NetCommWireless

VDSL/ADSL N300 WiFi Modem Router with VoIP

NF10WV

USER GUIDE

Copyright
Copyright © 2016 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless Limited. Trademarks and registered trademarks are the property of NetComm Wireless Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

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 your household 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.

This manual covers the following products:
NetComm Wireless VDSL/ADSL N300 WiFi Modem Router (NF10WV)

DOCUMENT VERSION	DATE
1.0 Initial document release	29 March 2016
1.1 Added Ethernet Priority Marking description to SIP Advanced page.	14 April 2016
1.2 Updated based on firmware version R5B019	26 September 2016

Table 1 - Document Revision History

NetCommWireless

Table of contents

Overview 5
Introduction 5
Target audience 5
Prerequisites 5
Notation 5
Welcome 6
Product overview 6
Package contents 6
Product features 7
Physical dimensions and indicators 8
LED indicators 8
Physical Dimensions and Weight 9
NF10WV Default Settings 9
Interfaces 10
Rear 10
Left Side 11
Safety and product care 12
Transport and handling 12
Installation and configuration of the NF10WV 13
Placement of your NF10WV 13
Avoiding obstacles and interference 13
Cordless phones 13
Choosing the “quietest” channel for your wireless network 14
Hardware installation 14
Connecting a client via Ethernet cable 14
Connecting a client wirelessly 14
Web based configuration interface 15
First-time setup wizard 15
ADSL 15
VDSL 16
Ethernet WAN 18
Device Info 20
Summary 20
WAN 21
Statistics 21
Route 24
ARP 24
DHCP 24
Advanced Setup 25
Layer2 Interface 25
WAN Service 27
LAN 31
NAT 33
Security 36
Parental Control 39
Quality of Service 41
Routing 43
DNS 45
DSL 46
UPnP 47
DNS Proxy 47
DLNA 48
Storage Service 48
Interface Grouping 49
IP Tunnel 50
IPSec 51
Multicast (IGMP Configuration) 52
Wireless 53
Basic 53
Voice 58

VoIP Status 58
SIP Basic Setting 58
SIP Advanced 60
SIP Extra Setting 62
SIP Star Code Setting 62
SIP Debug Setting 63
VoIP Functionality 64
Registering 64
Placing a Call 64
Anonymous call 64
Do Not Disturb (DND) 64
Call Return 64
Call Hold 64
Call Waiting 64
Blind Transfer 65
Consultative Transfer 65
Call Forwarding No Answer 65
Call Forwarding Busy 65
Call Forwarding All 65
Three-Way Conference 65
T38 Faxing 66
Pass-Through Faxing 66
Diagnostics 67
Diagnostics 67
Ethernet OAM 68
Diagnostics 69
Management 69
Settings 69
System Log 70
SNMP Agent 71
TR-069 Client 71
Internet Time 72
Access Control 72
Update Firmware 73
Reboot 74
Additional Product Information 74
Establishing a wireless connection 74
Windows 7 74
Windows 8/8.1/10 74
Mac OSX 10.6 74
Troubleshooting 76
Using the indicator lights (LEDs) to Diagnose Problems 76
Appendix: Quality of Service Setup Example 77
Reserving IP addresses 77
QoS Configuration Settings 78
High Priority QoS Queue Configuration 79
Low Priority QoS Queue Configuration 80
High Priority QoS Classification 80
Low Priority QoS Classification 82
Limiting the upstream rate 83
Limiting the downstream rate 84
Legal & Regulatory Information 85
Intellectual Property Rights 85
Customer Information 85
Consumer Protection Laws 85
Product Warranty 86
Limitation of Liability 86
Contact 87

Overview

Introduction

This manual provides information related to the installation, operation, and use of the NF10WV.

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 NF10WV, 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 802.11b/g/n 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:

Indicates a note requiring attention.

Indicates a note providing a warning.

Indicates a note providing useful information.

Welcome

Thank you for purchasing a NetComm Wireless VDSL/ADSL N300 WiFi Modem Router with VoIP. This guide contains all the information you need to configure your device.

Product overview

- Fully featured VDSL2 / ADSL2+ Modem Router
- 4 x 10/100 Fast Ethernet LAN ports for wired connections
- 1 x 10/100/1000 Gigabit Ethernet WAN port for connection to fibre services
- Wireless N Access Point for multiple high speed WiFi connections
- 2 x USB host ports – supports two USB storage devices for file sharing
- NBN ready: carefully developed hardware and software features to ensure this device is optimised for use on the National Broadband Network
- IPv6 ready for the next generation IP addressing
- WPS button for simple setup of your wireless network

Package contents

The NF10WV package consists of:

- 1 x NetComm Wireless VDSL/ADSL N300 WiFi Modem Router with VoIP (NF10WV)
- 1 x Quick Start Guide
- 1 x 1.5m 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

Featuring a VDSL2/ADSL2+ modem and a Gigabit WAN port, you can choose whether you connect to the Internet via DSL or a fibre service. If you don't have a fibre connection, the Gigabit WAN port will have you protected should you choose to update in the future. With uncertainty around the future of the NBN, NetComm Wireless will have you covered should the network connection switch to VDSL.

This router also includes 2 x USB host ports that can be used to connect USB devices so that their capabilities can be shared with all connected users. Connect a USB hard drive so that all files stored can be accessed and shared.

All of these features can be shared with multiple users via the built-in wireless access point or the four Ethernet LAN ports. The high speed Wireless N provides a signal strong enough to penetrate the far corners of a house and can connect all WiFi enabled devices, such as laptops, smartphones, gaming consoles, tablets and PCs. The four Fast Ethernet ports provide a wired connection that can be used to connect desktop computers, media devices or any Ethernet equipped product.

Note: Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g, and 802.11n 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 NF10WV 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 NF10WV to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.

LED INDICATOR	ICON	COLOUR	DEFINITION
Power		Green	The NF10WV is powered on and operating normally.
		Off	The power is off.
DSL		Off	No DSL signal detected.
		Green Blinking	Synching
		Green	DSL synchronized.
Internet		Green	The NF10WV is connected to an internet service.
		Green Blinking	Data is being transmitted to or from the internet.
		Off	The NF10WV is not connected to the internet.
WAN		Green	A device is connected to the Ethernet WAN port.
		Green Blinking	Data is being transmitted to or from the WAN.
		Off	No device is connected to the Ethernet WAN port.
LAN 1-4		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		Green	WiFi is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	WiFi is disabled.
WPS		Green	WPS is enabled
		Green Blinking	WPS pairing is triggered.
		Off	WPS is disabled.
USB 1 - 2		Green	A USB hard drive is connected.
		Green Blinking	Data is being transmitted through the USB interface.
		Off	No USB hard drive is connected to the USB interface.

Physical Dimensions and Weight

The table below lists the physical dimensions and weight of the NF10WV.

DIMENSIONS	
Width	190 mm
Height	146 mm
Depth	54 mm
Weight	326 grams

NF10WV Default Settings

The following tables list the default settings for the NF10WV.

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

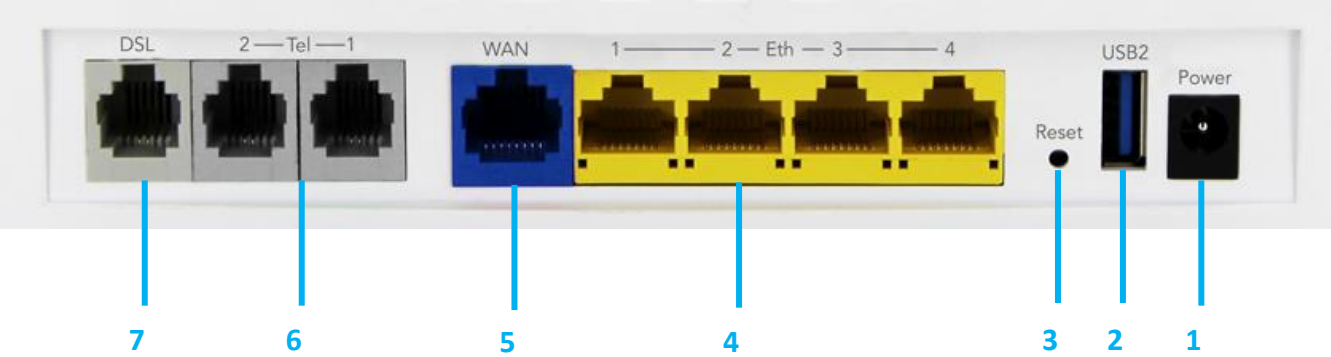
WIRELESS (WIFI)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA2-PSK (AES)
Security Key	(Refer to the included Wireless Security Card)

NF10WV WEB INTERFACE ACCESS	
Username	admin
Password	admin

Interfaces

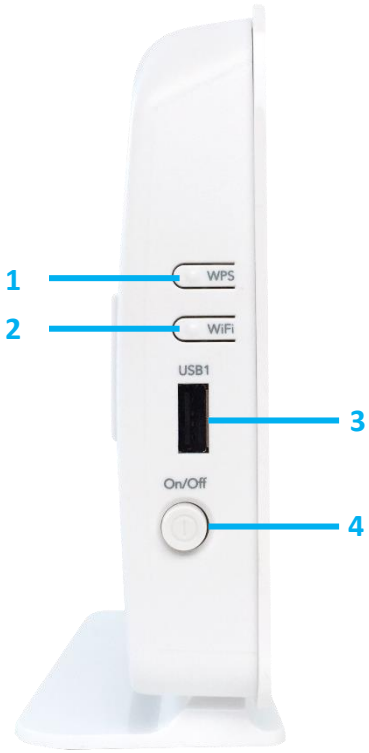
Rear

The following interfaces are available on the NF10WV:



NUMBER	INTERFACE	DESCRIPTION
1	Power supply jack	Connection point for the included power adapter. Connect the power supply here.
2	USB 2	Connect an external USB hard drive here to use the NAS feature of the NF10WV.
3	Reset button	Reset unit to the default factory configuration by holding the Reset button down for 7 seconds or until all the LEDs turn off.
4	Ethernet 1 - 4	Fast Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
5	WAN	Gigabit capable WAN port for connection to a WAN network.
6	Telephone 1 and 2	Connect a regular telephone handset here for use with a VoIP account.
7	DSL	Use the provided RJ-11 cable to connect the router to the telephone line operating your xDSL service.

Left Side



NUMBER	INTERFACE	DESCRIPTION
1	WPS button	Press the WPS button to activate the WPS pairing function. The WPS feature is disabled by default, to enable it, refer to the Security section.
2	WiFi button	Press the WiFi button to turn the WiFi radio on or off. When the WiFi radio is off, the WiFi LED on the front panel turns off.
3	USB 1	Connect an external USB hard drive here to use the NAS feature of the NF10WV.
4	Power button	Toggles the power on and off.

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 NF10WV, it is recommended to return the product in the original packaging. This ensures that the product will not be damaged.

Note: 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 NF10WV

Placement of your NF10WV

The wireless connection between your NF10WV 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 NF10WV 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 NF10WV 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 NF10WV, please try the following steps:

- In multi-storey homes, place the NF10WV on a floor that is as close to the centre of the home as possible. This may mean placing the NF10WV on an upper floor.
- Try not to place the NF10WV near a cordless telephone that operates at the same radio frequency as the NF10WV (2.4GHz).

Avoiding obstacles and interference

Avoid placing your NF10WV 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 NF10WV).

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 NF10WV and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NF10WV.
- 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 NF10WV to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz 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 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 NF10WV.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF10WV to power up.

