NetCommWireless

NF18ACV

VDSL/ADSL2+ Dual Band AC1600 Gigabit Gateway with VoIP

User Guide

Important Notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless NF18ACV to transmit or receive such data.

Copyright

Note – This document is subject to change without notice.

Save our environment

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with domestic waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

Document history

This guide covers the following products:

VDSL/ADSL2+ Dual Band AC1600 Gigabit Gateway with VoIP (NF18ACV)

Ver.	Document description	Date
v1.0	Initial document release	August 2017

Table i. – Document revision history

Contents

Overview

Introduction

This manual provides information related to the installation, operation, and use of the NF18ACV.

Target audience

The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

Prerequisites

Before continuing with the installation of your NF18ACV, please confirm that you meet the minimum system requirements below.

- An activated ADSL/VDSL or pre-configured WAN connection.
- A computer with a working Ethernet adapter or wireless 802.11a/b/g/n/ac capability and the TCP/IP Protocol installed.
- A current version of a web browser such as Internet Explorer®, Mozilla Firefox® or Google Chrome™.

Notation

The following symbols are used in this manual:

Note – The following note provides useful information.

Attention – The following situation requires attention.

Warning – The following note provides a warning.

Welcome

Thank you for purchasing a NetComm Wireless NF18ACV. This guide contains all the information you need to configure your device.

Product overview

- Fully featured VDSL2 / ADSL2+ gateway
- 4 x Gigabit Ethernet 10/100/1000 LAN ports
- nbn and UFB ready – ultra-fast connection to nbn and UFB fibre network - 1 x 10/100/1000 Gigabit Ethernet WAN port
- VoIP feature for HD quality voice calls - connect up to 2 telephones
- Next generation WiFi 802.11 AC1600, dual band concurrent, for multiple high-speed wireless connections
- 2 x WPS push buttons for the quick and easy connection of wireless devices on both 2.4GHz and 5GHz bands
- Access and share media and file content across the wireless home network
- Device performance monitoring and management through TR-069

Package contents

The NF18ACV package consists of:

- 1 x NetComm Wireless NF18ACV VDSL2/ADSL2+ Dual Band AC1600 Wireless Gigabit Gateway with VoIP
- 1 x RJ45 Ethernet cable
- 1 x RJ11 Telephone cable
- 1 x WiFi Security card
- 1 x Warranty card
- 1 x Power supply (12V/2A)

If any of these items are missing or damaged, please contact NetComm Wireless Support immediately by visiting the NetComm Wireless Support website at: http://www.netcommwireless.com/contact-forms/support

Product features

Perfect for

- Ultra-fast connection to your fixed line VDSL2/ADSL2+ service
- High-speed connection to nbn or UFB Fibre networks FTTN/FTTB and FTTH/FTTP
- Triple play services offer including Voice over IP
- Creating a powerful wireless home network and media sharing

Key Features

- Fully featured VDSL2 / ADSL2+ gateway
- 4 x Gigabit Ethernet 10/100/1000 LAN ports
- nbn and UFB ready – ultra-fast connection to nbn and UFB fibre network - 1 x 10/100/1000 Gigabit Ethernet WAN port
- VoIP feature for HD quality voice calls - connect up to 2 telephones
- Next generation WiFi 802.11 AC1600, dual band concurrent, for multiple high-speed wireless connections
- 2x WPS push buttons for the quick and easy connection of wireless devices on both 2.4GHz and 5GHz bands
- Access and share media and file content across the wireless home network
- Device performance monitoring and management through TR-069

NF18ACV

The NetComm Wireless NF18ACV smart residential VDSL2/ADSL2+ wireless gateway brings an enhanced and blazing fast broadband experience to the home.

nbn and UFB ready

Featuring VDSL2/ADSL2 technologies as well as a Gigabit WAN port, the NF18ACV is a 3-in-1 gateway that provides access to **ADSL** networks, **VDSL** and all **nbn** and **UFB** fibre network options: **FTTN**, **FTTB**, **FTTH**.

Triple play services

The NF18ACV is a triple play services enabler that supports the transmission of high-speed data, multi HD/UHD IPTV and over the top video streaming, VoIP feature for HD quality voice calls with the capacity to connect 2 phones.

Enhanced wireless experience

The NF18ACV gateway embeds the newest generation of WiFi (802.11 ac) for powerful access point and video grade wireless capabilities. It allows both **2.4GHz** and **5GHz** bands to work concurrently, ensuring interoperability with all wireless equipment in the house.

The NF18ACV is equipped with 5GHz 3 x 3 MIMO and 2.4GHz 2 x 2 MIMO internal antennas to provide optimum reception while offering a powerful signal throughout the home. Create an ultra-fast **1600 Mbps**[1] **WiFi** home network and connect a multitude of wireless devices such as smart TVs, set top boxes, laptops, tablets, computers, NAS, smart phones and gaming consoles with upgraded coverage and performance.

Media sharing

Connect a **USB device** to the NF18ACV gateway, access and share all A/V media and file content with all of the connected devices in the house in real time. The NF18ACV becomes the media hub of the house using **DLNA/UPnP** standard and enhanced wireless capabilities to create a reliable high-speed home network.

[1] Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11n and 802.11ac specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

Physical dimensions and indicators

LED indicators

The NF18ACV has been designed to be placed on a desktop. All of the cables exit from the rear for easy organization. The display is visible on the front of the NF18ACV to provide you with information about network activity and the device status. The following is an explanation of each of the indicator lights.

LED INDICATOR	ICON	COLOUR	DEFINITION
Power		Green	The NF18ACV is powered on and operating normally.
		Off	The power is off.
DSL	DSL	Off	No DSL signal detected.
		Green Blinking	Synching
		Green	DSL synchronized.
Internet	WWW	Green	The NF18ACV is connected to an internet service.
		Green Blinking	Data is being transmitted to or from the internet.
		Off	The NF18ACV is not connected to the internet.
WAN	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.
Ethernet 1-4	1 2 3 4	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.
WiFi 2.4	2.4G	Green	WiFi is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	WiFi is disabled.
WiFi 5	5G	Green	WiFi is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	WiFi is disabled.
WPS	WPS	Green	WPS is enabled
		Green Blinking	WPS pairing is triggered.
		Off	WPS is disabled.

USB 1	1	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.
Telephone 1	1	Green	A handset is registered.
Telephone 2	2	Green Blinking	Incoming call or the handset is in use.
		Off	No handset registered

Table 1 – LED indicator table

Physical dimensions and weight

The table below lists the physical dimensions and weight of the NF18ACV.

Dimensions	
Width	216 mm
Height	173 mm
Depth	61 mm
Weight	420 grams

Table 2 – Physical dimensions and weigh table

NF18ACV Default Settings

The following tables list the default settings for the NF18ACV.

LAN (Management)	
Static IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1

Table 3 – LAN (Management) table

Wireless (WiFi)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA2-PSK (AES)
Security Key	(Refer to the included Wireless Security Card)

Table 4 – Wireless (WIFI) table

NF18ACV WEB Interface Access	
Username	admin
Password	admin

Table 5 – NF18ACV WEB Interface Access table

Interfaces

Rear

The following interfaces are available on the NF18ACV:

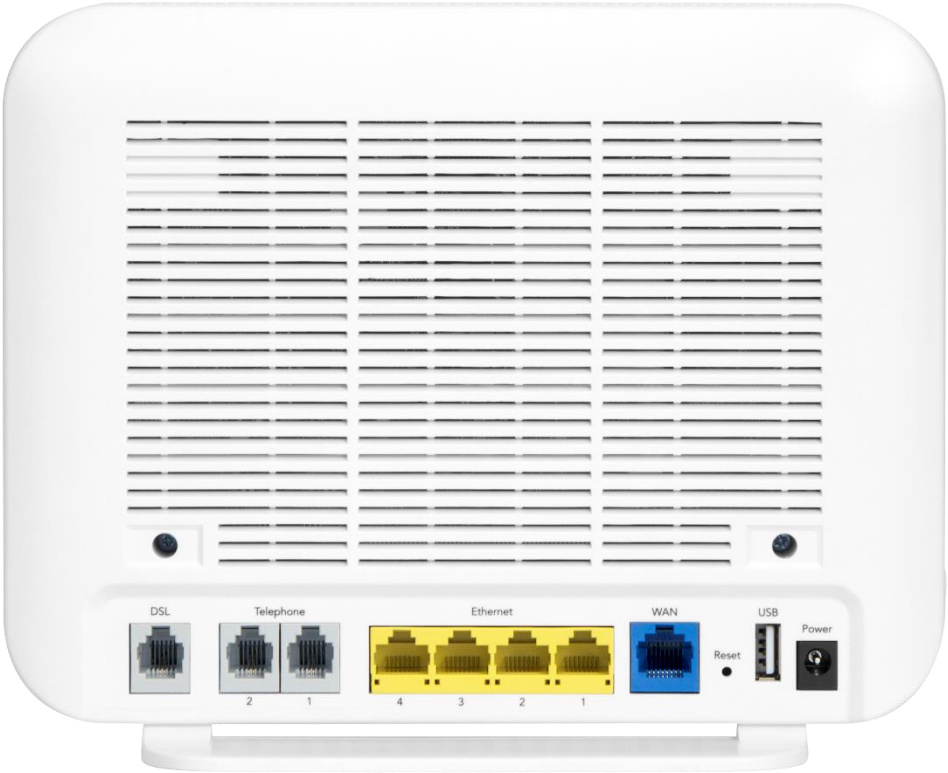


Figure 1 – NF18ACV router rear view

No.	Interface	Description
1	**DSL**	Use the provided RJ11 cable to connect the router to the telephone line operating your xDSL service.
2	**Telephone 1 and 2**	Connect a regular analogue telephone handset here for use with a VoIP service.
3	**Ethernet 1 - 4**	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
4	**WAN**	Gigabit capable WAN port for connection to a WAN network. Connect to your Network Termination Device (NTD) for high-speed internet access.
5	**Reset button**	Reset unit to Default by holding the Reset button down for 10 seconds when unit is powered on.
6	**USB**	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the NF18ACV.

No.	Interface	Description
7	**Power supply jack**	Connection point for the included power adapter. Connect the power supply here.

Table 6 – Rear interface table

Left Side

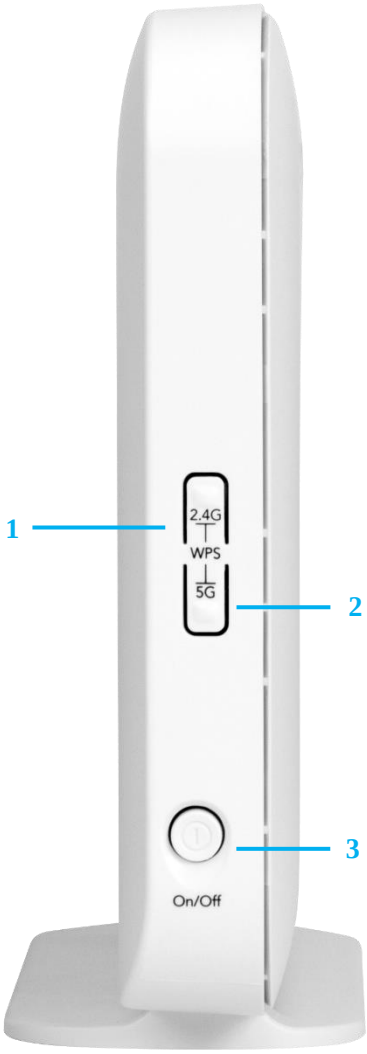


Figure 2 – NF18ACV router side view

No	Interface	Description
1	**2.4G WPS** button	Press the **2.4G WPS** button to activate the WPS PBC pairing function for the 2.4GHz radio.
2	**5G WPS** button	Press the **5G WP**S button to activate the WPS PBC pairing function for the 5GHz radio.
3	**On/Off** button	Toggles the power on and off.

Table 7 – *Side interface table*

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 NF18ACV, it is recommended to return the product in the original packaging. This ensures that the product will not be damaged.

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

Installation and configuration of the NF18ACV

Placement of your NF18ACV

The wireless connection between your NF18ACV and your WiFi 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 NF18ACV 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 meters from the NF18ACV in order 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

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF18ACV, please try the following steps:

- In multi-storey homes, place the NF18ACV on a floor that is as close to the centre of the home as possible. This may mean placing the NF18ACV on an upper floor.
- Try not to place the NF18ACV near a cordless telephone that operates at the same radio frequency as the NF18ACV (2.4GHz/5GHz).

Avoiding obstacles and interference

Avoid placing your NF18ACV 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
- Large aquariums
- 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 NF18ACV).

Cordless phones

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

- Try moving cordless phones away from your NF18ACV and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz or 5GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NF18ACV.

- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your NF18ACV to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 1800MHz cordless phone.

Choosing the "quietest" channel for your wireless network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Your wireless adapter may include a utility to assist in scanning for the least congested network, otherwise you may be able to find another piece of software that can be used. These tools display a graphical representation of the wireless networks in range and the channels on which they are operating. Try to find a channel which is not as busy and does not overlap with another one. Channels 1, 6 and 11 are the only channels on 2.4GHz which do not overlap with one another and you should ideally choose one of these channels. Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

Hardware installation

1 Connect the power adapter to the Power socket on the back of the NF18ACV.

2 Plug the power adapter into the wall socket and switch on the power.

3 Wait approximately 60 seconds for the NF18ACV to power up.

Connecting a client via Ethernet cable

1 Connect the yellow Ethernet cable provided to one of the yellow ports marked 'Ethernet' at the back of the NF18ACV.

2 Connect the other end of the yellow Ethernet cable to your computer.

3 Wait approximately 30 seconds for the connection to establish.

4 Open your Web browser, and enter http://192.168.20.1 into the address bar and press enter.

5 Follow the steps to set up your NF18ACV.

Connecting a client wirelessly

1 Ensure WiFi is enabled on your device (e.g. computer/laptop/smartphone).

2 Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NF18ACV.

Note – Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF18ACV.

3 When prompted for your wireless security settings, enter the Wireless security key configured on the NF18ACV.

4 Wait approximately 30 seconds for the connection to establish.

5 Open your Web browser, and enter http://192.168.20.1 into the address bar and press Enter.

6 Follow the steps to set up your NF18ACV.

Web based configuration interface

First-time setup wizard

Note – While we highly recommend that you set up your new router using the *First-time Setup Wizard* (**Basic Setup**), it is possible to configure your new router directly from the **Advanced Setup** features.

It is also possible to initially set up your router using the Basic Setup wizard and then later fine-tune your configuration using the Advanced Setup tools.

Please follow the steps below to configure your NF18ACV Wireless router via the web based configuration wizard.

1 Open a web browser and type http://192.168.20.1/ into the address bar at the top of the window.

2 At the login screen, type **admin** in the username and password field, then click the **Login** button.

Note – '**admin**' is the default username and password for the unit.

3 Click on the **Basic Setup** menu item on the left side of the screen.

Figure 3 – NF18ACV router – Select Basic Setup

4 To run the Wizard having all the basic set up details that your system requires, ⦿ select the Wan Connection type that you will be using: **ADSL**, **VDSL** or **Ethernet WAN**

ADSL

a Select **ADSL** and click the **Next** button.

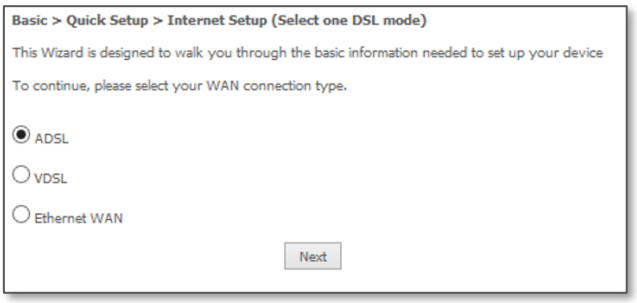


Figure 4 – NF18ACV router – Select ADSL as WAN connection type

b Select either the **PPPoE**, **PPPoA** or **Bridging** for your internet connection as specified by your Internet Service Provider (ISP).

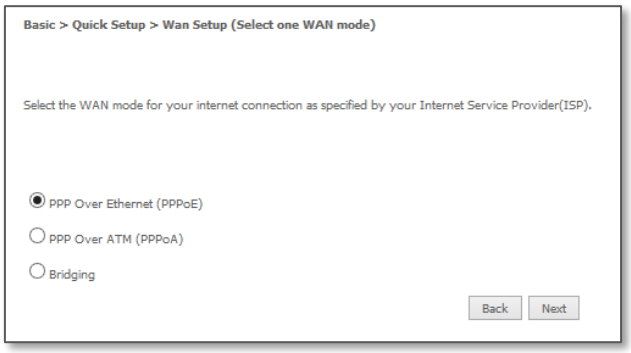


Figure 5 – Select PPPoE as WAN mode

Click the **Next** button.

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

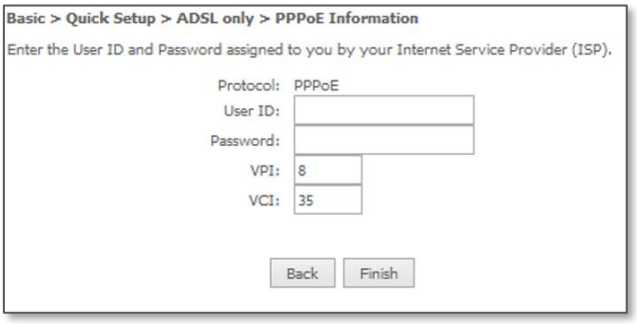


Figure 6 – Enter PPPoE User ID and Password

Click the **Finish** button.

d The account settings are saved and the NF18ACV connects to the internet.

VDSL

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

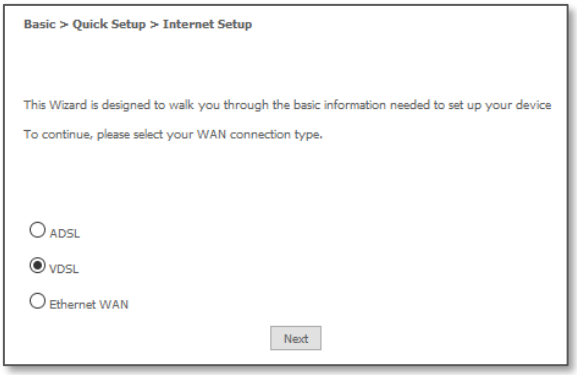


Figure 7 – NF18ACV router – Select VDSL as WAN connection type

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

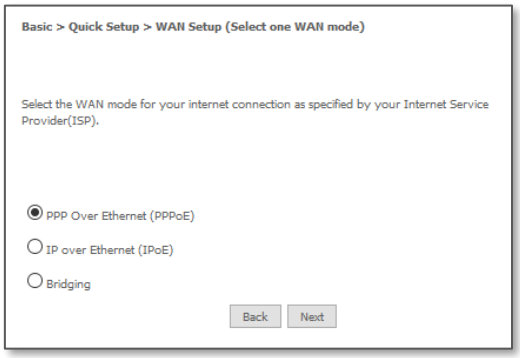


Figure 8 – Select WAN mode for VDSL connection

Click the **Next** button.

f 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.

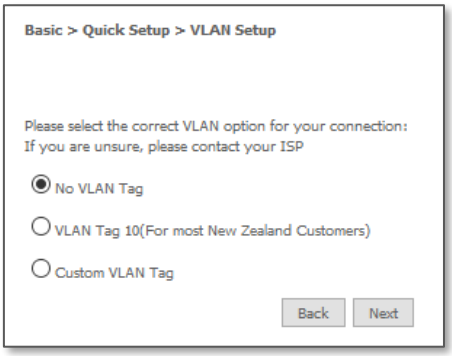


Figure 9 – Select VLAN option for VDSL connection

Click the **Next** button.

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

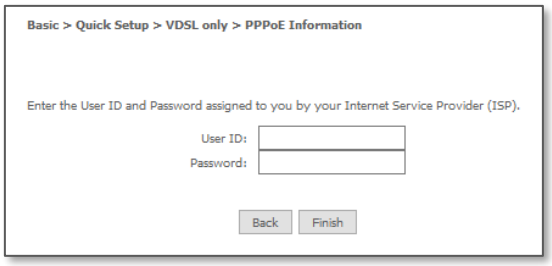


Figure 10 – VDSL connection – Enter User ID and Password

h Click the **Finish** button when you have entered the required details. The account settings are saved and the NF18ACV connects to the internet.

Ethernet WAN

a Connect an RJ45 Ethernet cable to the **WAN** port on the NF18ACV. Connect the other end of the cable to your WAN service.

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

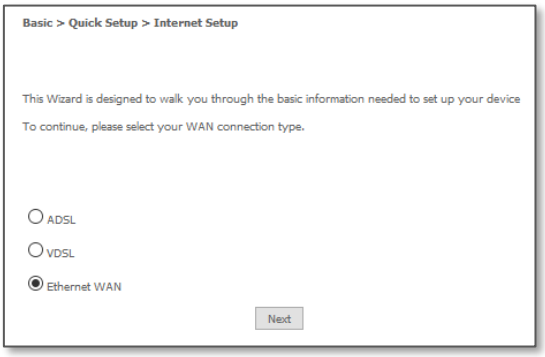


Figure 11 – NF18ACV router – Select Ethernet WAN as WAN connection type

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

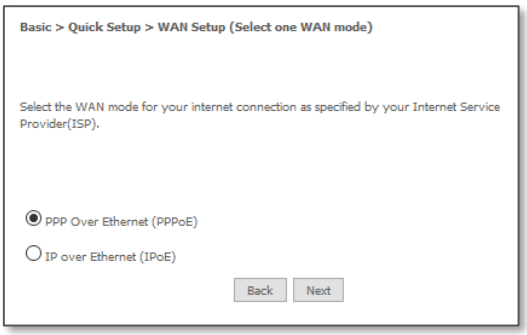


Figure 12 – Select WAN mode for Ethernet WAN connection

k Click the **Next** button.

PPP over Ethernet (PPPoE)

If at step 3 you selected **PPP over Ethernet (PPPoE):**

4 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.

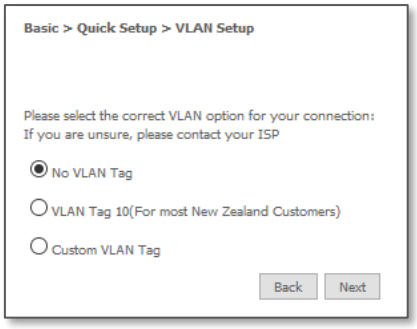


Figure 13 – Select VLAN option for PPPoE

Click the **Next** button.

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

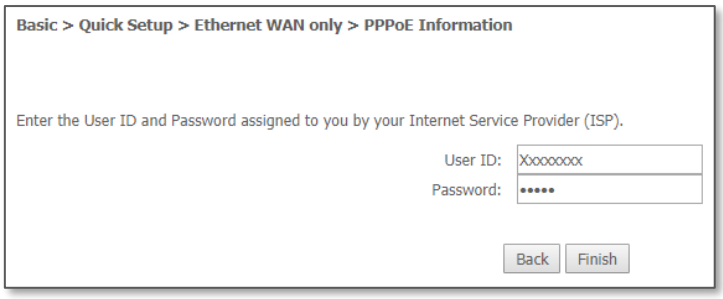


Figure 14 – Ethernet WAN connection – Enter User ID and Password

IP over Ethernet (IPoE)

If at step 3 you selected **IP over Ethernet (IPoE):**

4 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. Click the **Next** button.

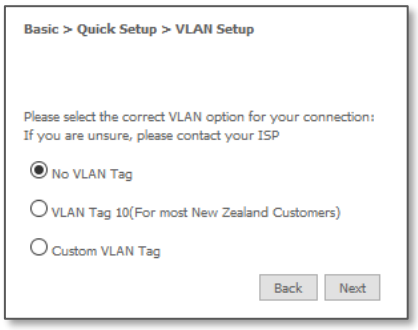


Figure 15 – IP over Ethernet (IPoE) -- VLAN Setup

3 If your ISP has supplied a static IP address, select **Use the following Static IP address** and enter the details, otherwise select **Obtain an IP address automatically**.

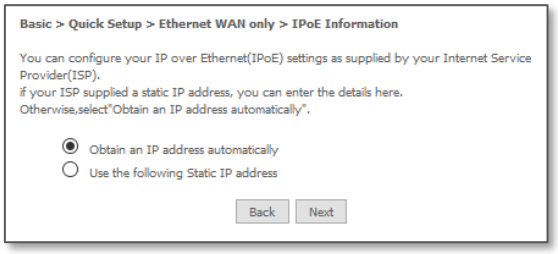


Figure 16 – IP over Ethernet (IPoE) – Static or Auto IP Address

Click the **Next** button.

4 The settings are displayed in a summary.

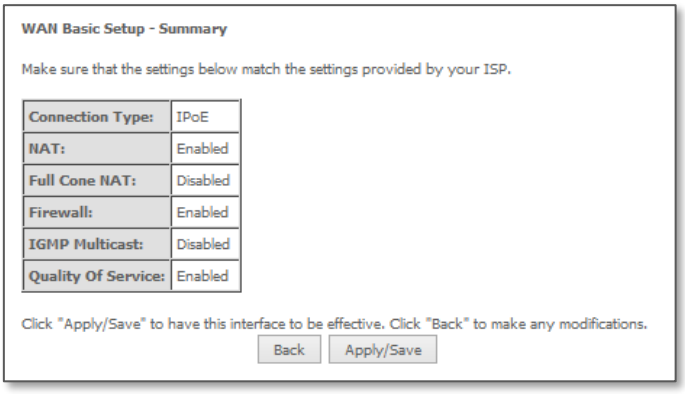


Figure 17 – WAN Setup Summary

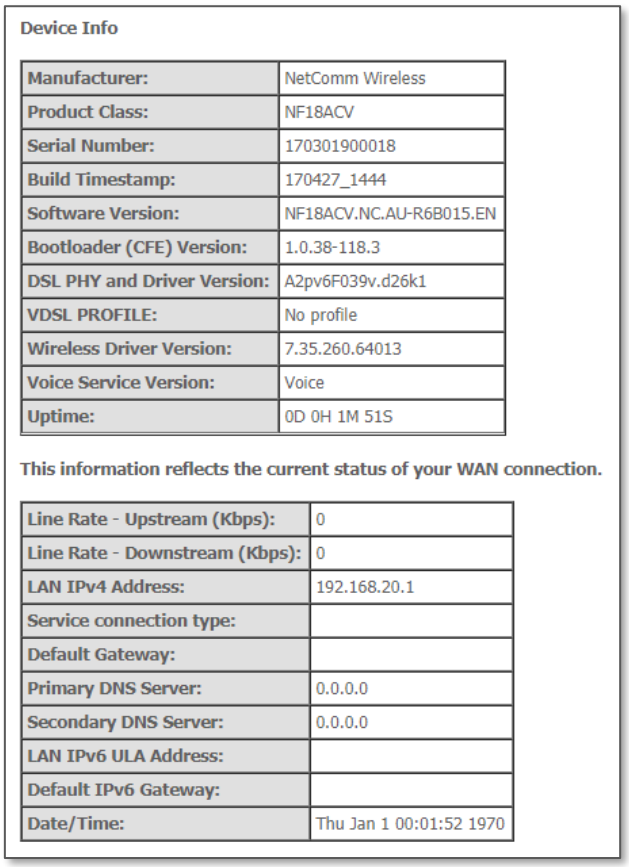
5 Click **Apply/Save** to save them.

The account settings are saved and the NF18ACV connects to the internet.

Device Info

Summary

When you log in to the router, the **Device Info** summary page is displayed, giving a general overview of the status of the router and the WAN connection.



