first party.

2 Press FLASH to put the first party on-hold.

3 Dial a third party.

4 After the third party answers the call, press FLASH again to invite the first party.

5 Now all three parties are in a three-way conference.

T.38 Faxing

To make T.38 faxing, enable T.38 support on the Web. After that, connect a fax machine to a FXS port of the DSL router. Now you can use it as a normal phone, and it is able to send or receive fax to or from other fax machines on the VoIP network.

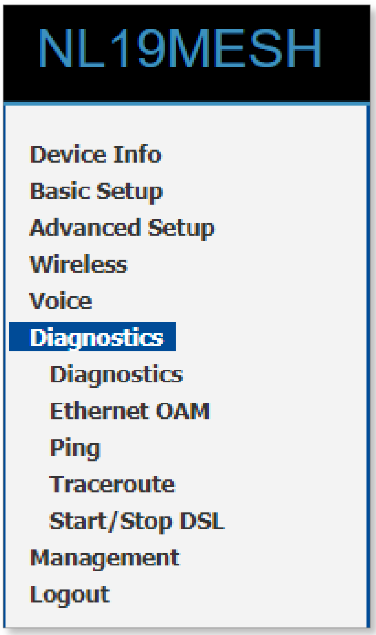
In the initial setup, faxing behaves like a normal call. After the DSL router detects the fax tone, it switch to T.38 mode, and use it as the transmit approach.

Check with your VoIP Provider if your service supports T.38 Faxing.

Pass-Through Faxing

If T.38 support is disabled, faxing uses normal voice codec as its coding approach. Therefore, this mode is more like normal phone calls.

Diagnostics



NL19MESH

Device Info
Basic Setup
Advanced Setup
Wireless
Voice
Diagnostics
Diagnostics
Ethernet OAM
Ping
Traceroute
Start/Stop DSL
Management
Logout

The **Diagnostics** menu provides a number of tools that can be used by you or a Support team member of your service provider to check the performance of your connection.

Diagnostics

The **Diagnostics** page provides feedback on the connection status of the device.

The individual tests that are displayed is dependent upon the connection type and the exact tests applicable to each of the various types will vary considerably and are primarily used by your carrier's technical support agents.

Regardless of the connection type and the test types displayed, if a test displays a FAIL status:

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

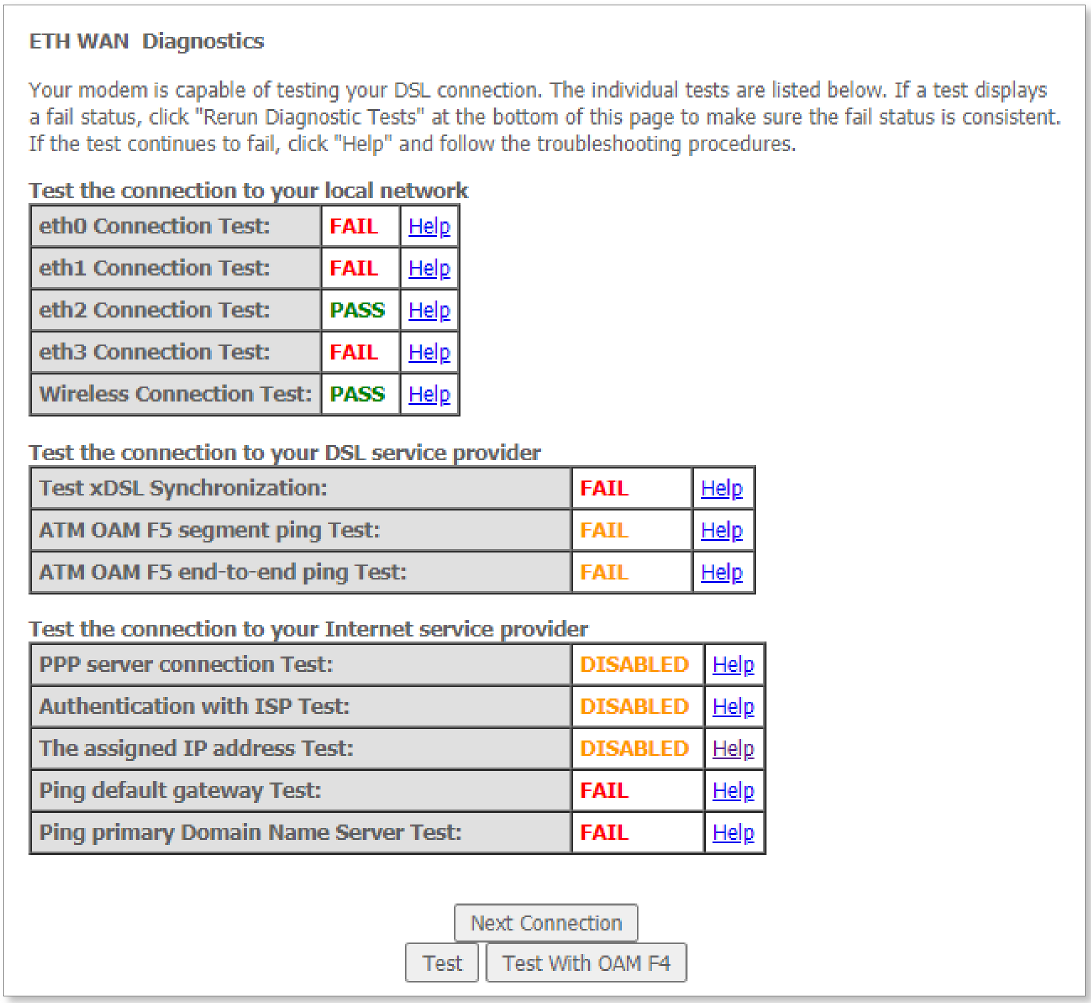
2 Next click the **Rerun Diagnostic Tests** button at the bottom of the screen to re-test and verify if the suggested action corrected the error.

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

⚠ Important – If there are multiple WAN connection created, each connection will have its own diagnostics page, and which shows up 1st is dependent on the WAN service list order.

Example Diagnostic page

The following example of ETH WAN Diagnostics menu provides details of the tests available when a PPPoE/A connection type is deployed.



ETH WAN Diagnostics

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

Test the connection to your local network

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

Test the connection to your DSL service provider

Test xDSL Synchronization:	FAIL	Help
ATM OAM F5 segment ping Test:	FAIL	Help
ATM OAM F5 end-to-end ping Test:	FAIL	Help

Test the connection to your Internet service provider

PPP server connection Test:	DISABLED	Help
Authentication with ISP Test:	DISABLED	Help
The assigned IP address Test:	DISABLED	Help
Ping default gateway Test:	FAIL	Help
Ping primary Domain Name Server Test:	FAIL	Help

Figure 124 – Diagnostics – ETH WAN Diagnostic test results

Local Network connection tests

Field	Description
eth# Connection Test	PASS – Indicates the Ethernet connection to your computer is connected to the numbered LAN port of the gateway. FAIL – Indicates that the gateway does not detect the Ethernet interface of your computer.
Wireless Connection Test	PASS – Indicates that the wireless interface from your computer is connected to the LAN port of the gateway. FAIL – Indicates that the gateway does not detect the wireless interface.
Help	Click the Help link for more details and for additional Troubleshooting advice for each test.

Table 27 – Connection to LAN diagnostic test result table

DSL Service Provider connection tests

Field	Description
xDSL Synchronization Test	PASS – Indicates the DSL modem has detected a DSL signal from the telephone company. FAIL – Indicates that the DSL modem does not detect a signal from the telephone company's DSL network.
ATM OAM F5 segment ping Test	PASS – Indicates that the DSL modem can communicate with the DSL provider network. FAIL – Indicates that the DSL modem may not be able to communicate with the DSL provider network.
ATM OAM F5 end-to-end ping Test	PASS – Indicates that the DSL modem can communicate with the DSL provider network. FAIL – Indicates that the DSL modem may not be able to communicate with the DSL provider network.
Help	Click the Help link for more details and for additional Troubleshooting advice for each test.

Table 28 – Connection to DSL service diagnostic test result table

DSL Service Provider connection tests

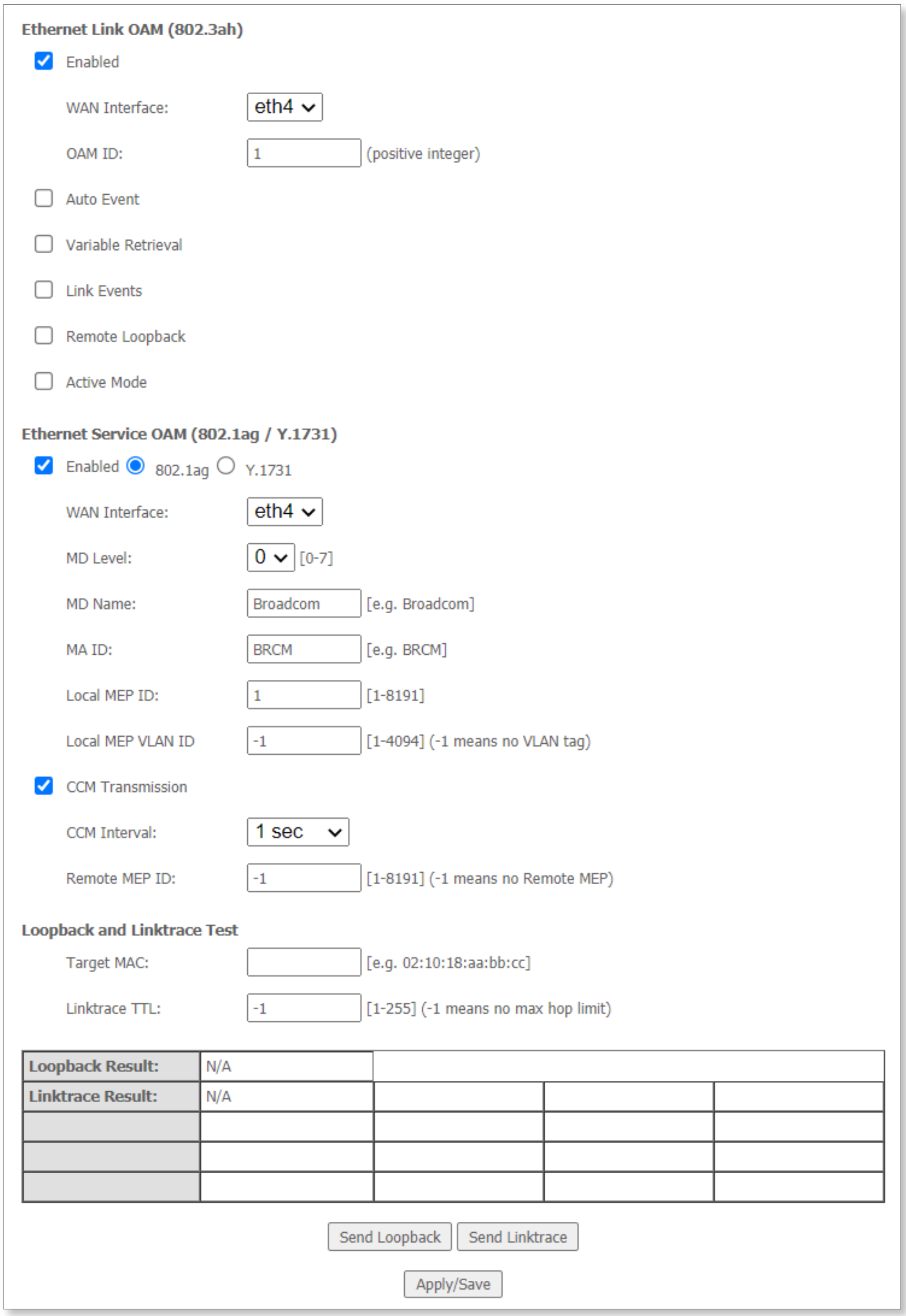
Field	Description
PPP server connection Test	PASS – Indicates that your DSL modem can see the PPP server (the DSL modem received a PADO packet from the PPP server). FAIL – Indicates that the DSL modem cannot see the PPP server (the DSL modem did not receive a PADO packet from the PPP server). A flashing green PPP LED on the modem signifies an attempt to establish a PPP connection.
Authentication with SIP Test	PASS – Indicates that your username and password stored in the DSL modem has authenticated with ISP's network. FAIL – Indicates that the DSL modem was unable to verify your username and password with ISP's network.
Assigned IP address Test	PASS – Indicates that the DSL modem has received a valid IP (Internet Protocol) address from the PPP server. FAIL – Indicates that the DSL modem does not have a valid IP address from the PPP server.
Ping default gateway Test	PASS – Indicates that the DSL modem can communicate with the first entry point to the network. It is usually the IP address of the ISP local router.. FAIL – Indicates that the DSL modem was unable to communicate with the first entry point on the network.
Ping primary Domain Name Server Test	PASS – Indicates that the DSL modem can communicate with the primary Domain Name Server (DNS). FAIL – that the DSL modem was unable to communicate the primary Domain Name Server (DNS).

Field	Description
Help	Click the Help link for more details and for additional Troubleshooting advice for each test.

Table 29 – Connection to ISP diagnostic test result table

Ethernet OAM

The **Ethernet OAM** page provides administrators with operation, administration and management features.