Connecting a client via Ethernet cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NF10WV.
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 NF10WV.

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 NF10WV.

Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF10WV

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF10WV.
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 NF10WV.

Web based configuration interface

First-time setup wizard

Please follow the steps below to configure your NF10WV Wireless router via the web based configuration wizard.

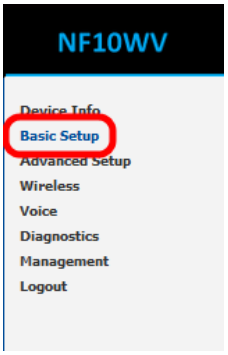
Open a web browser and type http://192.168.20.1/ into the address bar at the top of the window.

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.

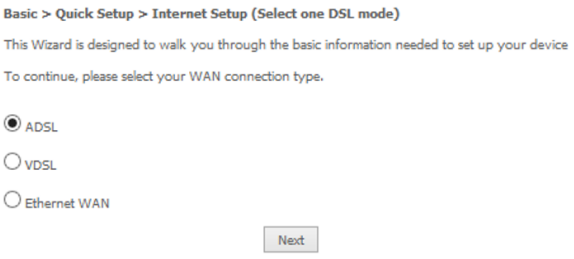
We highly recommend that immediately after initial installation you change the default passwords for admin, support and user access. You can do this from the **Management -> Access Control -> Passwords** page.
See Access Control -- Access Controls – Passwords on page 72 for more information.

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

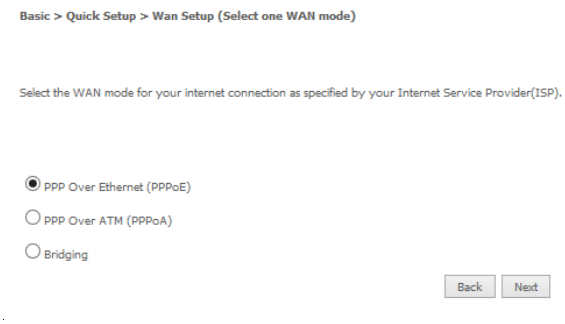


ADSL

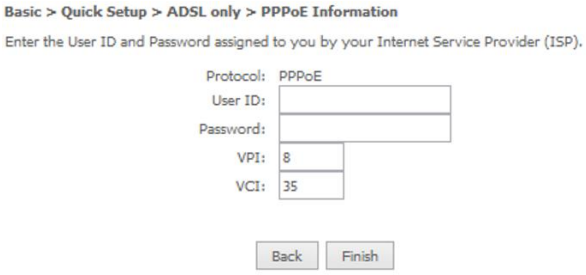
a) Select **ADSL** and click the **Next** button.



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



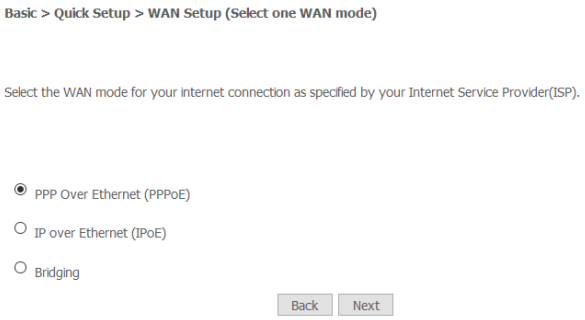
c) In the **User ID** and **Password** fields, enter the username and password assigned to you by your Internet Service Provider (ISP). Click the **Finish** button.



The account settings are saved and the NF10WV connects to the internet.

VDSL

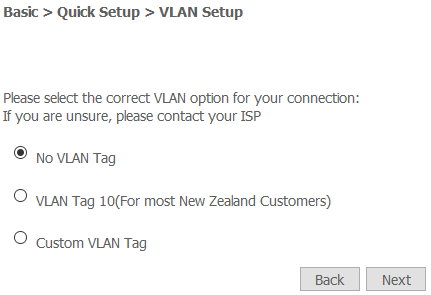
a) Select either **PPP over Ethernet (PPPoE)**, **IP over Ethernet (IPoE)** or **Bridging** depending on your Internet Service Provider's requirements.



b) Click **Next** to open a sequence of screens appropriate for the connection type selected.

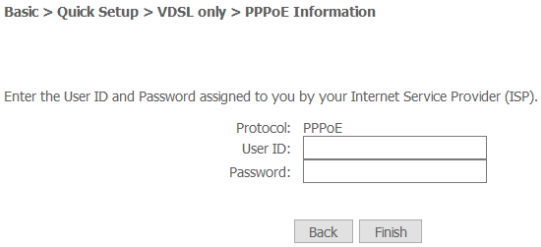
PPP over Ethernet (PPPoE)

a) For **PPP over Ethernet (PPPoE)** select the VLAN option required by your ISP:



- **No VLAN Tag** – If you ISP does not require a VLAN tag, select this option and click **Next** to go to the next page
- **VLAN Tag 10 (for most New Zealand Customers)** – If your ISP is in New Zealand, select this option and click **Next** to go to the next page, or
- **Custom VLAN Tag** – enter a VLAN tag number 0 through 4094, and then click **Next** to go to the next page

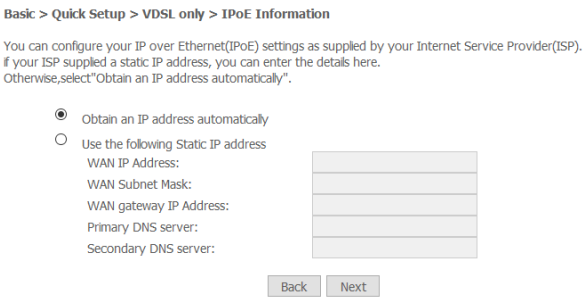
b) Enter the username and password supplied to you by your Internet Service Provider (ISP).



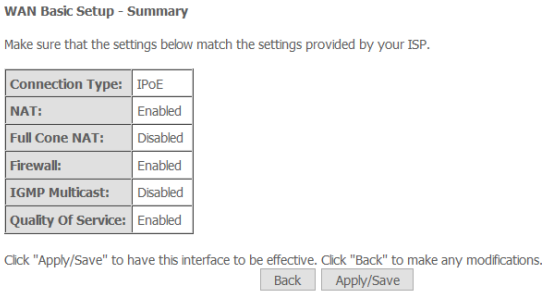
c) Click the **Finish** button when you have entered the required information.

IP over Ethernet (IPoE)

a) For **IP over Ethernet (IPoE)** either select the first option to automatically obtain the IP address details or manually enter the static IP address details as provided by your Internet Service Provider (ISP).



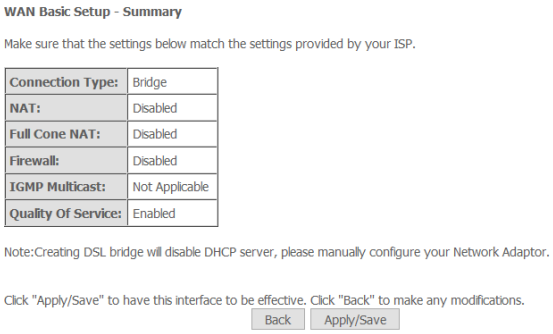
b) Click **Next** to review the automatically retrieved settings, or settings that you have manually entered.



c) When you are satisfied that the settings are correct, click the **Apply/Save** button.

Bridging

a) The **Bridging** settings are summarised in the following page:

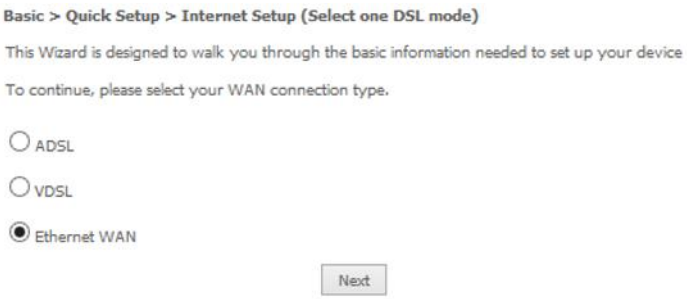


b) When you are satisfied that the settings are correct, click the **Apply/Save** button.

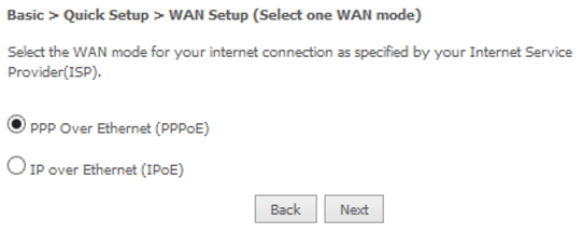
Ethernet WAN

a) Connect an RJ45 Ethernet cable to the WAN port on the NF10WV. Connect the other end of the cable to your WAN service.

b) Select **Ethernet WAN** then click the **Next** button.

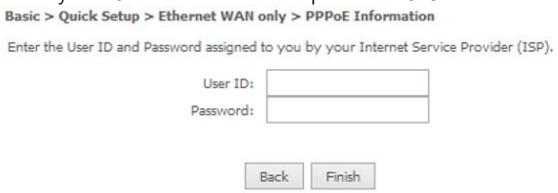


b) Select the WAN mode for your internet connection as specified by your Internet Service Provider (ISP). Click the **Next** button.



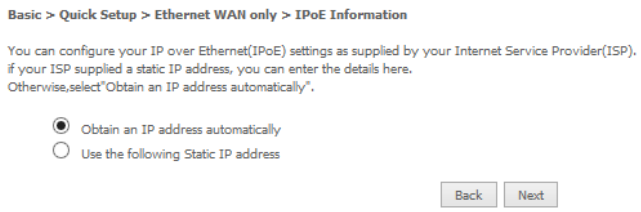
PPP over Ethernet (PPPoE)

In the **User ID** and **Password** fields, enter the username and password assigned to you by your Internet Service Provider (ISP). Click the **Finish** button when you have entered the required details.

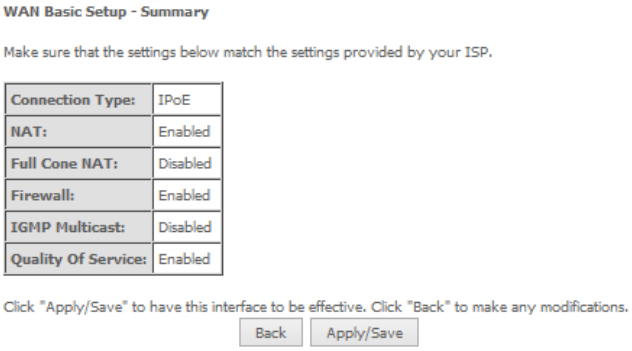


IP over Ethernet (IPoE)

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**. Click the **Next** button.



The settings are displayed in a summary. Click **Apply/Save** to save them.



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:	NF10W
Serial Number:	568747952610
Build Timestamp:	160112_1320
Software Version:	NF10WV.NC.AU_R5B013.EN
Bootloader (CFE) Version:	1.0.38-116.174
DSL PHY and Driver Version:	A2pvI041d2.d26b
VDSL PROFILE:	No profile
Wireless Driver Version:	7.14.89.14.cpe4.16L03.0-kdb
Voice Service Version:	Voice
Uptime:	0D 0H 36M 26S

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 00:36:27 1970

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 installed on the router.
DSL PHY and Driver Version	The driver version of the on-board DSL chip.
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 upstream speed of the DSL connection in Kbps.
Line Rate – Downstream (Kbps)	The current upstream speed of the DSL connection in Kbps.
LAN IPv4 Address	The current version 4 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 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 date and time set on the router.