Device Info

Manufacturer:	NetComm Wireless
Product Class:	NF18ACV
Serial Number:	170301900018
Build Timestamp:	170427_1444
Software Version:	NF18ACV.NC.AU-R6B015.EN
Bootloader (CFE) Version:	1.0.38-118.3
DSL PHY and Driver Version:	A2pv6F039v.d26k1
VDSL PROFILE:	No profile
Wireless Driver Version:	7.35.260.64013
Voice Service Version:	Voice
Uptime:	0D 0H 1M 51S

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 00:01:52 1970

Figure 18 – NF18ACV route – Device Info summary page

Item	Definition
Device Info	
Manufacturer	Indicates that NetComm Wireless is the manufacturer of this product.
Product Class	The model of the product.
Serial Number	The unique set of numbers assigned to the routers for identification purposes.
Build Timestamp	The date and time that the software running on the router was published.
Software Version	The current firmware version installed on the router.
Bootloader (CFE) Version	The current boot loader version installed on the router.
DSL PHY and Driver Version	The driver version of the on-board DSL chip.

Item	Definition
VDSL PROFILE	The VDSL profile in use. Supports 8a, 8b, 12a and 17a VDSL profiles.
DSL PHY and Driver Version	The current line driver installed on the router.
Wireless Driver Version	The current wireless driver installed on the router.
Uptime	The number of days, hours and minutes that the router has been running.
WAN connection	
Line Rate – Upstream (Kbps)	The current synchronisation upstream speed of the DSL connection in Kbps (Kilobits per second).
Line Rate – Downstream (Kbps)	The current synchronisation upstream speed of the DSL connection in Kbps (Kilobits per second).
LAN IPv4 Address	The current IPv4 LAN IP address assigned to the router.
Service connection type	Displays whether the WAN connection is ADSL/VDSL or Ethernet WAN.
Default Gateway	The current default gateway address of the WAN interface.
Primary DNS Server	The current primary DNS server in use
Secondary DNS Server	The current secondary DNS server is use.
LAN IPv6 ULA Address	The current IPv6 LAN IP address in use if assigned.
Default IPv6 Gateway	The current IPv6 default gateway if assigned.
Date/Time	The current local date and time set on the router.

Table 8 – Device Info summary table

WAN

The **WAN** page shows more detailed information related to the WAN interface configuration, including the firewall status, IPv4 and IPv6 addresses of the router.

WAN Info

Interface	Description	Type	VLAN Mux ID	IPv6	IGMP Pxy	IGMP Source Enable	MLD Pxy	MLD Source Enable	NAT	Firewall	Status	IPv4 Address	IPv6 Address
ipoa0	Great	IPoA	Disabled	Disabled	Disabled	Enabled			Enabled	Enabled	Unconfigured	0.0.0.0	
eth4.1	ETH WAN	IPoE	Disabled	Disabled	Disabled	Disabled			Enabled	Enabled	Unconfigured	0.0.0.0	
ppp0.1	VDSL	PPPoE	Disabled	Disabled	Disabled	Disabled			Disabled	Enabled	Unconfigured	0.0.0.0	

Figure 19 – NF18ACV router – WAN Info list

Item	Definition
Interface	The Interface of the WAN connection.
Description	The description of the WAN connection.
Type	The type of WAN connection.

Item	Definition
VLAN Mux ID	Details the status of VLAN Mux ID if used.
IPv6	The status of IPv6.
IGMP Pxy	Details the status of IGMP on each WAN connection. IGMP is only used with IP v4 connections. IGMP proxy enables the router to issue IGMP host messages on behalf of hosts that the router discovered through standard IGMP interfaces, allowing NAT transversal of Multicast traffic.
IGMP Source Enable	Details the status of IGMP Src on each WAN connection. IGMP Sources function send a membership report that includes a list of IGMP source addresses.
MLD Pxy	Shows the status of the Multicast Listener Discovery protocol when IPv6 is in use. Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router discovered through standard MLD interfaces.
MLD Source Enable	Details the status of MLD Src on each WAN connection. MLD Sources function can send a membership report that includes a list of MLD source addresses.
NAT	The NAT status of the WAN connection.
Firewall	The status of the router firewall across the WAN connection.
Status	The status of the WAN connection.
IPv4 Address	The current IP v4 address of the WAN interface.
IPv6 Address	The current IP v6 address of the WAN interface.

Table 9 – WAN Info table

Statistics

Statistics – LAN

The **Statistics – LAN** page shows detailed information about the number of bytes, packets, errors and dropped packets on each LAN interface in both directions of communication.

Statistics -- LAN

Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
eth0	742666	7173	0	1	0	1011	5512	650	7615128	7688	0	0	0	333	7342	13
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0	0	0	0	28	0	0	0	0	377791	4174	0	0	0	0	0	0
wl0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl0.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1	0	0	0	39	0	0	0	0	0	0	0	0	0	0	0	1
wl1.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1.2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
wl1.3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

Figure 20 – Device Info – Statistics -- LAN display

Interface	Description	
Received/Transmitted	**Bytes**	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 10 – Statistics -- LAN display table

Statistics – WAN Service

The Statistics – WAN Service page shows detailed information about the number of bytes, packets, errors and dropped packets on the WAN interface in both directions of communication.

Statistics -- WAN

Interface	Description	Received								Transmitted							
		Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
		Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
eth4.1	ETH WAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Reset Statistics

Figure 21 – Device Info – Statistics – WAN Service display

Interface	Description	
Received/Transmitted	**Bytes**	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Table 11 – Statistics – WAN Service table

Statistics – xTM

The Statistics – xTM page shows details related to the xTM (ATM/PTM) interface of the router.

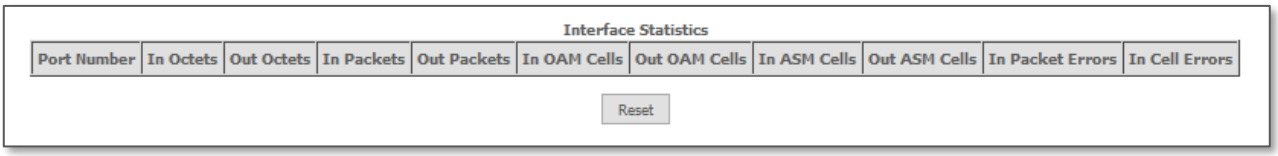


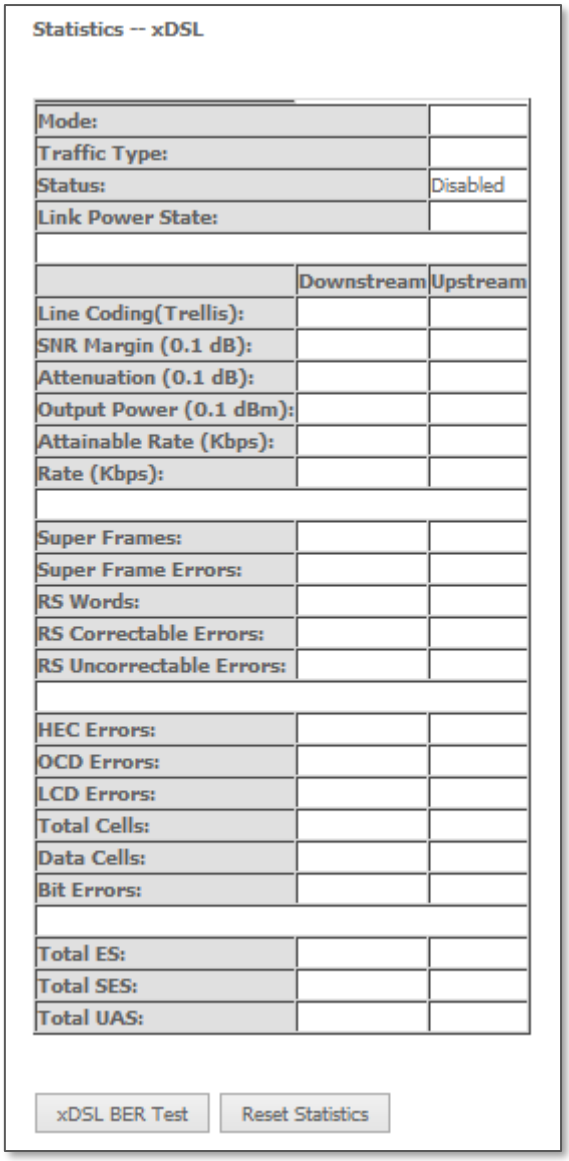
Figure 22 – Device Info – Statistics -- xTM display

Interface	DESCRIPTION
Port Number	The port number used by the xTM interface.
In Octets	The number of data packets in octets received over the ATM interface.
Out Octets	The number of data packets in octets transmitted over the ATM interface.
In Packets	The number of data packets received over the ATM interface.
Out Packets	The number of data packets transmitted over the ATM interface.
In OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
Out OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
In ASM Cells	The number of Any Source Multicast (ASM) cells received over the interface.
Out ASM Cells	The number of Any Source Multicast (ASM) cells transmitted over the interface.
In Packets Errors	The number of packets with errors detected over the xTM interface.
In Cell Errors	The number of cells with errors detected over the xTM interface.

Table 12 – Statistics – xTM settings table

Statistics – xDSL

The Statistics – xDSL page shows details related to the DSL interface of the router.



Statistics -- xDSL

Mode:		
Traffic Type:		
Status:		Disabled
Link Power State:		
	Downstream	Upstream
Line Coding(Trellis):		
SNR Margin (0.1 dB):		
Attenuation (0.1 dB):		
Output Power (0.1 dBm):		
Attainable Rate (Kbps):		
Rate (Kbps):		
Super Frames:		
Super Frame Errors:		
RS Words:		
RS Correctable Errors:		
RS Uncorrectable Errors:		
HEC Errors:		
OCD Errors:		
LCD Errors:		
Total Cells:		
Data Cells:		
Bit Errors:		
Total ES:		
Total SES:		
Total UAS:		

xDSL BER Test Reset Statistics

Figure 23 – NF18ACV router

Route

The Route page displays any routes that the router has created.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.20.0	0.0.0.0	255.255.255.0	U	0		br0

Figure 24 – Device Info -- Route list

ARP

Click **ARP** to display the address resolution protocol information.

This option can be used to determine which IP address / MAC address is assigned to a particular host. This can be useful when setting up URL filtering, Time of Day filtering or Static DHCP addressing.

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.20.2	Complete	2c:44:fd:12:3c:6e	br0

Figure 25 – Device Info -- ARP list

DHCP

Click DHCP to display the Dynamic Host Configuration Protocol (DHCP) lease information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Connection Type	IP Address Assignment	Status	Expires In
	2c:44:fd:12:3c:6e	192.168.20.2	Ethernet	DHCP	Active	23 hours, 55 minutes, 47 seconds

Figure 26 – Device Info -- DHCP Leases list

You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

CPU & Memory

The CPU & Memory page shows real-time graphs charting the physical memory usage and the work load of the CPU.

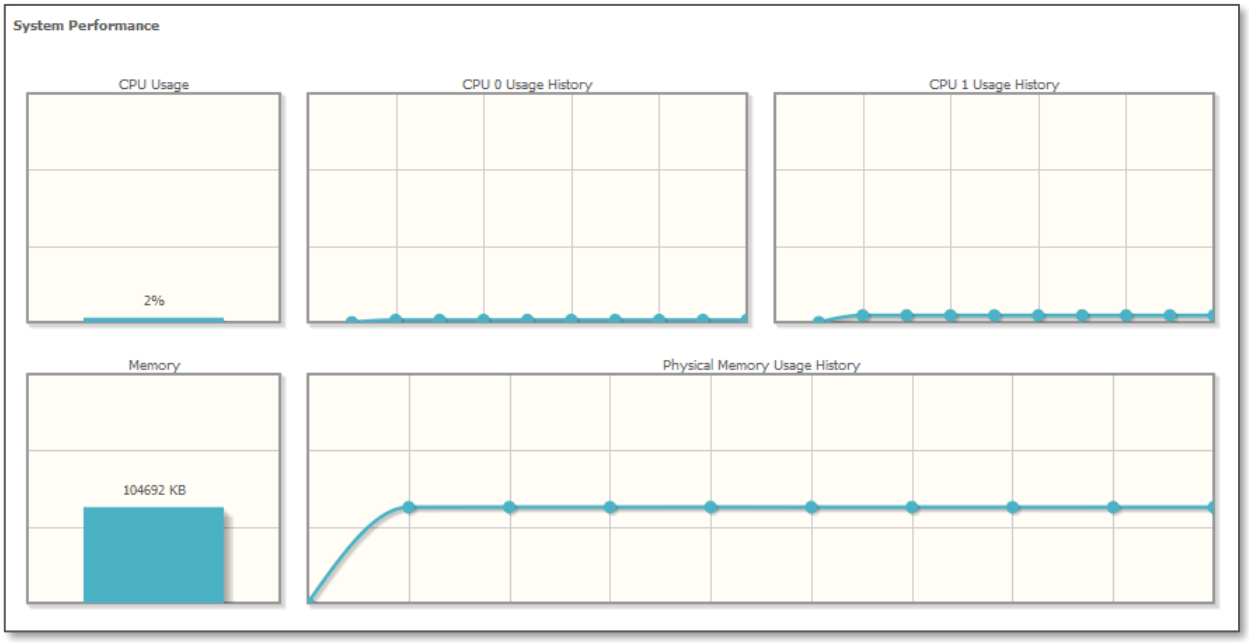


Figure 27 – Device Info – CPU & Memory display

Advanced Setup

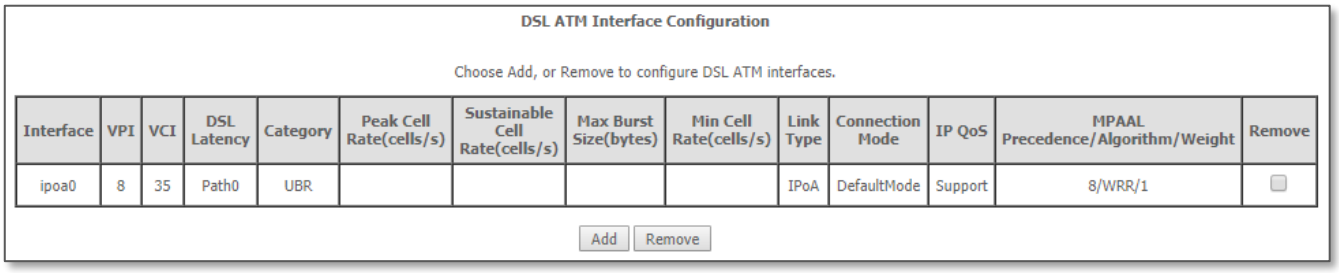
While you can set up your router directly from the **Advanced Setup** pages, we recommend that you use the *First-time Setup Wizard* contained in the **Basic Setup** section, see above.

Layer2 Interface

ATM Interface

The ATM (Asynchronous Transfer Mode) interface page shows the settings of all available DSL ATM interfaces.

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	Connection Mode	IP QoS	MPAAL Precedence/Algorithm/Weight	Remove
ipoa0	8	35	Path0	UBR					IPoA	DefaultMode	Support	8/WRR/1	

Add Remove

Figure 28 – 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.

Field	Description
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	Check ☑ the box in this field and click **Remove** to permanently delete the ATM configuration.

Table 13 – DSL ATM Interface Configuration settings table

To add an ATM interface, click the **Add** button. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.

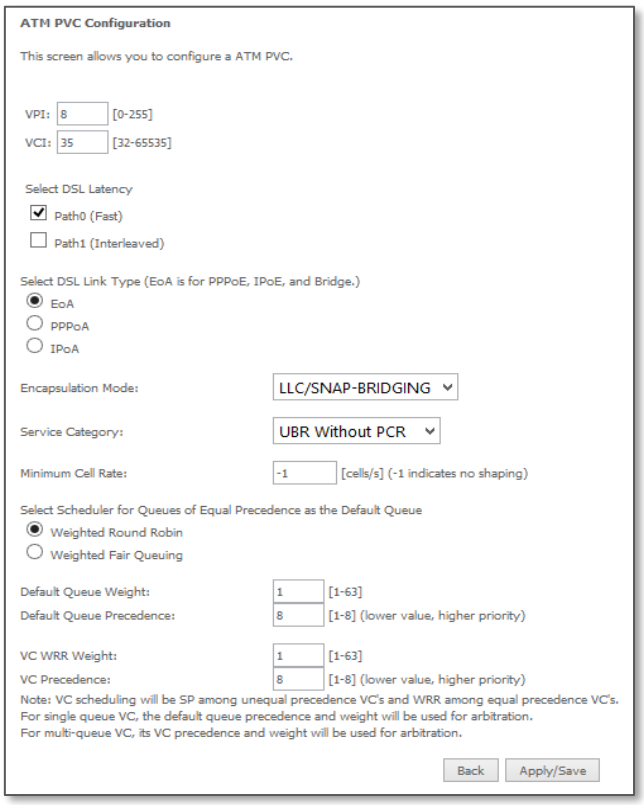


Figure 29 – ATM PVC Configuration page

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.

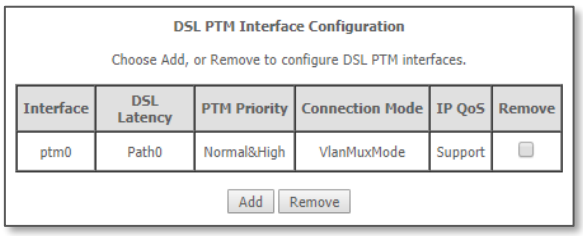


Figure 30 – DSL PTM Interface list

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.

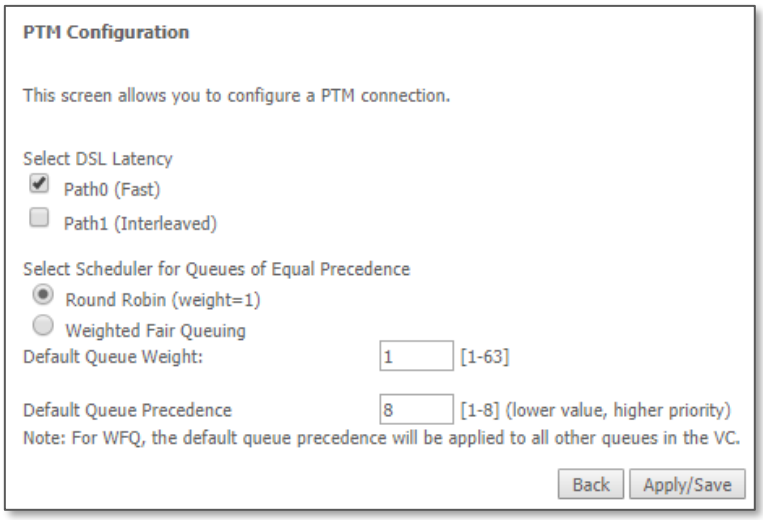


Figure 31 – PTM Configuration page

ETH Interface

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

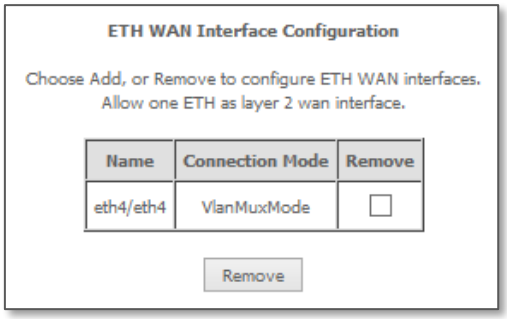


Figure 32 – ETH WAN interface list WAN Service

Note – When 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.

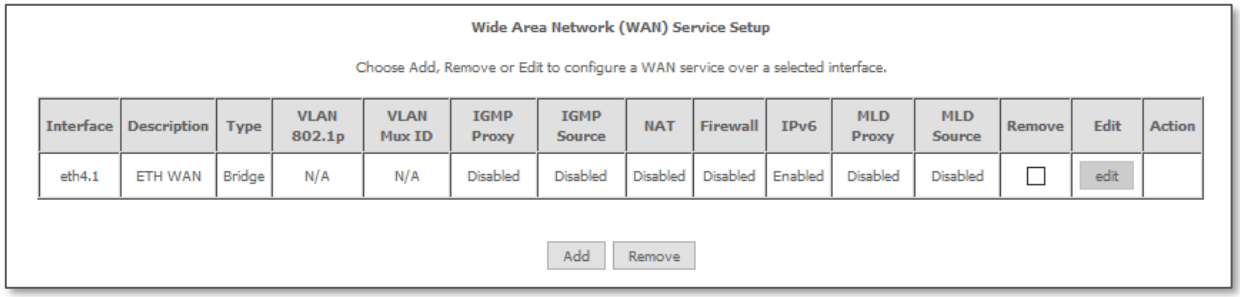


Figure 33 – NF18ACV router

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.

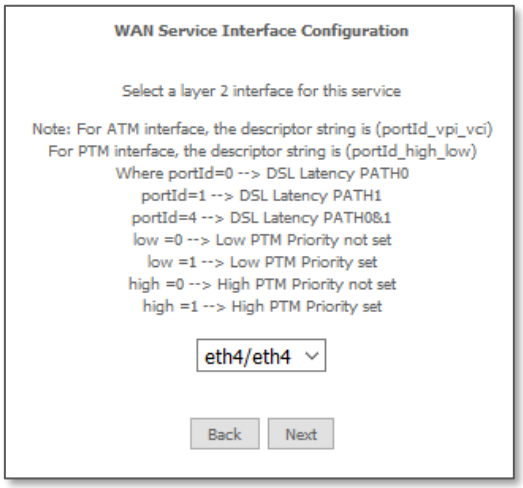


Figure 34 – WAN Service – Select layer 2 interface

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.

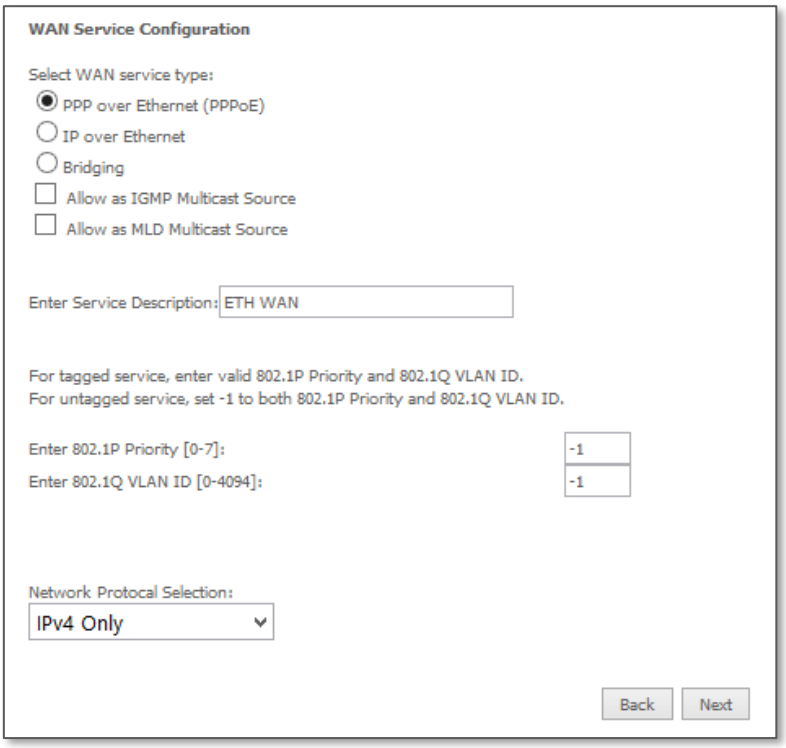


Figure 35 – WAN Service – Select WAN Service Type

PPP over Ethernet

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

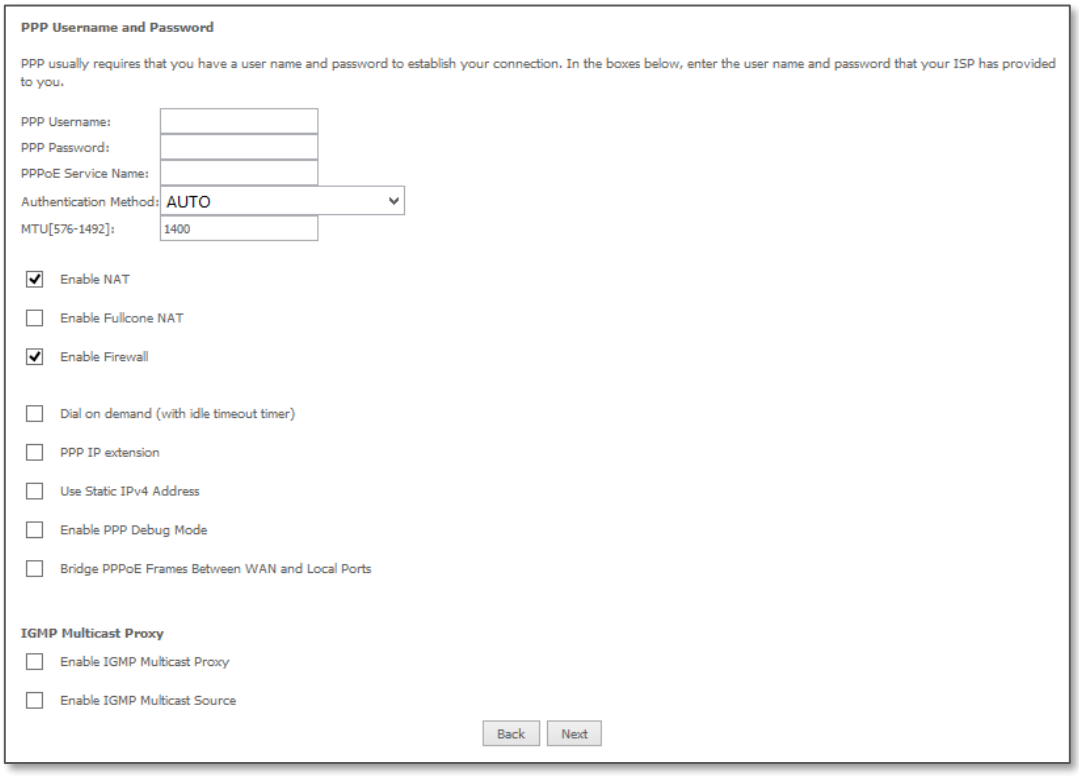


Figure 36 – Enter PPP over Ethernet details

IP over Ethernet

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

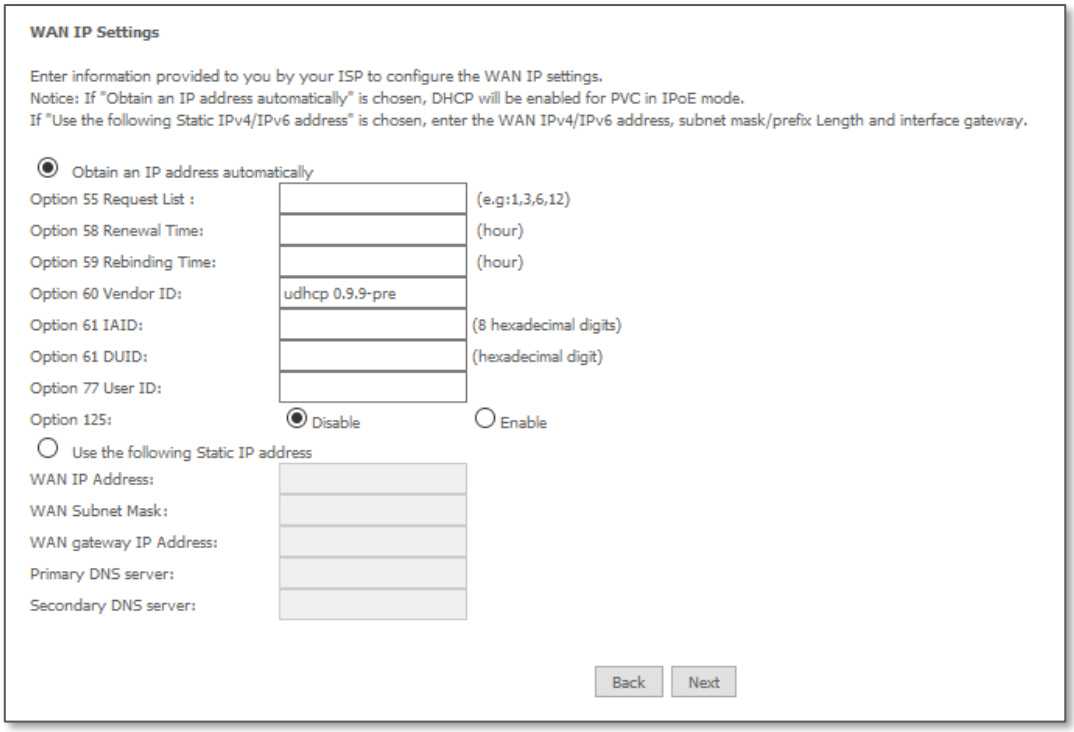


Figure 37 – Enter IP over Ethernet details

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

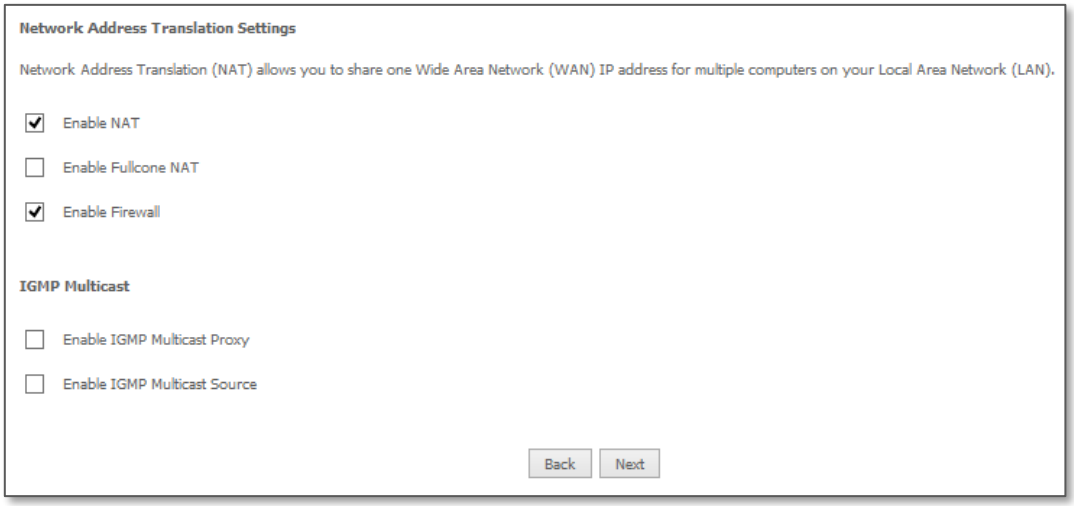


Figure 38 – Enter PPP over Ethernet NAT Translation settings

Bridging

When you select ⦿ **Bridging** mode, a summary of the settings is displayed. Click **Apply/Save** to commit the settings.