Ethernet Link OAM (802.3ah)

☑ Enabled

WAN Interface: eth4

OAM ID: 1 (positive integer)

□ Auto Event

□ Variable Retrieval

□ Link Events

□ Remote Loopback

□ Active Mode

Ethernet Service OAM (802.1ag / Y.1731)

☑ Enabled ● 802.1ag ○ Y.1731

WAN Interface: eth4

MD Level: 0 [0-7]

MD Name: Broadcom [e.g. Broadcom]

MA ID: BRCM [e.g. BRCM]

Local MEP ID: 1 [1-8191]

Local MEP VLAN ID -1 [1-4094] (-1 means no VLAN tag)

☑ CCM Transmission

CCM Interval: 1 sec

Remote MEP ID: -1 [1-8191] (-1 means no Remote MEP)

Loopback and Linktrace Test

Target MAC: [e.g. 02:10:18:aa:bb:cc]

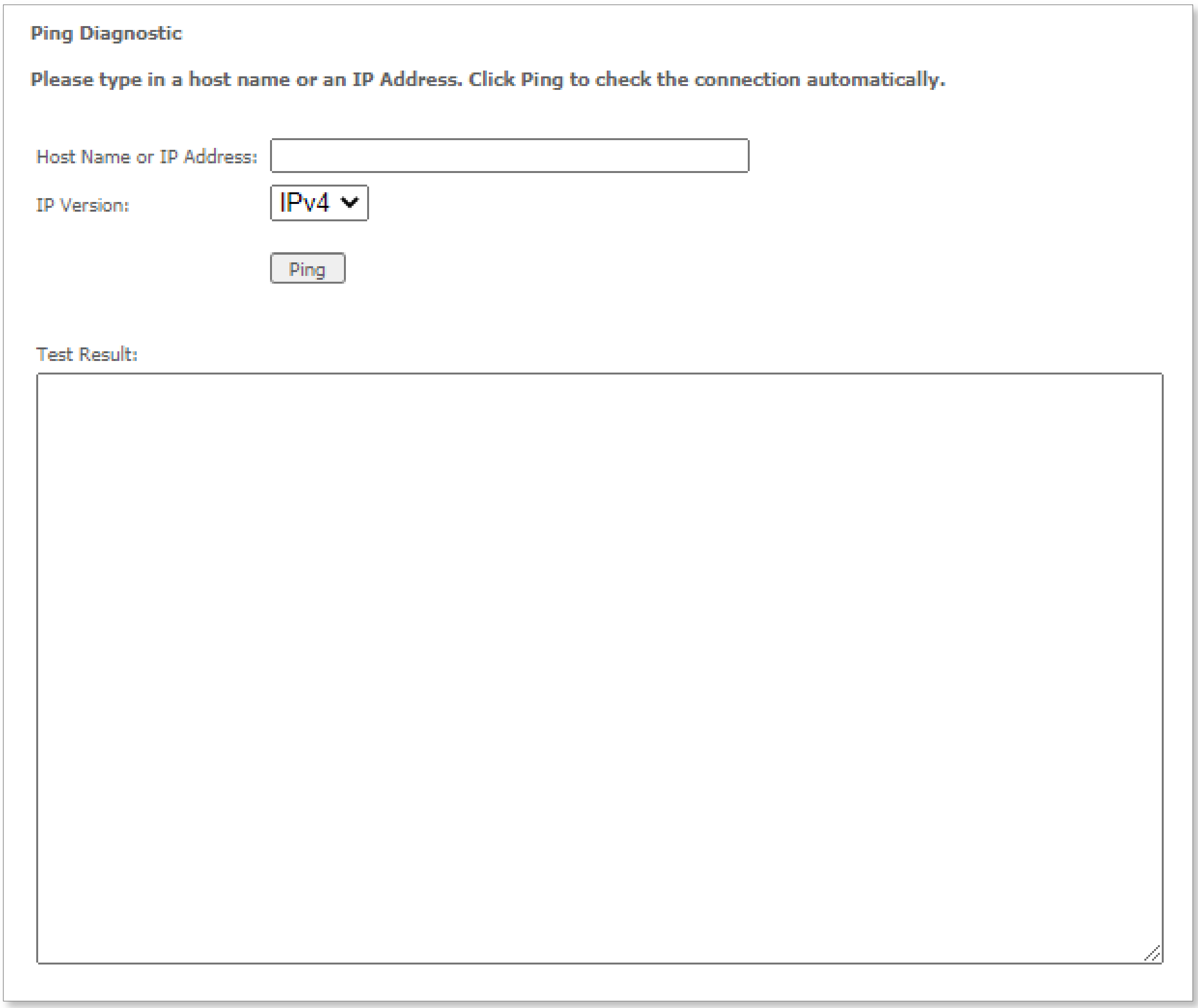
Linktrace TTL: -1 [1-255] (-1 means no max hop limit)

Loopback Result:	N/A				
Linktrace Result:	N/A				

Figure 125 – Ping IP address

Ping

The ping test page lets you ping a remote IP address or hostname to test the connection.



Ping Diagnostic

Please type in a host name or an IP Address. Click Ping to check the connection automatically.

Host Name or IP Address:

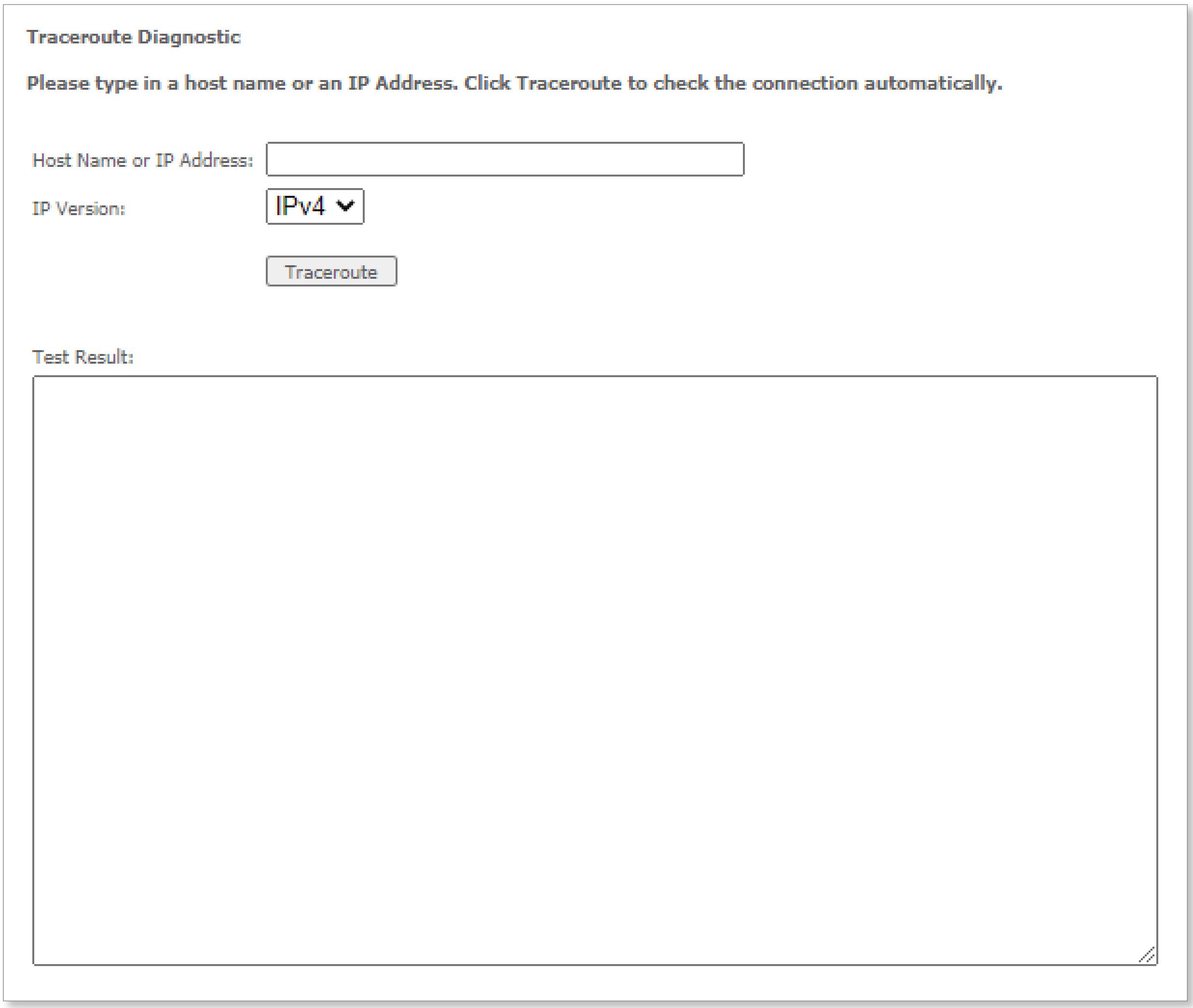
IP Version: IPv4

Test Result:

Figure 126 – Ping IP address

Traceroute

The Traceroute Diagnostic page lets you perform a trace route to a remote IP address or host name in order to ensure that the correct interface is being used for routing.



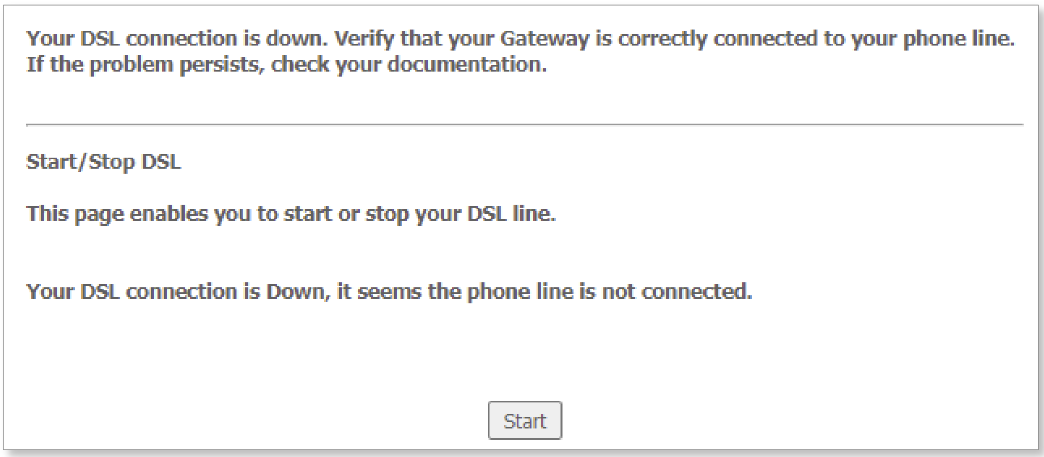
Traceroute Diagnostic

Please type in a host name or an IP Address. Click Traceroute to check the connection automatically.

Figure 127 – Diagnostics – Traceroute page

Start / Stop DSL

This page lets you stop or start the DSL service for troubleshooting purposes.



Your DSL connection is down. Verify that your Gateway is correctly connected to your phone line. If the problem persists, check your documentation.

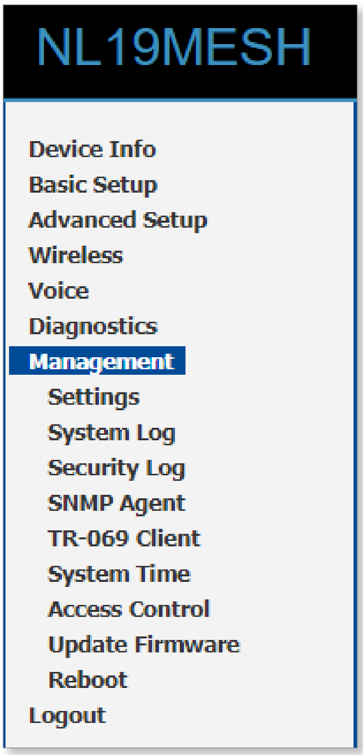
Start/Stop DSL

This page enables you to start or stop your DSL line.

Your DSL connection is Down, it seems the phone line is not connected.

Figure 121 – Diagnostics – Start/Stop DSL page

Management



NL19MESH

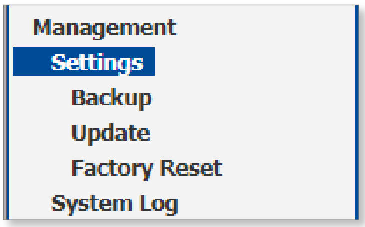
Device Info
Basic Setup
Advanced Setup
Wireless
Voice
Diagnostics
Management
Settings
System Log
Security Log
SNMP Agent
TR-069 Client
System Time
Access Control
Update Firmware
Reboot
Logout

The **Management** menu contains links to system wide settings and features.

The various settings help you to:

- Save your custom settings (Backup) and then restore those settings at a later date,
- Reset the gateway to is factory defaults,
- Set custom system logging parameters,
- Control access to your system,
- Control usage through your system, and
- Manage updates and other firmware issues.

Settings



Management
Settings
Backup
Update
Factory Reset
System Log

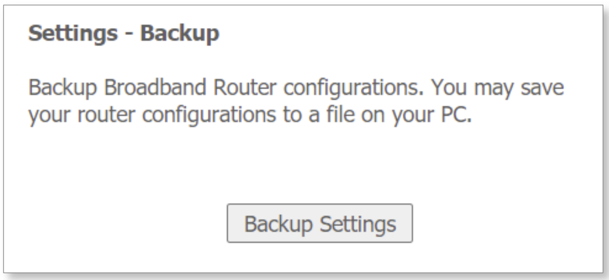
The **Management > Settings** sub-menu provides three tools to back up, retrieve and restore the default settings of your router.

It also provides a function for you to update your router's firmware.

Backup

This 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.

To back up the current configuration click the **Backup Settings** button to save the current configuration settings.



Settings - Backup

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

Figure 128 – Settings – Backup page

The configuration file is saved via your browser to the downloads folder configured in your browser. The file is named **`backupsetting (No.).conf`**, with **`(No.)`** being the sequential number assigned to multiple backup files. You can rename the file, keeping the **`.conf`** file extension and save it to a location of your choice.

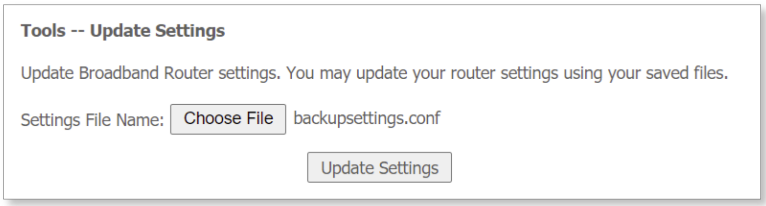
To restore the configuration on your CloudMesh Gateway, see the Update Settings section below.