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 Src Enbl	MLD Pxy	MLD Src Enbl	NAT	Firewall	Status	IPv4 Address	IPv6 Address
eth4.1	ETH WAN	IPoE	Disabled	Disabled	Disabled	Disabled			Enabled	Enabled	Disconnected	0.0.0.0	

ITEM	DEFINITION
Interface	The Interface of the WAN connection.
Description	The description of the WAN connection.
Type	The type of WAN connection.
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 Src Enbl	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 Src Enbl	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 connection.
IPv6 Address	The current IP v6 address of the WAN connection.

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

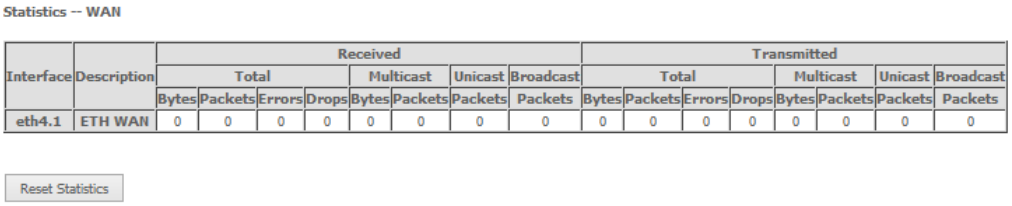
Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets	Bytes	Packets	Errors	Drops	Bytes	Packets	Packets	Packets
eth1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
eth0	1613299	15020	0	3	0	1517	12677	826	15363432	18473	0	0	0	1822	16228	423
wl0	0	0	0	43	0	0	0	0	0	0	0	0	0	0	0	1
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

Reset Statistics

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.

Statistics – WAN Service

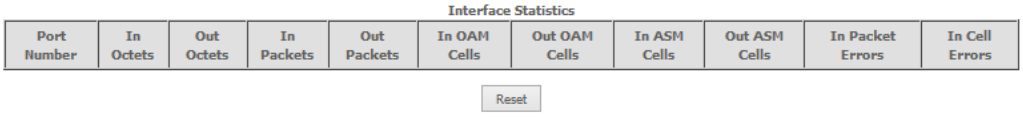
The Statistics – WAN Service page shows detailed information about the number of bytes, packets, errors and dropped packets on the WAN interface in both directions of communication.



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.

Statistics – xTM

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



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.

Statistics – xDSL

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

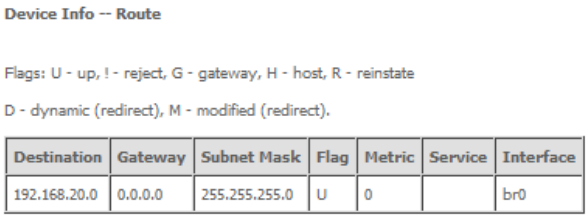
Statistics -- xDSL

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

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

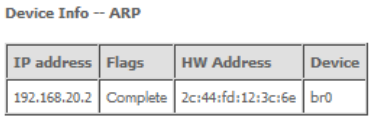
D - dynamic (redirect), M - modified (redirect).

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

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.

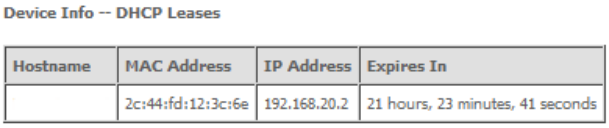


Device Info -- ARP

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

DHCP

Click DHCP to display the DHCP lease information.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
	2c:44:fd:12:3c:6e	192.168.20.2	21 hours, 23 minutes, 41 seconds

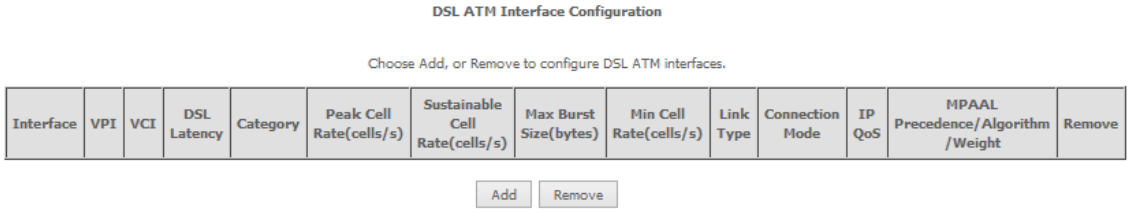
You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

Advanced Setup

Layer2 Interface

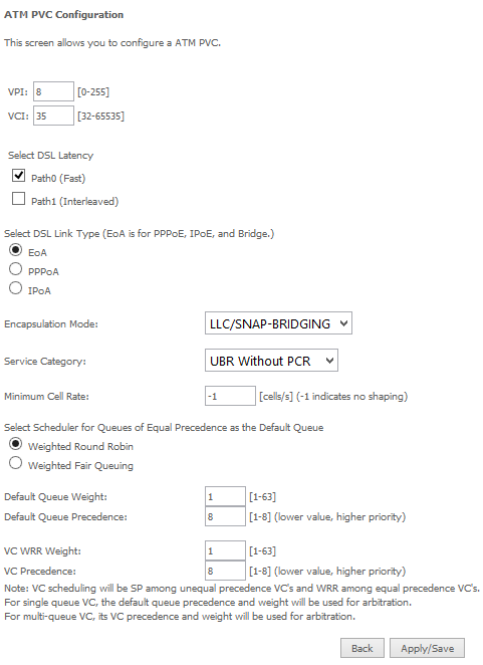
ATM Interface

The ATM (Asynchronous Transfer Mode) interface page shows the settings of all available DSL ATM interfaces. ATM interface is used for ADSL connections.



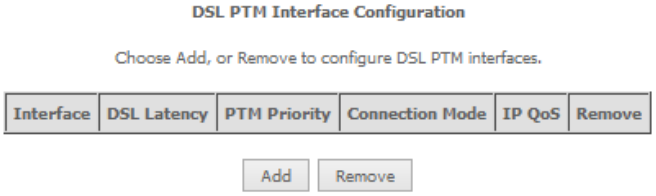
FIELD	DESCRIPTION
Interface	This field shows the interface name.
VPI	This field shows the Virtual Path Identifier (VPI) value. For most Australia connections the VPI is 8, for most new Zealand connections the VPI is 0. Please refer to your ISP for correct value.
VCI	This field shows the Virtual Channel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

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.

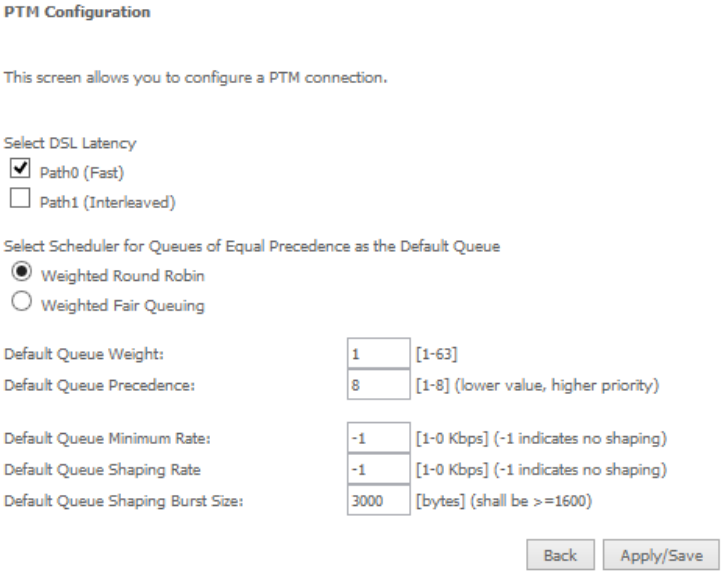


PTM Interface

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.

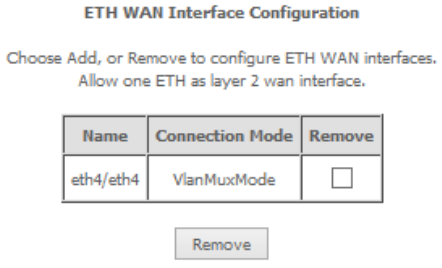


Click the **Add** button to create a new PTM interface. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.



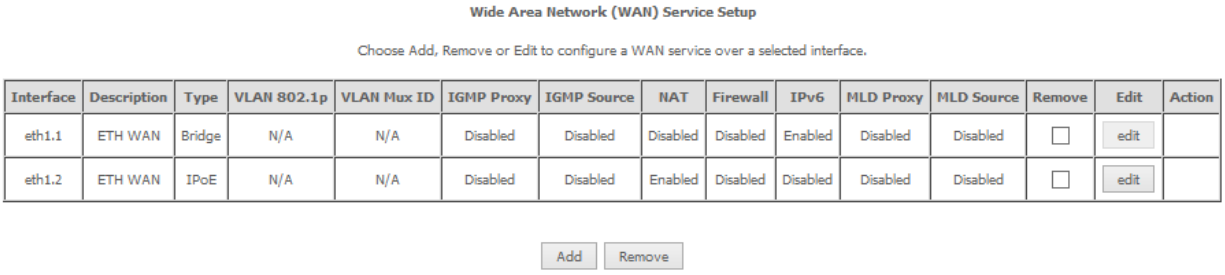
ETH Interface

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

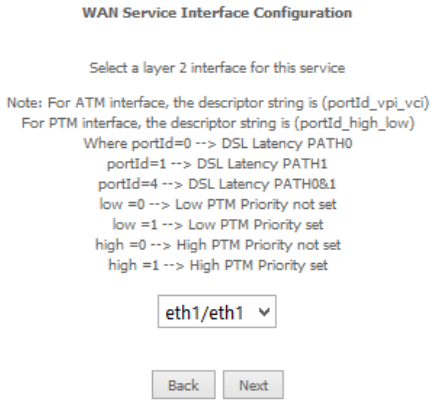


WAN Service

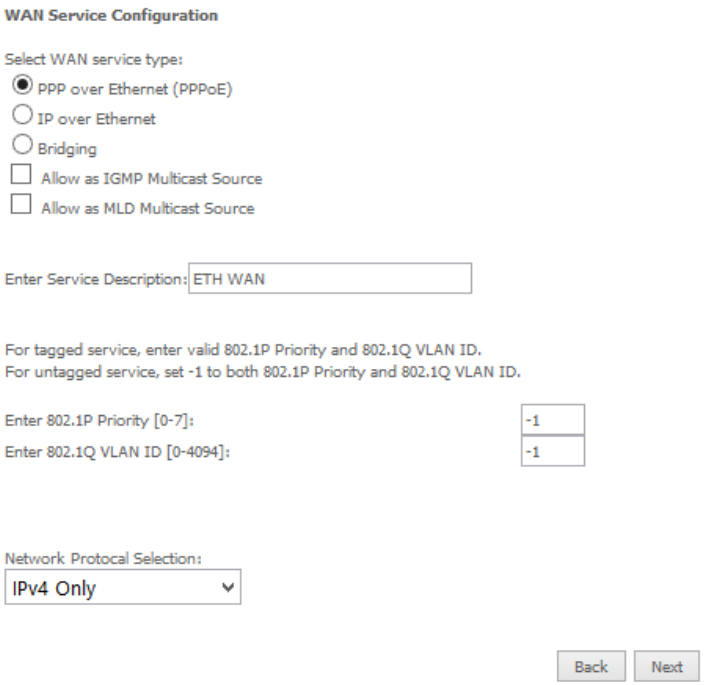
The WAN Service page displays the current Wide Area Network service setup and allows you to configure the router to connect to a larger network for Internet access.
WAN service require a preconfigured Layer 2 interface, be it ATM/PTM or Ethernet WAN.