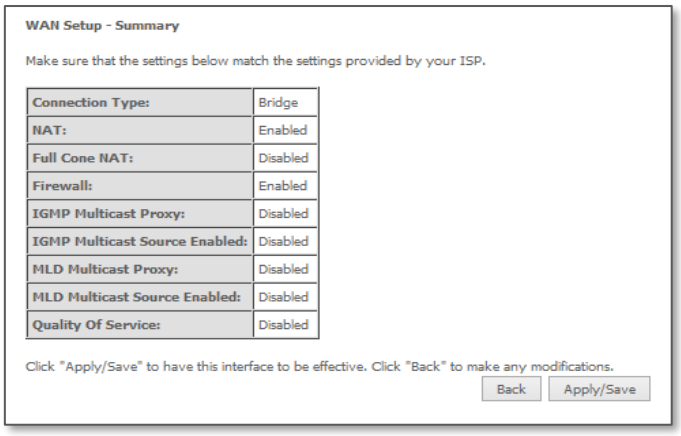


Figure 39 – Enter PPP over Ethernet details

LAN

IPv4 Autoconfig

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

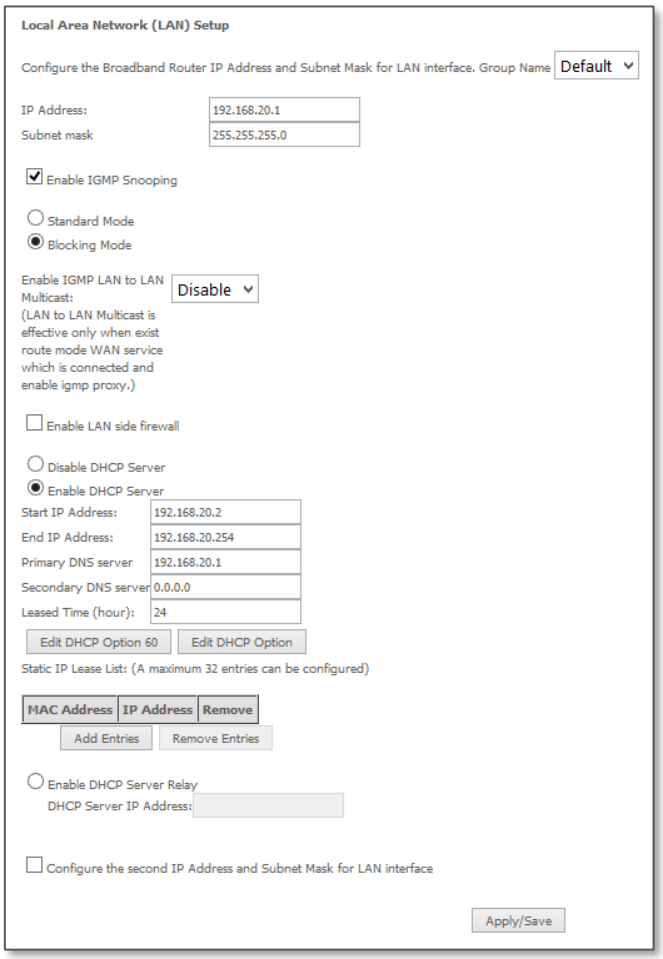


Figure 40 – LAN setup -- IPv4 Autoconfig settings

The following options are available to configure:

Parameter	Definition
IP Address	Enter the Local IP Address to use for the NF18ACV.
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.
Enable DHCP Server Relay	Disabled DHCP server, and relay all request to external server specified by the IP address.
Configure the second IP Address	This option enables you to set a secondary IP Address for the NF18ACV

Table 14 – IPv4 Autoconfig settings table

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

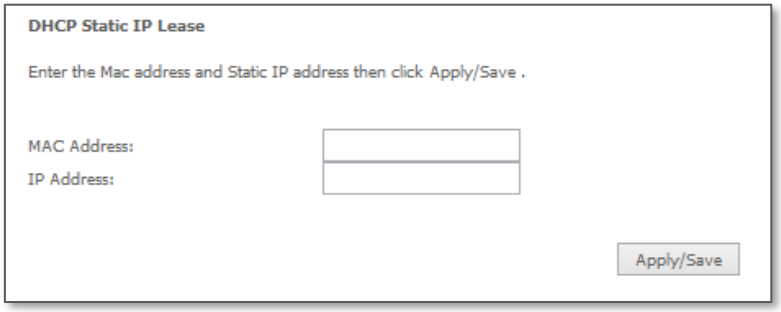


Figure 41 – Enter DHCP Static IP Addresses

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

The NF18ACV 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 Autoconfig

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

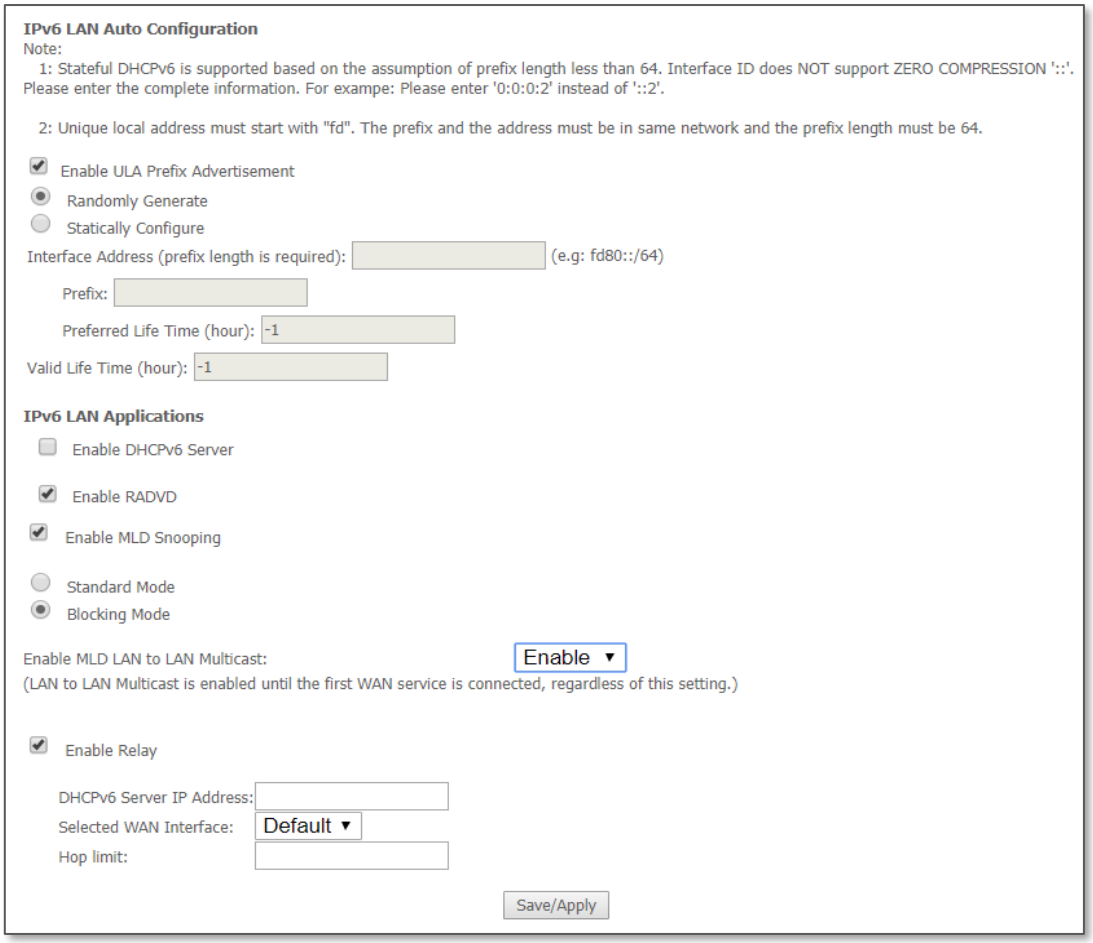


Figure 42 – IPv6 LAN Auto Configuration page

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

Option	Definition
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.
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.
Enable Relay	When enabled, relays DHCP messages between DHCPv6 clients and DHCPv6 servers on different IPv6 networks.

Table 15 – IPv6 LAN Auto Configuration settings

LAN VLAN Setting

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

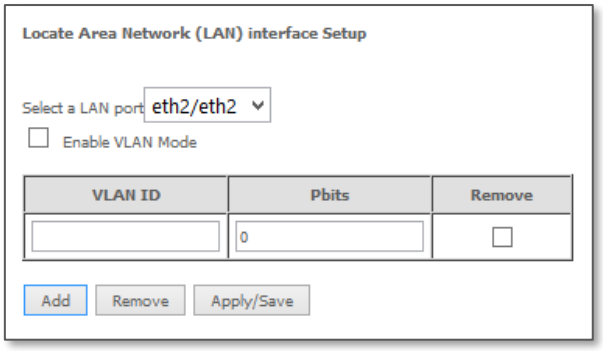


Figure 43 – Specify a LAN port for VLAN tagging

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.

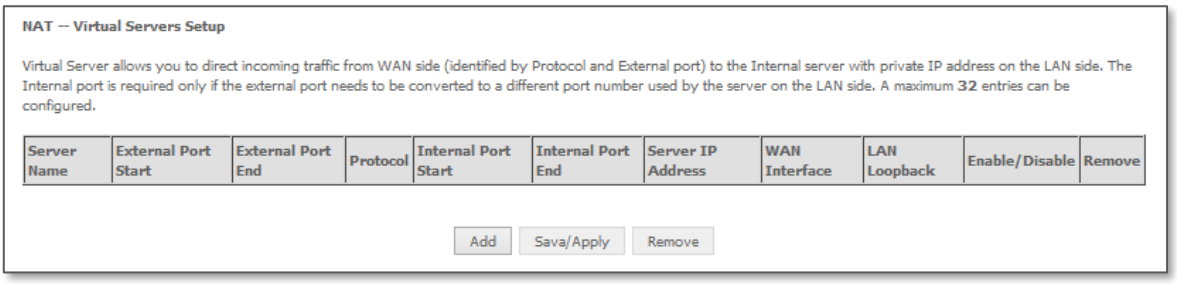


Figure 44 – NAT -- Virtual Server list

Click the **Add** button to add a virtual server.

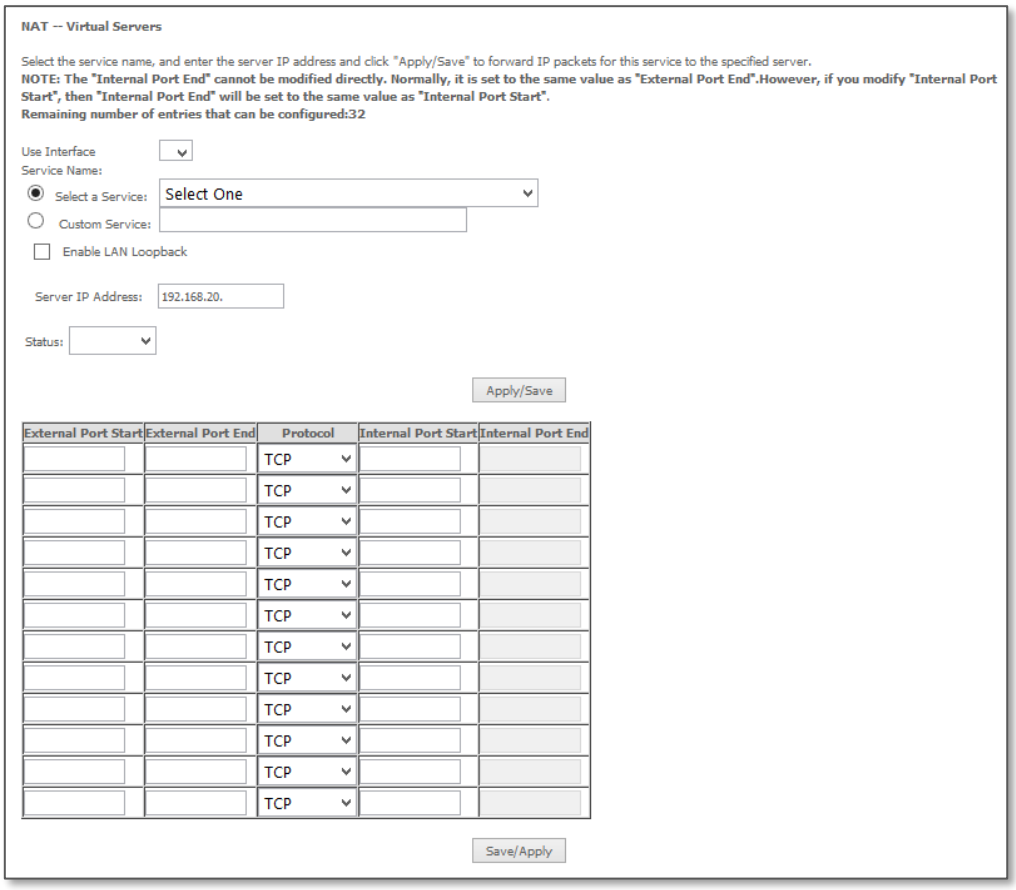


Figure 45 – NAT -- Virtual Server Configuration page

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.

Table 16 – 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 32 entries can be configured.

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

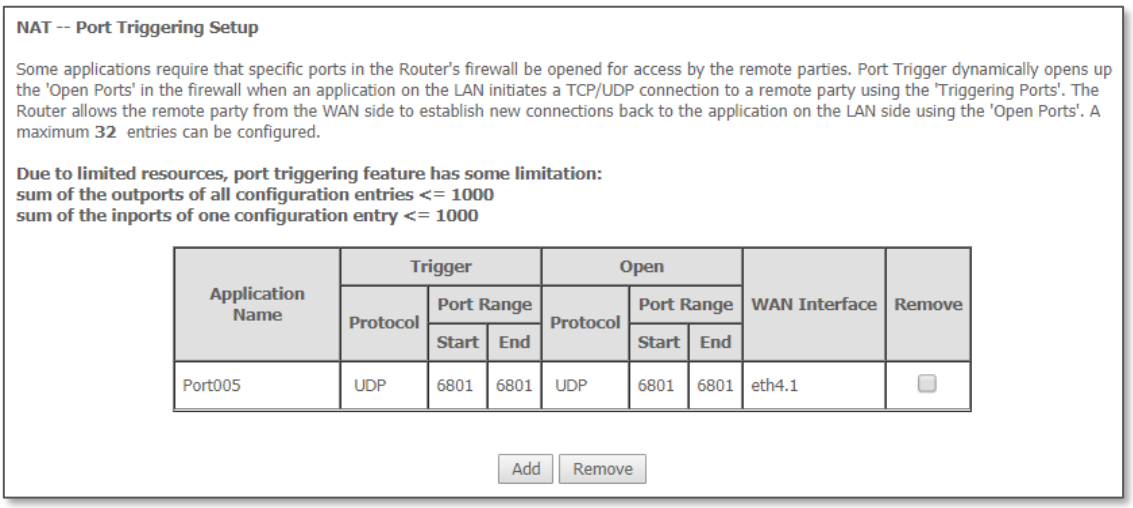


Figure 46 – NAT -- Port Triggering list

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

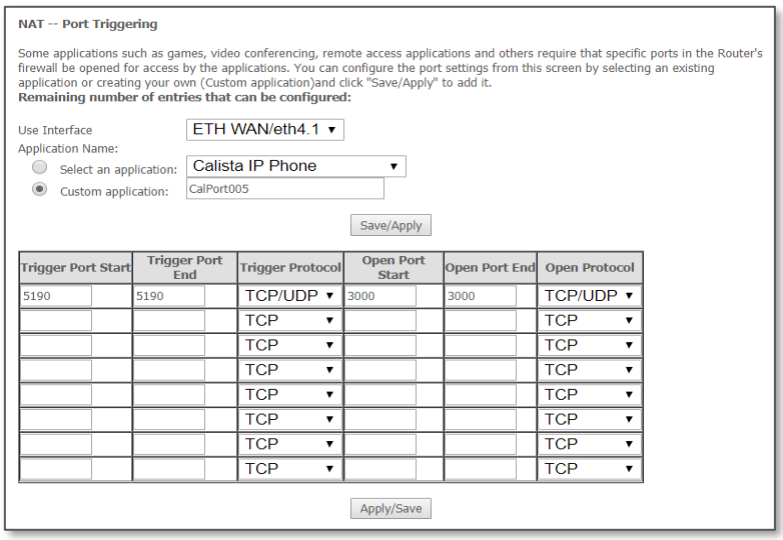


Figure 47 – NAT -- Port Trigger Configuration page

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.

Table 17 – NAT -- Port Trigger Configuration settings

DMZ Host

The NF18ACV 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.

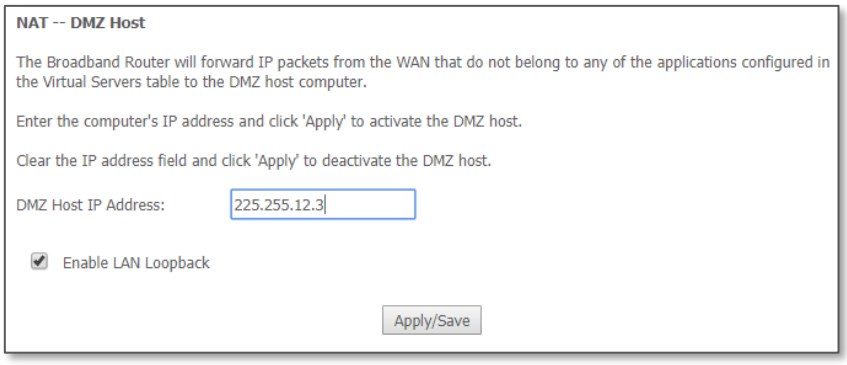


Figure 48 – NAT – DMZ Host settings

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.

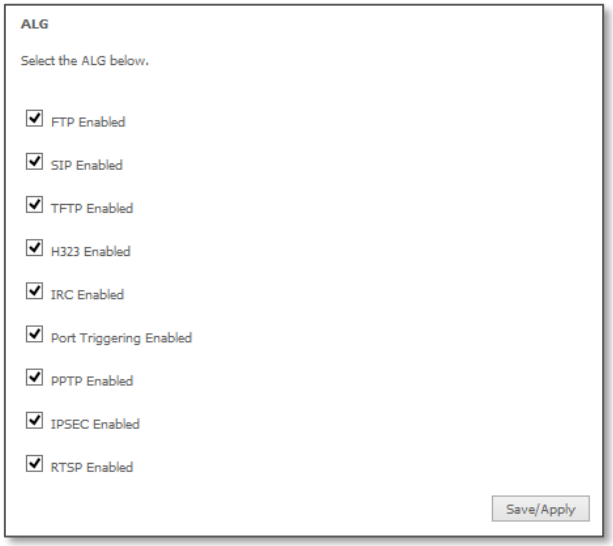


Figure 49 – NAT – Application Layer Gateway (ALG) settings

Security

IP Filtering

The router supports IP Filtering which allows you to easily set up rules to control incoming and outgoing Internet traffic. The router provides two types of IP filtering: **Outgoing IP Filtering** and **Incoming IP Filtering**

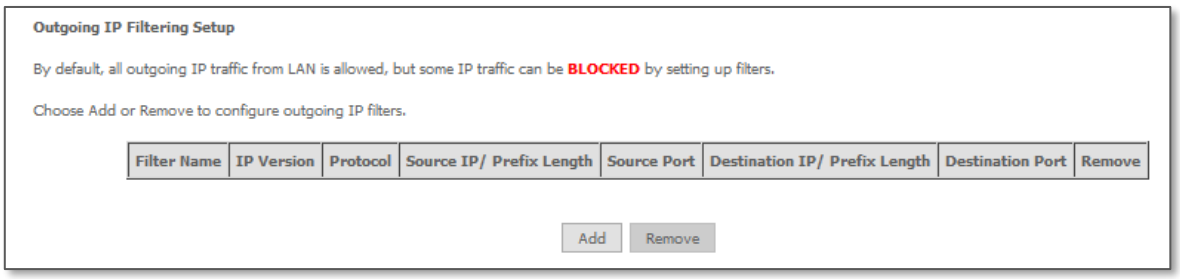


Figure 50 – IP Filtering List

Outgoing IP Filtering

By default, the router allows all outgoing Internet traffic from the LAN but by setting up Outgoing IP Filtering rules, you can block some users and/or applications from accessing the Internet.

To delete the rule, click ☑ in the **Remove** column next to the selected rule and then click the **Remove** button.

To create a new outgoing IP filter, click **Add**. The Add IP Filter-Outgoing page will be displayed.

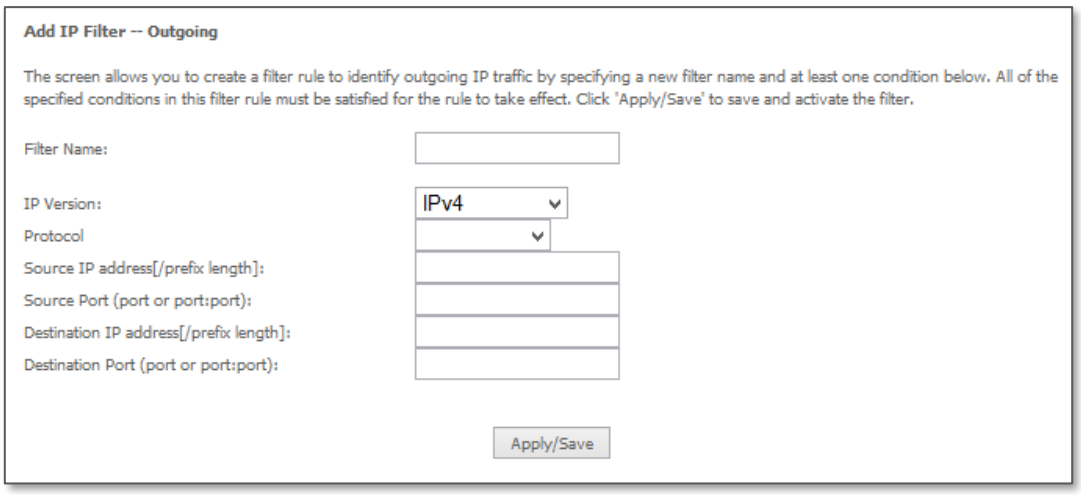


Figure 51 –Outgoing IP Filter settings

Parameter	Definition
Filter Name	Enter a name to identify the filtering rule.
IP Version	Select the IP version to apply the filter to. (IPv4/IPv6)
Protocol	Select the protocol type to block(UDP/TCP/Both)
Source IP Address/Subnet Mask	Enter the IP Address of the host on the LAN to block
Source Port	Enter the port number used by the application to block
Destination IP Address/Subnet Mask	Enter the IP Address of the Remote Server/host to which connections should be blocked
Destination Port	Enter the destination port number used by the application to block

Table 18 – Outgoing IP Filter settings table

Click **Apply/Save** to take effect the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

Incoming IP Filtering

By default, when NAT is enabled, all incoming IP traffic from WAN is blocked except for responses to requests from the LAN. However, some specific incoming traffic from the Internet can be accepted by setting up Incoming IP Filtering rules.

To delete the rule, click ☑ in the **Remove** column next to the selected rule and click the **Remove** button.

To create a new incoming IP filter, click **Add**. The Add IP Filter-Incoming page will be displayed.

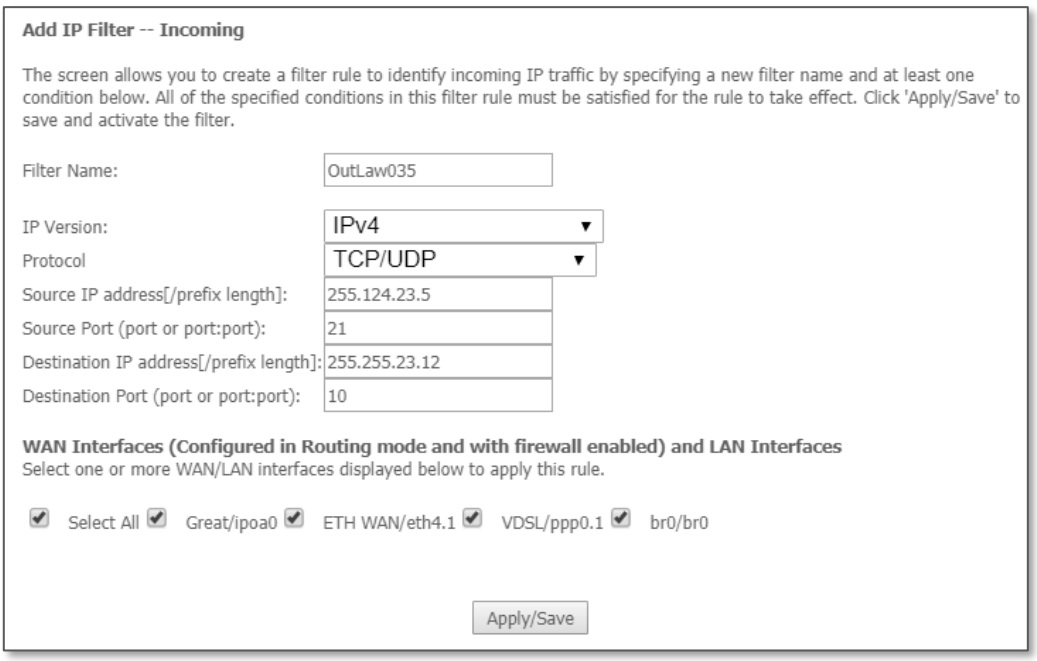


Figure 52 – Incoming IP Filter settings

Enter the following parameters:

Parameter	Definition
Filter Name	Enter a name to identify the filtering rule
IP Version	Select the IP version to apply the filter to
Protocol	Select the protocol type to allow
Source IP Address/ Subnet Mask	Enter the IP Address of the Remote Server/Host from which to allow connections
Source Port	Enter the port number used by the application to allow
Destination IP Address/Subnet Mask	Enter the IP Address of the Host on the LAN to which connections should be allowed
Destination Port	Enter the destination port number used by the application to allow
WAN Interface	Select the WAN Interface to apply the filter to

Table 19 – Incoming IP Filter settings table

Click **Save/Apply** to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.