Update Settings

Use this feature to restore a previously saved configuration using the Backup feature (described above).

To restore a saved configuration, click the Choose File button and locate a file that you have saved to restore a previous configuration. Once selected, the filename will appear to the right of the Choose File button.

Click the Update Settings button to upload the selected file.



Tools -- Update Settings

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

Settings File Name: Choose File backupsettings.conf

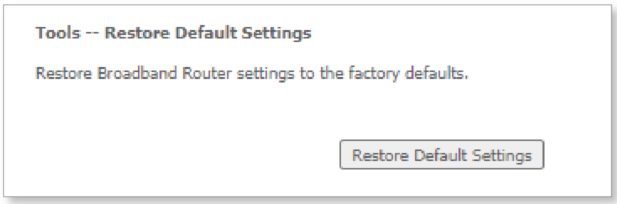
Figure 129 – Settings – Update Settings page

Allow up to 5 minutes for the system to apply the configuration and reboot.

Factory Reset

This feature resets all the settings of the gateway to the factory default settings. When you select this option, the settings will be erased and the gateway reboots.

Click the Restore Default Settings button to start the factory reset process.



Tools -- Restore Default Settings

Restore Broadband Router settings to the factory defaults.

Figure 130 – Settings – Factory Reset page

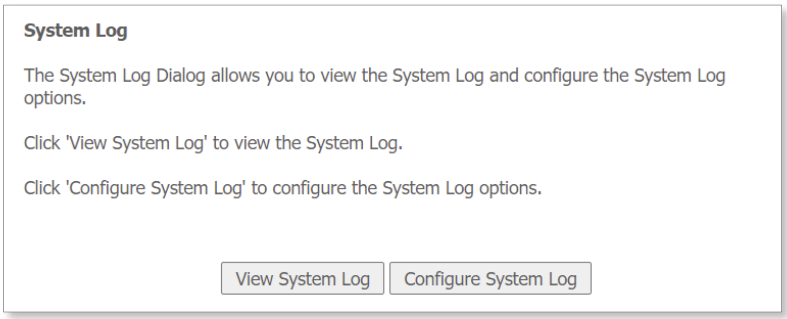
A warning dialog saying "*Are you sure you want to restore factory default settings?*" will display. Click the OK button to proceed with the factory reset process.

Allow up to 2 minutes for the settings to be reset and the gateway to restart.

System Log

The System log page allows you to view the log of the gateway and also to configure the logging level.

To view the system log, click the View System Log button.



System Log

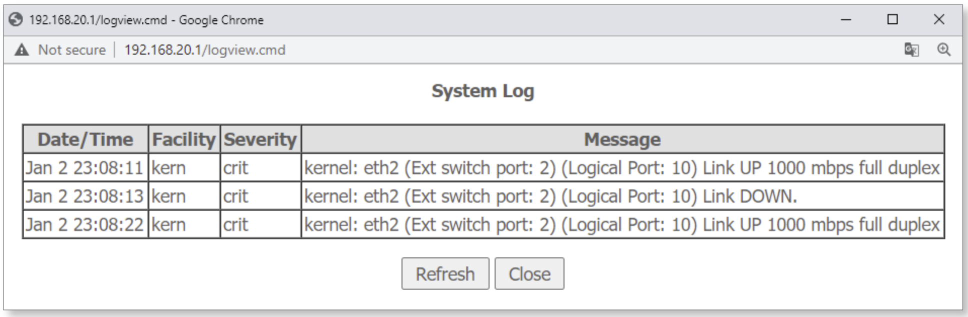
The System Log Dialog allows you to view the System Log and configure the System Log options.

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

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

Figure 131 – Management – View System Log

The System Log will display in a popup window:



System Log

Date/Time	Facility	Severity	Message
Jan 2 23:08:11	kern	crit	kernel: eth2 (Ext switch port: 2) (Logical Port: 10) Link UP 1000 mbps full duplex
Jan 2 23:08:13	kern	crit	kernel: eth2 (Ext switch port: 2) (Logical Port: 10) Link DOWN.
Jan 2 23:08:22	kern	crit	kernel: eth2 (Ext switch port: 2) (Logical Port: 10) Link UP 1000 mbps full duplex

Figure 132 – System Log display

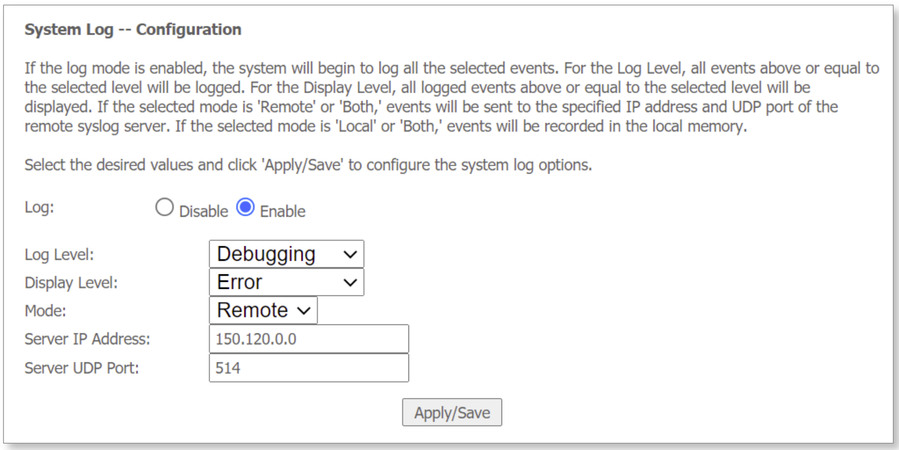
To configure the system log, click the Configure System Log button.

To maintain a log, select Log: ⦿ Enable

For the Log Level, all events above or equal to the selected level will be logged.

For the Display Level, all logged events above or equal to the selected level will be displayed.

You can send system log data to a remote server by selecting the "Both", or "Remote" option for the Mode setting. The gateway will prompt you for a Server IP Address and Server UDP Port. To receive the system log data remotely, you must run some third-party syslog software.



System Log -- Configuration

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

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

Log: ○ Disable ● Enable

Log Level: Debugging

Display Level: Error

Mode: Remote

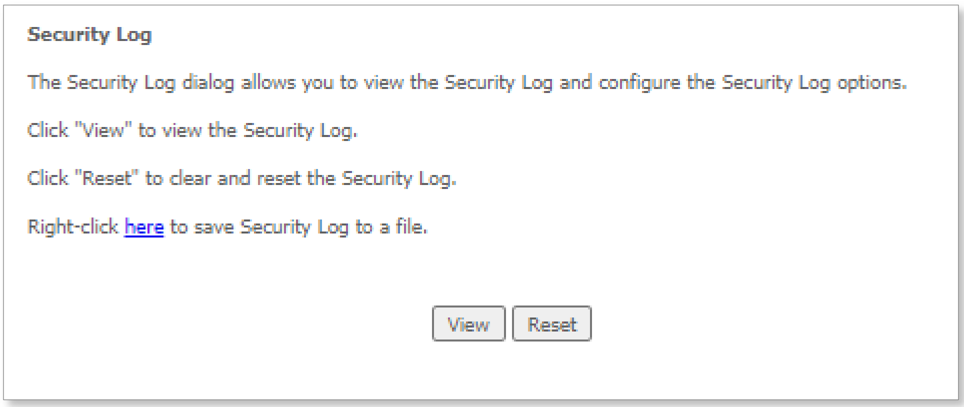
Server IP Address: 150.120.0.0

Server UDP Port: 514

Figure 133 – Management – Configure System Log

Security Log

The Security log page allows you to view the log of the gateway and to configure the logging level. To view the Security log, click the **View Security Log** button.



Security Log

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

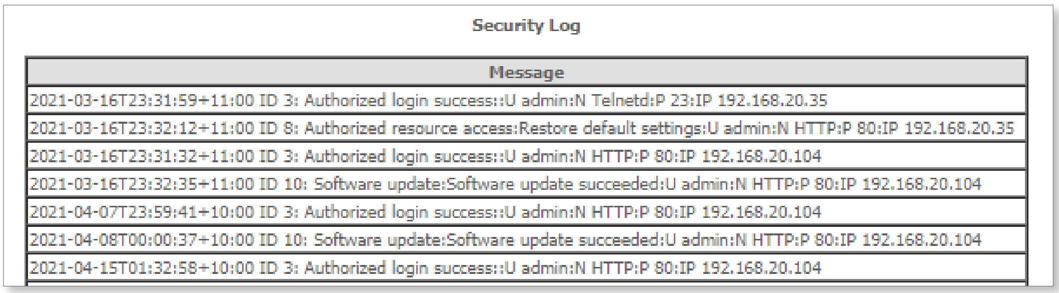
Click "View" to view the Security Log.

Click "Reset" to clear and reset the Security Log.

Right-click here to save Security Log to a file.

Figure 134 – Management – View Security Log

To view the Security log, click the **View** button. The Security log will open in a browser pop up window:



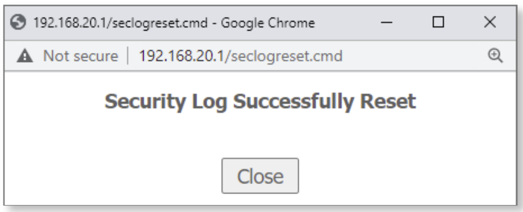
Security Log

Message
2021-03-16T23:31:59+11:00 ID 3: Authorized login success::U admin:N Telnetd:P 23:IP 192.168.20.35
2021-03-16T23:32:12+11:00 ID 8: Authorized resource access:Restore default settings:U admin:N HTTP:P 80:IP 192.168.20.35
2021-03-16T23:31:32+11:00 ID 3: Authorized login success::U admin:N HTTP:P 80:IP 192.168.20.104
2021-03-16T23:32:35+11:00 ID 10: Software update:Software update succeeded:U admin:N HTTP:P 80:IP 192.168.20.104
2021-04-07T23:59:41+10:00 ID 3: Authorized login success::U admin:N HTTP:P 80:IP 192.168.20.104
2021-04-08T00:00:37+10:00 ID 10: Software update:Software update succeeded:U admin:N HTTP:P 80:IP 192.168.20.104
2021-04-15T01:32:58+10:00 ID 3: Authorized login success::U admin:N HTTP:P 80:IP 192.168.20.104

Figure 135 – Management – Download Security Log

To clear the security log and begin logging in an empty log, click the **Reset** button.

A confirmation dialog will display and the Security log will be cleared.



192.168.20.1/seclogreset.cmd - Google Chrome

Not secure | 192.168.20.1/seclogreset.cmd

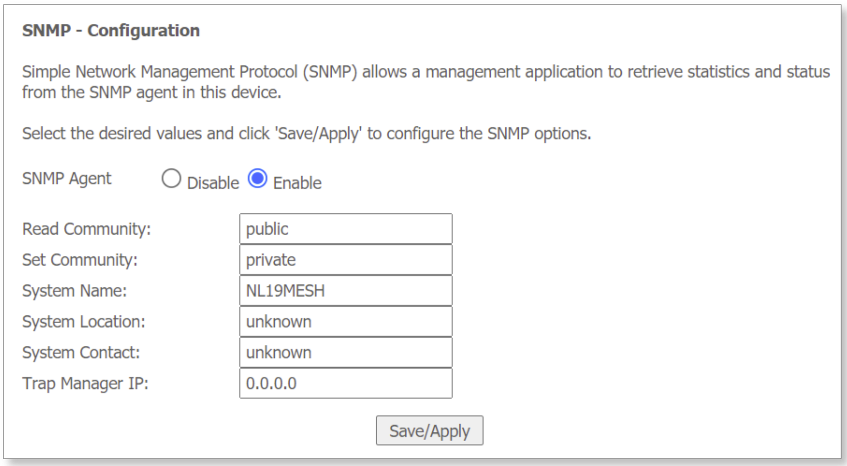
Security Log Successfully Reset

Figure 136 –Security Log Reset confirmation

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 CloudMesh 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.



SNMP - Configuration

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

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

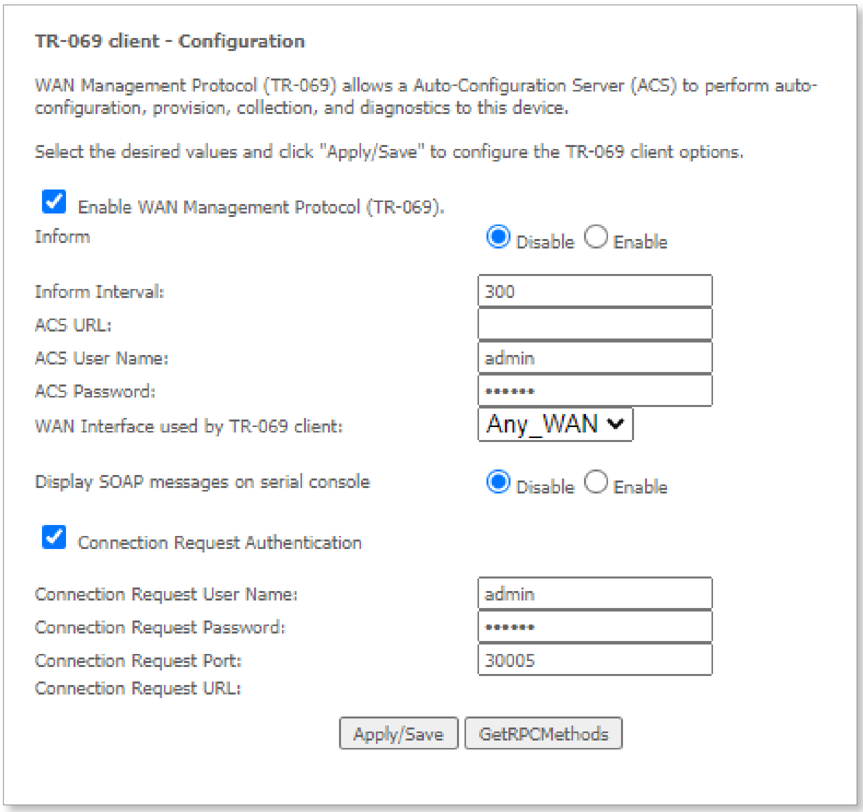
SNMP Agent ○ Disable ● Enable

Read Community:	public
Set Community:	private
System Name:	NL19MESH
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

Figure 137 – Management – Enable SNMP Agent

TR-069 Client

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router if supported by your Internet Service Provider (ISP).