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.

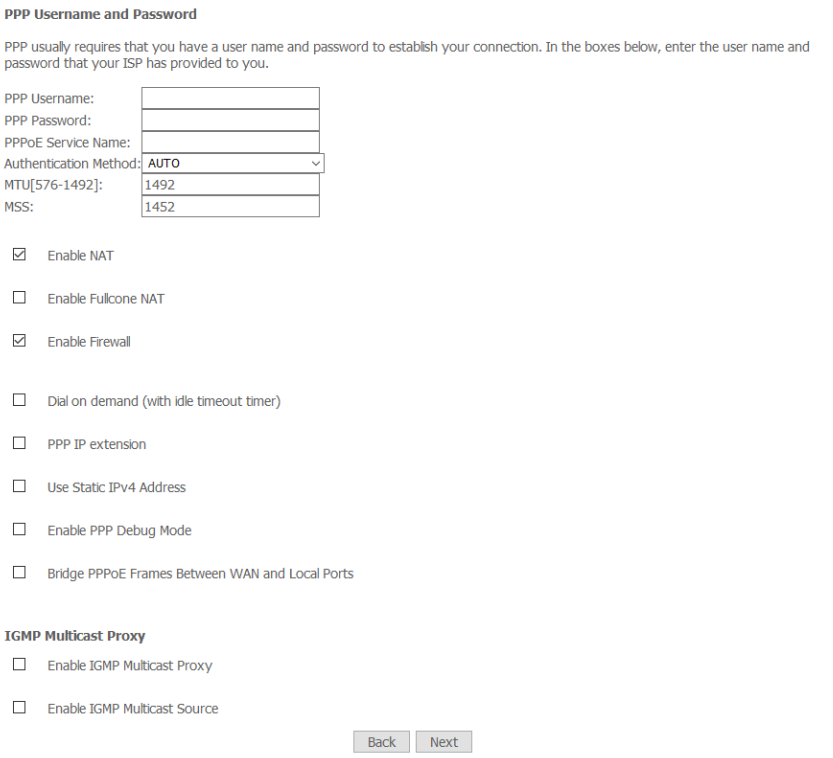


Select a WAN service type, enter a **Service Description**, enter the **802.1P Priority** and **802.1 VLAN ID** then click the **Next** button. **To disable VLAN tagging, place input value of -1. Refer to your ISP for VLAN information** as required by your Internet Service Provider.



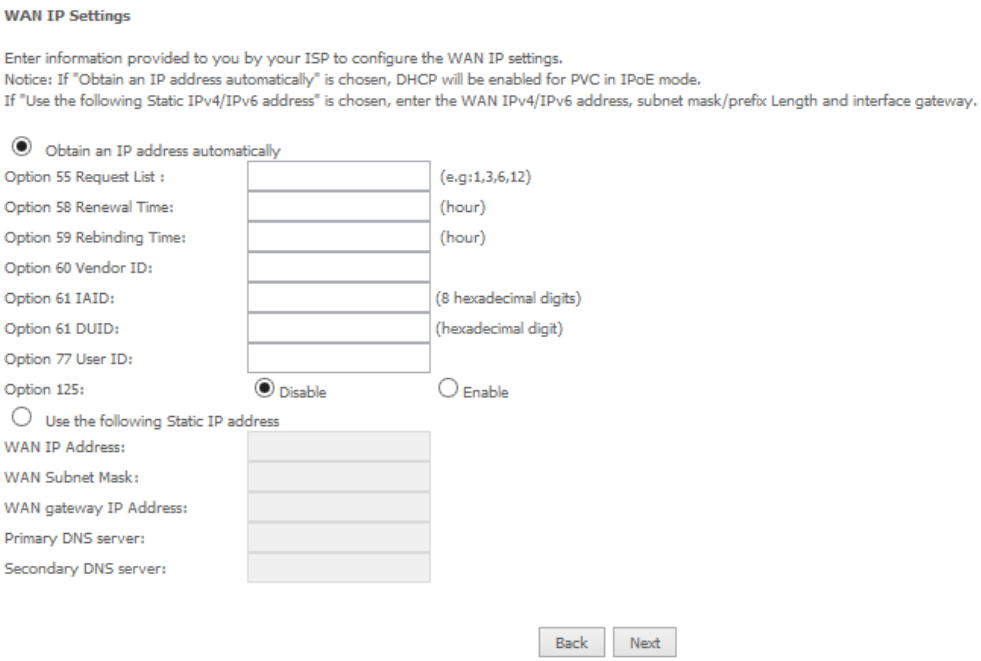
PPP over Ethernet

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

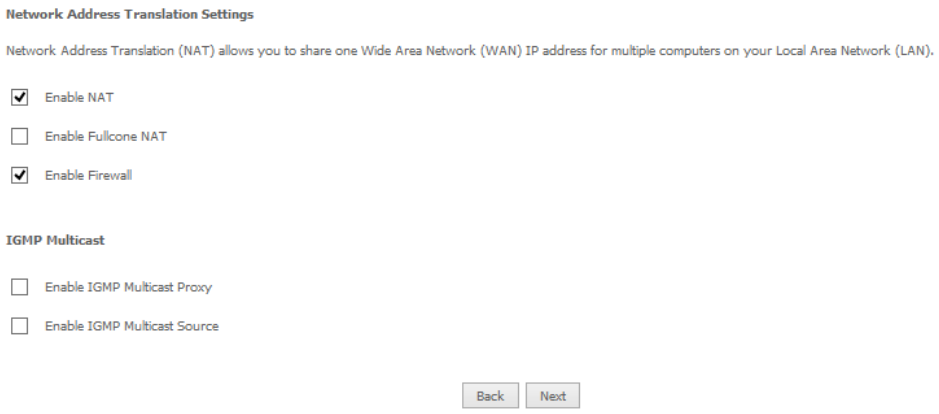


IP over Ethernet

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

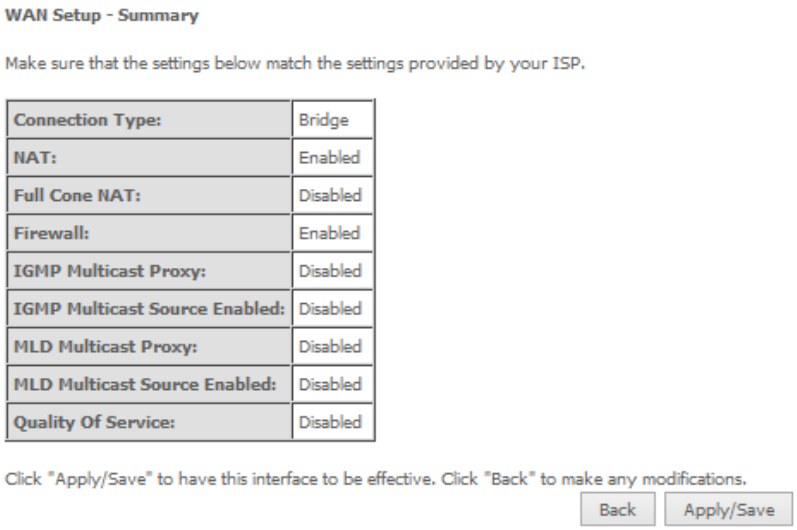


Select the NAT Translation settings as desired and click the **Next** button.



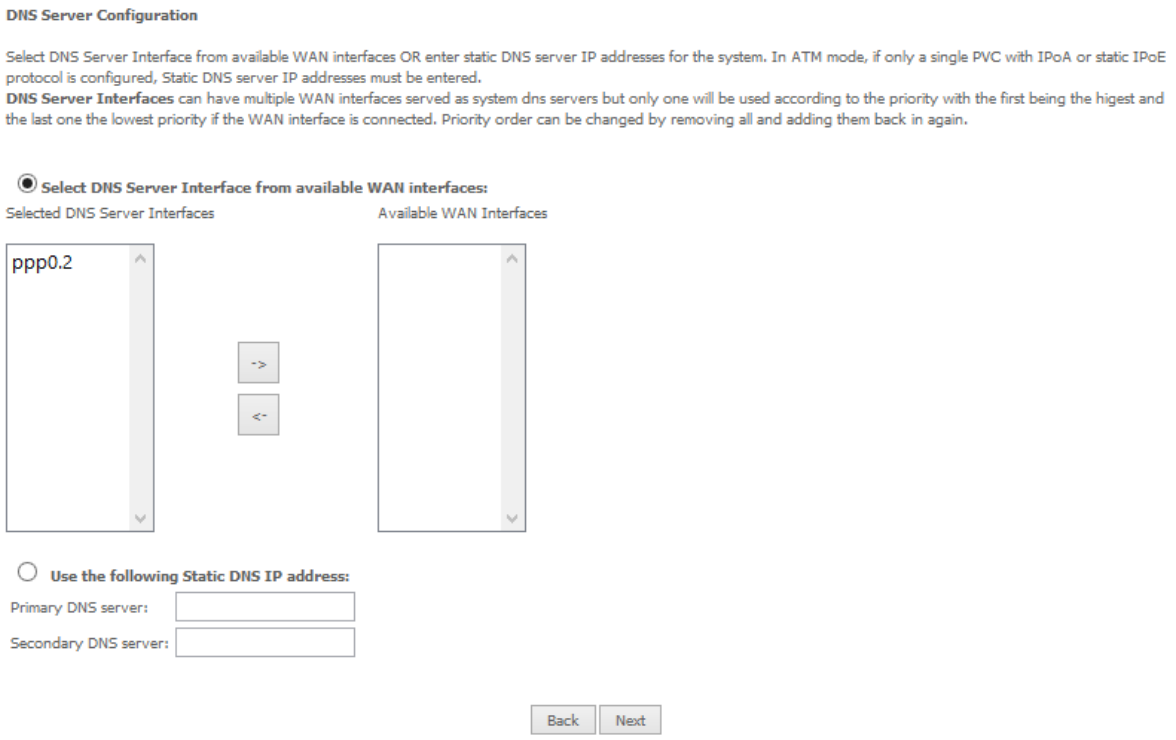
Bridging

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

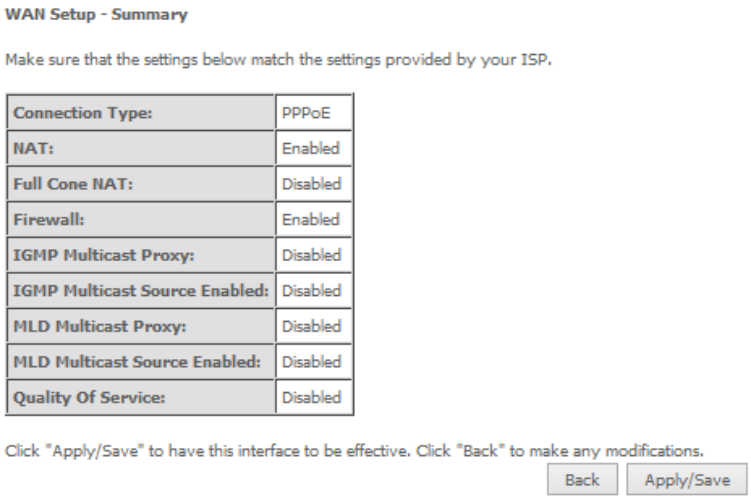


Use the arrow buttons to move the interfaces required to the list on the left. Click **Next**.