MAC Filtering

The NF18ACV 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.

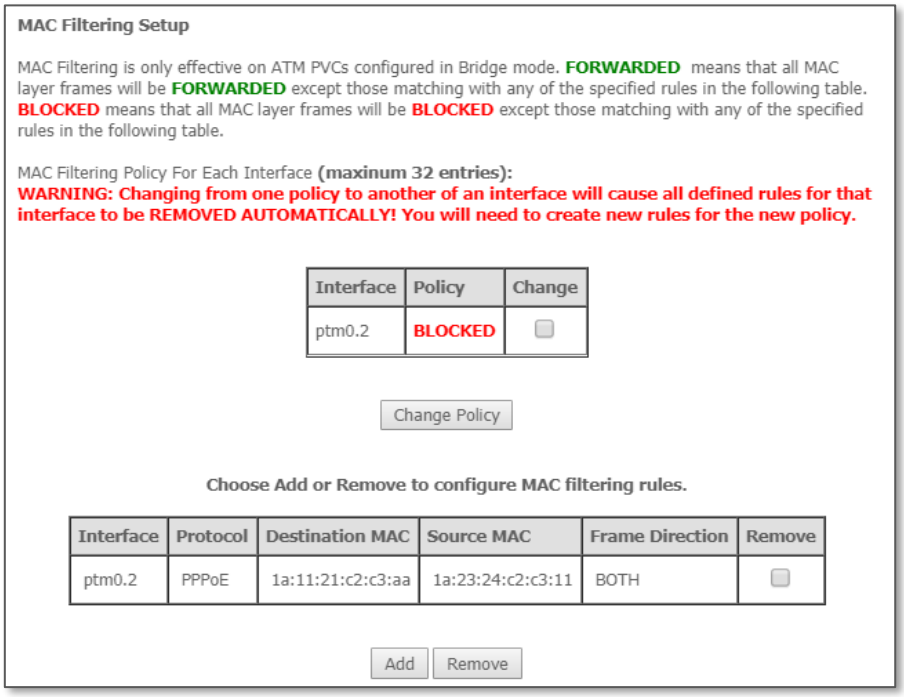


Figure 53 – Security – MAC Filter list

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

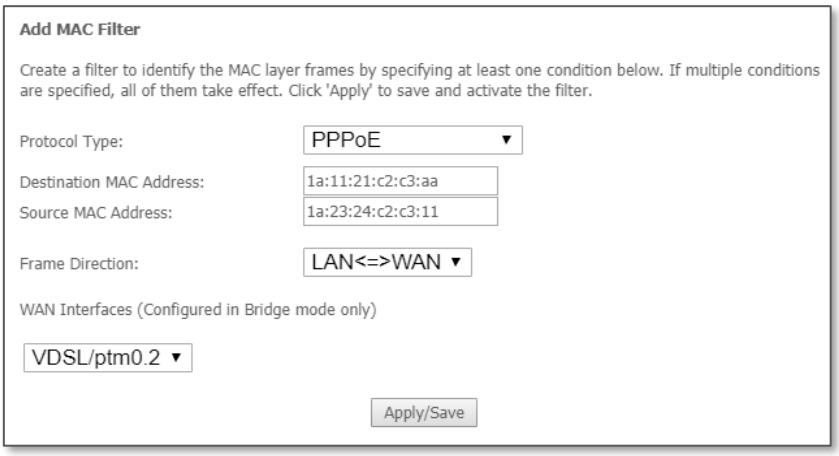


Figure 54 – Security – MAC Filter settings

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.

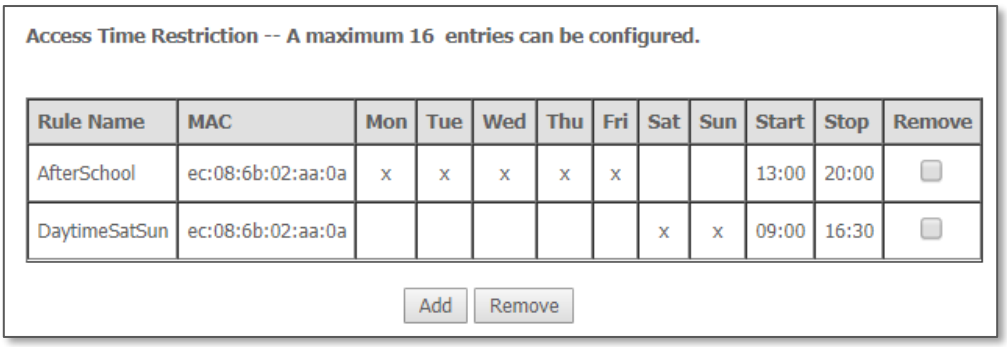


Figure 55 – Advanced – Parental Control – Time Restriction

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

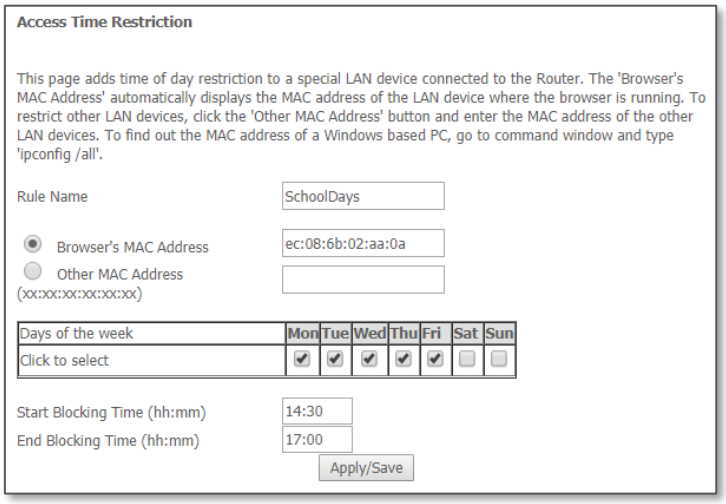


Figure 56 – Advanced – Parental Control – Add Time Restriction

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)

Field	Description
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 20 – Advanced – Parental Control – Add Time Restriction Settings

URL Filter

With the URL filter, you are able to 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 NF18ACV.

Select the **Black List** (to block) or **White List** (to allow) option and then click **Add** to enter the URL you wish to add to the URL Filter list.

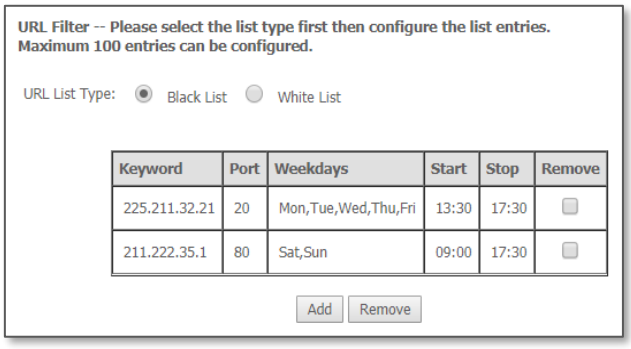


Figure 57 – Advanced – Parental Control – URL Filter

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.

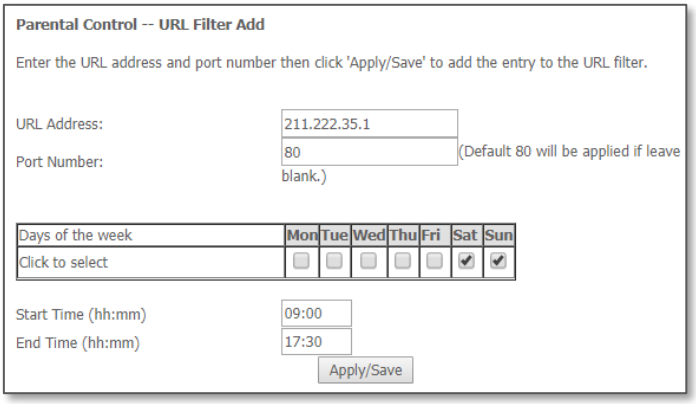


Figure 58 – Advanced – Parental Control – Add URL Filter

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.

Field	Description
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 21 – Advanced – Parental Control – Add URL Restriction Settings

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.

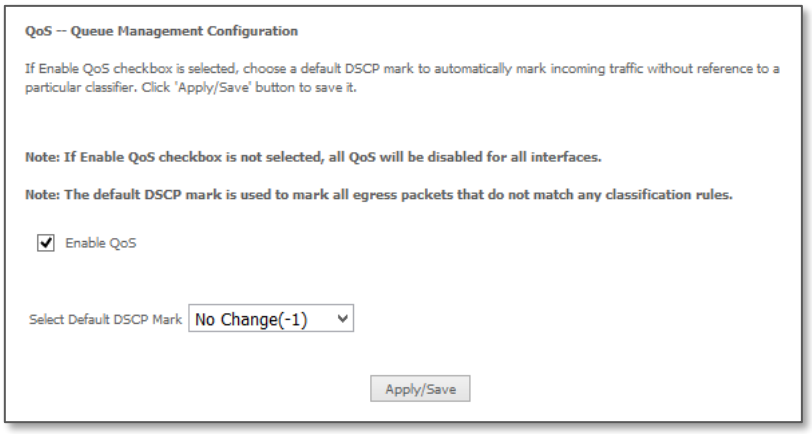
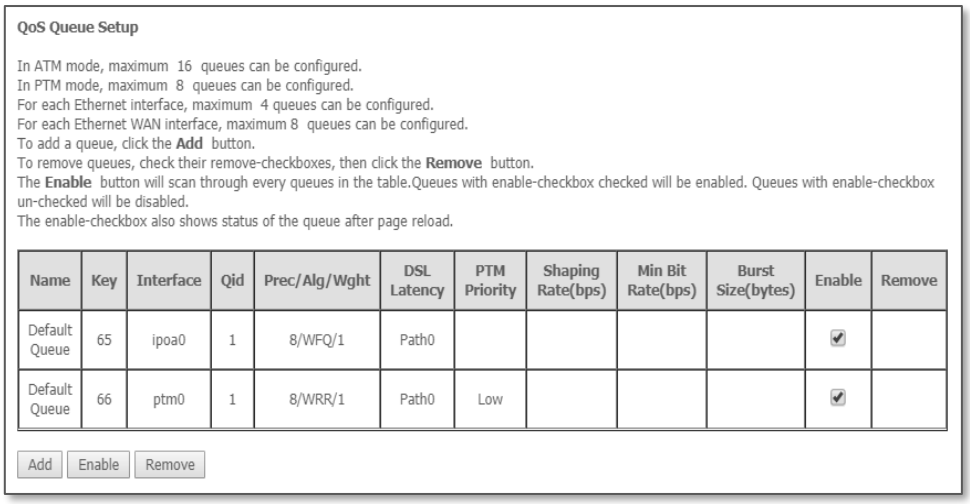


Figure 59 – Advanced – Enable QoS

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

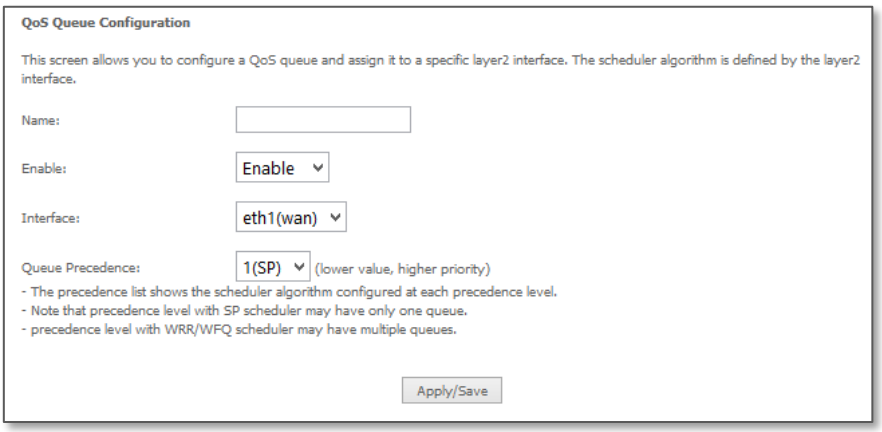
In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 4 queues can be configured.
For each Ethernet WAN interface, maximum 8 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their 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	DSL Latency	PTM Priority	Shaping Rate(bps)	Min Bit Rate(bps)	Burst Size(bytes)	Enable	Remove
Default Queue	65	ipoa0	1	8/WFQ/1	Path0					☑	
Default Queue	66	ptm0	1	8/WRR/1	Path0	Low				☑	

Add Enable Remove

Figure 60 – 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 assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Name:

Enable: Enable

Interface: eth1(wan)

Queue Precedence: 1(SP) (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.

Apply/Save

Figure 61 – 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 62 – Advanced – QoS – WLAN Queue

QoS Classification

QoS Classification Setup -- A maximum 32 entries 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	Min:Max/ IpLength	Protocol	Source Port	Destination	DSCP Check	802.1P Check	TC Check	Queue Key	DSCP Mark	802.1P Mark	TC Mark	Rate Limit(kbps)	Enable	Remove

Add Enable Remove

Figure 63 – Advanced – QoS Classification list

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

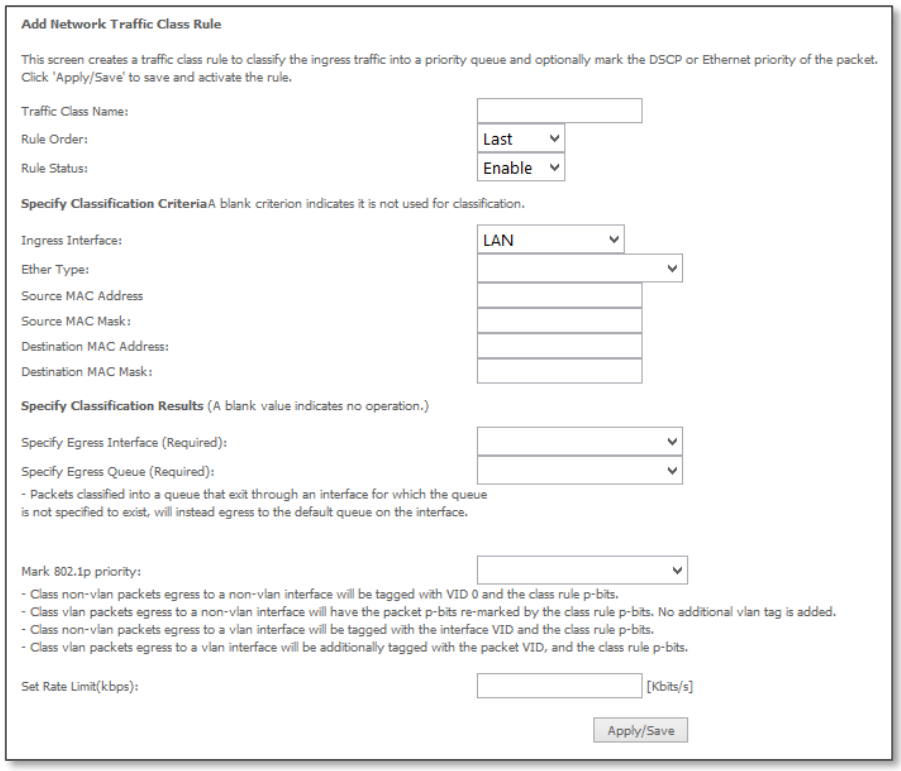


Figure 64 – Advanced – QoS – Network Traffic Class settings

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.

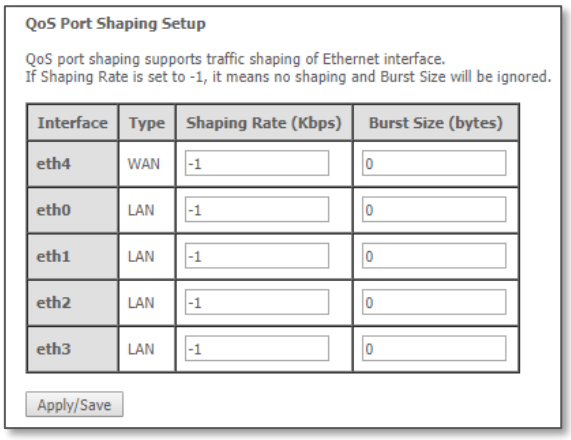


Figure 65 – QoS Port Shaping settings

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 66 – 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.

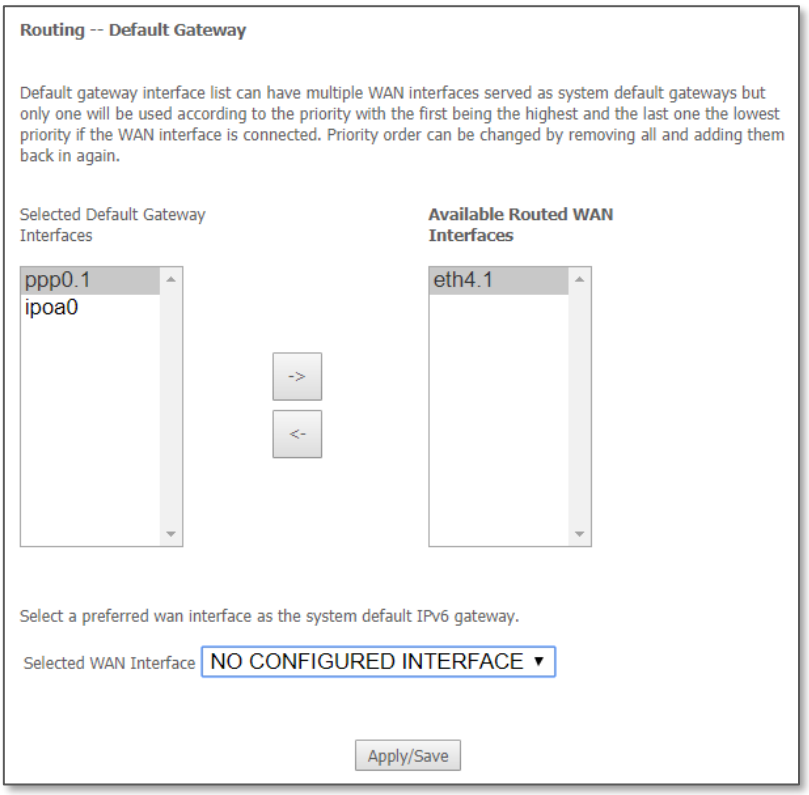


Figure 67 – Routing – Set Default Gateway

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 router.

Static Route

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

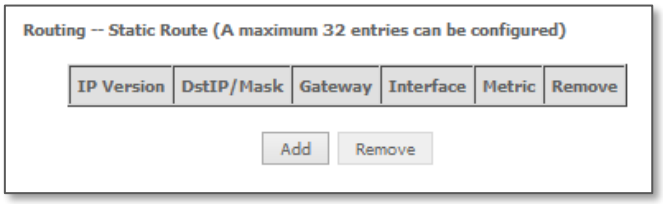


Figure 68 – Routing – Static Route list

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

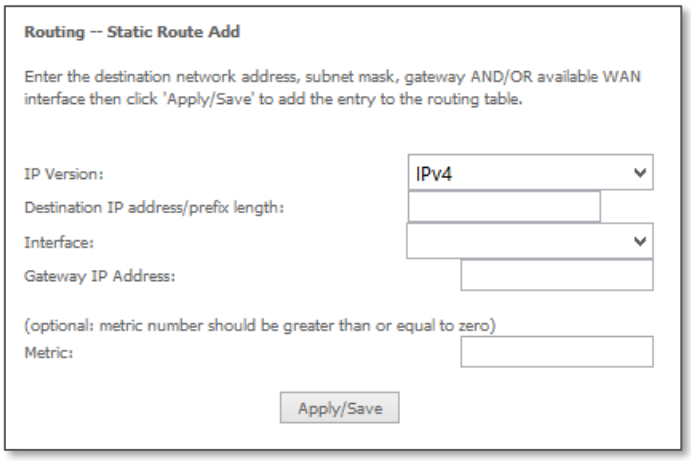


Figure 69 – Routing – Static Route configuration

Select the **IP Version**, 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 the 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.

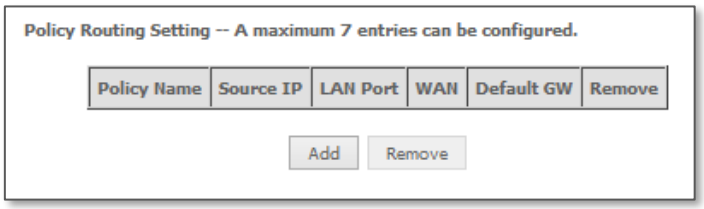


Figure 70 – Routing – Policy Routing list

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

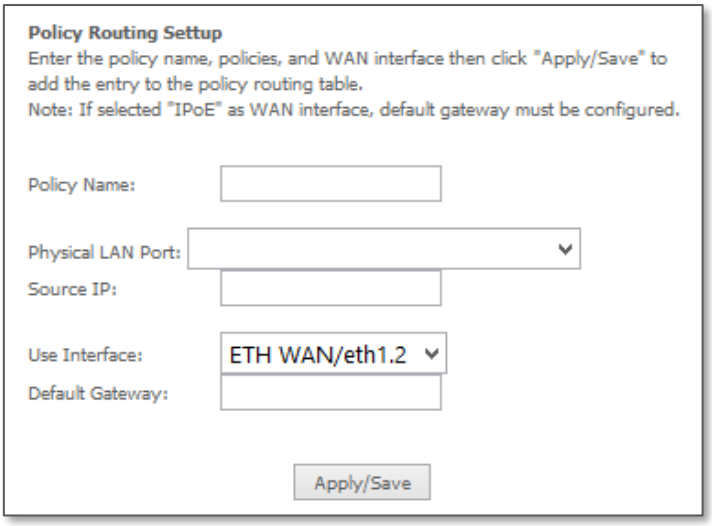


Figure 71 – Advanced – Routing – Policy Route configuration

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	Enter the gateway address.

Table 22 – Routing – Policy Route settings table

RIP

The Routing Information Protocol (RIP) allows routers 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.

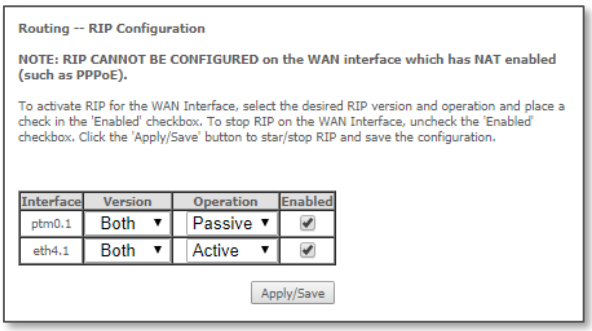


Figure 72 – Routing – RIP list

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 routers.
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**.

Item	Description
Apply/Save button	Click the **Apply/Save** button to initiate the change.

Table 23 – Routing – RIP settings

DNS

DNS Server Configuration

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.netcommwireless.com into their browser, your router is contacting the DNS server and requesting the webserver IP address.

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

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

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

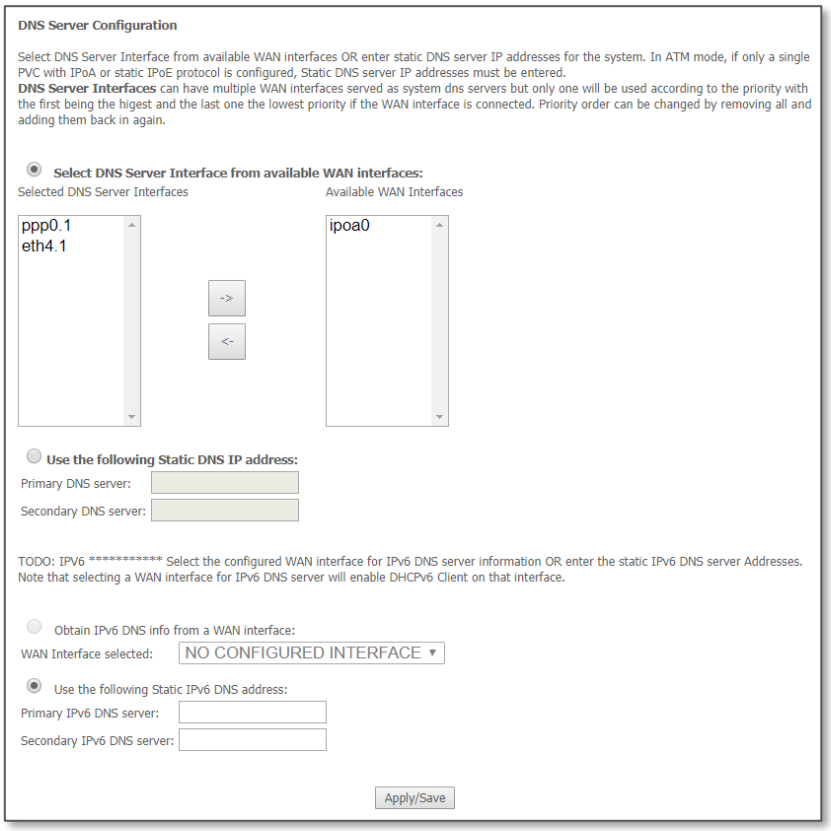


Figure 73 – DNS Server Configuration

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 24 – 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.

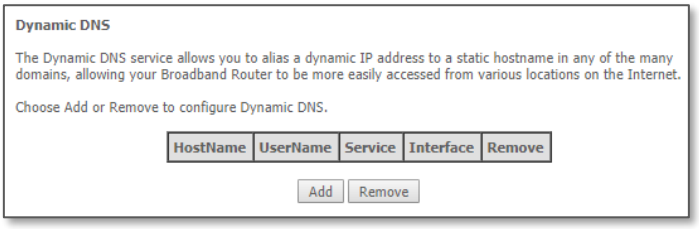


Figure 74 – Dynamic DNS list

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

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**.