TR-069 client - Configuration

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

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

☑ Enable WAN Management Protocol (TR-069).

Inform	● Disable ○ Enable
Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	••••••
WAN Interface used by TR-069 client:	Any_WAN
Display SOAP messages on serial console	● Disable ○ Enable

☑ Connection Request Authentication

Connection Request User Name:	admin
Connection Request Password:	••••••
Connection Request Port:	30005
Connection Request URL:	

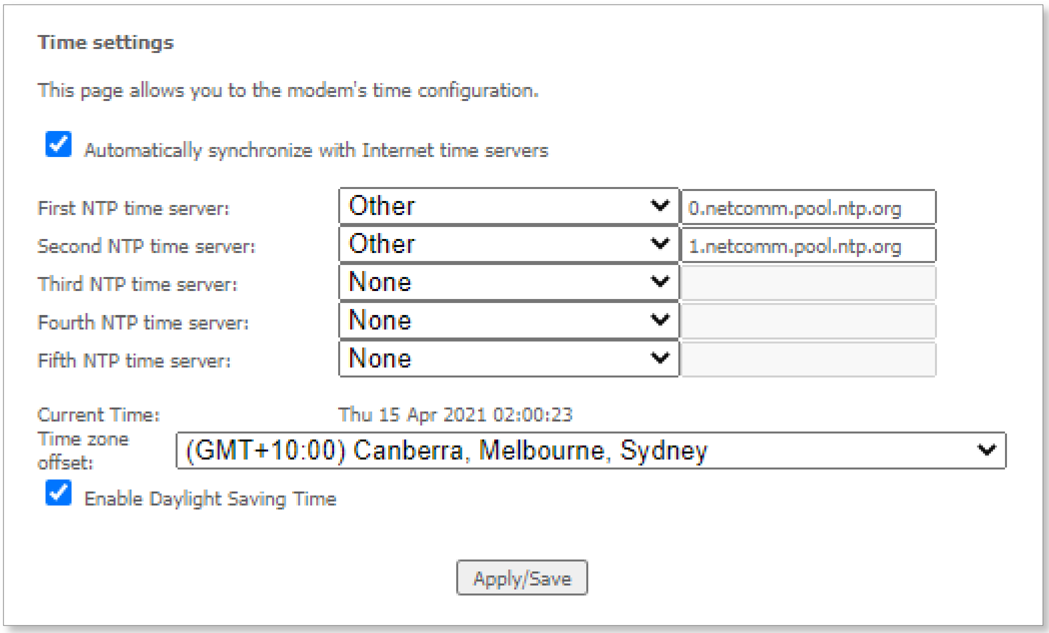
Figure 138 – Management – Enable TR-069 Client

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 where the ACS server is located.
ACS User Name	The user name 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.

Table 30 – TR-069 Client settings table

Internet Time

The tools on this 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).



Time settings

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

☑ Automatically synchronize with Internet time servers

First NTP time server:	Other	0.netcomm.pool.ntp.org
Second NTP time server:	Other	1.netcomm.pool.ntp.org
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Current Time: Thu 15 Apr 2021 02:00:23

Time zone offset: (GMT+10:00) Canberra, Melbourne, Sydney

☑ Enable Daylight Saving Time

Figure 139 – Management – Internet Time Settings

Drop down to select existing time server to use, or select Other to manually enter a time server.

Click the Apply/Save button to initiate the change.

Access Control

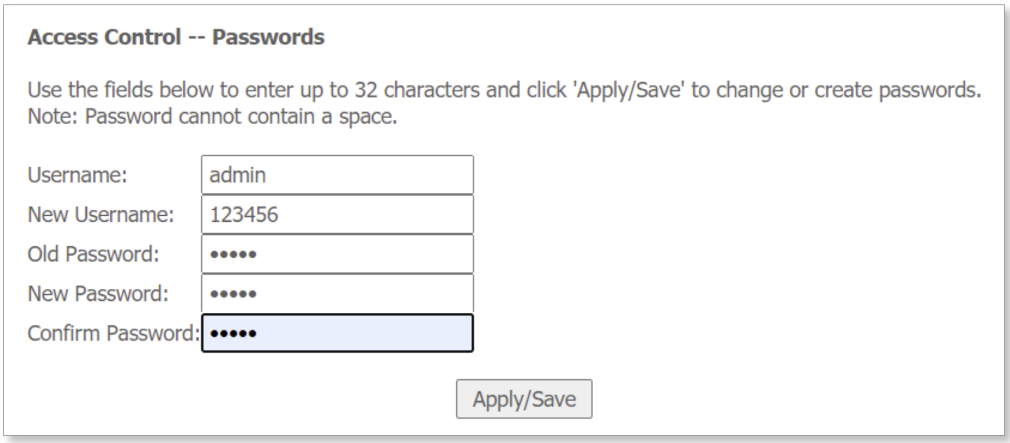
The Access Control option found in the Management drop-down menu configures access related parameters in the following three areas:

- Passwords
- Access list
- Services Control

Access Control is used to control local and remote management settings for your router.

Passwords

The **Passwords** option configures your account access password for your modem. Use the fields illustrated in the screen below to change or create your password. Passwords must be 32 characters or less with no spaces.



Access Control -- Passwords

Use the fields below to enter up to 32 characters and click 'Apply/Save' to change or create passwords.
Note: Password cannot contain a space.

Username:	admin
New Username:	123456
Old Password:	•••••
New Password:	•••••
Confirm Password:	•••••

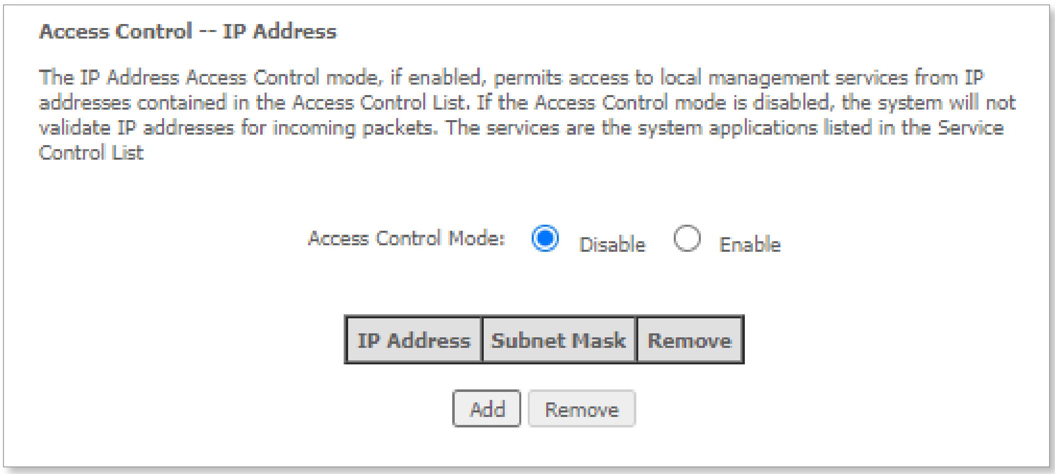
Figure 140 – Access Control – Passwords

Click the **Apply/Save** button after making any changes to continue.

Access List

When this function is enabled, only those IP addresses in the list can access local management services on the device.

This is used to restrict management access from the internet to the specified IP address.



Access Control -- IP Address

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

Access Control Mode: ● Disable ○ Enable

IP Address	Subnet Mask	Remove

Figure 141 – Access Control – IP Address Access List

To add a device to the list, click the Add button and then enter its IP Address and Subnet Mask using CIDR slash notation:

```
123.123.123.123/32
```

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

Services Control

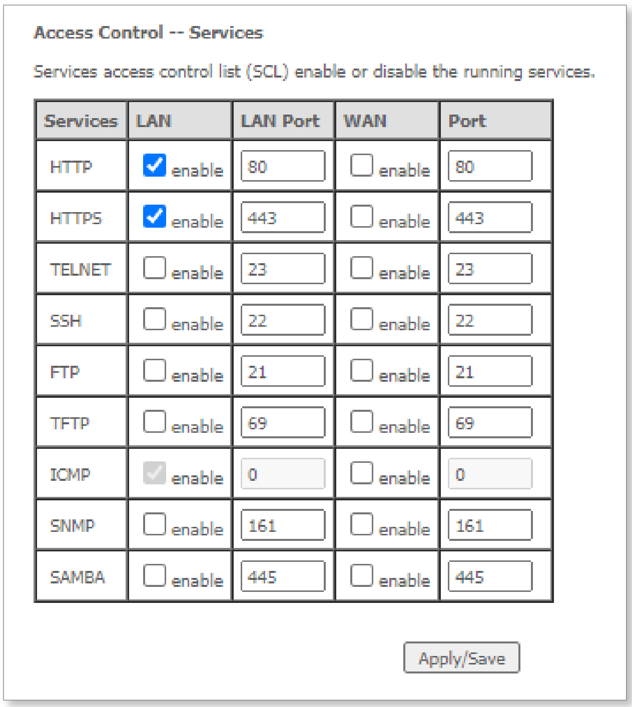
The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the ☑ enable checkbox as illustrated below and specifying the service port assigned to the service.

The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP

Click the Apply/Save button after making any changes to continue.

⚠ Important – Due to heightened security concerns, the most recent versions of some operating systems have disabled SAMBA (SMB) v1 by default. If this applies to your operating system, you may have to enable SAMBA (SMB) v1 on your operating system and then restart before this service will work.

Note – You should change your default password, before enabling a WAN service.



Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	LAN Port	WAN	Port
HTTP	☑ enable	80	□ enable	80
HTTPS	☑ enable	443	□ enable	443
TELNET	□ enable	23	□ enable	23
SSH	□ enable	22	□ enable	22
FTP	□ enable	21	□ enable	21
TFTP	□ enable	69	□ enable	69
ICMP	☑ enable	0	□ enable	0
SNMP	□ enable	161	□ enable	161
SAMBA	□ enable	445	□ enable	445

Figure 142 – Service Control List (SCL)

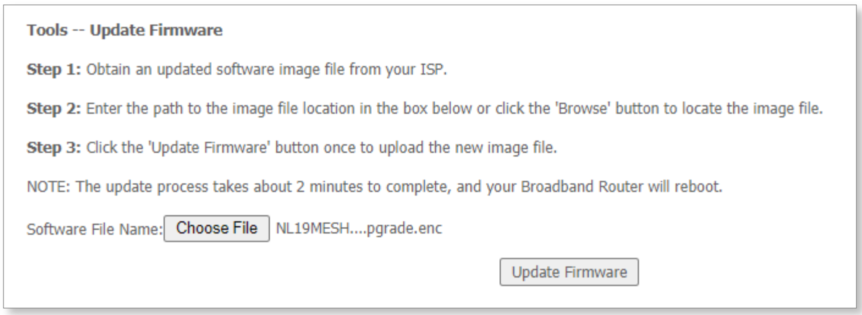
Update Firmware

This page is used to manually update your gateway's firmware. Use caution with this feature. Some ISPs may have their own custom firmware for the Wi-Fi 6 Gateway and manage this for you remotely. In this situation, manually updating the firmware yourself could cause some problems, so we recommend that you consult with your ISP first.

Generic firmware images are occasionally updated and hosted at http://support.netcommwireless.com/

1 Click the Choose File button to locate the image file.

2 Click the Update Firmware button once to upload and install the file.



Tools -- Update Firmware

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

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

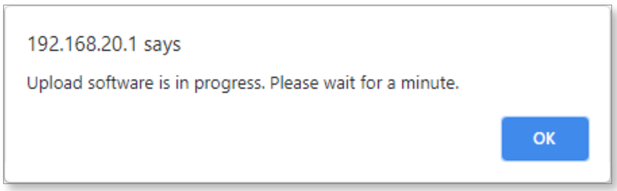
Step 3: Click the 'Update Firmware' button once to upload the new image file.

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

Software File Name: NL19MESH....pgrade.enc

Figure 143 – Update Firmware page

The following warning will appear.



192.168.20.1 says

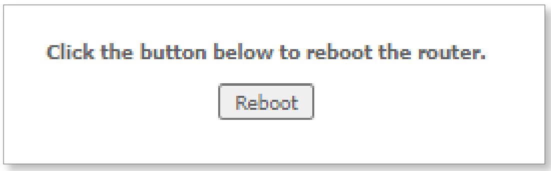
Upload software is in progress. Please wait for a minute.

Figure 144 – Update Firmware page

3 The gateway performs the firmware installation and reboots on completion.

Reboot

This option reboots the CloudMesh Gateway.



Click the button below to reboot the router.

Figure 145 – Reboot button

Please allow up to 5 minutes for device to reboot.

ⓘ Note 1. – It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings to your Network interface card (NIC).

ⓘ Note 2. – If you lose all access to your web user interface, simply press and hold the reset button on the rear panel for 10 seconds to restore default settings

Appendix: Quality of Service setup example

The following Quality of Service (QoS) settings offer a basic setup example, setting up 2 devices connecting to a CloudMesh Gateway, one with the highest priority for data and the other with the lowest priority for data. All other data packet traffic through the router assumes a default best effort setting.

Quality of Service refers to the reservation of bandwidth resources on the CloudMesh Gateway to provide different priorities to different applications, users or data flows or to guarantee a certain level of performance to a data flow.