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 **Next** to continue.



A summary of your settings is displayed. Click **Apply/Save** to commit your settings to the router.



LAN

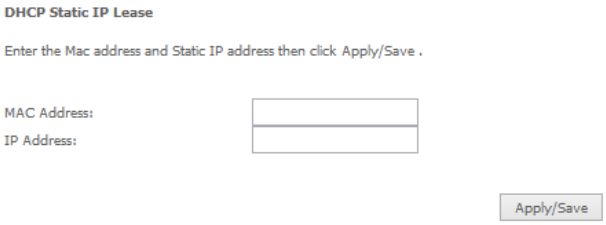
IPv4 Autoconfig

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

The following options are available to configure:

PARAMETER	DEFINITION
IP Address	Enter the Local IP Address to use for the NF10WV.
Subnet Mask	Enter the subnet mask 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 hosts.
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 NF10WV

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

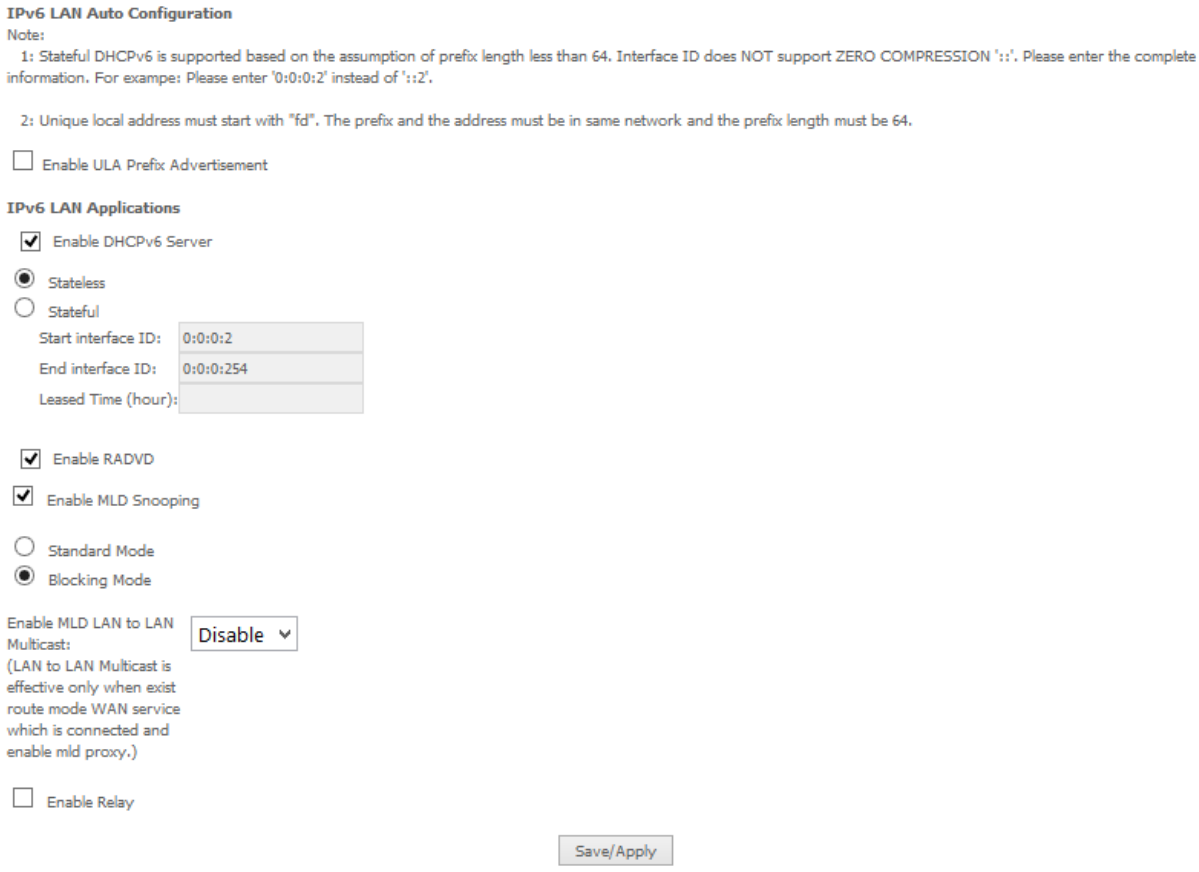


To set a DHCP reservation, enter the MAC Address of the chosen host and IP to use and then click **Apply/Save**.
The NF10WV enables you to set the DHCP options which are provided to hosts attempting to connect to the DHCP server.

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

IPv6 Autoconfig

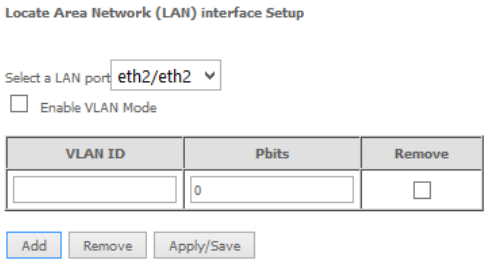
The IPv6 LAN Auto Configuration page allows you to configure settings pertaining to the IPv6 DHCP server.



OPTION	DEFINITION
Enable Unique Local Addresses and Prefix Advertisement	Enable the use of unique local addresses. The router will advertise the IPv6 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.
IPv6 LAN Applications	Enable IPv6 DHCP server
Enable DHCPv6 Server and 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 Neighbor 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	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	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 VLANs on the router.

LAN VLAN Setting

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

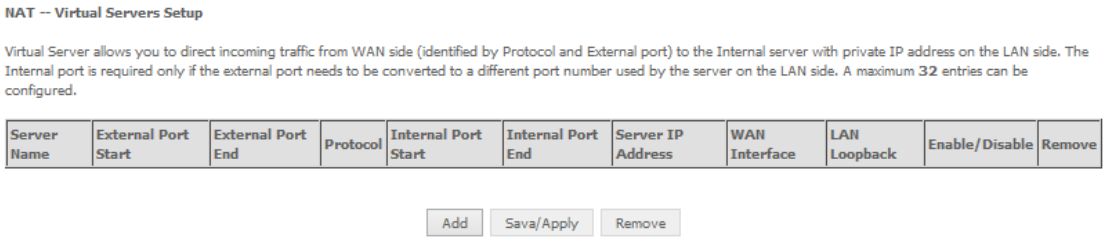


Select the LAN port using the drop down menu, then click the **Add** button. Enter the **VLAN ID** and in the Pbits field, enter a value from 0-7 indicating the priority bits that dictates the priority of the VLAN. Click **Apply/Save** when you have finished.

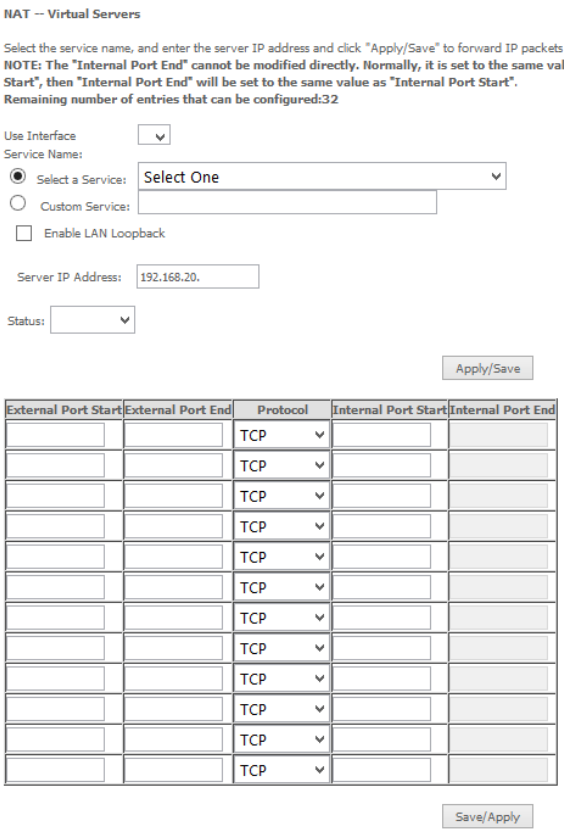
NAT

Virtual Servers

A virtual server allows you to direct incoming traffic from the WAN side to the Internal server with a private IP address on the LAN side.



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



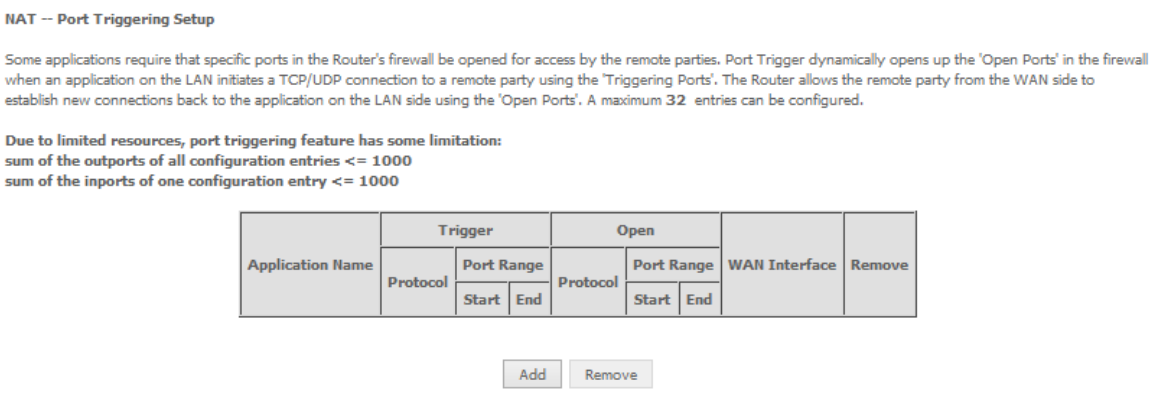
FIELD	DESCRIPTION
Select a Service or custom Server	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Server IP Address	Enter the IP address of the local server.
External Port Start	Enter the starting external port number (when custom server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

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

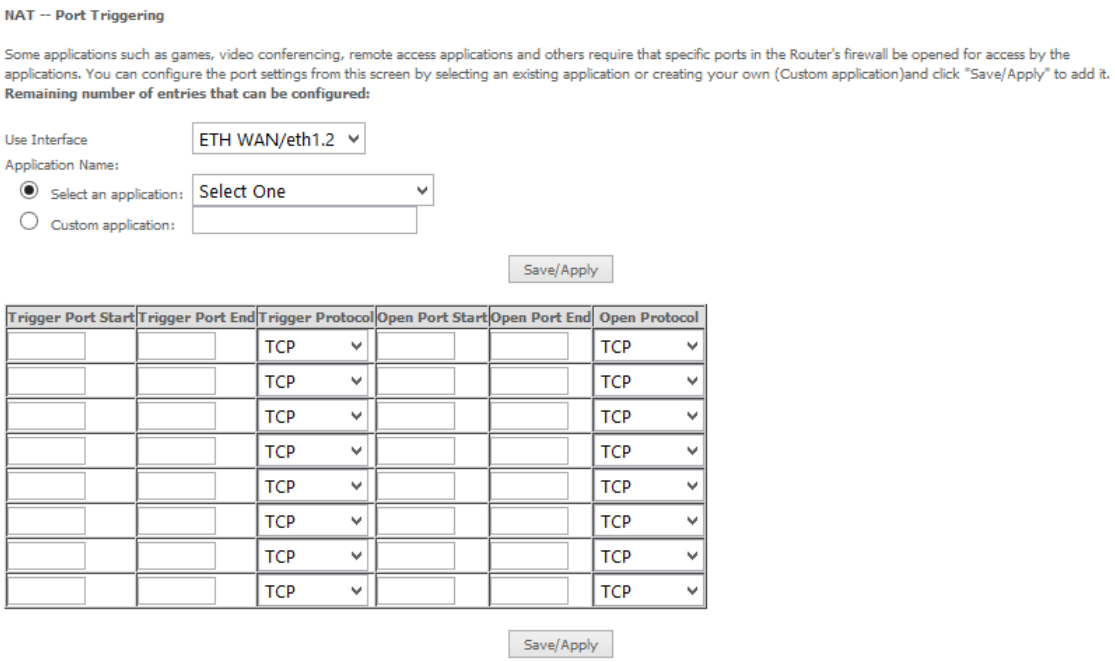
Port Triggering

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.