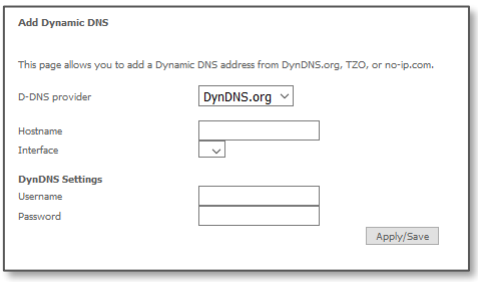


Figure 75 – Add Dynamic DNS

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

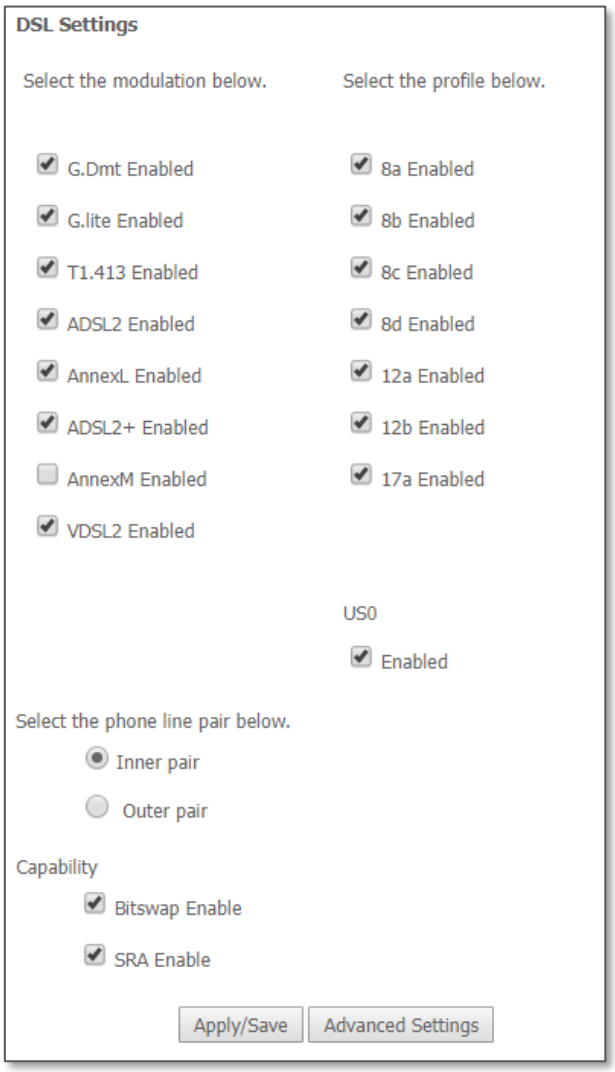


Figure 76 – DSL settings page

Field	Description
Modulation	A user defined name for the policy route.
Profile	The LAN port to be used for the policy.
USO	The IP address of the LAN device involved with the policy.
Phone line type	Select the Interface that the policy will employ.
Capability	Enter the gateway address.
Apply/Save button	Click the **Apply/Save** button to initiate the change.
Advanced Settings button	Allow configuration of the Modem state for diagnostic purposes.

Table 25 – DSL settings table

DSL Advanced settings

For advanced DSL options press the **Advanced Settings** button.

The DSL advanced settings relate to test mode settings. The default selection is **Normal**.

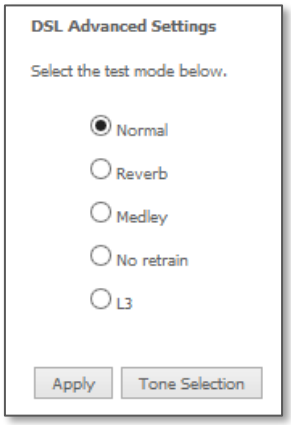


Figure 77 – DSL Advanced Settings page

Field	Description
Normal	Puts the modem in normal operation mode.
Reverb	Puts the modem in a test mode in which it only sends a Reverb signal.
Medley	Puts the modem in a test mode in which it only sends a Medley signal.
No retrain	In this mode, the modem will try to establish a connection as in normal mode, but once the connection is up it will not retrain if the signal is lost.
L3	Puts the modem in the Link state (Idle) at the start of the initialization procedure.
Apply button	Click the **Apply** button to initiate the change.
Tone Selection button	Allow selection of frequency band for data transfer.

Table 26 – DSL settings table

ADSL Tone Settings

To alter the ADSL Tone Settings, click the **Tone Selection** button on the *DSL Advanced Settings* page.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125kHz apart. With each tone carrying separate data, the technique operates as if 256 separate routers were running in parallel. The tone range is from 0 to 31 for upstream traffic and from 32 to 255 for downstream traffic.

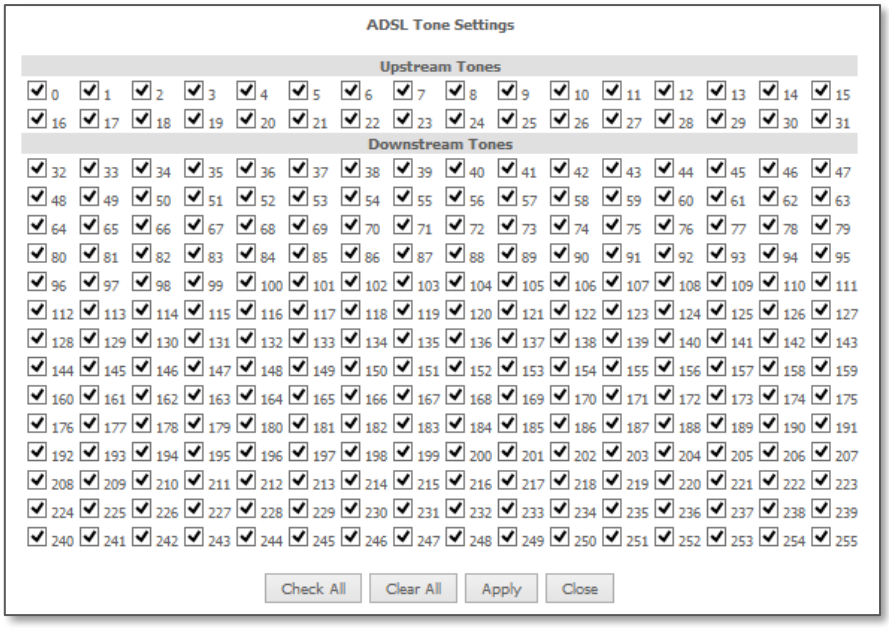


Figure 78 – ADSL Tone Settings page

Warning – Do not change these settings unless you are directed to by your Internet Service Provider.

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, gaming console, WiFi 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.

Enable UPnP to allow automatic port forwarding configuration detection for your UPnP devices.

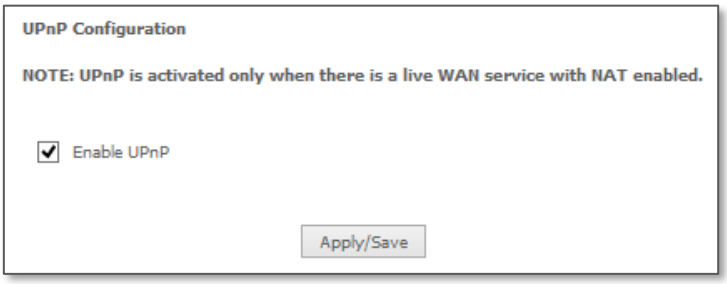


Figure 79 – UPnP activation page

DNS Proxy

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

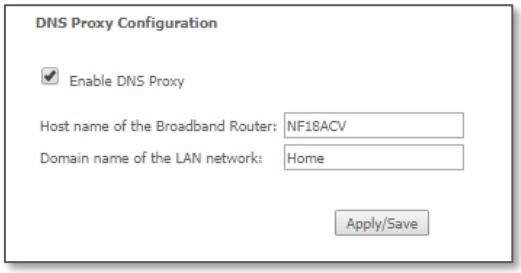


Figure 80 – DNS Proxy activation page

The Host name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the user interface of the router with a local name rather than by using the router IP address. For example, you can access your router by entering http://NF18ACV into your web browser.

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 NF18ACV and the router will make it accessible to other devices on your network.

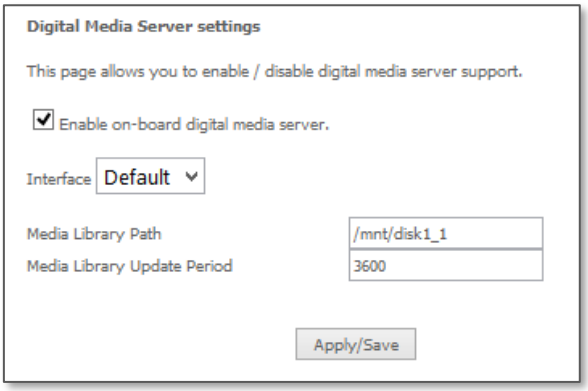


Figure 81 – DLNA setting page

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

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.

Storage Device Info

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

Figure 82 – 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.

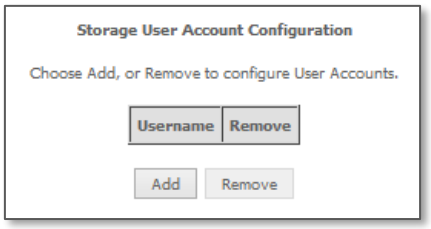


Figure 83 – Storage User Accounts list

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.

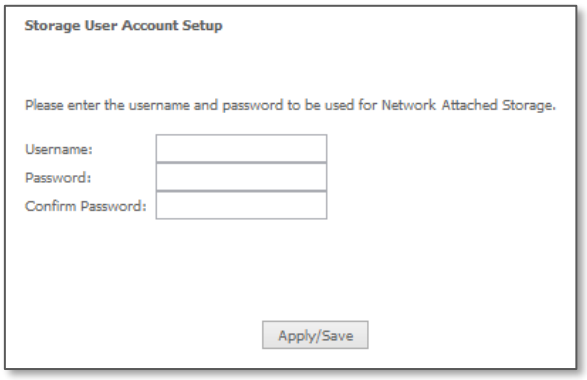


Figure 84 – Storage User Account Setup page

Interface Grouping

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

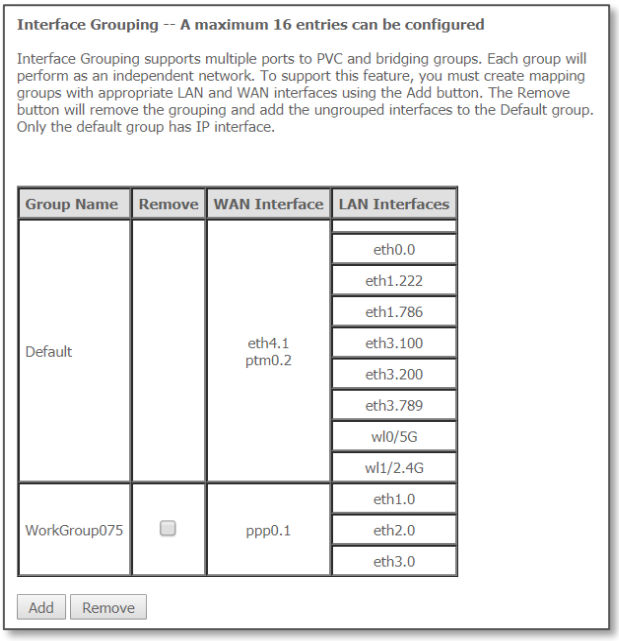


Figure 85 – Interface Grouping list

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

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

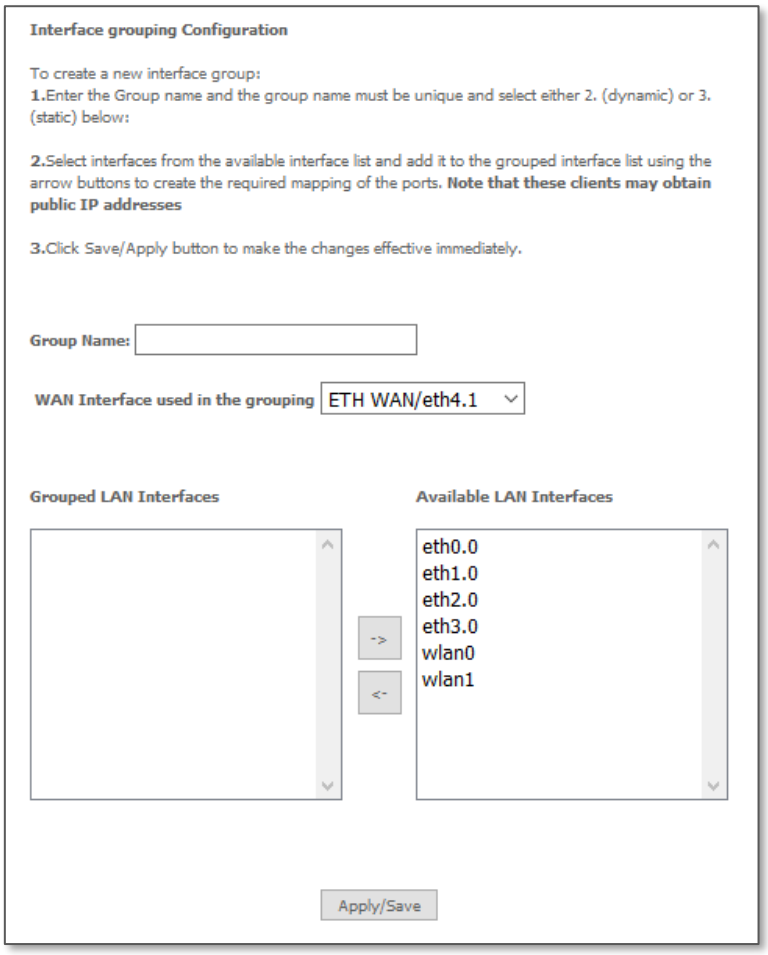


Figure 86 – Interface Grouping configuration

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.

IP Tunnel

The IP Tunnelling feature allows you to configure tunnelling of traffic between IPv6 and IPv4 network using a tunnelling service.

IPv6inIPv4

To use IPv6inIPv4 tunnelling service an active subscription to a tunnelling provider are required.

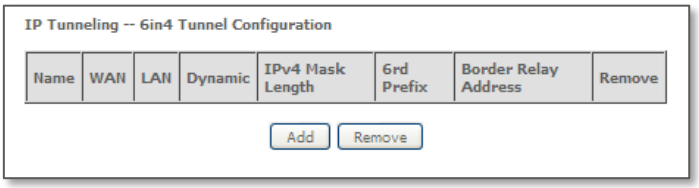


Figure 87 – IPv6inIPv4 Tunnel list

Click the **Add** button to add a new tunnel.

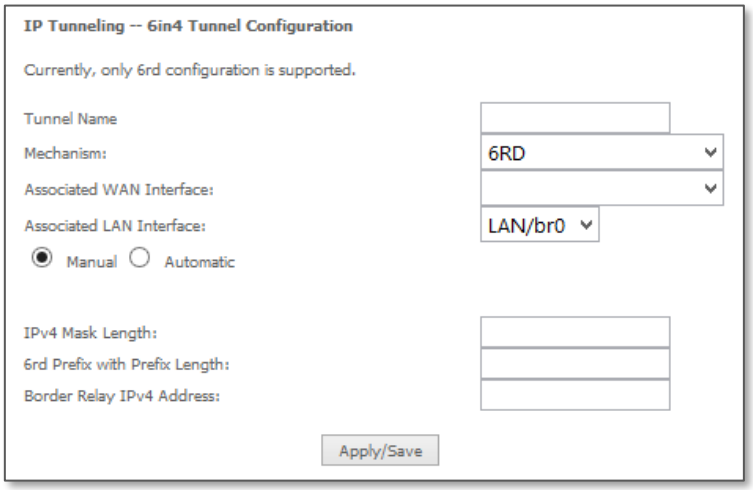


Figure 88 – 6in4 Tunnel configuration

IPv4inIPv6

Your ISP must support the DS-Lite IPv4inIPv6 tunnelling service, to enable this feature

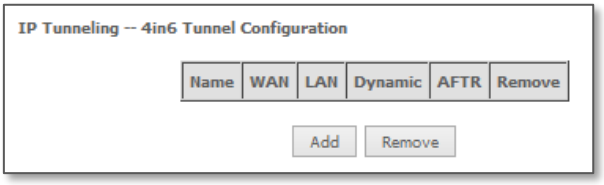


Figure 89 – IPv4inIPv6 Tunnel list

Click the **Add** button to add a new tunnel.

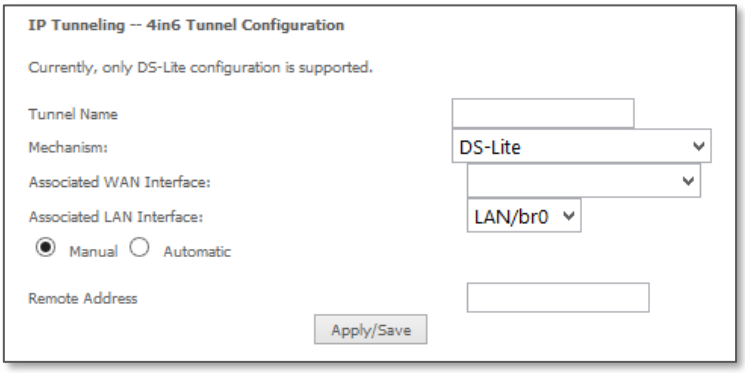


Figure 90 – 4in6 Tunnel configuration

Multicast (IGMP Configuration)

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is a protocol only used on the network between a host and the router. It allows a host to inform the router whenever that host needs to join or leave a particular multicast group. IGMP provides for more efficient allocation of resources when used with online gaming and video streaming.

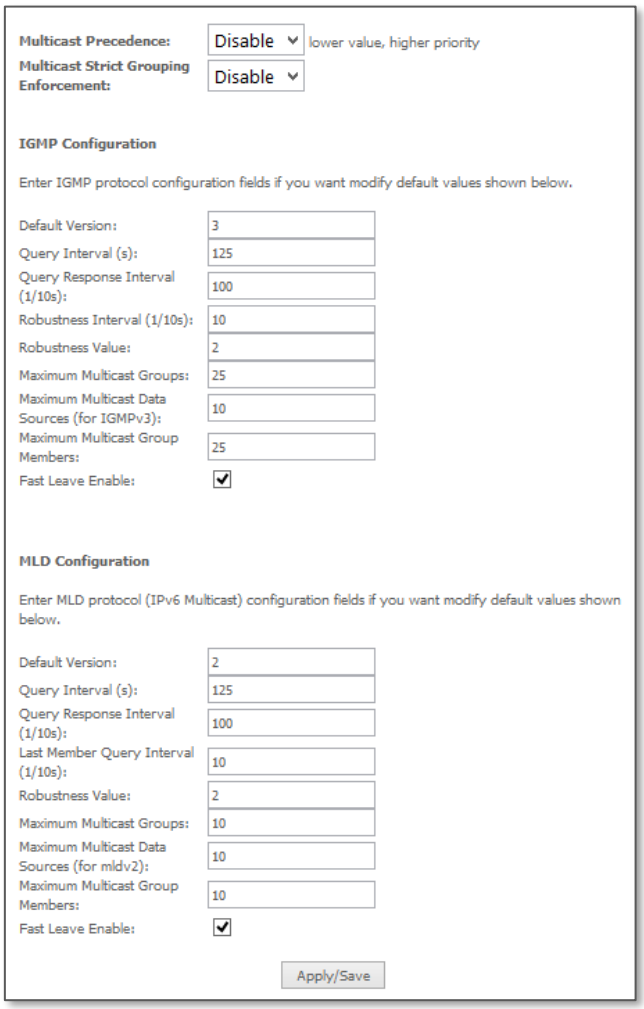


Figure 91 – Multicast

Field	Definition
Default Version	The version IGMP in use by the router.
Query Interval	The hosts on the segment report their group membership in response to the router's queries. The query interval timer is also used to define the amount of time a router will store particular IGMP state if it does not hear any reports on the group. The query interval is the time in seconds between queries sent from the router to IGMP hosts.
Query Response Interval	When a host receives the query packet, it starts counting to a random value, less the maximum response time. When this time expires, the host replies with a report, provided that no other host has responded yet. This accomplishes two purposes:

Field	Definition
	a) Allows controlling the amount of IGMP reports sent during a time window. b) Engages the report suppression feature, which permits a host to suppress its own report and conserve bandwidth.
Last Member Query Interval	IGMP uses this value when router hears IGMP Leave report. This means that at least one host wants to leave the group. After router receives the Leave report, it checks that the interface is not configured for IGMP Immediate Leave (single-host on the segment) and if not, it sends out an out-of-sequence query.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	The maximum number of multicast groups that the router can control at any one time.
Maximum Multicast Data Sources	The maximum number of data sources a multicast group can have.
Maximum Multicast Group Members	The maximum number of hosts a multicast group can have.
Fast Leave Enable	With IGMP fast-leave processing, which means that the router immediately removes the interface attached to a receiver upon receiving a Leave Group message from an IGMP host.

Table 27 – Multicast settings table

IPSec

Displays the IPSec tunnel connections.

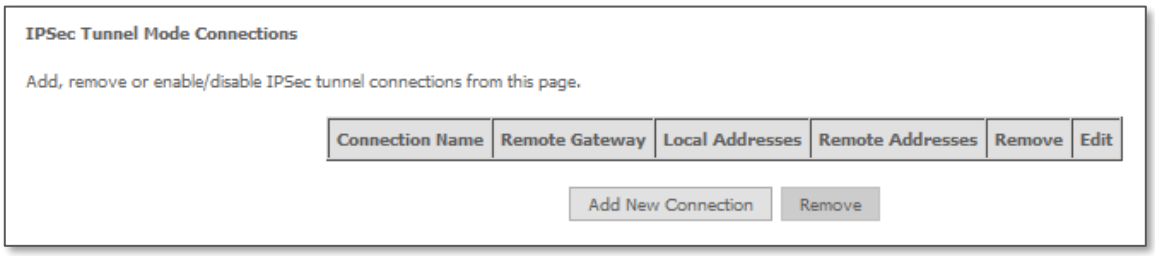


Figure 92 – IPSec Tunnel Mode Connections list

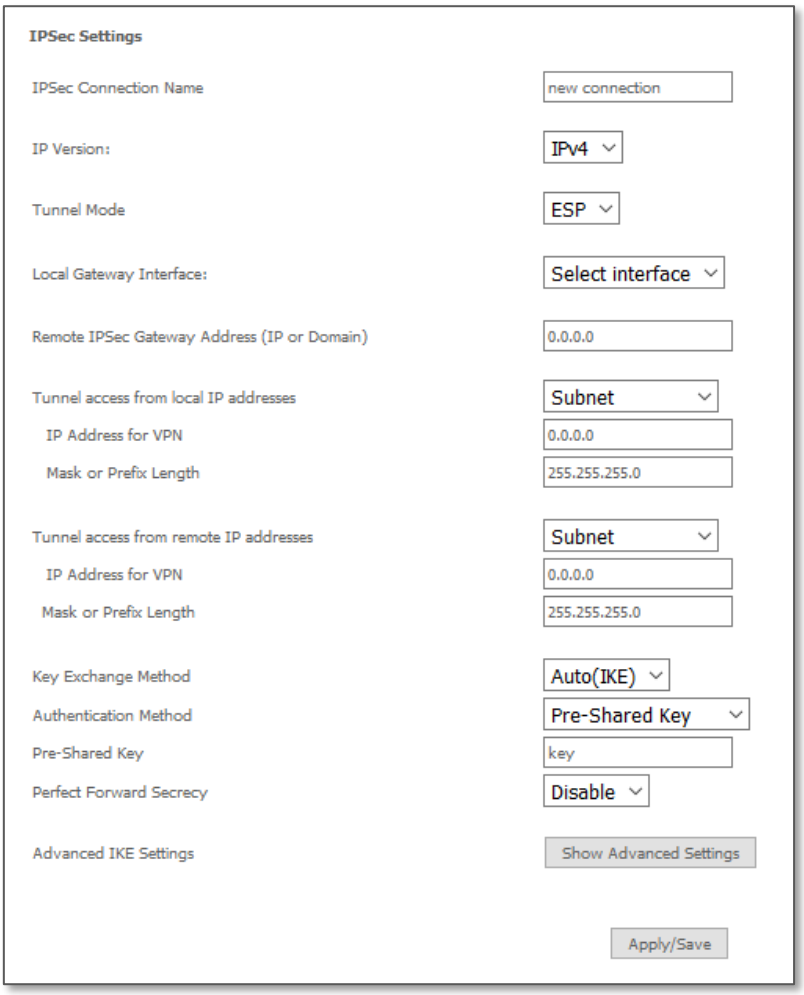


Figure 93 – IPSeC configuration

Parameter	Definition
IPSec Connection Name	Enter a name to identify the IPSec tunnel.
Tunnel Mode	Select the applicable IPSec tunnel mode.
Remote IPSec Gateway	Enter the IP Address of the IPSec server to connect to.
Tunnel access from Local	Select which remote addresses local IPSec connections are able to access .
IP Address from VPN	Enter the IP Address to be used locally for the IPSec tunnel.
Subnet mask for VPN	Enter the subnet mask to be used locally for the IPSec tunnel.
Tunnel Access from Remote	Select which local addresses remote IPSec connections are able to access.
IP Address for VPN	Enter the IP Address to be used on the remote end for the IPSec tunnel.
Subnet mask for VPN	Enter the subnet mask to be used on the remote end for the IPSec tunnel.
Key Exchange Method	Select the type of IPSec exchange is to be used on the IPSec tunnel.
Authentication Method	Select the applicable authentication for the IPSec tunnel.
Pre-Shared Key	Enter the pre-shared key (if applicable) to grant access to the IPSec tunnel.

Parameter	Definition
Perfect Forward Secrecy	Select to use Perfect Forward Secrecy during key exchange for the IPSec tunnel.
Advanced IKE Settings	Configure advanced IKE settings for the IPSec tunnel such as the encryption method or key life time.

Table 28 – IPSeC settings table

Wireless

WiFi 2.4GHz/WiFi 5GHz

The NF18ACV router 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

5 GHz Wireless Configuration pages

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

Wireless – Basic

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

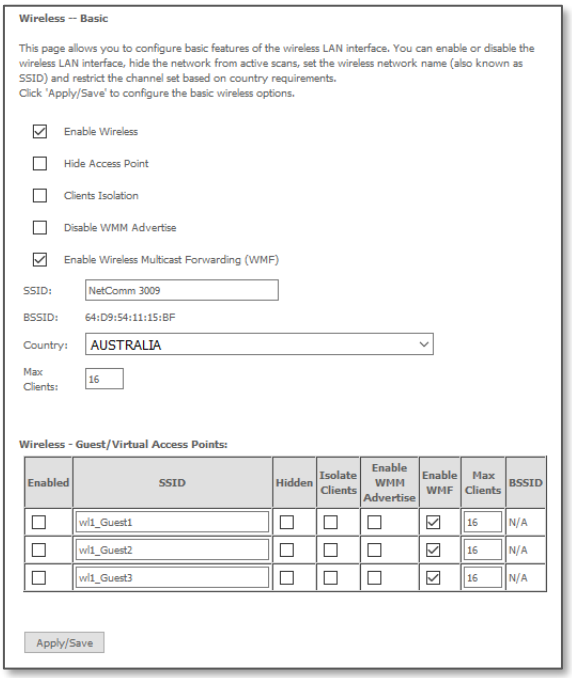


Figure 94 – Wireless - Basic Configuration

The following parameters are available:

Parameter	Definition
Enable Wireless	Select ☑ **Enable Wireless** 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 NF18ACV 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
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 29 – 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

Wireless – Security

The NF18ACV supports all encryptions within the 802.11 standard. The factory default is **WPA2-PSK**. The NF18ACV also supports: **WPA**, **WPA-PSK**, **WPA2** or **WPA2-PSK**

You can also select to disable WPS mode.