In this implementation, QoS employs DSCP (Differentiated Services Code Point), a computer networking architecture that specifies a simple, scalable and course-grained mechanism for classifying and managing network traffic.

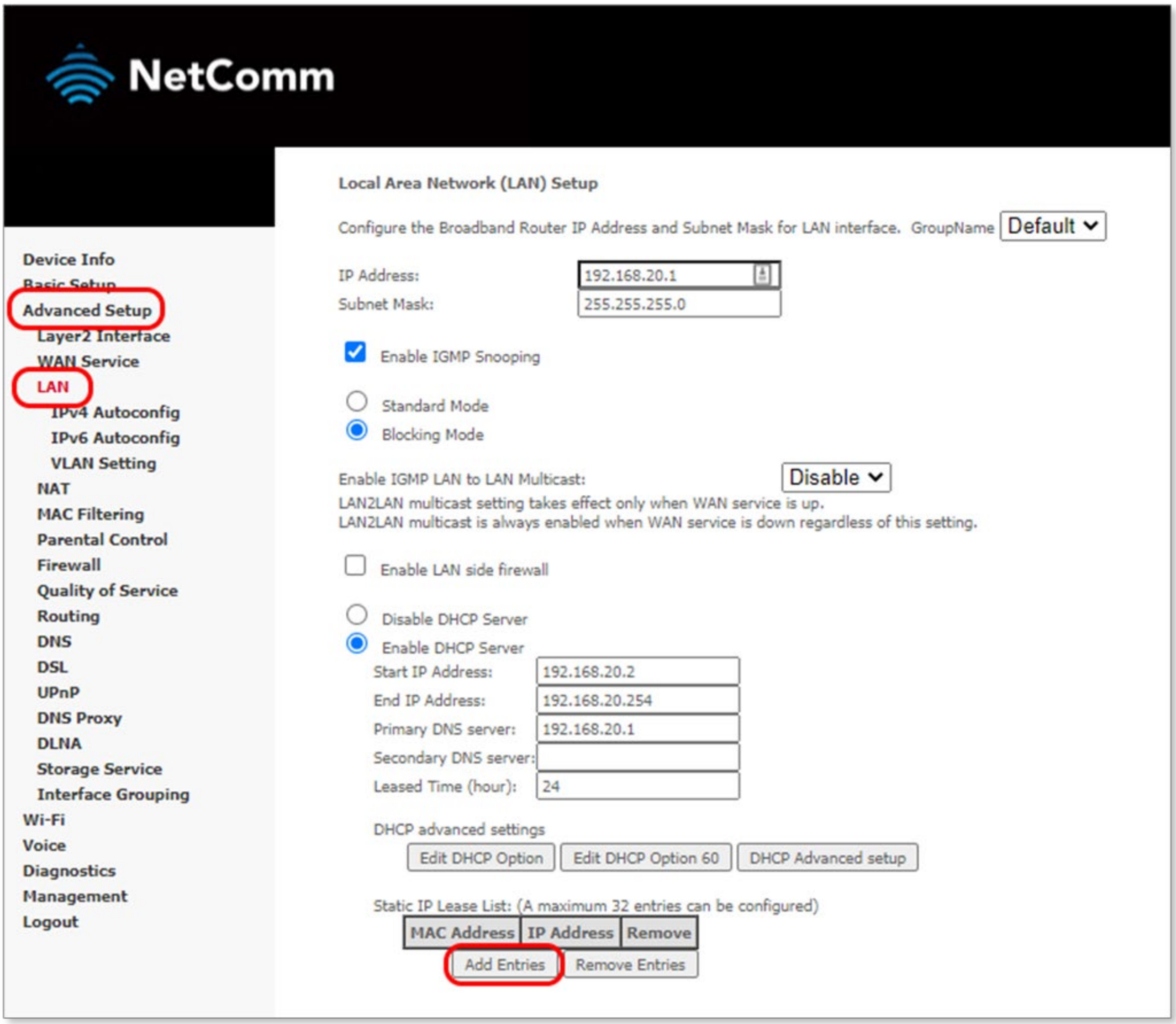
This example guide sets up QoS with two devices (PC and laptop) connecting via Ethernet cable to a CloudMesh Gateway. One device (PC) is assigned high priority traffic while the other device (laptop) is assigned a low priority. Before Quality of Service can be implemented, the first step involves reserving an IP address for each device, identified by their unique MAC addresses.

Reserving IP addresses

So that QoS settings, custom NAT settings, and parental control settings can be managed for each device, it is necessary to reserve an IP address for each of the devices connecting to the CloudMesh Gateway.

Reserved IP addresses are not required to be within the DHCP server range, however they are required to be with-in the LAN subnet range:

1. Navigate to http://192.168.20.1 in a web browser.
2. When prompted, enter `admin` as both the username and password.
3. Select Advanced Setup > LAN



Local Area Network (LAN) Setup

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

IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode

● Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable

LAN2LAN multicast setting takes effect only when WAN service is up.
LAN2LAN multicast is always enabled when WAN service is down regardless of this setting.

□ Enable LAN side firewall

○ Disable DHCP Server

● Enable DHCP Server

Start IP Address: 192.168.20.2

End IP Address: 192.168.20.254

Primary DNS server: 192.168.20.1

Secondary DNS server:

Leased Time (hour): 24

DHCP advanced settings

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

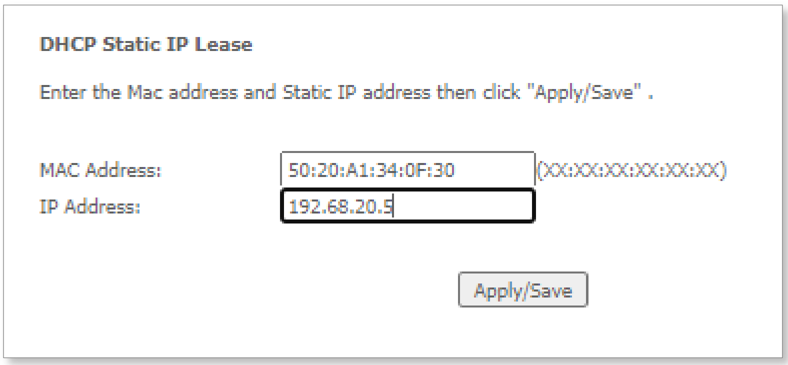
MAC Address	IP Address	Remove

Figure 146 – Advanced Setup > LAN page

4 Click the Add Entries button.

5 Enter the MAC address of the computer/device you are connecting to the router. The MAC address is a 12-character set of numbers and letters (A-F), where every 2 characters separated by a colon (:).

6 Enter the IP address of the computer/device. This is the local address in the range of 192.168.20.x where x = a number between 2 and 254.



DHCP Static IP Lease

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

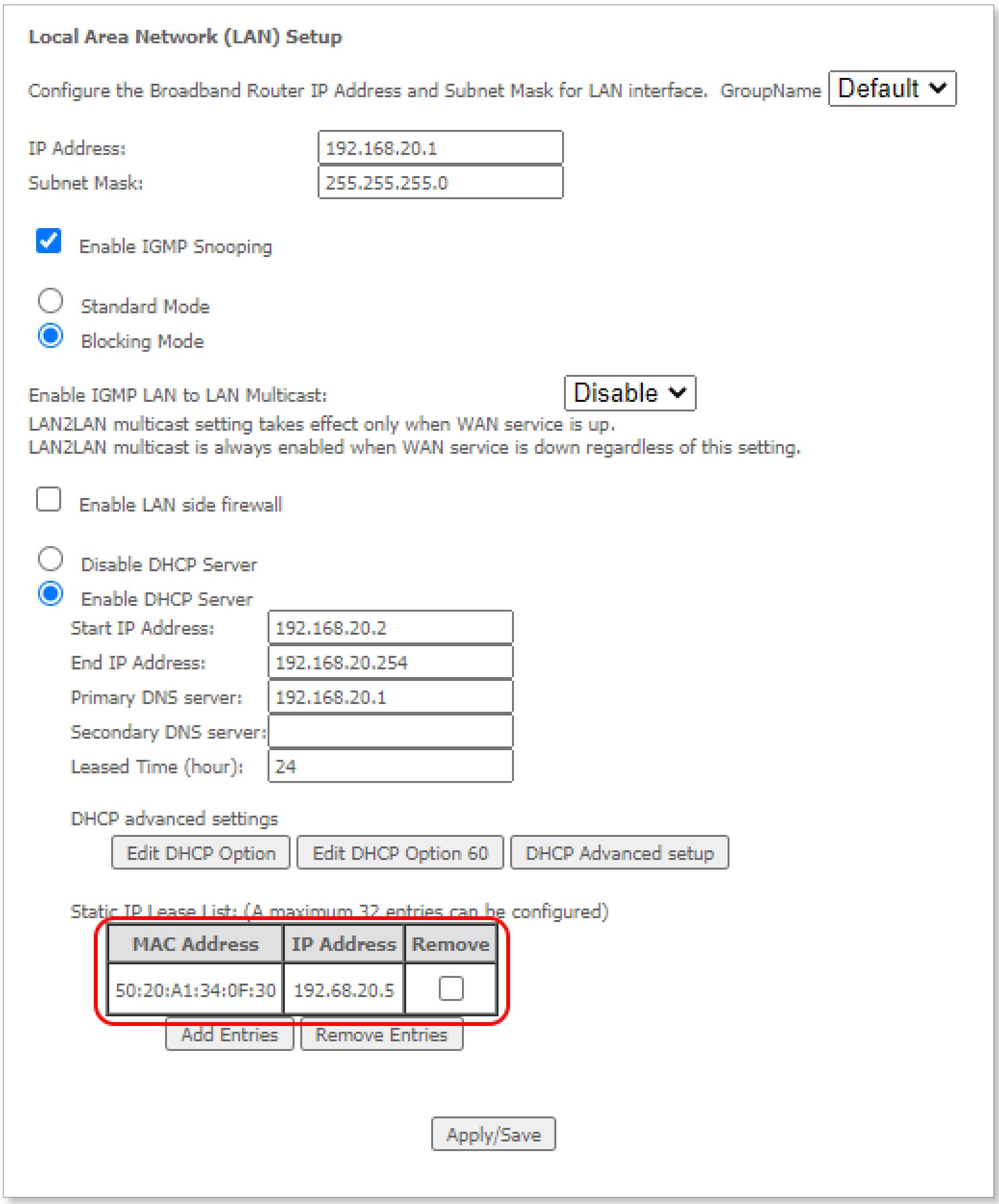
MAC Address: 50:20:A1:34:0F:30 (XX:XX:XX:XX:XX:XX)

IP Address: 192.68.20.5

Figure 147 – DHCP Static IP Lease details

7 Click the **Apply/Save** button.

8 Complete steps 4 through 7 for each device connected to the CloudMesh Gateway. Each entry will be listed in the Static IP Lease List as shown below.



Local Area Network (LAN) Setup

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

IP Address:	192.168.20.1
Subnet Mask:	255.255.255.0

☑ Enable IGMP Snooping

○ Standard Mode
● Blocking Mode

Enable IGMP LAN to LAN Multicast: Disable
LAN2LAN multicast setting takes effect only when WAN service is up.
LAN2LAN multicast is always enabled when WAN service is down regardless of this setting.

□ Enable LAN side firewall

○ Disable DHCP Server
● Enable DHCP Server

Start IP Address:	192.168.20.2
End IP Address:	192.168.20.254
Primary DNS server:	192.168.20.1
Secondary DNS server:	
Leased Time (hour):	24

DHCP advanced settings

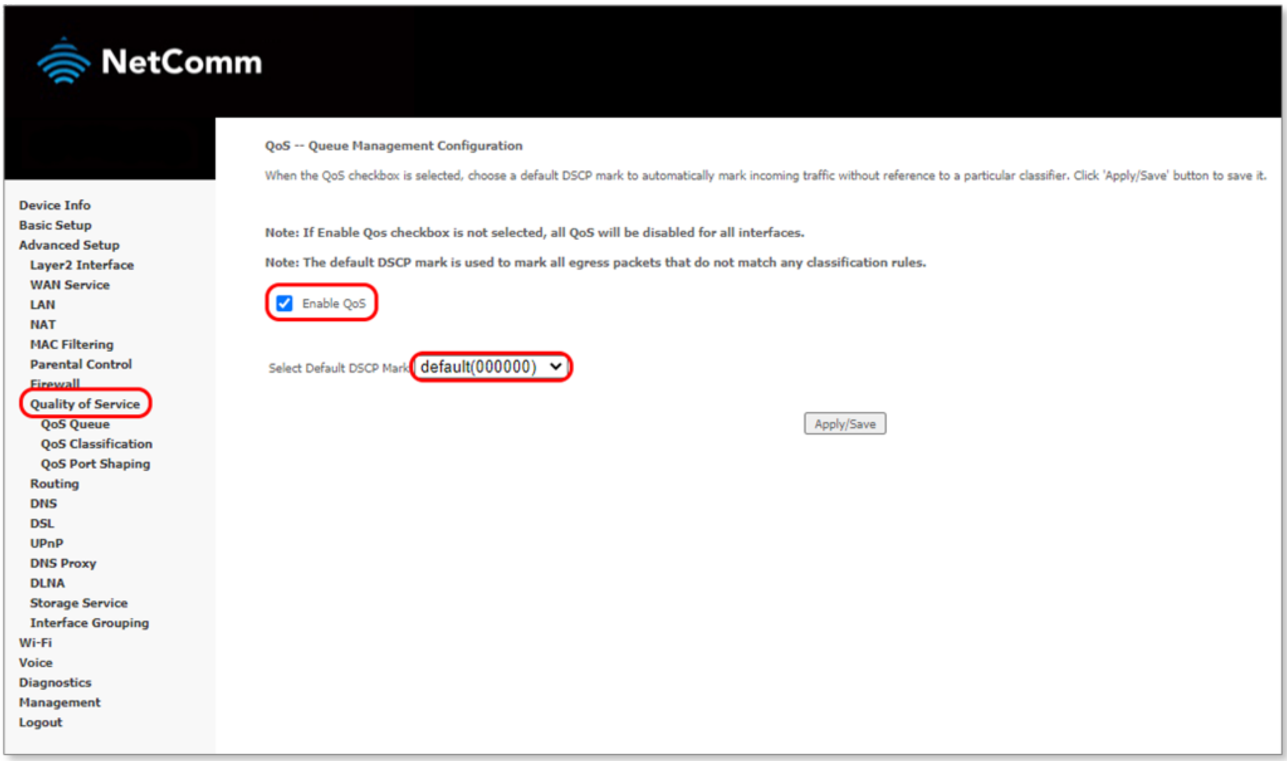
Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
50:20:A1:34:0F:30	192.68.20.5	□