To add a Trigger Port, press the **Add** button.

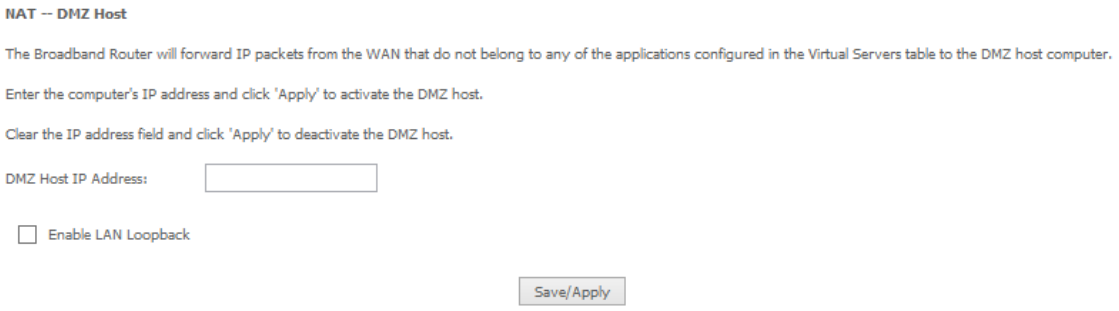


FIELD	DESCRIPTION
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When 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.

DMZ Host

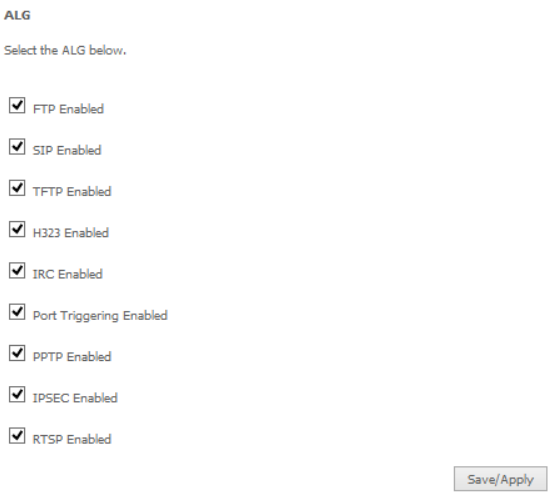
The NF10WV will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer'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.



ALG

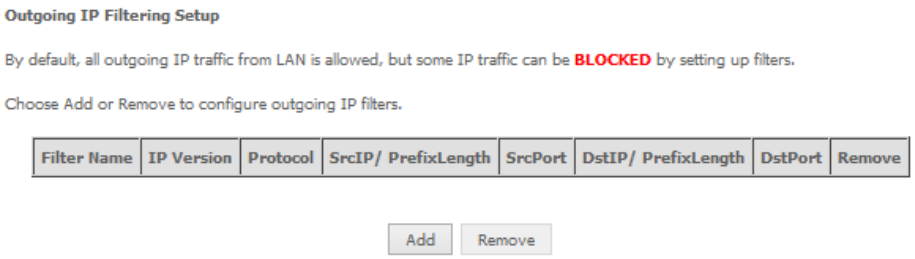
The Application Layer Gateway (ALG) is a feature which enables the router to parse application layer packets and support address and port translation for certain protocols. We recommend that you leave these protocols enabled unless you have a specific reason for disabling them.



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.

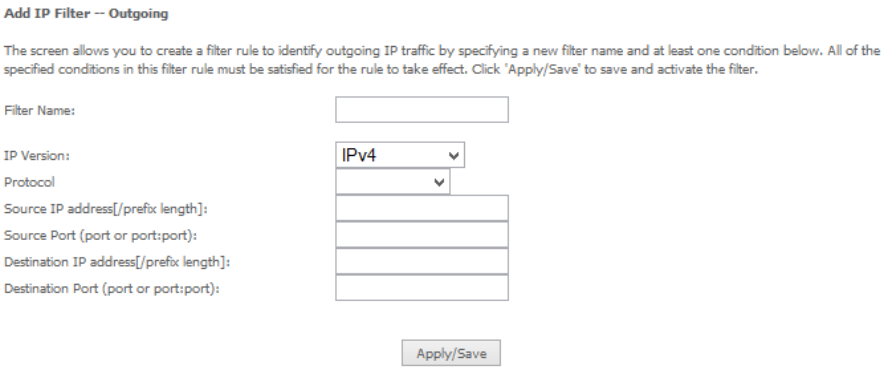


Outgoing IP Filtering

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 Remove checkbox next to the selected rule and click Remove.

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



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 block
Source IP Address/Subnet Mask	Enter the IP Address of the PC 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 to which connections should be blocked
Destination Port	Enter the destination port number used by the application to block

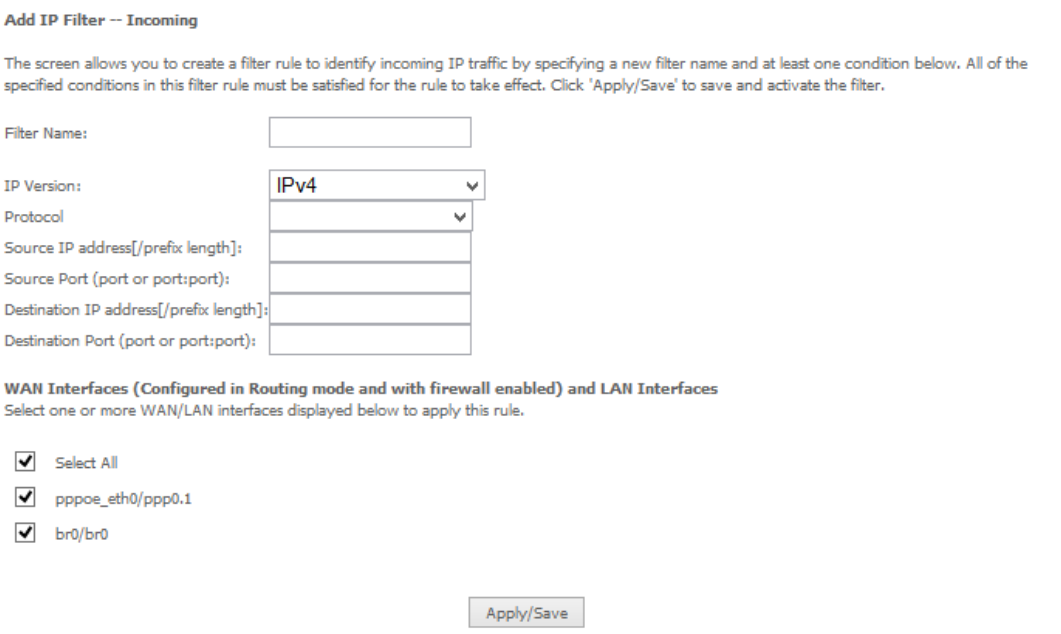
Click **Apply/Save** to take effect the settings. The new rule will then be displayed in the Outgoing IP Filtering table list.

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 incoming traffic from the Internet can be accepted by setting up Incoming IP Filtering rules.

To delete the rule, click Remove checkbox next to the selected rule and click Remove.

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



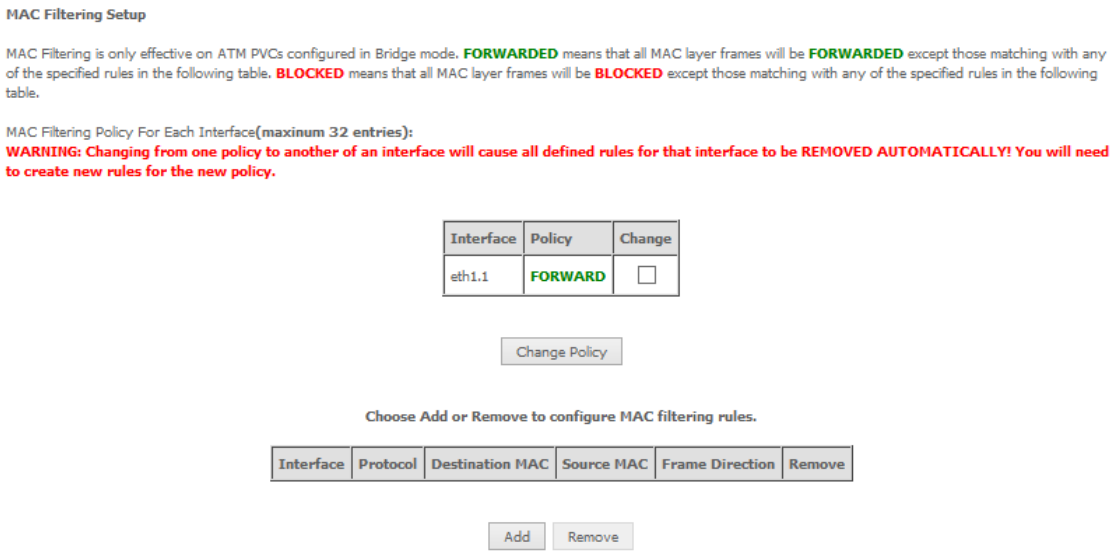
Enter the following parameters:

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 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 PC 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

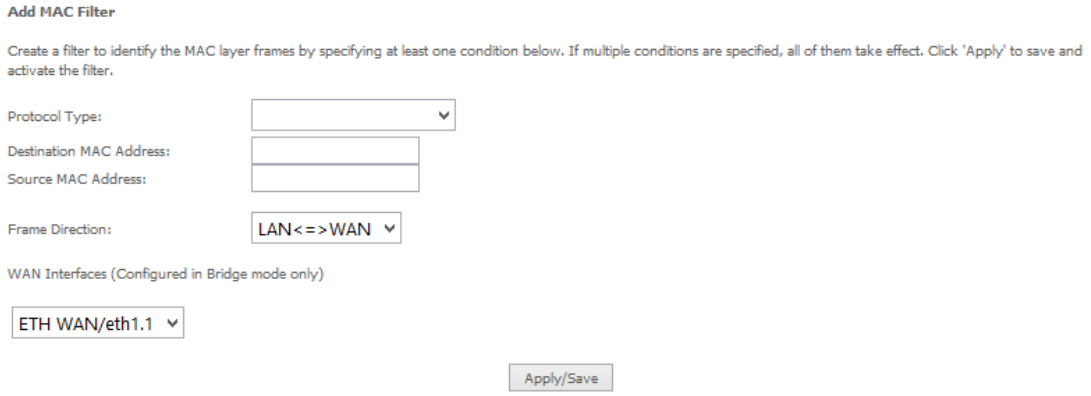
Click Save/Apply to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.