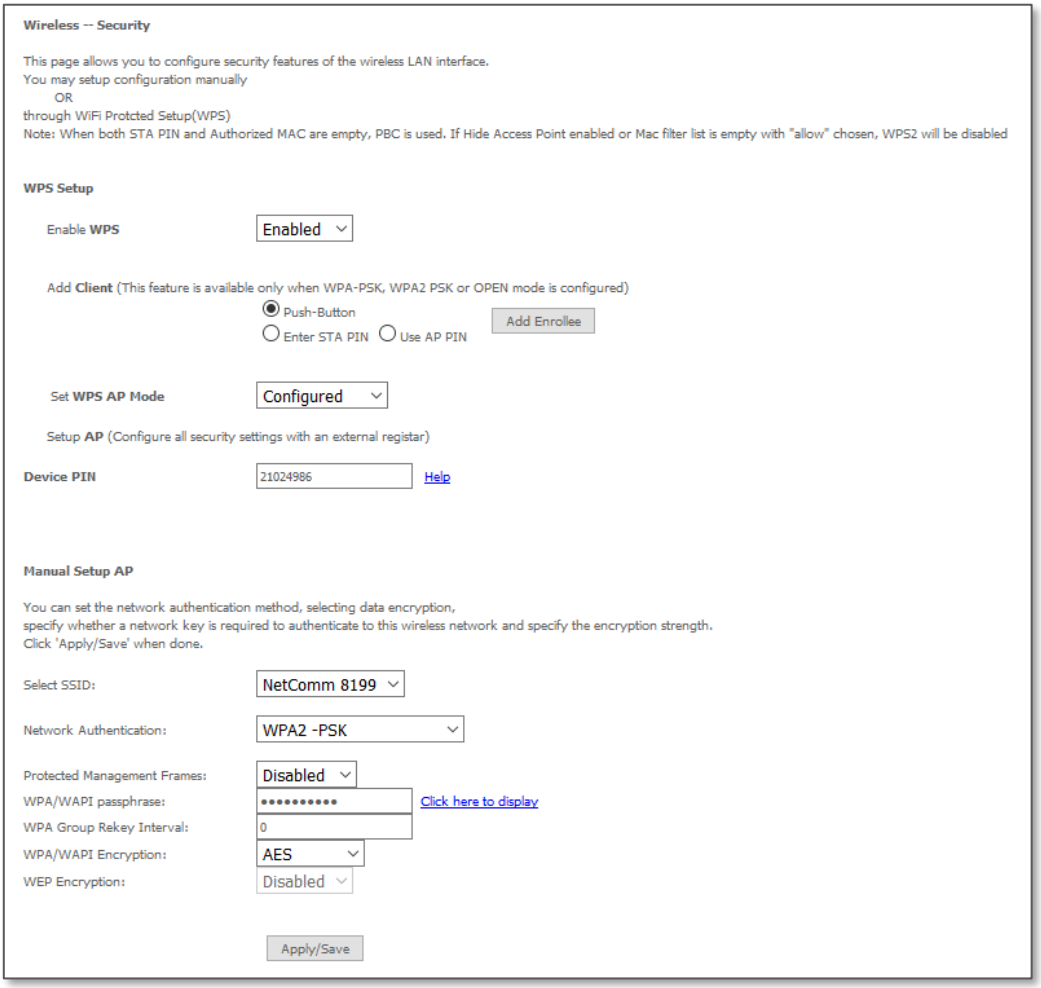


Figure 95 – Wireless Security

The following parameters are available:

Parameter	Definition
Enable WPS	Select to enable or disable the WPS function of the NF18ACV.
Select SSID	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 NF18ACV also supports: **WPA**, **WPA-PSK**, **WPA2**, **WPA2-PSK**
WPA/WAPI passphrase	Enter the security key to use with the wireless network.
WPA Group Rekey Interval	Enter the group rekey interval. This should not need to change.
WPA/WAPI Encryption	Select the type of encryption to use on the wireless network.

Parameter	Definition
WEP Encryption	Select to utilise WEP encryption on the wireless network connection.

Table 30 – Wireless security settings table

Note – **WPA** with **TKIP** and **Open WEP** are no longer considered secure. **WPA2** with **AES** is the most secure option.

Mixed **WPA2/WPA (TKIP+AES)** will provide maximum compatibility with legacy devices

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

Wireless – 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 **Select SSID** drop down list to select the wireless network you wish to configure, then select to either allow or deny access to the MAC addresses listed.

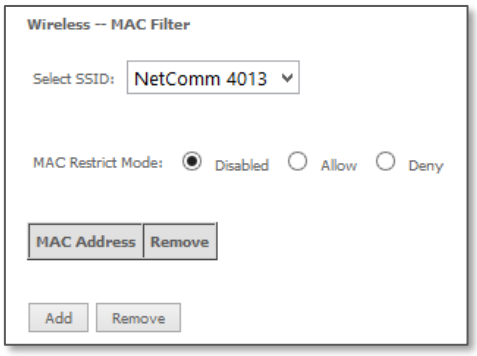


Figure 96 – Wireless – MAC Filter list

Click **Add** to add a MAC Address Filter.

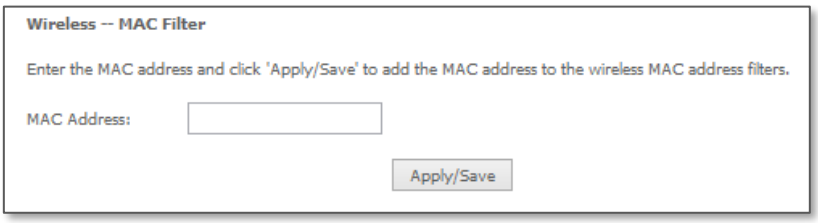


Figure 97 – Wireless – MAC Filter configuration

Enter the MAC Address to be filtered and click **Apply/Save** to save the new MAC Address filter settings.

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.

Wireless – Wireless Bridge (Wireless Distribution Service)

Wireless Bridge allows you to configure the router's access point as a Wireless Distribution Service.

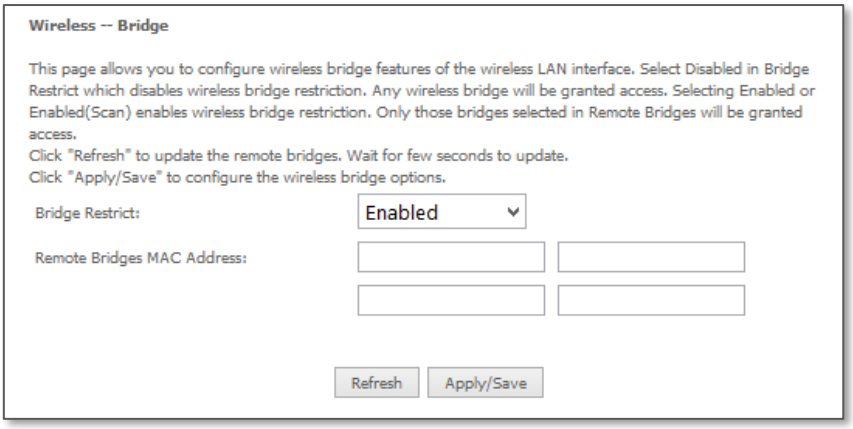


Figure 98 – Wireless Bridge page

Select the mode for the Wireless Access Point built into the NF18ACV. You can specify which wireless networks will be allowed to connect to the NF18ACV by using the **Bridge Restrict** option and then entering the applicable MAC Addresses of the other wireless access points.

Note – WPA/WPA2 encryption may not be compatible with other vendors, when operating in Wireless Bridge (WDS) mode.

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

Wireless – Advanced

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

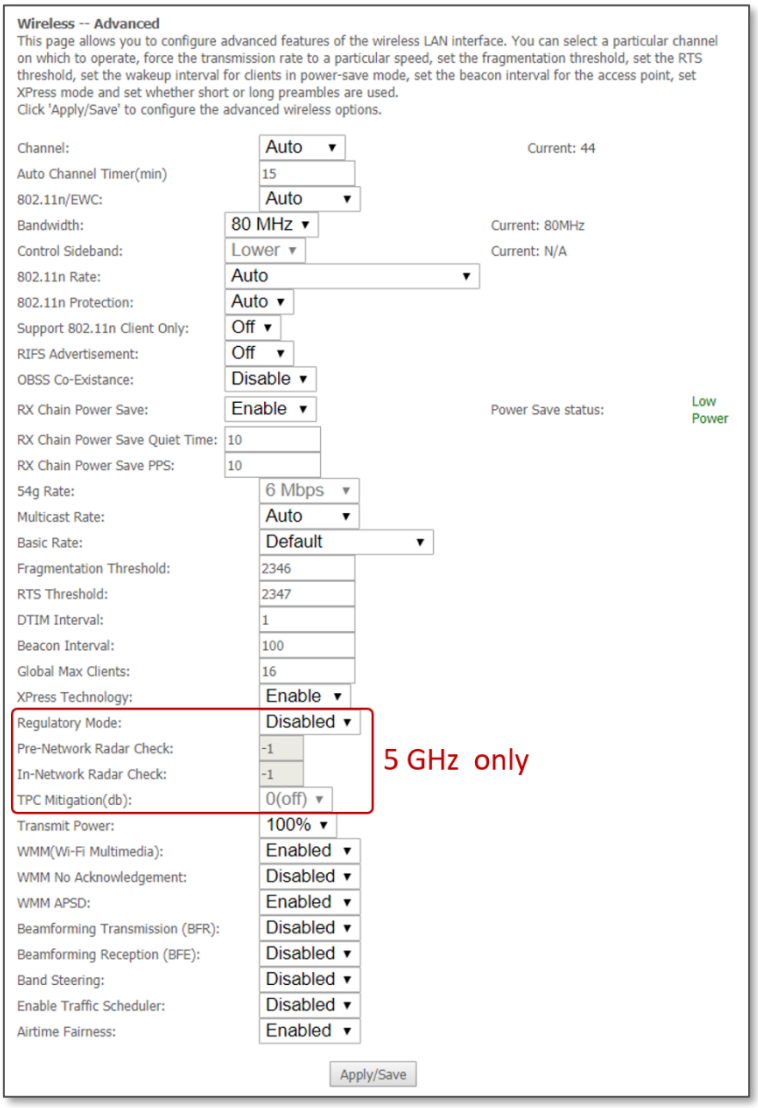


Figure 99 – Wireless – Advanced configuration page

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

Parameter	Definition
Band	Shows your current frequency band.
Channel	Fill in 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 router supports auto channelling functionality.
Auto Channel Timer(min)	Specifies the timer of auto channelling.
802.11n/EWC	Select disable 802.11n or Auto.

Parameter	Definition
Bandwidth	Select the bandwidth for the network. In high wireless activity/interference environment, reduce band to 20MHz for better stability.
Control Sideband	If you select 20MHz in Both Bands you cannot select sideband does not work as you are not utilizing side bands. When you select 40MHz in Both Bands as the bandwidth and manual select channel, the following options will appear. Then you can select Lower or Upper as the value of sideband. As the control sideband, when you select Lower, the channel is 1~7. When you select Upper, the channel is 5~11.
802.11n Rate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
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.
Support 802.11n Client Only	Only stations that are configured in 802.11n mode can associate.
54g Rate	Allows you to specify the maximum bandwidth of the 802.11g network.
Multicast Rate	Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to 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.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (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

Parameter	Definition
	transmission. The RTS Threshold value should remain at its default value of 2347.
DTIM Interval	(Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast 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 a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
XPress Technology	Select **Enable** or **Disable**. This is a special frame-bursting accelerating technology for IEEE802.11g. The default is **Enabled**.
Regulatory Mode (5 GHz only)	Select: **Disabled**, **802.11h** or **802.11d** The default is **Disabled**.
Pre-Network Radar check (5 GHz only)	Available only in the 802.11h Regulatory Mode, see last setting. The default is: **-1**
Pre-Network Radar check (5 GHz only)	Available only in the 802.11h Regulatory Mode, see last setting. The default is: **-1**
TPC Migration (db) (5 GHz only)	Select: **0(off)**, **2, 3** or **4** The default is 0**(off)**
WMM (WiFi Multimedia)	Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	APSD is short for automatic power save delivery, selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Table 31 -Wireless – Advanced configuration settings

Wireless – Station Info

This page shows the MAC address of authenticated wireless stations that are connected to the NF18ACV and their status

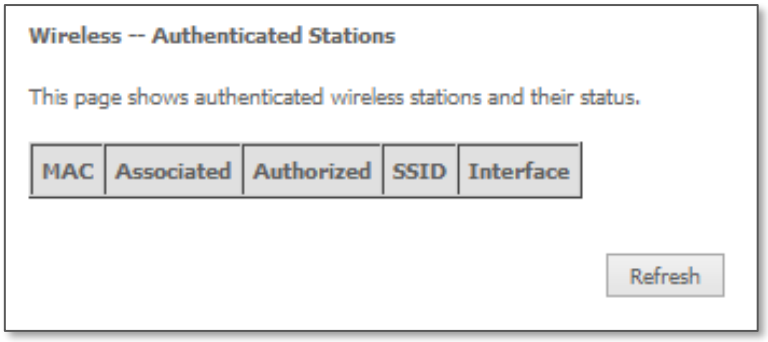


Figure 100 – Wireless – Station Info list

Voice

This section explains how to configure the VoIP settings of the NF18ACV.

VoIP Status

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

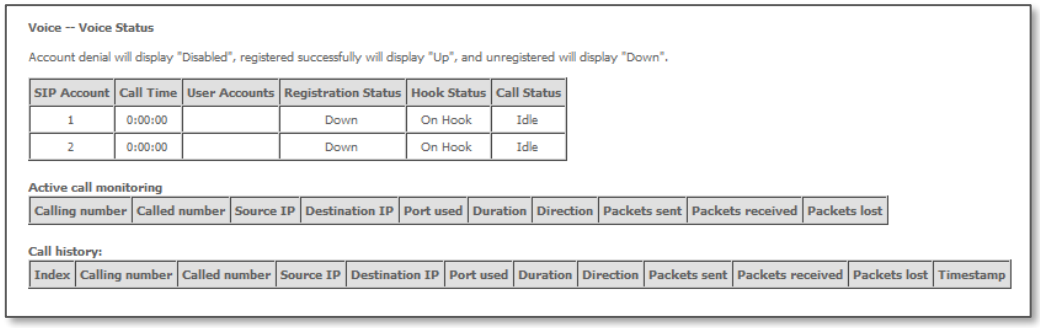


Figure 101 – Voice Status page

SIP Basic Setting

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

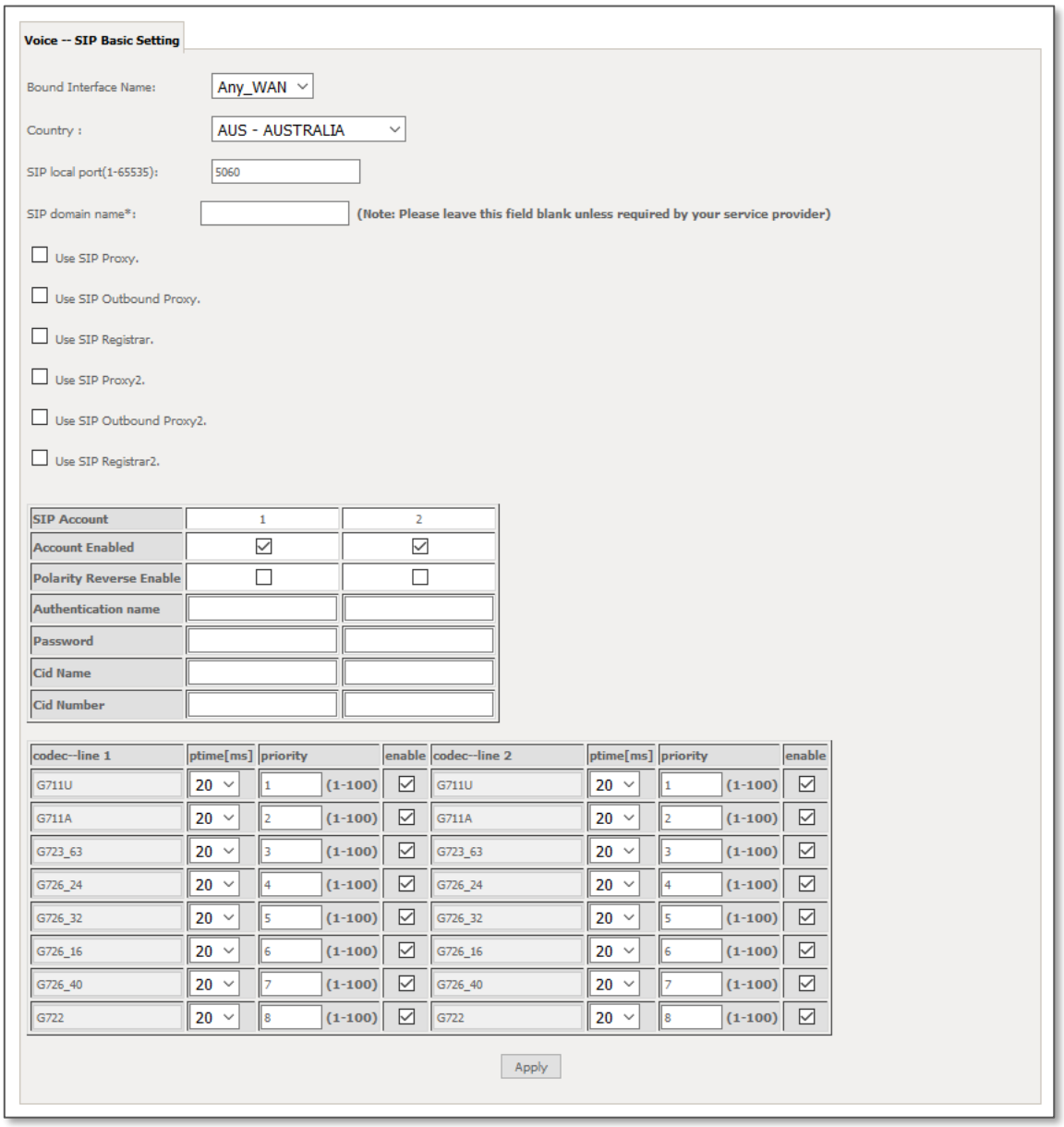


Figure 102 – SIP Basic Settings page

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.

Option	Definition
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.

Option	Definition
Priority	The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the DSL router chooses the codec automatically.

Table 32 – 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

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

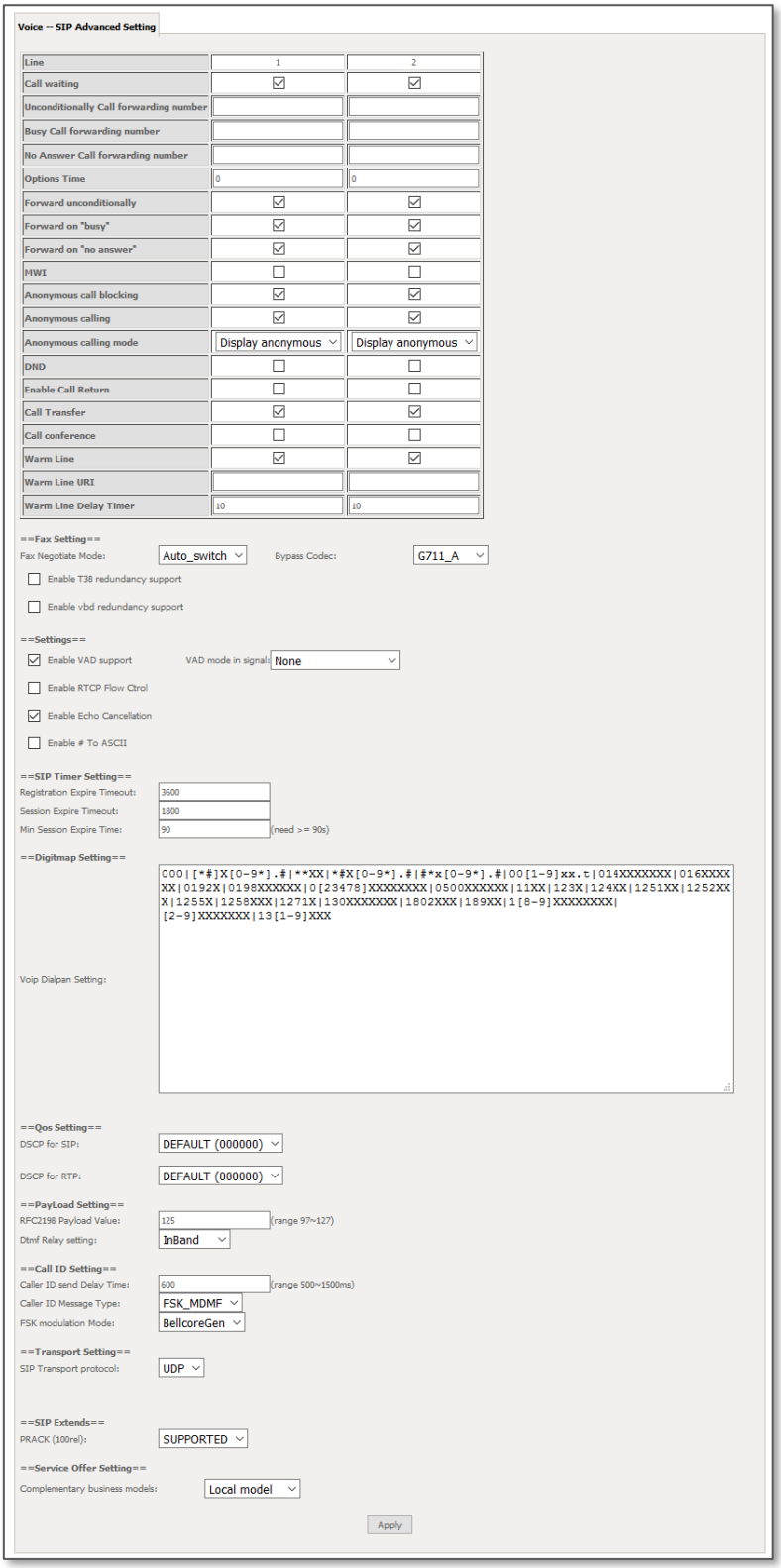


Figure 103 – Voice- SIP Advanced settings

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.
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.

Option	Definition
RFC2198 Payload Value (range 97-127)	Enter the RFC2198 payload value that the valid range is 96 ~ 127.
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	The interval of dialog refreshing time.
Min Session Expire Time	The minimum interval of dialog refreshing time.
VoIP DialPlan Setting	Set the VoIP dial plan. If user-dialled number matches it, the number is processed by the VoIP router immediately.
DSCP for SIP	Set the DSCP QoS tagging for Session Initiation Protocol. You can select it from the drop-down list.
DSCP for RTP	Set the DSCP QoS tagging for Real-time Transport Protocol. You can select it from the drop-down list.
Dtmf Relay Setting	Set DTMF transmit method, which can be following values: SIP Info: Use SIP INFO message to transmit DTMF digits. RFC2833: Use RTP packet to encapsulate DTMF events, as specified in RFC 2833. InBand: DTMF events are mixed with user voice in RTP packet.
SIP Transport Protocol	Select the transport protocol to use for SIP signalling. Note that your SIP proxy and registrar will need to support the protocol you select.
Enable Local Supplementary Service	Select the checkbox to enable the supplementary service settings by the telephone set. If you deselect the checkbox, the supplementary service cannot be set by the telephone set.

Table 33: VoIP – Advanced – Service Provider settings

Configuring a VoIP dial plan

The router 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 34 – Dial Plan Syntax table

Dial plan example: Australia Dial Plan

```
000|[*#]X[0-9*]|*#X[0-9*]|00[1-
9]XX.t|014XXXXXXX|016XXXXXX|0192X|0198XXXXXX|0[23478]XXXXXXXX|0500XXXXXX|11XX|123X|124XX|
1251XX|1252XXX|1255X|1258XXX|1271X|130XXXXXXX|13[1-9]XXX|1802XXX|189XX|1[8-9]XXXXXXXX|[2-
9]XXXXXXX
```

---

000 = Australia Emergency Call Service

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

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

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

130XXXXXXX = 1300 business numbers

13[1-9]XXX = 13 business numbers

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

SIP Extra Setting

This page displays additional settings related to the SIP service.

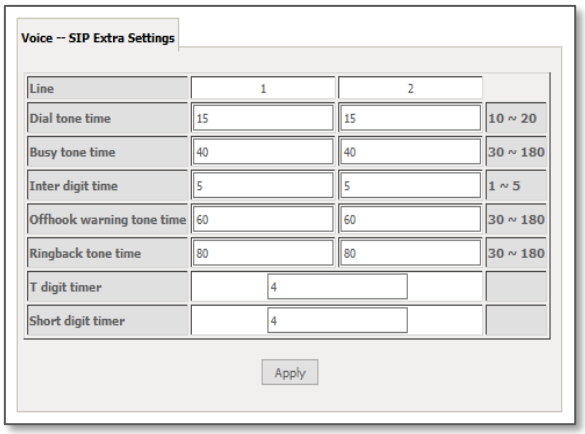


Figure 104 – SIP Extra Setting page

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 35 – 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.

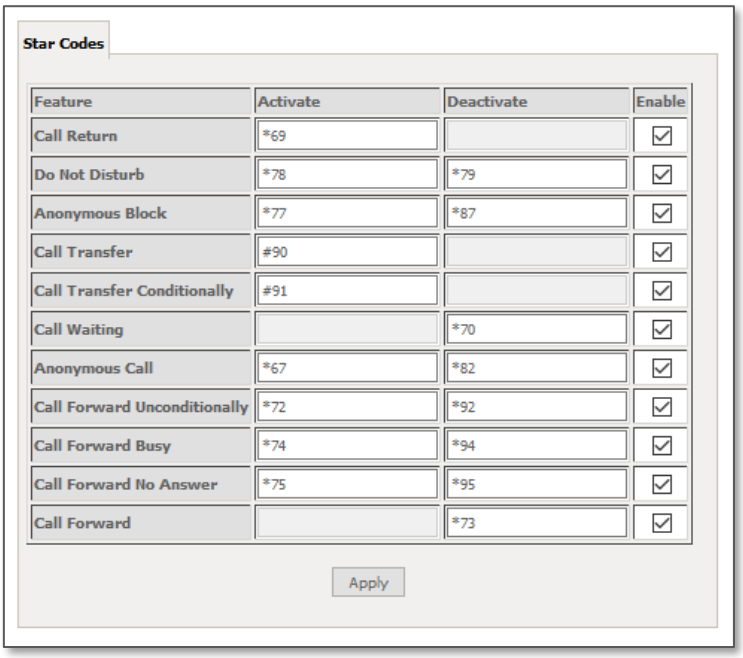


Figure 105 – SIP Star Code Setting page

SIP Debug Setting

This page allows you to configure various settings regarding the logging levels of the SIP service.

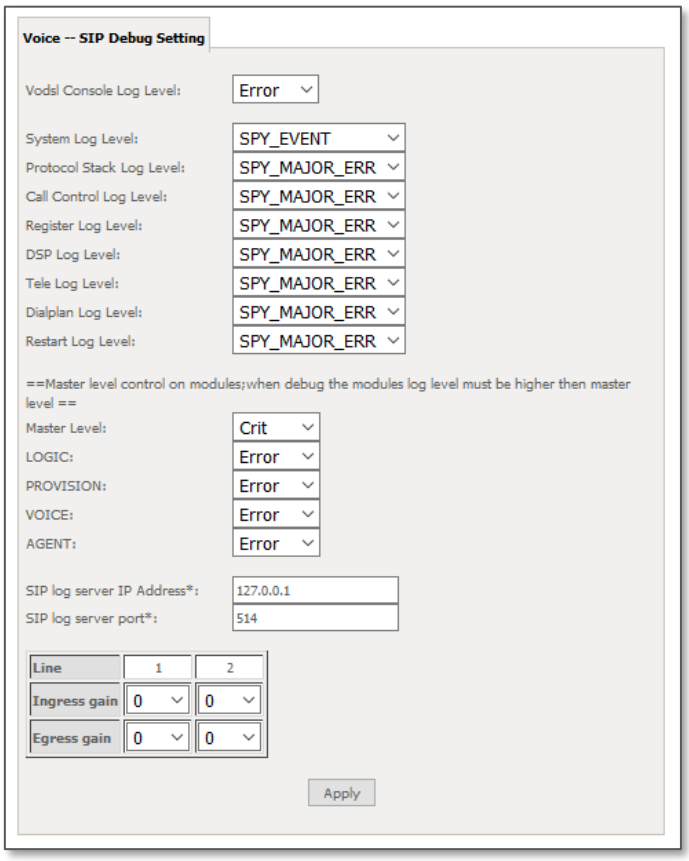


Figure 106 – SIP Debug Settings page

Option	Definition
SIP Log Server IP Address	Enter the Log Server IP address where the SIP Log data for the router will be sent to.
SIP Log Server port	Enter the port to be used for transmitting the SIP Log data.
Ingress Gain	Setting allow control of Speaker volume on handset.
Egress Gain	Settings allow control of Microphone volume on handset.