Figure 148 – LAN Setup

QoS Configuration Settings

1 Select Advanced Setup > Quality of Service



QoS -- Queue Management Configuration

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

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

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

☑ Enable QoS

Select Default DSCP Mark: default(000000)

Figure 149 – QoS – Queue Management Configuration

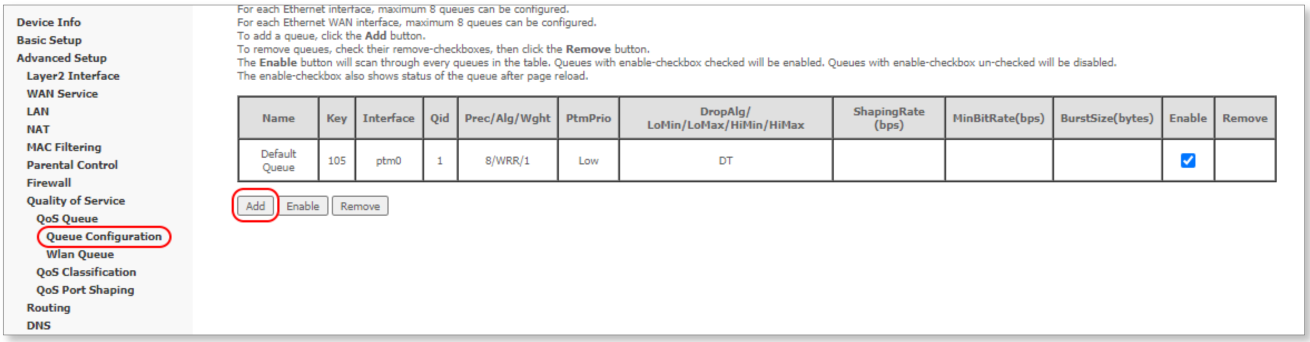
2 Select the Enable QoS option.

3 Select the Default DSCP Mark as default(000000).

4 Click the Apply/Save button.

High Priority QoS Queue Configuration

1 Select Advanced > Quality of Service > Queue Config.

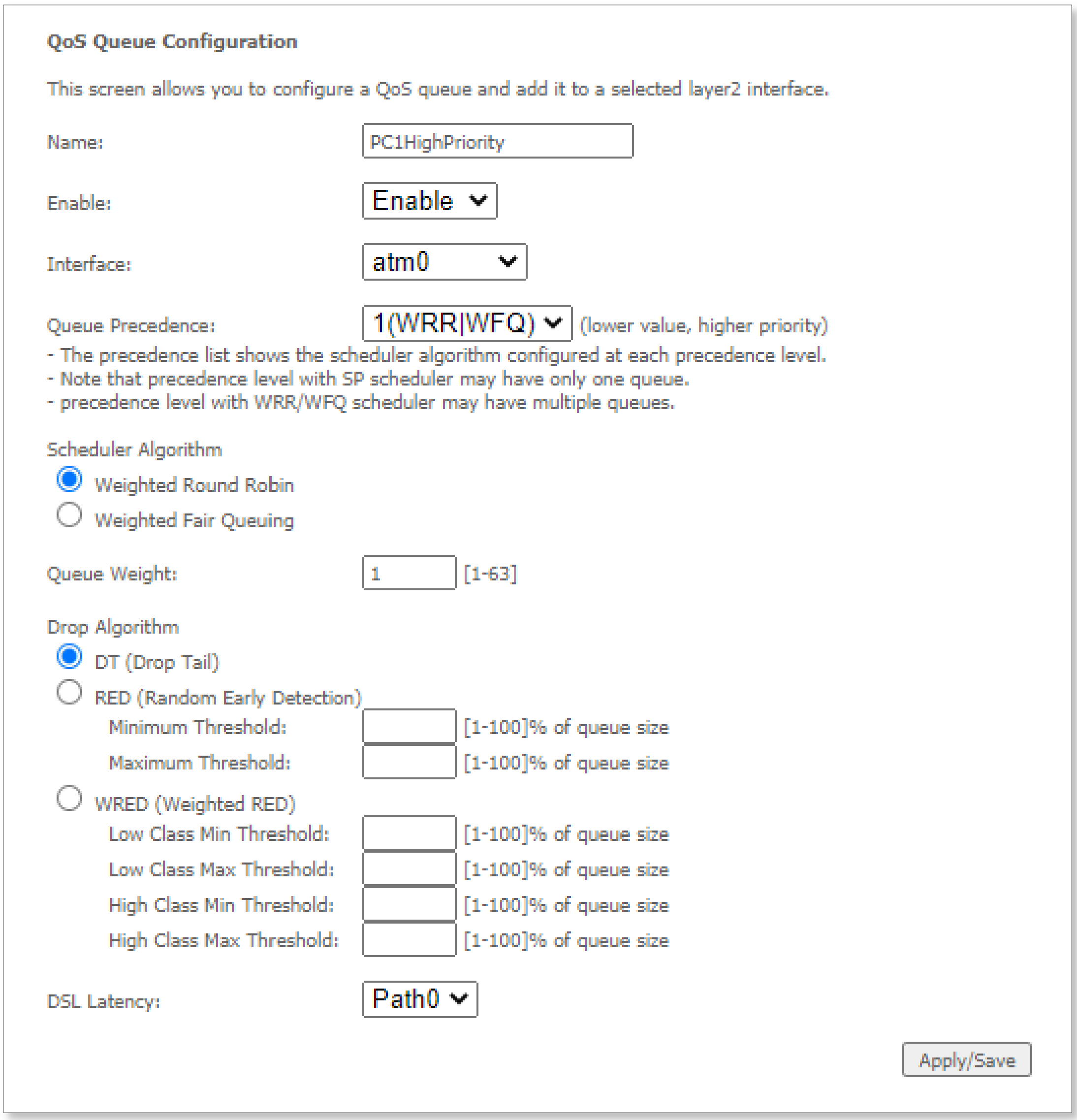


For each Ethernet interface, maximum 8 queues can be configured.
For each Ethernet WAN interface, maximum 8 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.

Name	Key	Interface	Qid	Prec/Alg/Wght	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
Default Queue	105	ptm0	1	8/WRR/1	Low	DT				☑	

Figure 150 – QoS – Queue List

2 Click the Add button.



QoS Queue Configuration

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

Name:	PC1HighPriority
Enable:	Enable
Interface:	atm0
Queue Precedence:	1(WRR|WFQ) (lower value, higher priority)

- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Scheduler Algorithm

● Weighted Round Robin

○ Weighted Fair Queuing

Queue Weight: 1 [1-63]

Drop Algorithm

● DT (Drop Tail)

○ RED (Random Early Detection)

Minimum Threshold: [1-100]% of queue size

Maximum Threshold: [1-100]% of queue size

○ WRED (Weighted RED)

Low Class Min Threshold: [1-100]% of queue size

Low Class Max Threshold: [1-100]% of queue size

High Class Min Threshold: [1-100]% of queue size

High Class Max Threshold: [1-100]% of queue size

DSL Latency: Path0

Figure 151 – QoS – Queue Configuration 1

3 Enter a name of 15 characters or less to reflect the device that will have high priority QoS, e.g. PC1HighPriority.

4 Set the Enable option to **Enable**.

5 Set the Interface to **atm0**

6 Enter a **Precedence**. For the highest priority, set it to **1**. For the lowest priority use **3**.

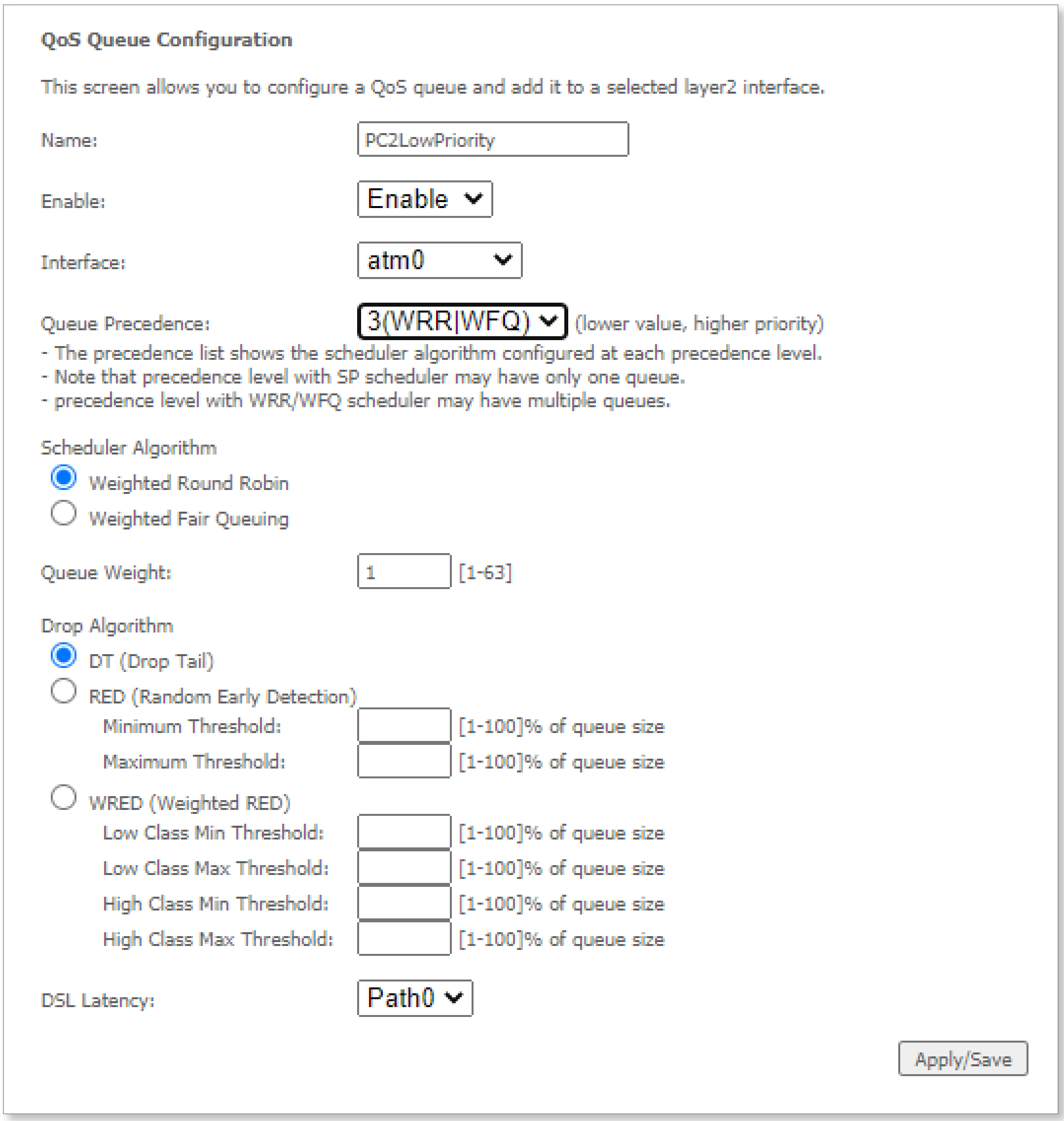
7 Set the **DSL Latency** as **Path0**.

8 Click the **Save/Apply** button.

Low Priority QoS Queue Configuration

1 Select Advanced > Quality of Service > Queue Config.

2 Click the Add button.



QoS Queue Configuration

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

Name: PC2LowPriority

Enable: Enable

Interface: atm0

Queue Precedence: 3(WRR|WFQ) (lower value, higher priority)
- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Scheduler Algorithm
● Weighted Round Robin
○ Weighted Fair Queuing

Queue Weight: 1 [1-63]

Drop Algorithm
● DT (Drop Tail)
○ RED (Random Early Detection)
Minimum Threshold: [1-100]% of queue size
Maximum Threshold: [1-100]% of queue size
○ WRED (Weighted RED)
Low Class Min Threshold: [1-100]% of queue size
Low Class Max Threshold: [1-100]% of queue size
High Class Min Threshold: [1-100]% of queue size
High Class Max Threshold: [1-100]% of queue size

DSL Latency: Path0

Figure 152 – QoS – Queue Configuration 2

3 Enter a name of 15 characters or less to reflect the device that will have low priority QoS e.g. PC2LowPriority.

4 Set the Enable option to Enable.

5 Set the Interface to atm0

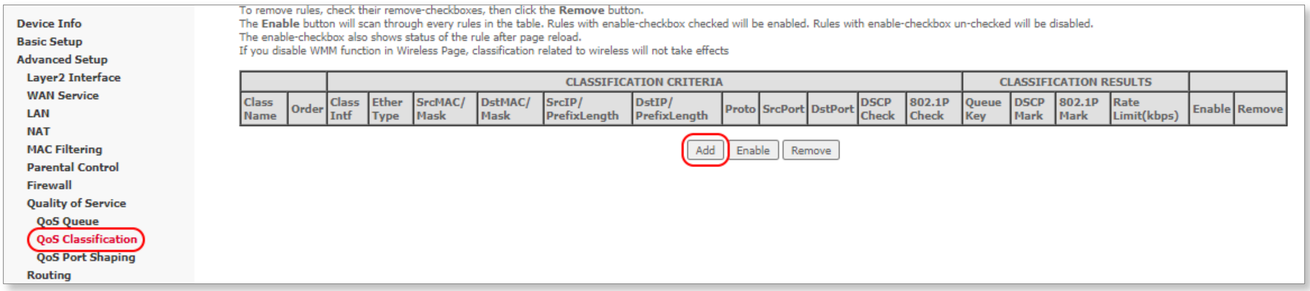
6 Enter a Precedence. For the lowest priority, set it to 3. For the highest priority use 1.