MAC Filtering

The NF10WV 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 connections which match the criteria.



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



1. Enter the Protocol type to which the filter should apply.
2. Enter the Source and Destination MAC Address
3. Enter the 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.

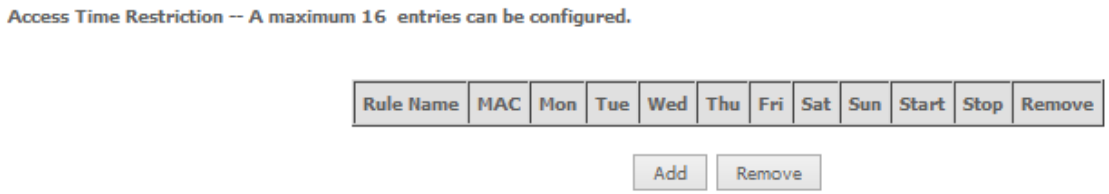


Figure 1: Advanced - Parental Control – Time Restriction

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

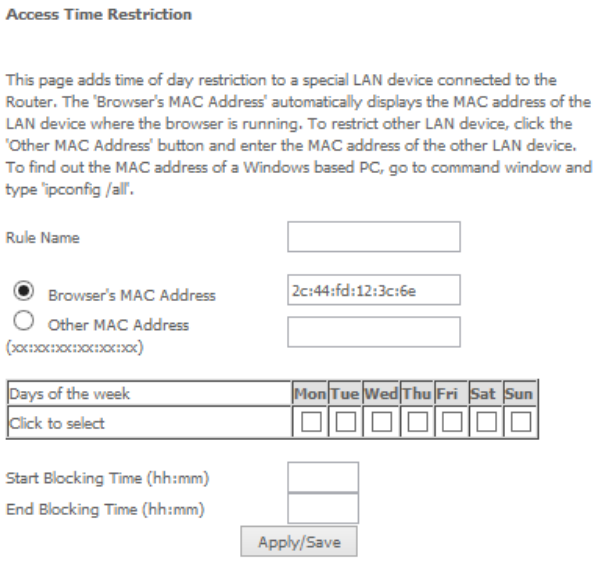


Figure 2: Advanced - Parental Control - Add Time Restriction

See the instructions below. Press the **Apply/Save** button to save a time restriction rule.

FIELD	DESCRIPTION
Rule Name	A user defined name for the time restriction rule.
Browser's MAC Address	The MAC address of the network card of the computer running the browser.
Other MAC Address	The MAC address of a second 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.
End blocking time	The time of day when the restriction ends.

Table 2: 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 NF10WV.

Select the 'To block' or 'To allow' option and then click Add to enter the URL you wish to add to the URL Filter list.

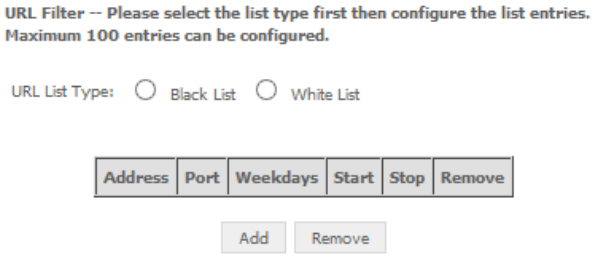


Figure 3: Advanced - Parental Control - URL Filter

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.

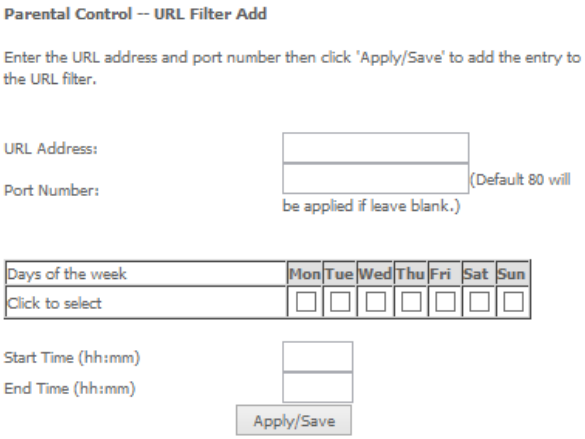


Figure 4: Advanced - Parental Control - Add URL Filter

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.

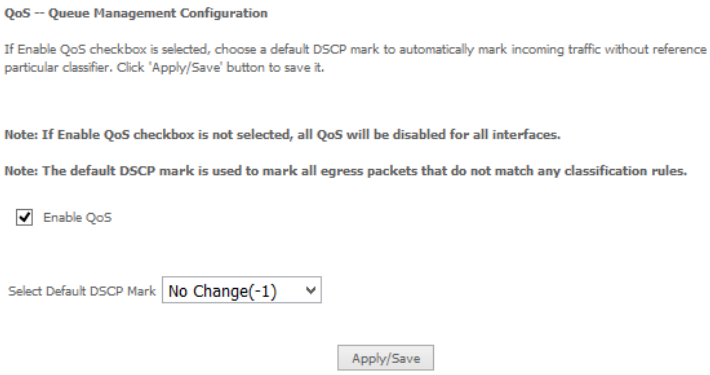


Figure 5: Advanced - Enable QoS

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

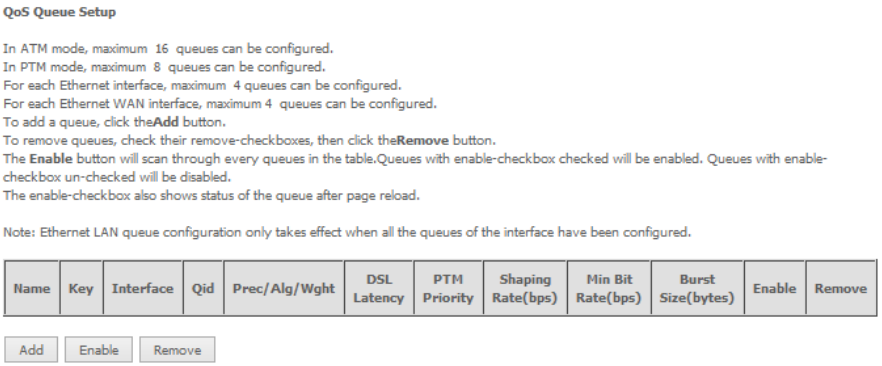


Figure 6: Advanced - QoS Queue Setup

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

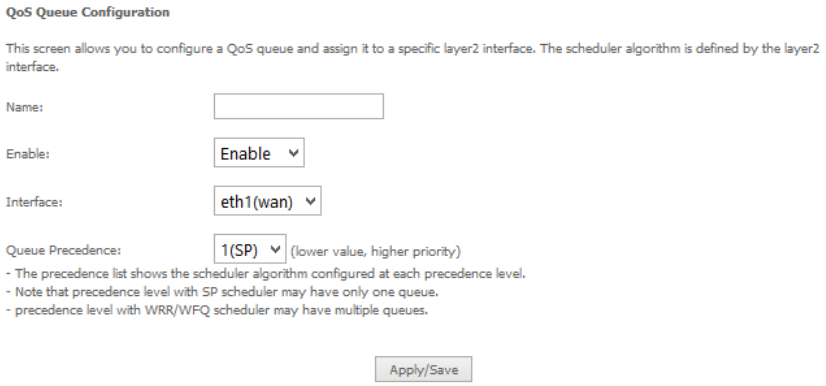


Figure 7: Advanced - QoS - Add QoS Queue

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.

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

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

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

Add Network Traffic Class Rule

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

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

Specify Classification CriteriaA blank criterion indicates it is not used for classification.

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

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

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

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

Set Rate Limit(kbps): [Kbits/s]

Apply/Save

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.

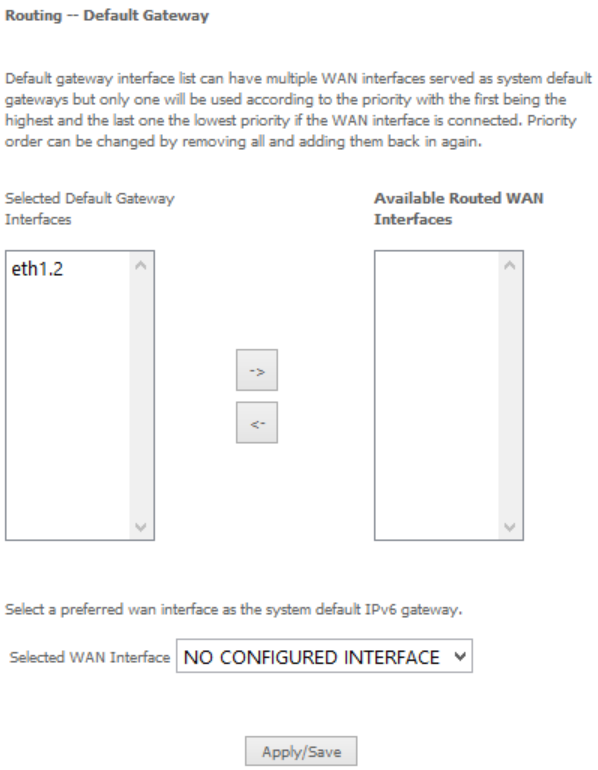
Click the **Apply/Save** button to save and activate the rule.

Routing

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

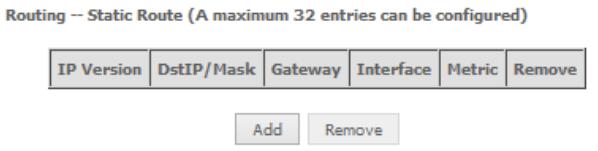
Default Gateway

Select your preferred WAN interface from the available options.

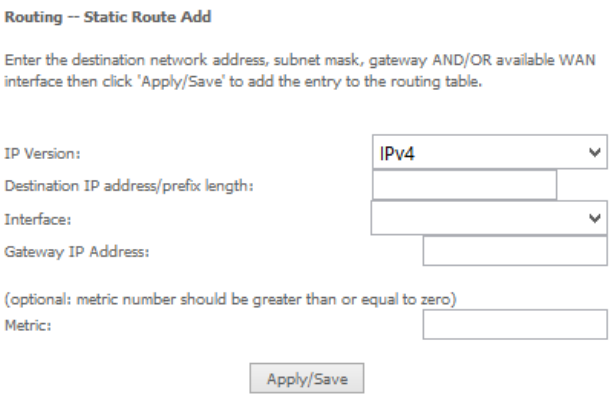


Static Route

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



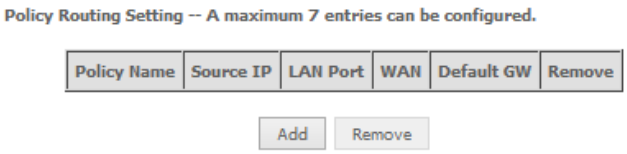
To add a static route rule click the **Add** button. The following screen is displayed.



Enter the Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. 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.