Table 36 – SIP Debug Settings table

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 enabled, incoming calls are forwarded to third party when you does 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

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

Note – Your Internet service provider must support diagnostics features in order for correct DSL diagnostics results.

Diagnostics – Diagnostics

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

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

6 Now click **Rerun Diagnostic Tests** at the bottom of the screen to re-test and confirm the error.

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

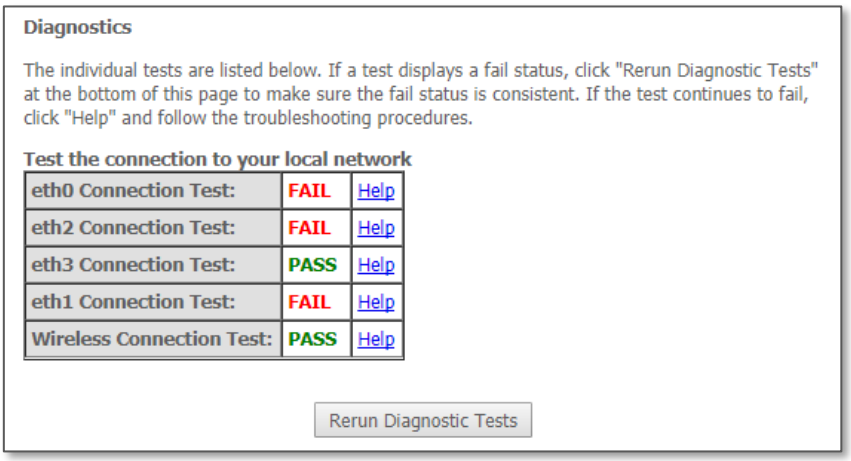


Figure 107 – Diagnostics – Diagnostic tests

Field	Description
LAN# Connection	**PASS** – Indicates the Ethernet connection to your computer is connected to the LAN port of the router. **FAIL** – Indicates that the router does not detect the Ethernet interface of your computer.
Wireless Connection Test	**PASS** – Indicates that the wireless card is switched **ON**. **FAIL** – Indicates that the wireless card is switched **OFF**.

Table 37 – Diagnostic test result table

Diagnostics – Ethernet OAM

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

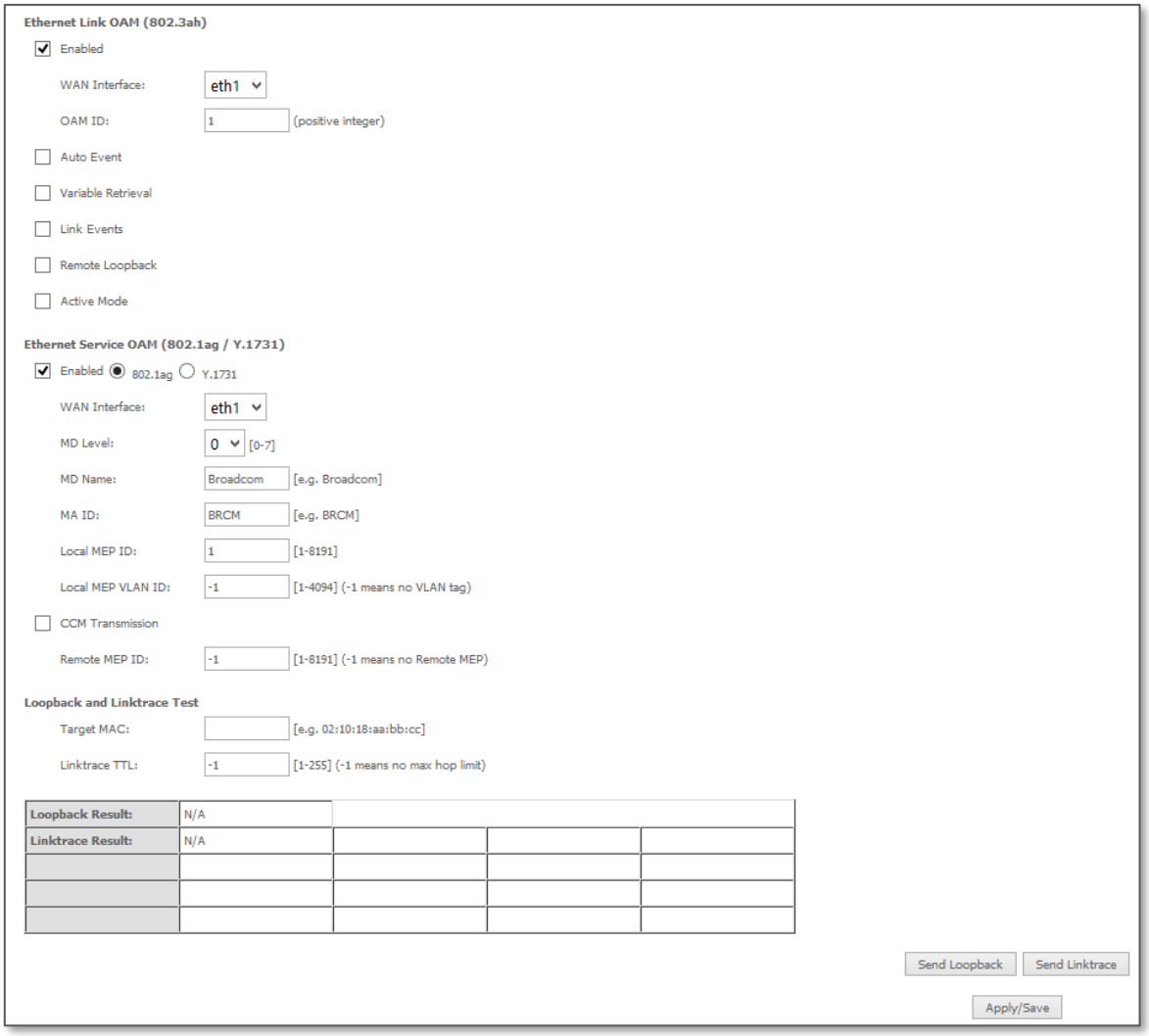


Figure 108 – Diagnostics – Ethernet OAM

Diagnostics – Ping

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

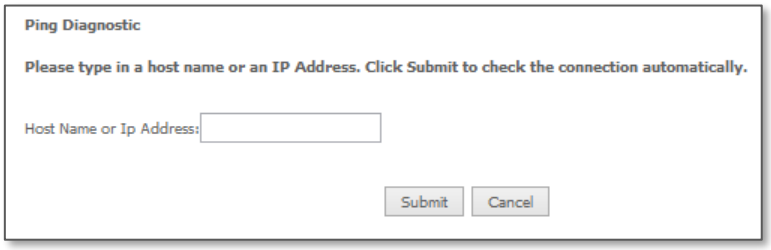


Figure 109 – Ping IP address

Diagnostics – Traceroute

The Traceroute page lets you perform a trace route to a remote IP address or host name, To ensure correct interface is used for routing.

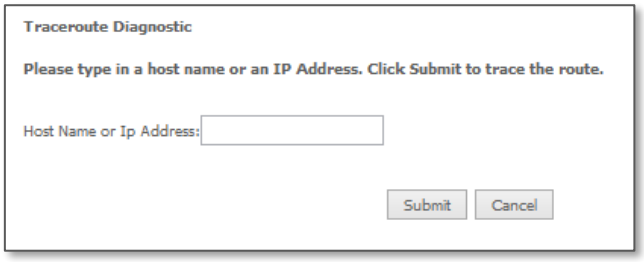


Figure 110 – Diagnostics – Traceroute page

Diagnostics – Start/Stop DSL

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

Figure 111 – Diagnostics – Start/Stop DSL page

Management

Management – Settings

The Settings screens allow you 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

The following screen appears when Backup is selected. Click the **Backup Settings** button to save the current configuration settings.

You will be prompted for the location to save the backup file to on your PC.

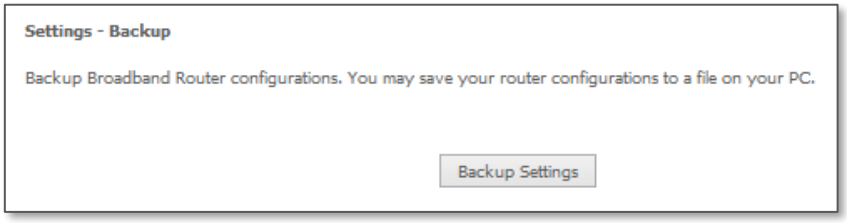


Figure 112 – Settings – Backup page

Update Settings

The following screen appears when selecting Update from the Settings submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings button to upload the selected file. Please allow up to 5 minutes for system updates and reboot.

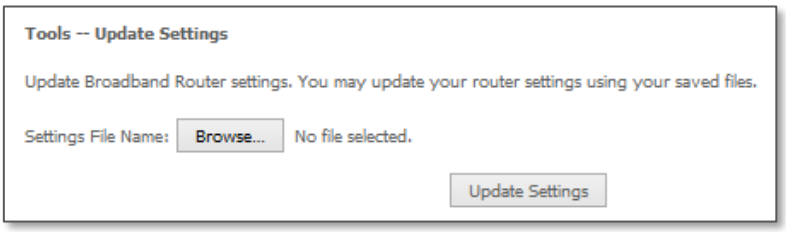


Figure 113 – Settings – Update Settings page

Factory Reset

The following screen appears when selecting Factory Reset from the Settings submenu. By clicking on the Restore Default Settings button, you can restore your Routers default firmware settings. Restore system settings will reboot your Router, please allow up to 2 minutes for restore and reboot.

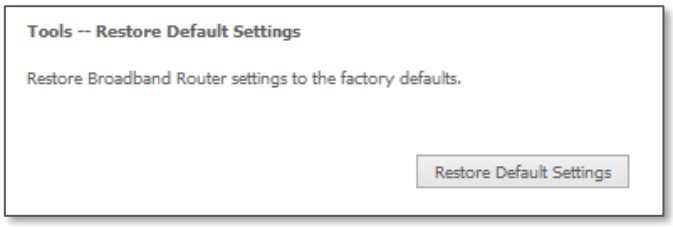


Figure 114 – Settings – Factory Reset page

Management – System Log

The System log page allows you to view the log of the modem and configure the logging level also. To view the system log, click the **View System Log** button.

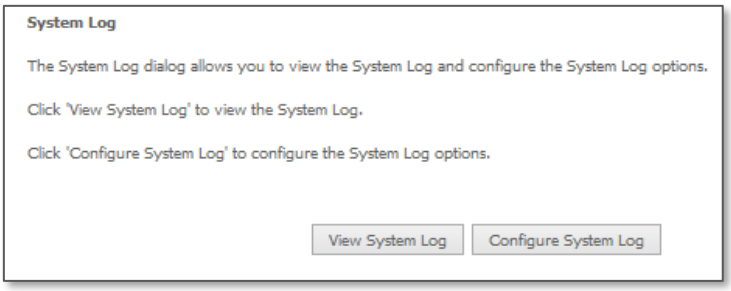


Figure 115 – Management – View System Log

To configure the system log, click the **Configure System Log** button. You can sent system log to remote server via selecting both, or remote under “Mode” option.

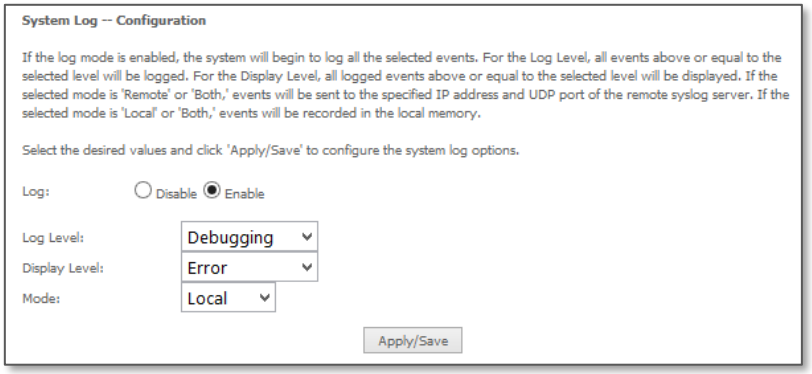


Figure 116 – Management – Configure System Log

Management – Security Log

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

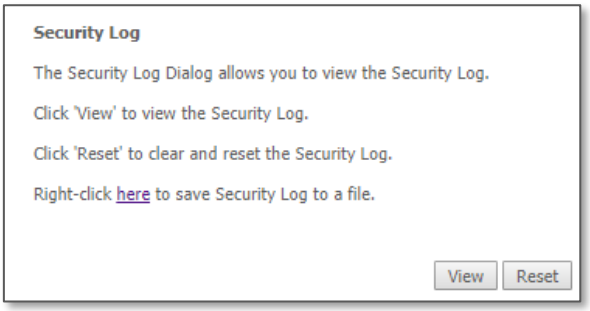


Figure 117 – Management – View Security Log

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

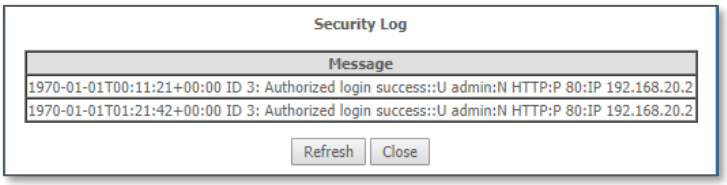


Figure 118 – Management – Download Security Log

You can also click the here link to save the Security Log to a downloadable file.

Management – 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 NF18ACV (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

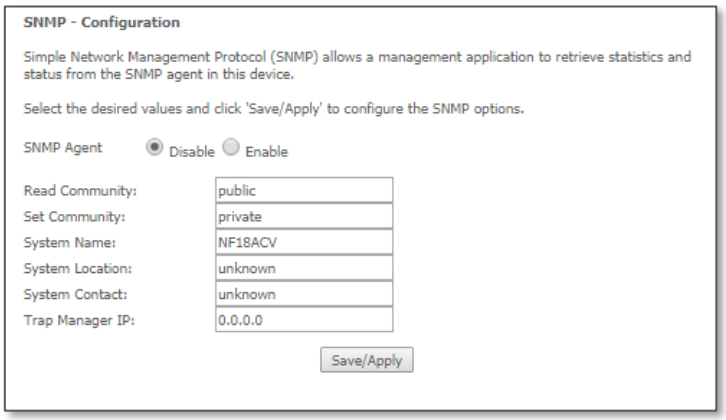


Figure 119 – Management – Enable SNMP Agent

Management – 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).

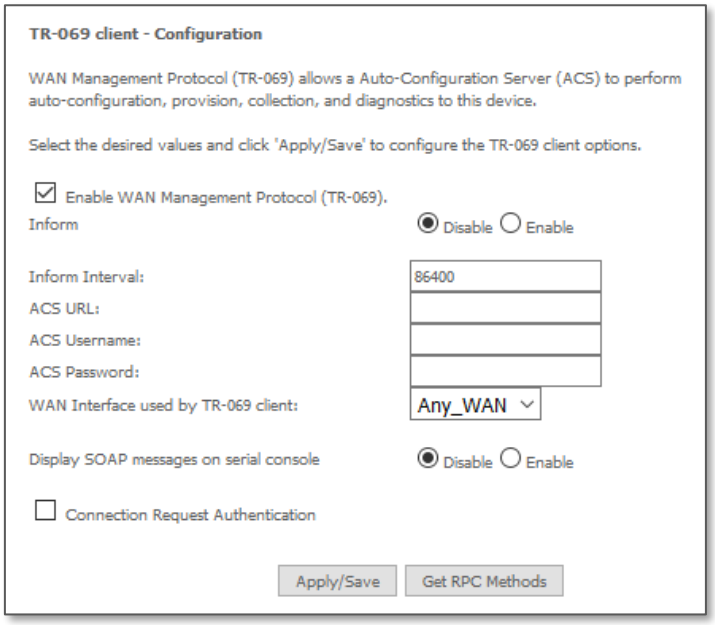


Figure 120 – Management – Enable TR-069 Client

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 38 – TR-069 Client settings table

Management – 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).

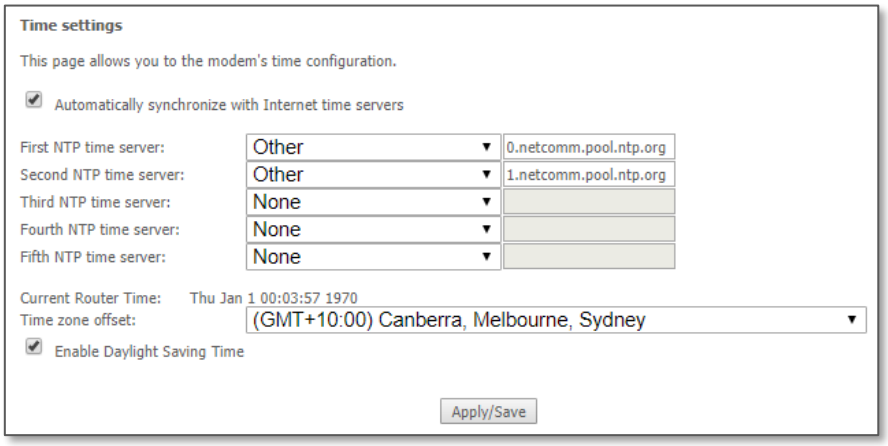


Figure 121 – Management – Internet Time Settings

Drop down to select existing time server to use, or select **"Other"** to manually enter time server. Click the "**Apply/Save"** button to initiate the change.

Management – 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 16 characters or less with no spaces. Click the **Apply/Save** button after making any changes to continue.

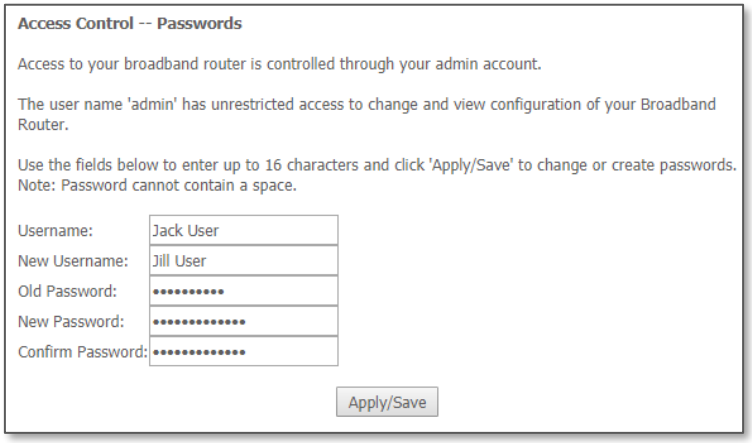


Figure 122 – Access Control – Passwords

Access List

When this facility 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.

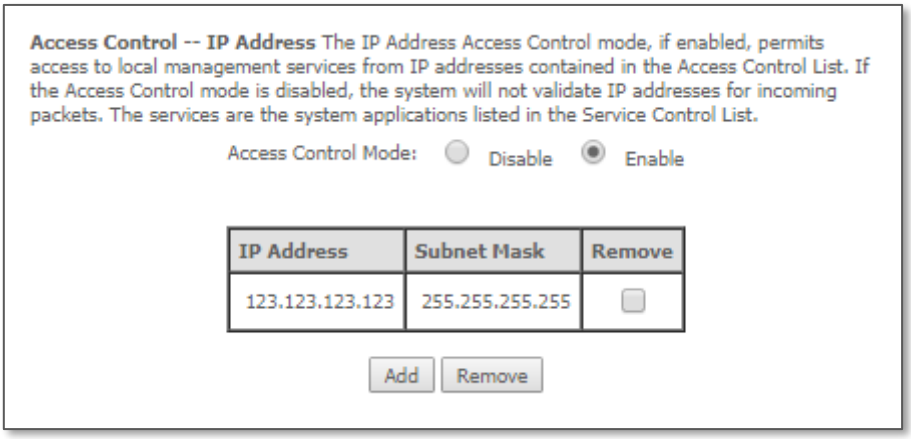


Figure 123 – Access Control – IP Address Access List

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.

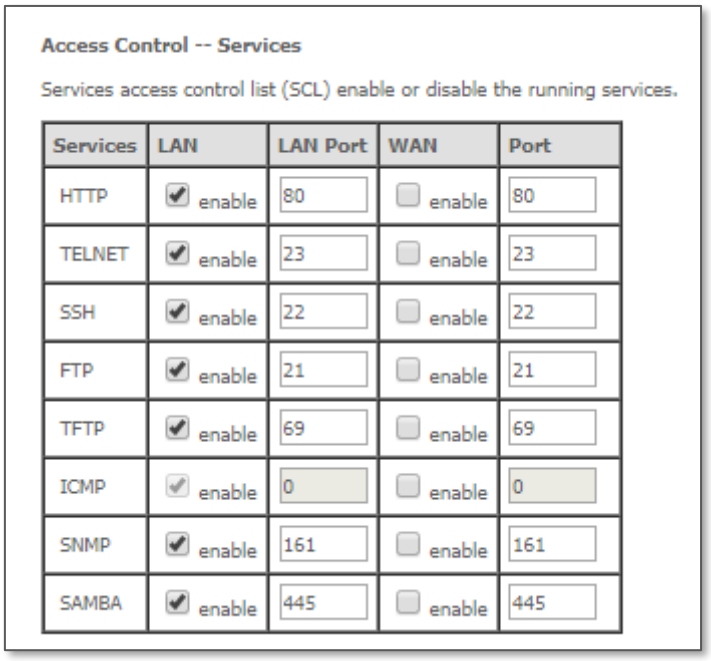
Services Control

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 checkbox as illustrated below and specifying the service port assign 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.

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
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 124 – Service Control List (SCL)

Management – Update Firmware

The following screen appears when selecting the **Update Firmware** option from the **Management** menu. By following this screen's steps, you can update your modem's firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

1. Obtain an updated software image file from: `http://support.netcommwireless.com/`
2. Click the **Choose File** button to locate the image file.
3. Click the **Update Firmware** button once to upload and install the file.

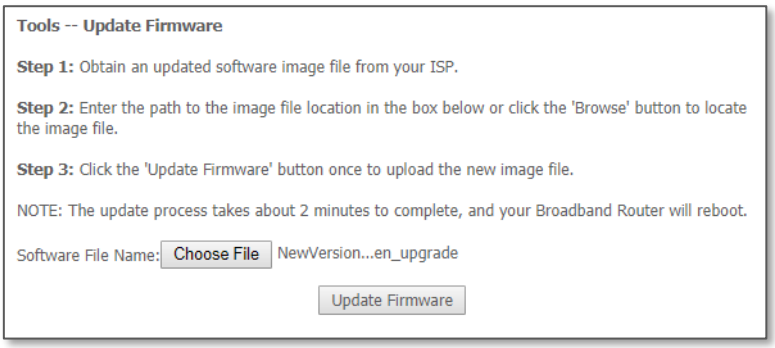


Figure 125 – Update Firmware page

Management – Reboot

This option reboots the NF18ACV. Please allow up to 5 minutes for device to reboot.

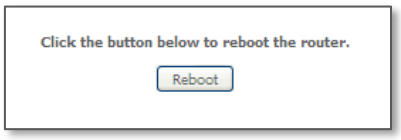


Figure 126 – Reboot button

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

Additional Product Information

Establishing a wireless connection

Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for the default wireless network key).
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NF18ACV with "Connected" next to it.

Windows 8/8.1/10

1. Open the Network and Sharing Centre (Click on Start, Type “Network and Sharing Centre”)
2. Click on “Change adapter settings” on the left hand column.
3. Right-click on Wireless Network Adaptor and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for the default wireless network key).
6. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
7. After clicking on this, you should see an entry matching the SSID of your NF18ACV with "Connected" under it.

Mac OSX 10.6

1. Click on the Airport icon on the top right menu.
2. Select the wireless network listed on your included wireless security card and click Connect.
3. On the new window, select “Show Password”, type in the network key *(refer to the included wireless security card for the default wireless network key)* in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.

Note – For other operating systems, or if you use a wireless adaptor utility to configure your wireless connection, please consult the operating system documentation for instructions on establishing a wireless connection.

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful in diagnosing the possible cause of a variety of problems.

Power LED

The Power LED does not light up.

Step	Corrective Action
1	Make sure that the NF18ACV power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NF18ACV and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF18ACV off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Table 39 – Power LED trouble shooting table

Web Configuration

I cannot access the web configuration pages.

Step	Corrective Action
1	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
2	Your computer's and the NF18ACV's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
3	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.
4	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for 3 seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NF18ACV restarts. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

Table 40 – Web Configuration – no access trouble shooting table

The web configuration does not display properly.

Step	Corrective Action
1	Delete the temporary web files and log in again. In Internet Explorer, click **Tools**, **Internet Options** and then click the **Delete Files...** button. When a *Delete Files* window displays, select **Delete all offline content** and click **OK**.

Step	Corrective Action
	Note – Steps may vary depending on the version of your Internet browser.

Table 41 – Web Configuration – no display trouble shooting table

Login Username and Password

I forgot my login username and/or password.

Step	Corrective Action
1	Press and hold the Reset button for 10 seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF18ACV restarts. You can now login with the factory default username and password “admin” (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

Table 42 – Login Username and Password trouble shooting table

WLAN Interface

I cannot access the NF18ACV from the WLAN or ping any computer on the WLAN.

Step	Corrective Action
1	Check the WiFi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NF18ACV and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

Table 43 – WLAN Interface trouble shooting table

Appendix: Quality of Service setup example

The following Quality of Service (QoS) settings offer a basic setup example, setting up 2 devices connecting to an NF18ACV router, 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 NF18ACV router 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 an NF18ACV router. 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 NF18ACV.

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**

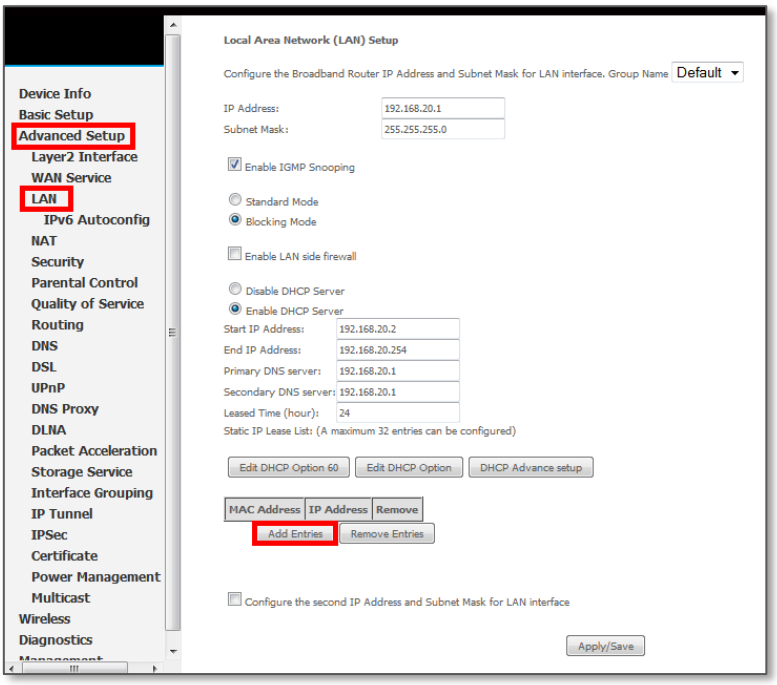


Figure 127 – Advanced Setup > LAN page

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.