7 Set the DSL Latency as Path0.

8 Click the Save/Apply button.

High Priority QoS Classification

1 Select **Advanced Setup > Quality of Service > QoS Classification**.

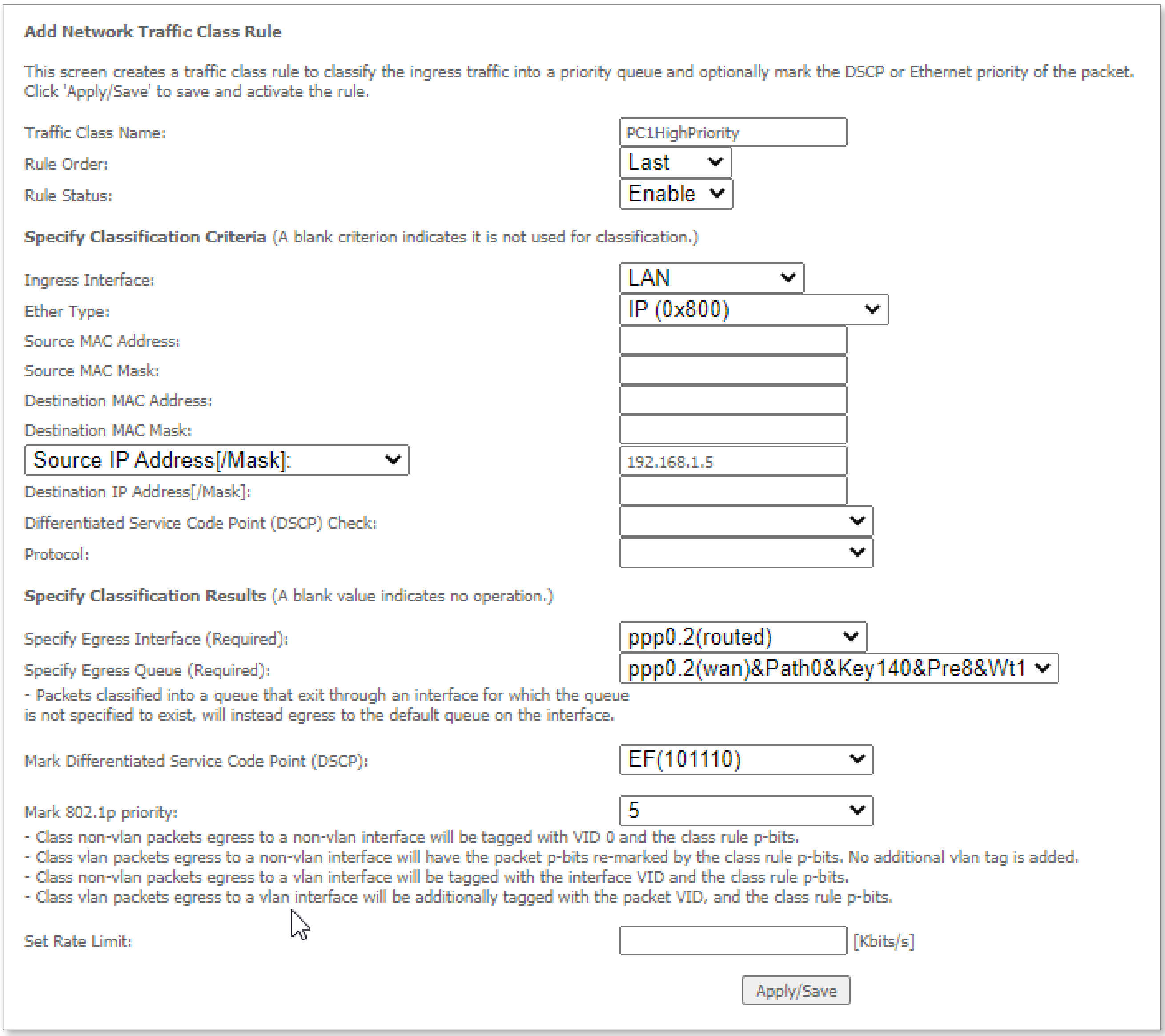


To remove rules, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every rules in the table. Rules with enable-checkbox checked will be enabled. Rules with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the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

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

Figure 153 – QoS Classification configuration

2 Click the **Add** button.



Add Network Traffic Class Rule

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

Traffic Class Name: PC1HighPriority
Rule Order: Last
Rule Status: Enable

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

Ingress Interface: LAN
Ether Type: IP (0x800)
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
Source IP Address[/Mask]: 192.168.1.5
Destination IP Address[/Mask]:
Differentiated Service Code Point (DSCP) Check:
Protocol:

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

Specify Egress Interface (Required): ppp0.2(routed)
Specify Egress Queue (Required): ppp0.2(wan)&Path0&Key140&Pre8&Wt1
- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP): EF(101110)

Mark 802.1p priority: 5
- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: [Kbits/s]

Figure 154 – Configure Network Traffic Class Rule

3 Enter a Traffic Class Name reflecting the High Priority QoS rule, e.g. PC1HighPriority.

4 Leave the Rule Order as Last.

5 Set the Rule Status to Enable.

6 Set the Class Interface according to how the device connects to the router. In the example above, LAN is selected. Other options are Wireless, Local and USB.

7 Set the Ether Type to IP(0x800). Other options include ARP(0x8086), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100).

8 Enter the Source MAC Address of the device, the unique 12 character signature with every 2 characters separated by a colon(:), that you previously entered to reserve the device's IP address.

9 Enter the Source IP Address of the device that you previously entered into the Static IP Lease List, in the range of 192.168.1.x In the example above the IP address is 192.168.1.5.

10 Enter a Destination MAC Address if the connection is to a single device. This is useful for VPN connections. If you wish the destination MAC address to be any address leave the field blank.

11 Enter a Destination IP Address if the connection is to a single device. This is useful for VPN connections. If you wish the destination IP address to be any address leave the field blank.

12 Enter a Destination Subnet Mask if you have entered a Destination MAC address and Destination IP address. This would normally be 255.255.255.0 unless your system administrator advises otherwise. If you have not entered a Destination MAC or IP address leave the field blank.

13 Set the Differentiated Service Code Point (DSCP) Check to EF(101110).

14 Set the Protocol to TCP. Other options include UDP, ICMP or IGMP.

15 Set "Assign Classification Queue" to Priority 1 (in the example above pppoa0&atm0&Path0&Key38&Pre1). Other options or priority 2 and 3. Priority 1 gives the highest priority with priority 3 being the lowest.

16 Set Mark Differentiated Service Code Point (DSCP) as EF(101110).

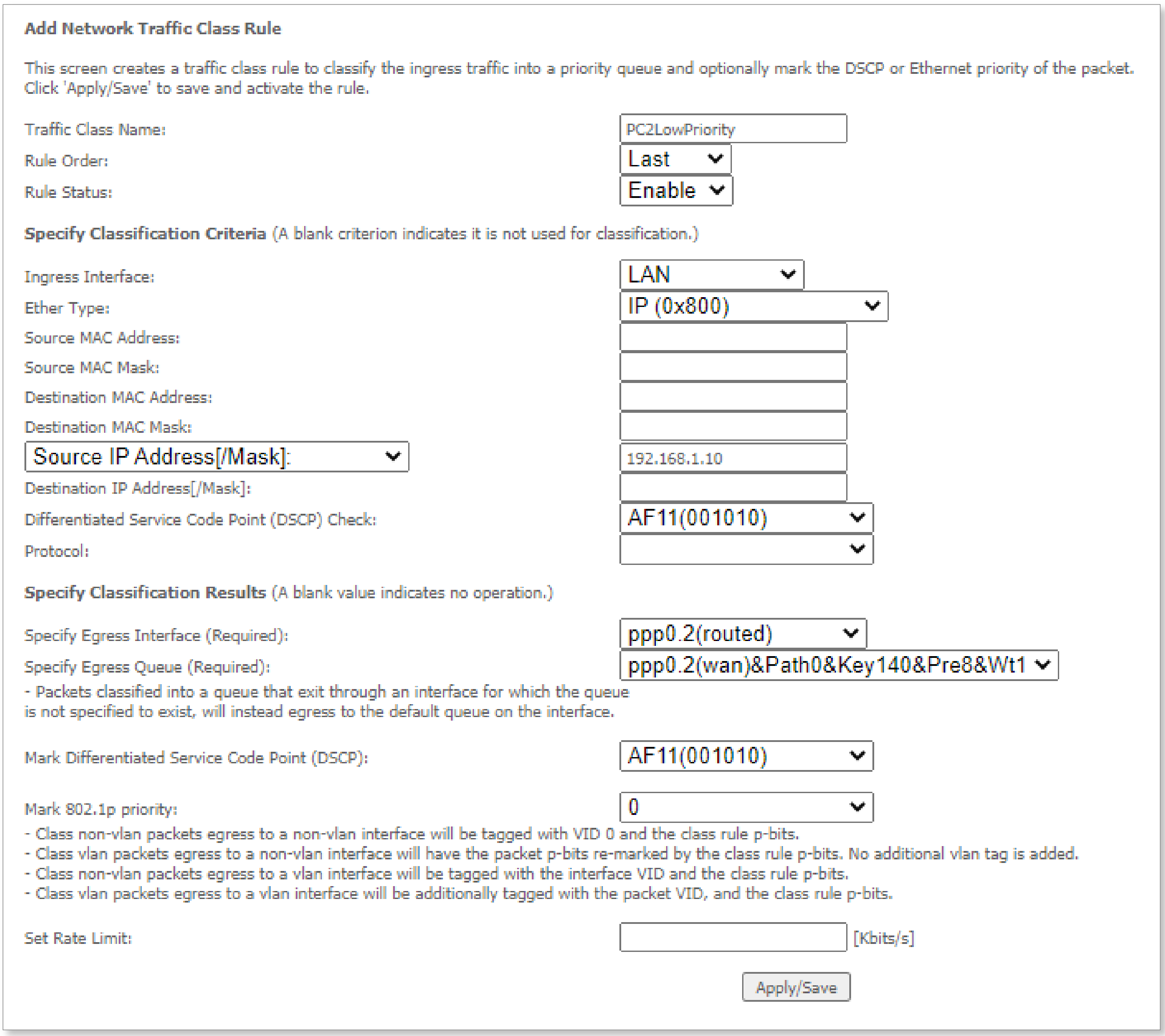
17 Set Mark 802.1p Priority as 5. In the scale 0-7, 0 is best effort, 6 and 7 are reserved for networking performance so set 5 as the highest priority.

18 Click the Apply/Save button.

Low Priority QoS Classification

1 Select Advanced Setup > Quality of Service > QoS Classification.

2 Click the Add button.



Add Network Traffic Class Rule

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

Traffic Class Name:	PC2LowPriority
Rule Order:	Last
Rule Status:	Enable

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

Ingress Interface:	LAN
Ether Type:	IP (0x800)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address[/Mask]:	192.168.1.10
Destination IP Address[/Mask]:	
Differentiated Service Code Point (DSCP) Check:	AF11(001010)
Protocol:	

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

Specify Egress Interface (Required):	ppp0.2(routed)
Specify Egress Queue (Required):	ppp0.2(wan)&Path0&Key140&Pre8&Wt1

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

Mark Differentiated Service Code Point (DSCP):	AF11(001010)
Mark 802.1p priority:	0

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

Set Rate Limit: [Kbits/s]

Figure 155 – QoS Network Traffic Class Rule configuration

3 Enter a Traffic Class Name reflecting the High Priority QoS rule; e.g. PC2LowPriority.

4 Leave the Rule Order as Last.

5 Set the Rule Status to Enable.

6 Set the Class Interface according to how the device connects to the router. In the example above LAN is selected. Other options are Wireless, Local and USB.

7 Set the Ether Type to IP(0x800). Other options include ARP(0x8086), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100).

8. Enter the **Source MAC Address** of the device, the unique 12 character signature with every 2 characters separated by a colon(:), that you previously entered to reserve the device's IP address.

9. Enter the **Source IP Address** of the device that you previously entered into the Static IP Lease List, in the range of 192.168.1.x. In the example above the IP address is 192.168.1.10.

10. Enter a **Destination MAC Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination MAC address to be any address leave the field blank.

11. Enter a **Destination IP Address** if the connection is to a single device. This is useful for VPN connections. If you wish the destination IP address to be any address leave the field blank.

12. Enter a **Destination Subnet Mask** if you have entered a Destination MAC address and Destination IP address. This would normally be 255.255.255.0 unless your system administrator advises otherwise. If you have not entered a Destination MAC or IP address leave the field blank.

13. Set the **Differentiated Service Code Point (DSCP)** Check to **AF11(001010).**

14. Set the **Protocol** to **TCP**. Other options include **UDP**, **ICMP** or **IGMP**.

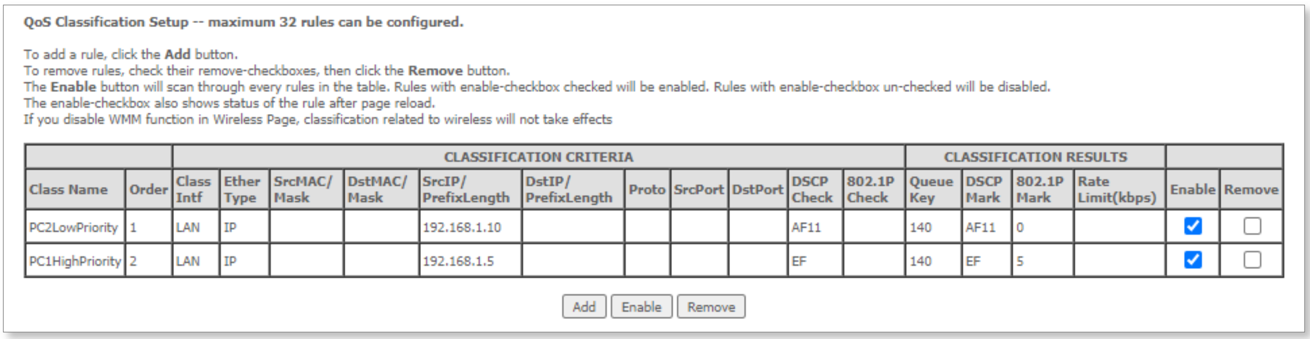
15. Set "**Assign Classification Queue**" to Priority 3 (in the example above pppoa0&atm0&Path0&Key39&Pre3). Other options are priority 1 and 2. Priority 1 gives the highest priority with priority 3 being the lowest.

16. Set **Mark Differentiated Service Code Point (DSCP)** as **AF11(001010).**

17. Set **Mark 802.1p Priority** as **0**. In the scale 0-7, 0 is best effort, 6 and 7 are reserved for networking performance so set 0 as the lowest priority.

18. Click the **Apply/Save** button.

19. You now have 2 Quality of Service rules implemented for 2 devices connecting to the CloudMesh Gateway.



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

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

		CLASSIFICATION CRITERIA											CLASSIFICATION RESULTS					
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ PrefixLength	DstIP/ PrefixLength	Proto	SrcPort	DstPort	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
PC2LowPriority	1	LAN	IP			192.168.1.10					AF11		140	AF11	0		☑	☐
PC1HighPriority	2	LAN	IP			192.168.1.5					EF		140	EF	5		☑	☐

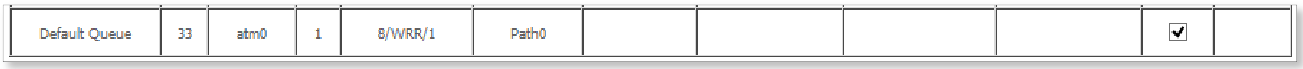
Figure 156 – QoS Classification setup page

20. Select **Management** > **Reboot**. Click the **Reboot** button to restart the router and save the new settings.

21. To test your Quality of Service settings try running speed-tests (http://speedtest.net) on both PCs/devices **simultaneously**.

Limiting the upstream rate

1 By default, a QoS queue is created when a WAN interface is created but it is disabled by default. On the QoS Queue page, enable the queue for the appropriate WAN interface.

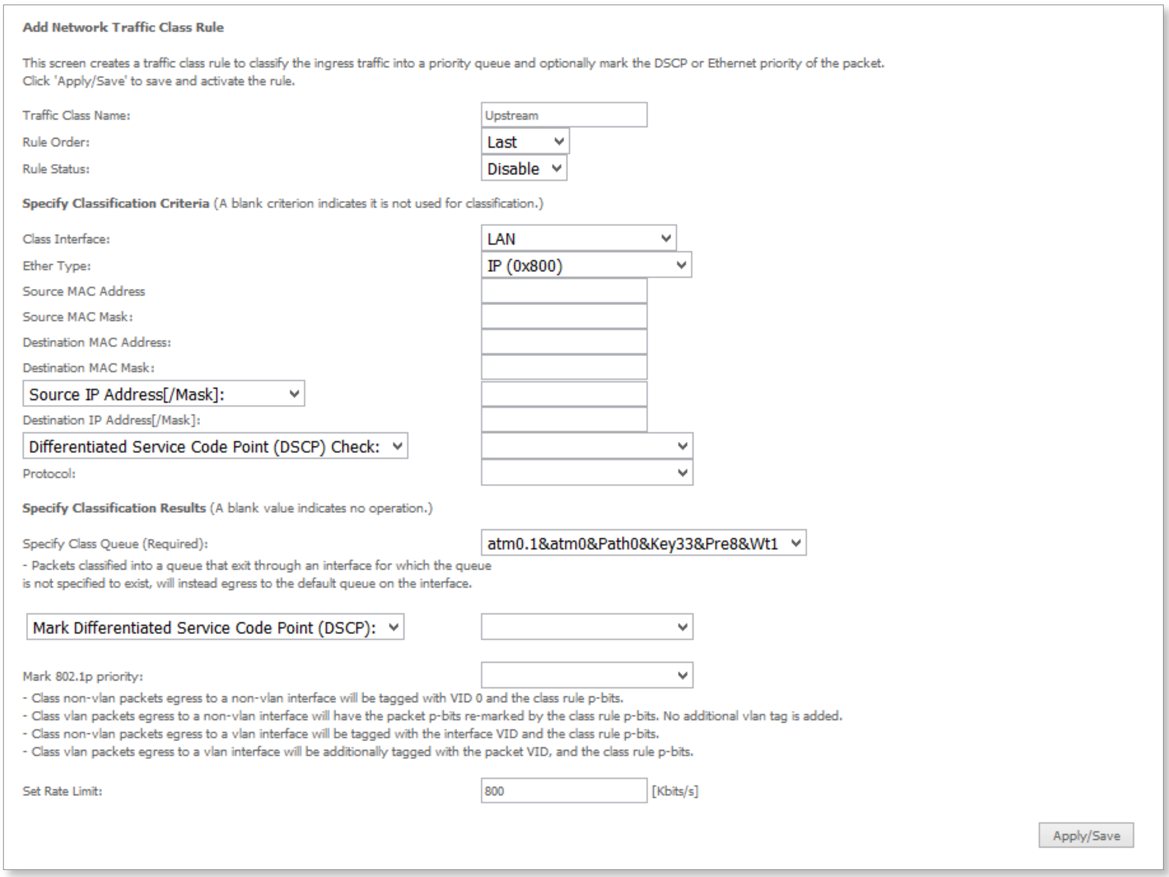


Default Queue	33	atm0	1	8/WRR/1	Path0					☑	

Figure 157 – QoS Queue details

2 On the QoS Classification page, add a rule to limit the upstream rate, for example:

- Classification Criteria:
- Class Interface: LAN
- Ether type: IP
- Classification Results:
- Class Queue: the queue that was enabled in Step 1
- Set rate-limit: set according to your preference



Add Network Traffic Class Rule

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

Traffic Class Name: Upstream
Rule Order: Last
Rule Status: Disable

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

Class Interface: LAN
Ether Type: IP (0x800)
Source MAC Address
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:
Source IP Address[/Mask]:
Destination IP Address[/Mask]:
Differentiated Service Code Point (DSCP) Check:
Protocol:

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

Specify Class Queue (Required): atm0.1&atm0&Path0&Key33&Pre8&Wt1
- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:
- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

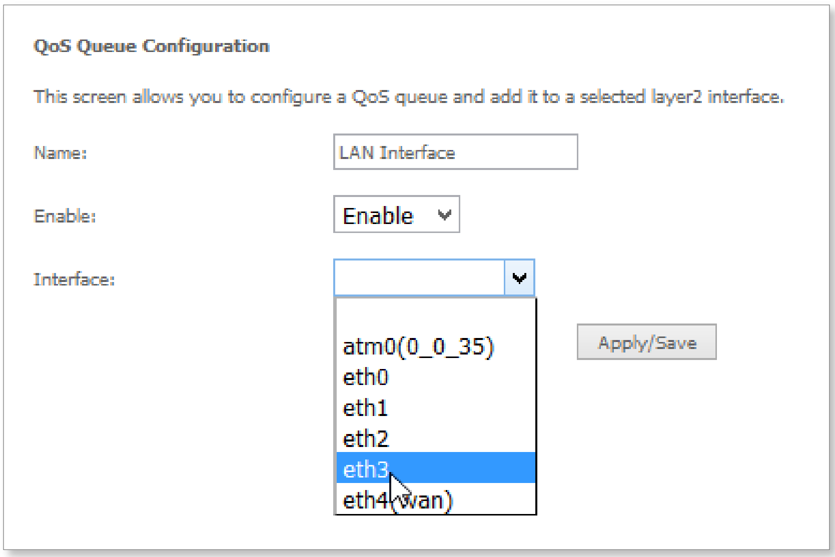
Set Rate Limit: 800 [Kbits/s]

Figure 158 – Network Traffic Class Rule

3 Click **Apply/Save**.

Limiting the downstream rate

1 Navigate to the QoS Queue Configuration page to add a queue for the LAN interface, for example:



QoS Queue Configuration

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

Name: LAN Interface

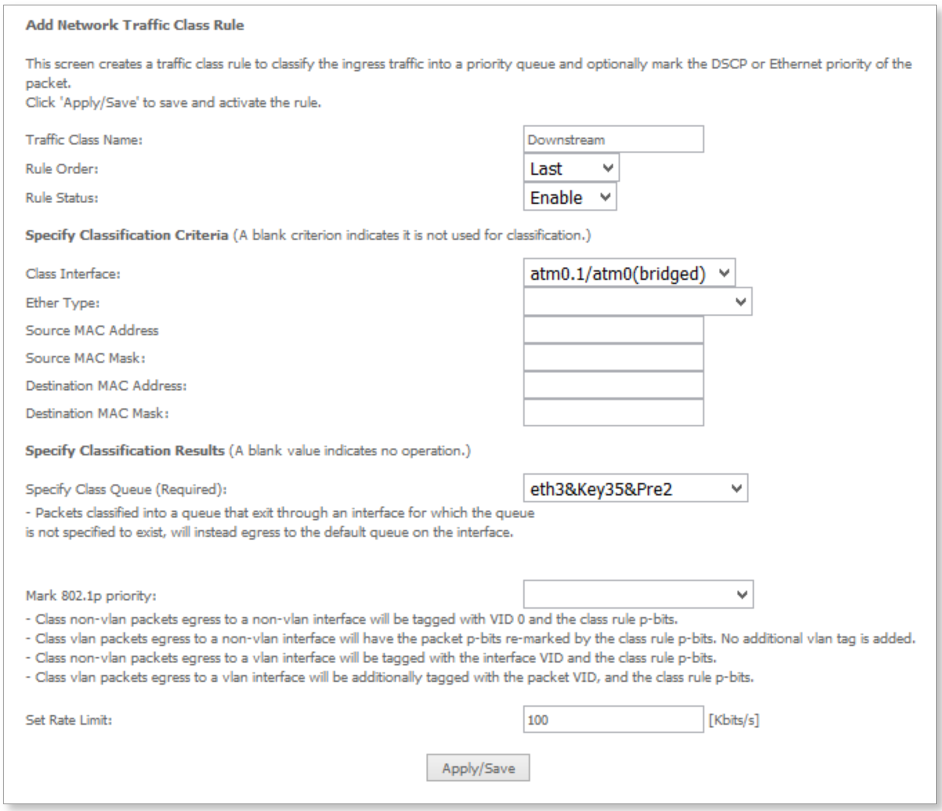
Enable: Enable

Interface:

Figure 159 – QoS Queue Configuration

2 On the QoS Classification page, add a rule to limit the downstream rate, for example:

- Classification Criteria:
- Class Interface: the appropriate WAN interface
- Classification Results:
- Class Queue: the queue that was created on Step 1
- Set rate-limit: set according to your preference



Add Network Traffic Class Rule

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

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

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

Class Interface:	atm0.1/atm0(bridged)
Ether Type:	
Source MAC Address	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

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

Specify Class Queue (Required): eth3&Key35&Pre2
- Packets classified into a queue that exit through an interface for which the queue is not specified to exist, will instead egress to the default queue on the interface.

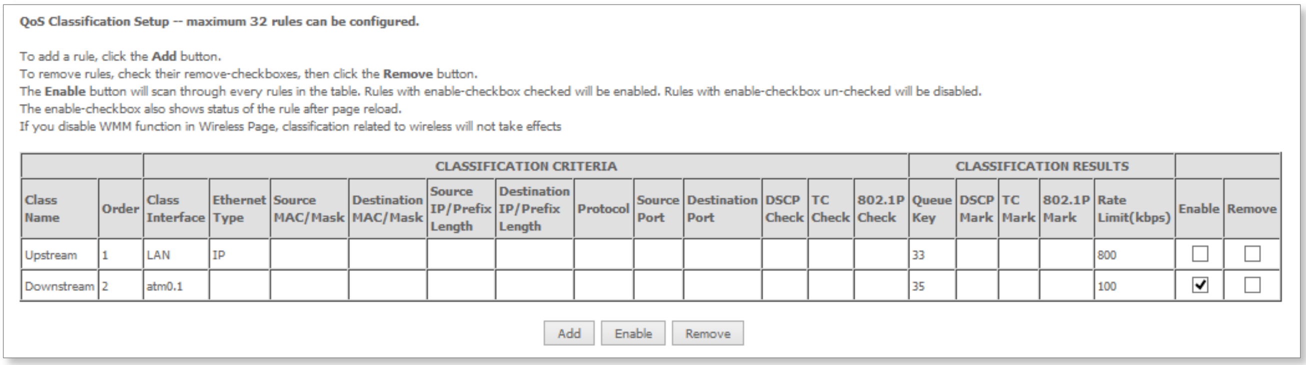
Mark 802.1p priority:
- Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.
- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added.
- Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits.
- Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit: 100 [Kbits/s]

Figure 160 – Network Traffic class Rule

3 Click the **Apply/ Save** button.

The QoS Classification table looks like this:



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 Interface	Ethernet Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Prefix Length	Destination IP/Prefix Length	Protocol	Source Port	Destination Port	DSCP Check	TC Check	802.1P Check	Queue Key	DSCP Mark	TC Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove
Upstream	1	LAN	IP											33				800	□	□
Downstream	2	atm0.1												35				100	☑	□

Figure 161 – QoS Classification list