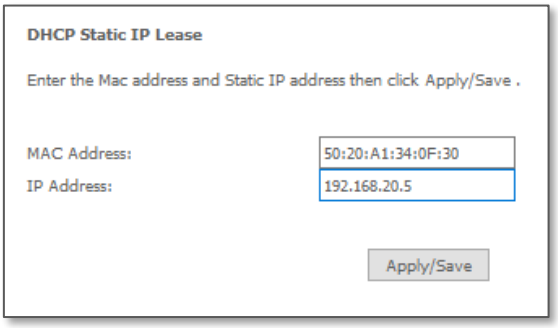


Figure 128 – DHCP Static IP Lease details

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

8 Complete steps 4 through 7 for each device connected to the NF18ACV router. Each entry will be listed in the Static IP Lease List as shown below.

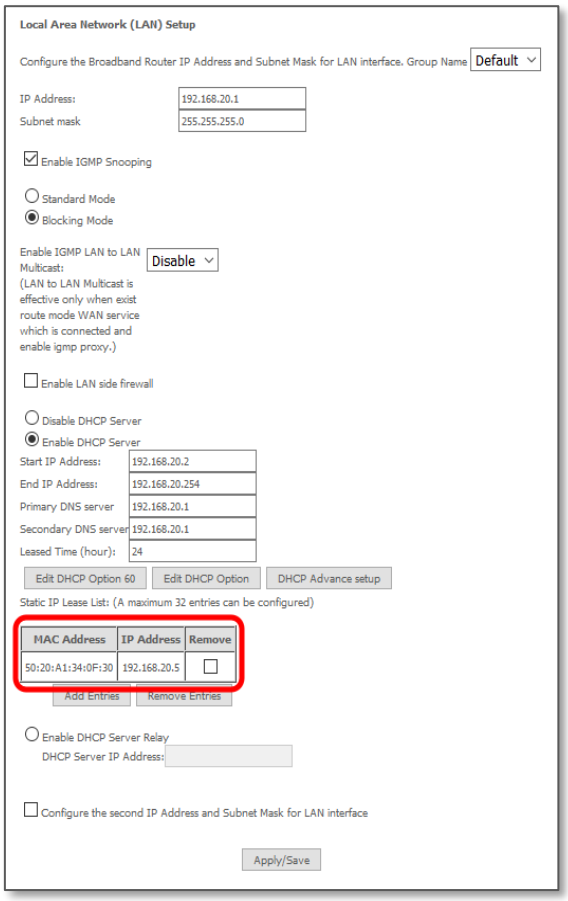


Figure 129 – LAN Setup

QoS Configuration Settings

1 Select Advanced Setup > Quality of Service

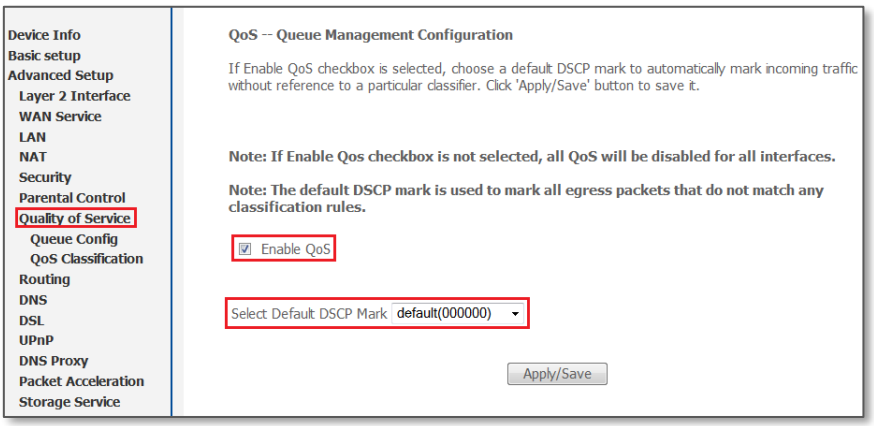


Figure 130 – QoS – Queue Management Configuration

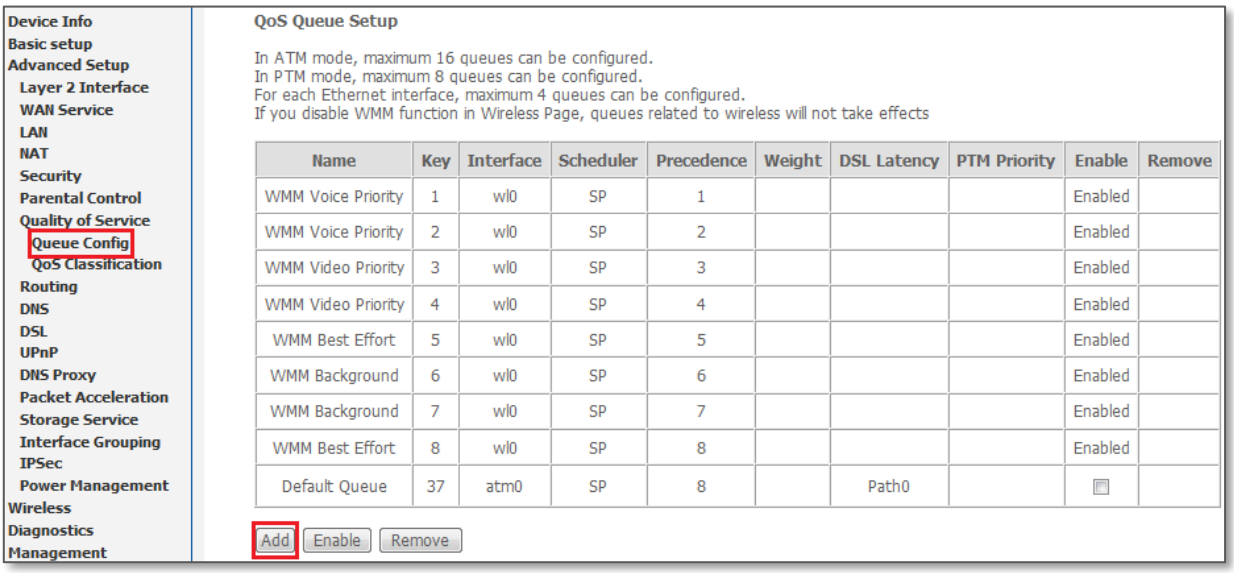
2 Select the **Enable QoS** option.

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**.



Name	Key	Interface	Scheduler	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	wl0	SP	1				Enabled	
WMM Voice Priority	2	wl0	SP	2				Enabled	
WMM Video Priority	3	wl0	SP	3				Enabled	
WMM Video Priority	4	wl0	SP	4				Enabled	
WMM Best Effort	5	wl0	SP	5				Enabled	
WMM Background	6	wl0	SP	6				Enabled	
WMM Background	7	wl0	SP	7				Enabled	
WMM Best Effort	8	wl0	SP	8				Enabled	
Default Queue	37	atm0	SP	8		Path0			

Figure 131 – QoS – Queue List

2 Click the **Add** button.

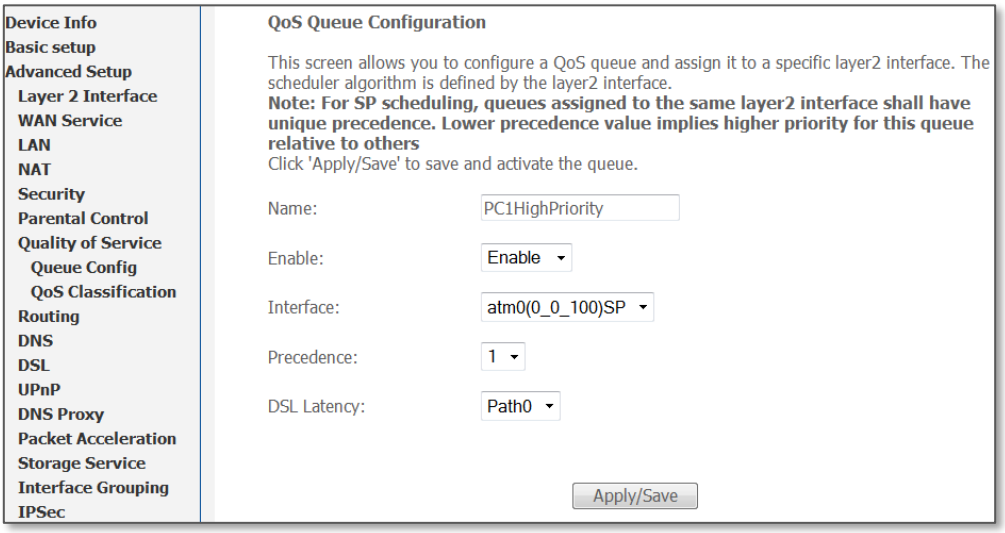


Figure 132 – QoS – Queue Configuration 1

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 (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0_0_100)**).

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.

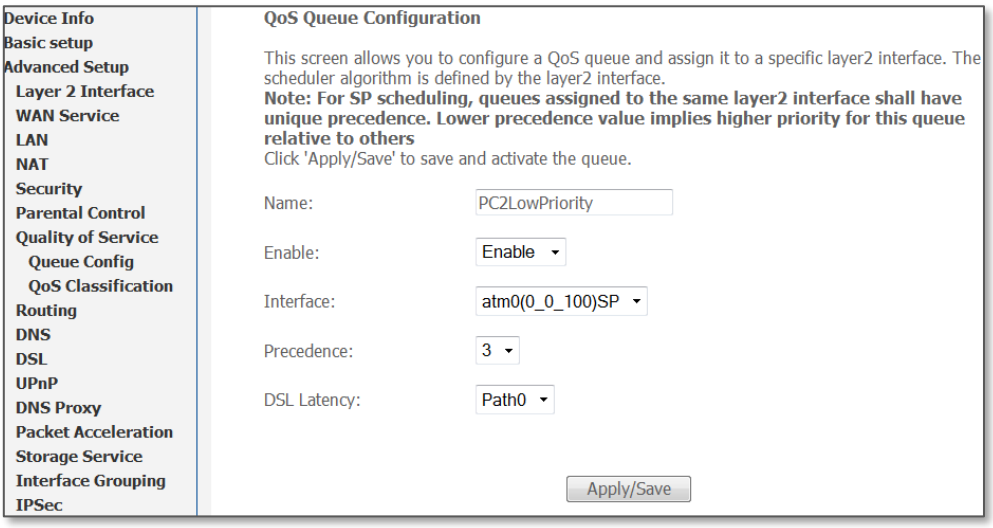


Figure 133 – QoS – Queue Configuration 2

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 (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0)100)**).

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**.

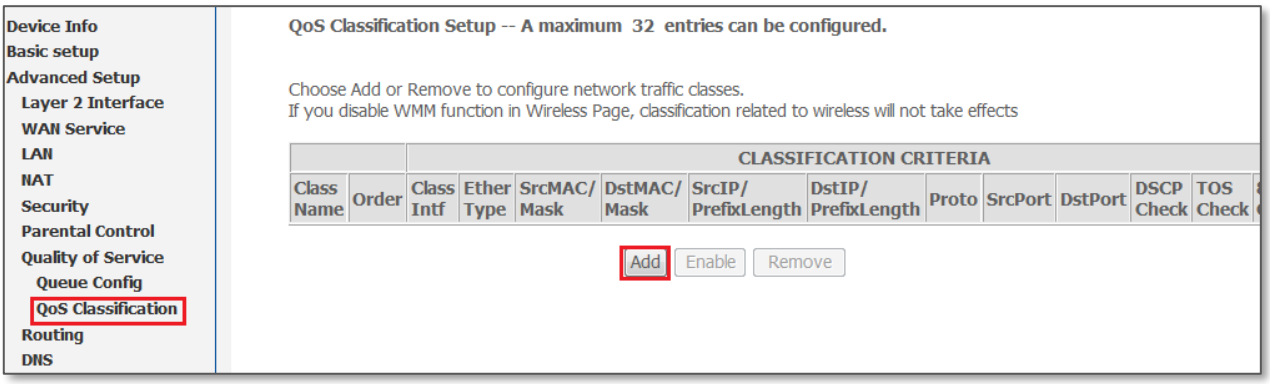


Figure 134 – QoS Classification configuration

2 Click the **Add** button.

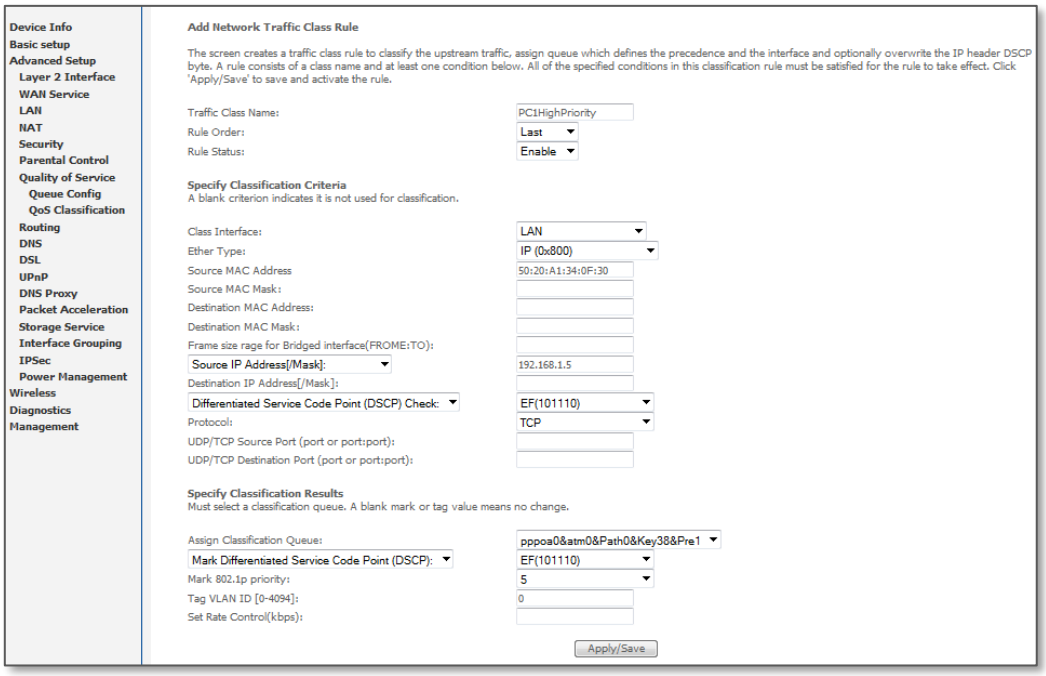


Figure 135 – Configure Network Traffic Class Rule

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.

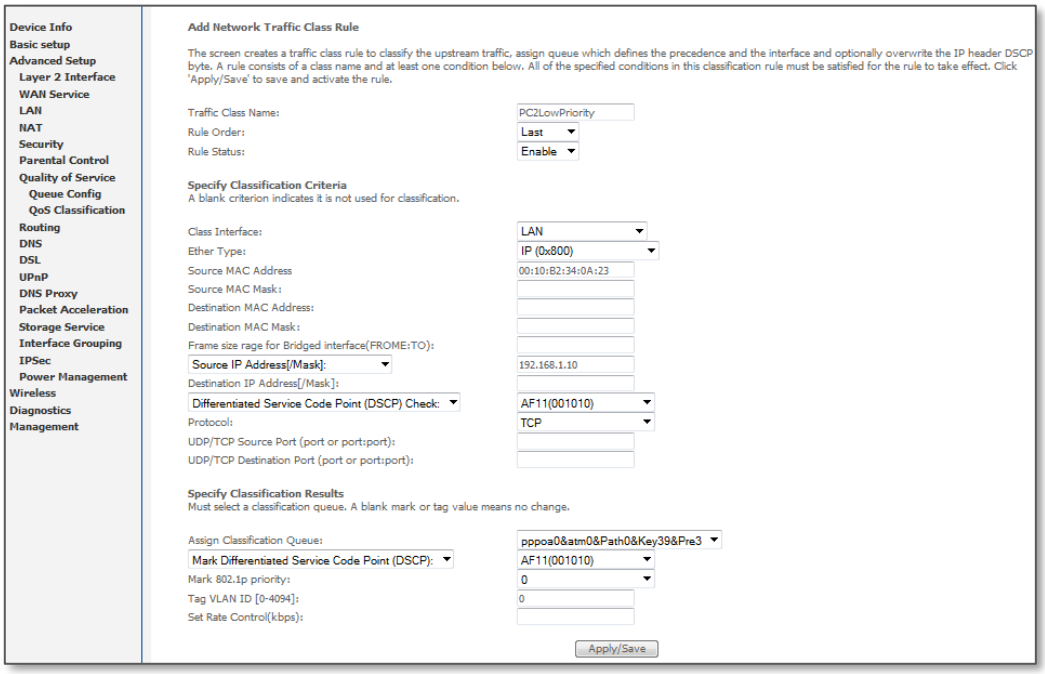


Figure 136 – QoS Network Traffic Class Rule configuration

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 NF18ACV router.

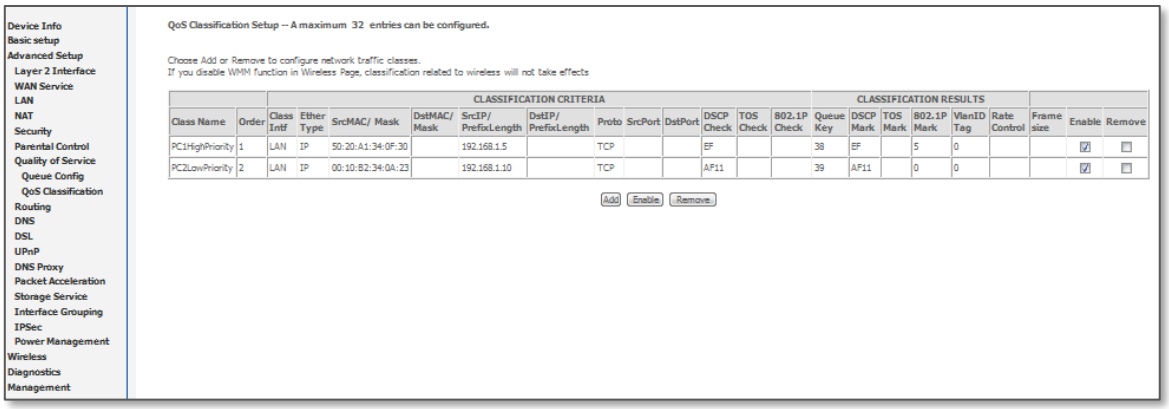


Figure 137 – QoS Classification setup page

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.

Figure 138 – 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

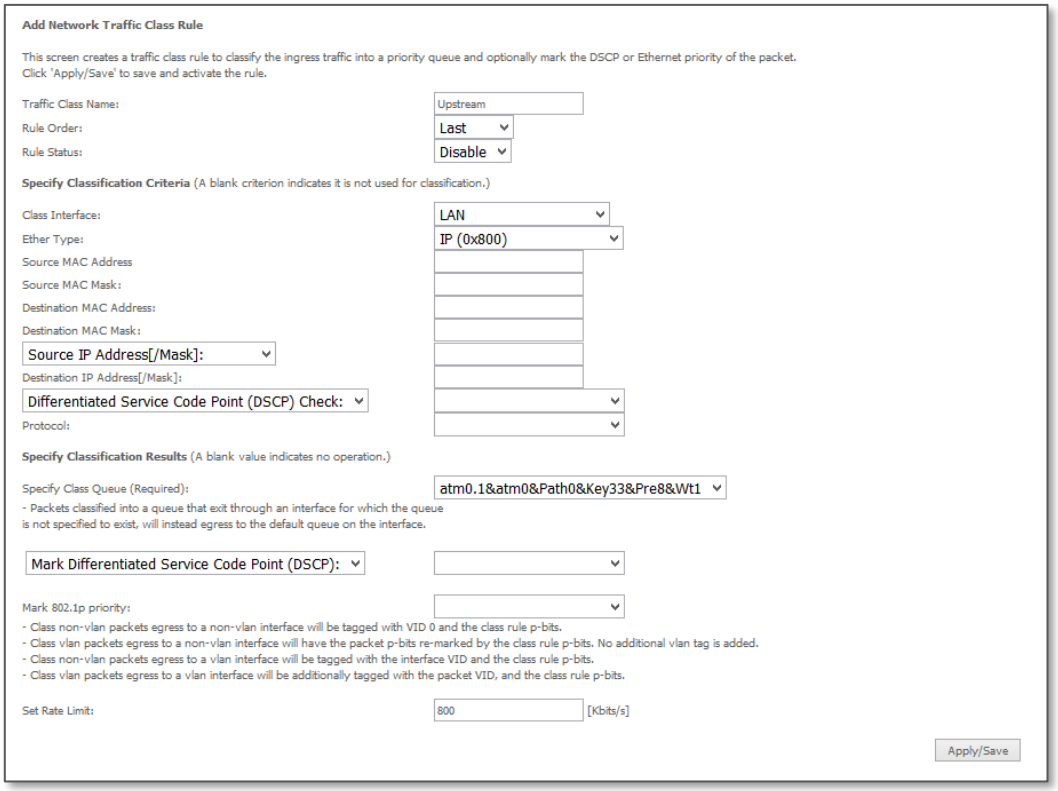


Figure 139 – Network Traffic Class Rule

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:

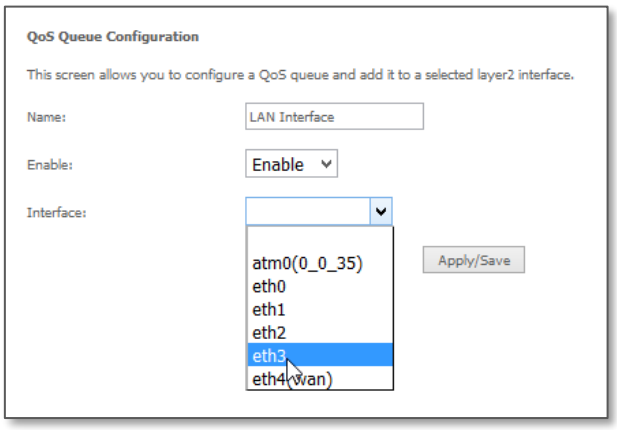


Figure 140 – QoS Queue Configuration

1 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

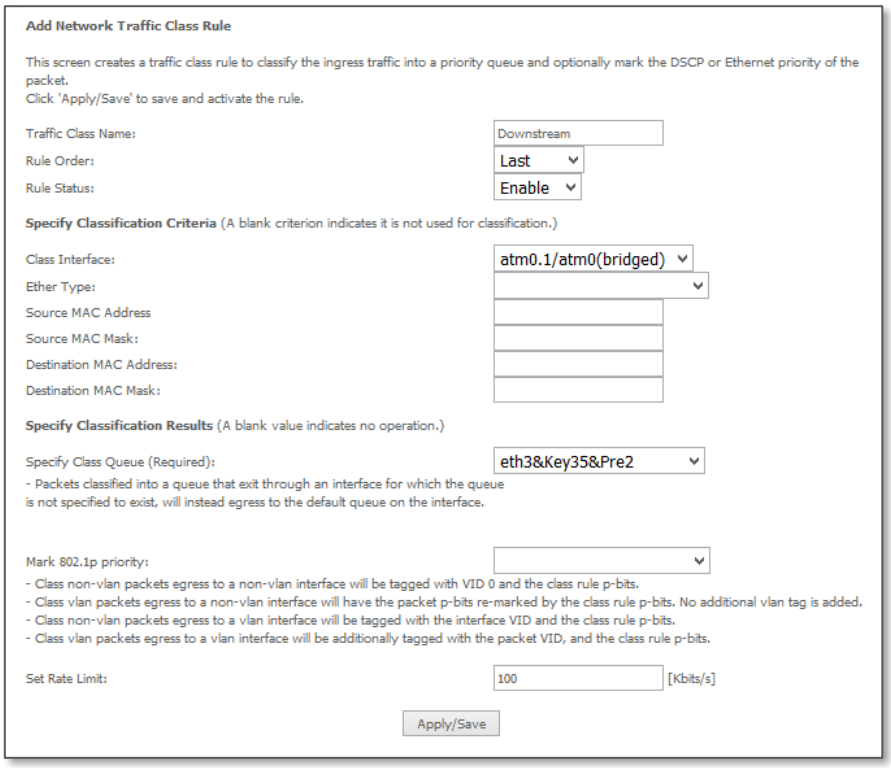
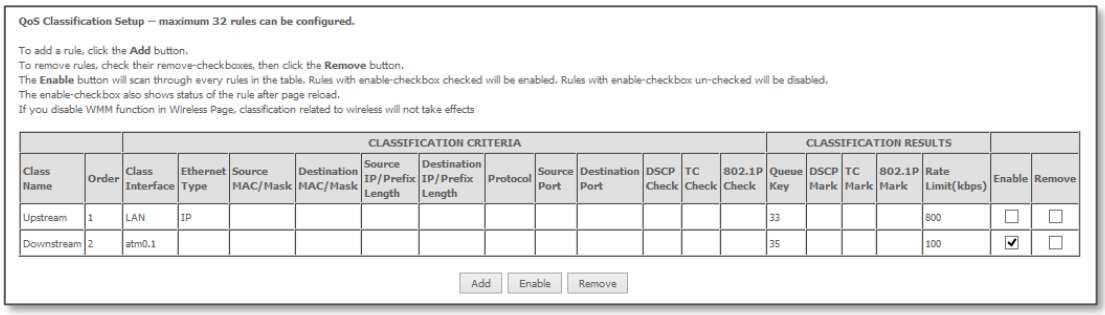


Figure 141 – Network Traffic class Rule

2 Click **Apply/ Save**

The QoS Classification table looks like this:



		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 142 – QoS Classification list

Table of Figures

Table of Tables

Legal & Regulatory Information

Intellectual Property Rights

Customer Information

The Australian Communications & Media Authority (ACMA) requires you to be aware of the following information and warnings:

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
2. This equipment incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
3. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
    - i Change the direction or relocate the receiving antenna.
    - ii Increase the separation between this equipment and the receiver.
    - iii Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
    - iv Consult an experienced radio/TV technician for help.

4 The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm Wireless. Failure to do so may cause damage to this product, fire or result in personal injury.

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the Consumer Protection Laws). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.

If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

Product Warranty

All NetComm Wireless products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a Product Warranty). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Wireless Limited within 30 days of the original purchase date by registering online via the NetComm Wireless web site at www.netcommwireless.com. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Consumer Protection Laws Section above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the Consumer Protection Laws Section above), the Product Warranty is granted on the following conditions:

1 the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;

2 the Product Warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;

3 the customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;

4 the cost of transporting product to and from NetComm's nominated premises is your responsibility;

5 NetComm Wireless Limited does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and

6 the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm Wireless Limited recommends that you enable these features to enhance your security.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 above), the Product Warranty is automatically voided if:

1 you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;

2 the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);

3 the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;

4 your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;

5 your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm Wireless Limited; or

6 the serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitation of Liability

This clause does not apply to New Zealand consumers. Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the Consumer Protection Laws Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm Wireless's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm Wireless's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Wireless Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm Wireless Limited is unable to limit its liability as set out above, NetComm Wireless Limited limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM WIRELESS LIMITED Head Office

PO Box 1200, Lane Cove NSW 2066 Australia

Phone: +61(0)2 9424 2070

Fax: +61(0)2 9424 2010

Email: sales@netcommwireless.com techsupport@netcommwireless.com