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

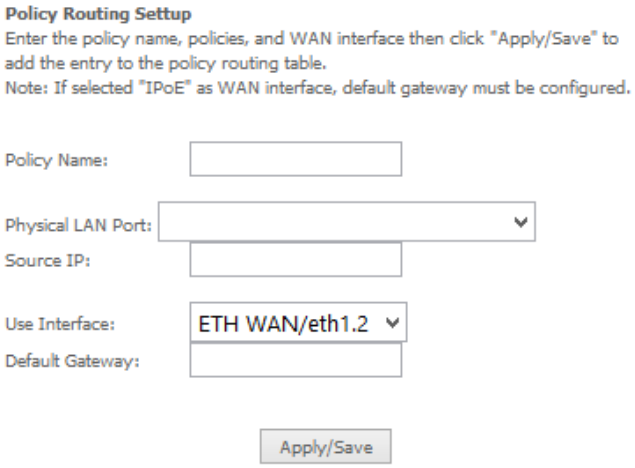


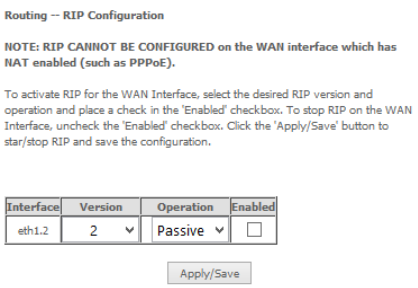
Figure 8: Advanced - Routing - Add Policy Route

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.

RIP (Routing Information Protocol)

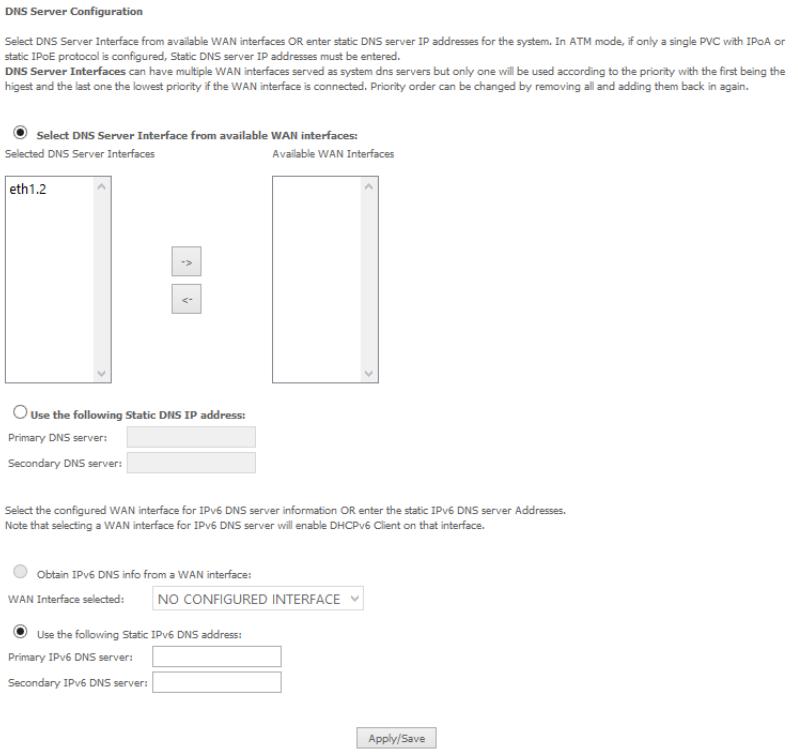
To activate this option, select the Enabled checkbox.
To configure an individual interface, select the desired RIP version and operation, and select the Enabled checkbox for that interface. Click **Apply/Save** to save the configuration.



DNS

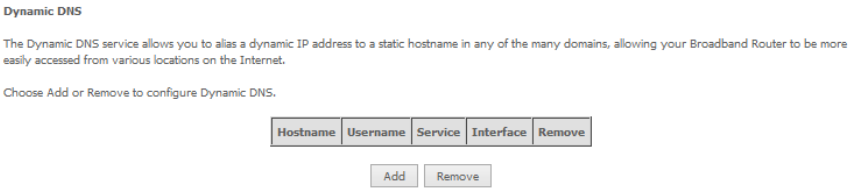
DNS Server

This page allows you to enable automatic DNS settings detected from the Internet Service Provider or specify your own DNS server address manually.



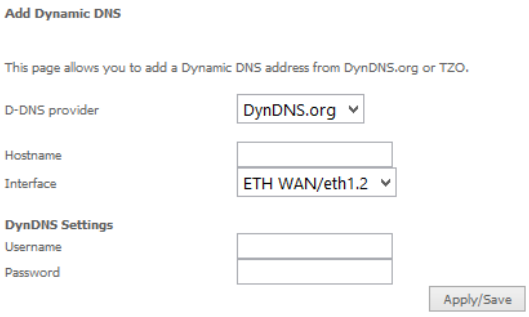
Dynamic DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the router to be more easily accessed from various locations on the internet. You will require a Dynamic DNS subscription from a Dynamic DNS provider.



Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and the following screen will display.

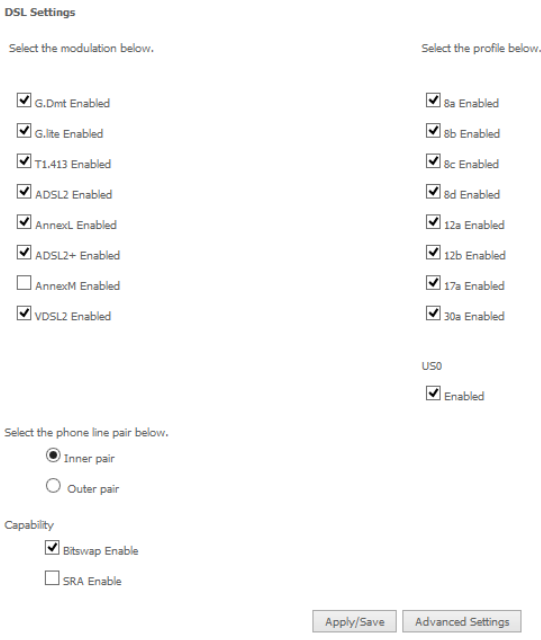


FIELD	DESCRIPTION
D-DNS Provider	Select the dynamic DNS provider from the list.
Hostname	The name of the dynamic DNS provider.
Interface	Select the interface from the list.
Username	Enter the Dynamic DNS account username.
Password	Enter the Dynamic DNS account password.

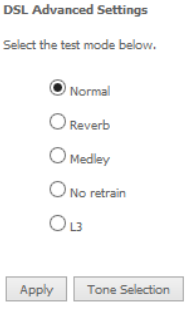
Table 3: Advanced - DNS - Add Dynamic DNS Account Settings

DSL

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



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

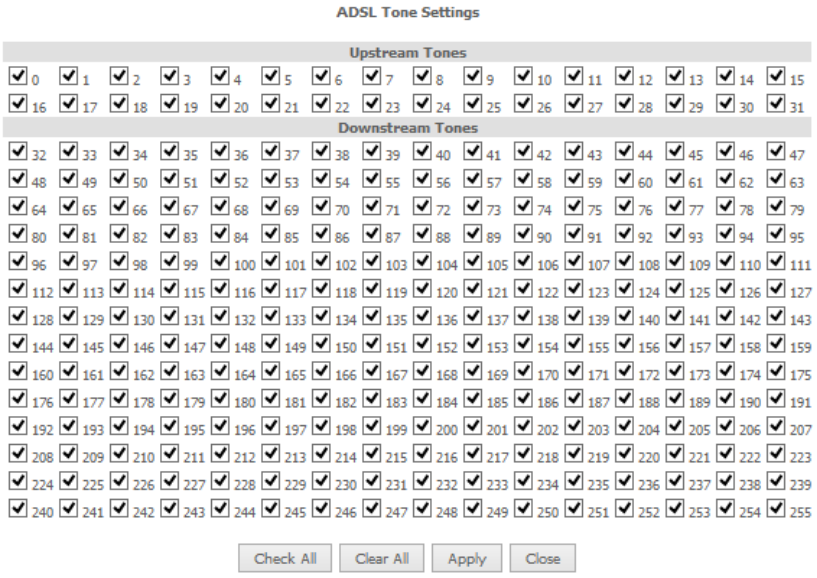


The DSL advanced settings relate to test mode settings. The default selection is 'Normal'.

ADSL Tone Settings

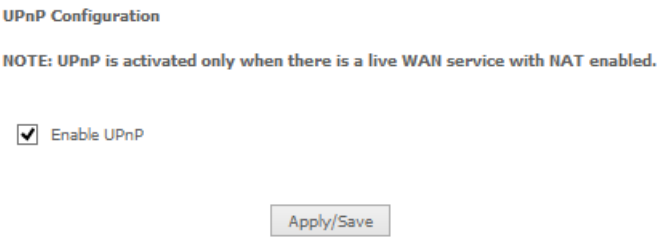
For ADSL Tone Settings select the 'Tone Selection' button on the DSL Advanced Settings page.

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



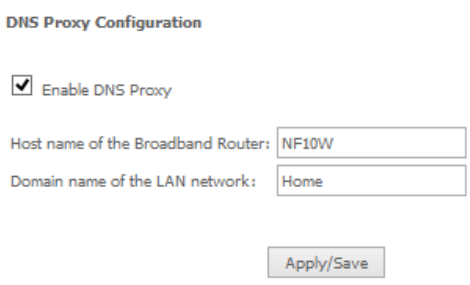
UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, 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. UPnP allow automatic port forwarding configuration form your UPnP devices.



DNS Proxy

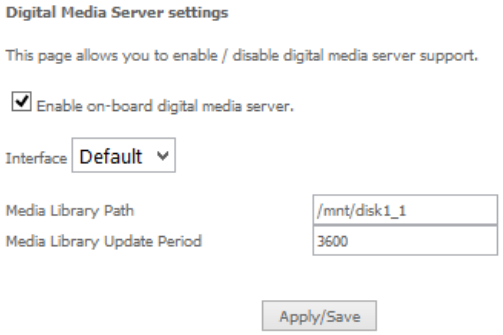
To enable DNS Proxy settings, select the corresponding checkbox and then enter the Host and Domain name, as in the example shown below. Click **Apply/Save** to continue.



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. Eg. You can access your router by entering http://NF10WV 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 NF10WV and the router will make it accessible to other devices on your network.



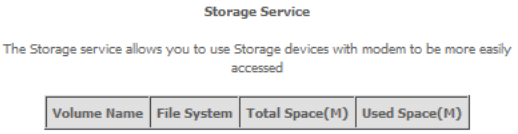
Select **Enable on-board digital media server** and then use the drop down list to select the Interface. In the **Media Library Path** field, enter the path to the media and then enter a period between media library updates in seconds. Click the **Apply/Save** button when you have finished.

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.

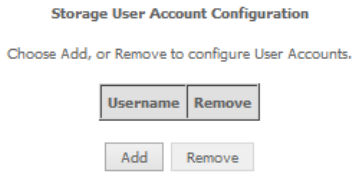
Storage Device Info

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

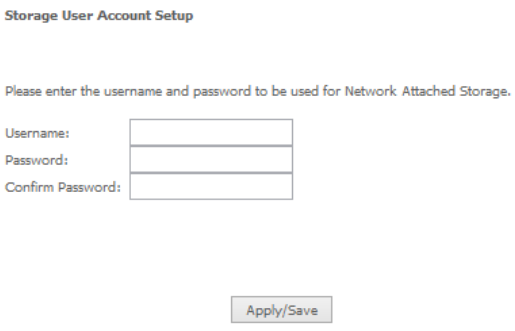


User Accounts

User accounts are used to restrict access to the attached USB Storage device.
To delete a User account entry, click the **Remove** checkbox next to the selected account entry and click **Remove**.
Click **Add** to create a user account.



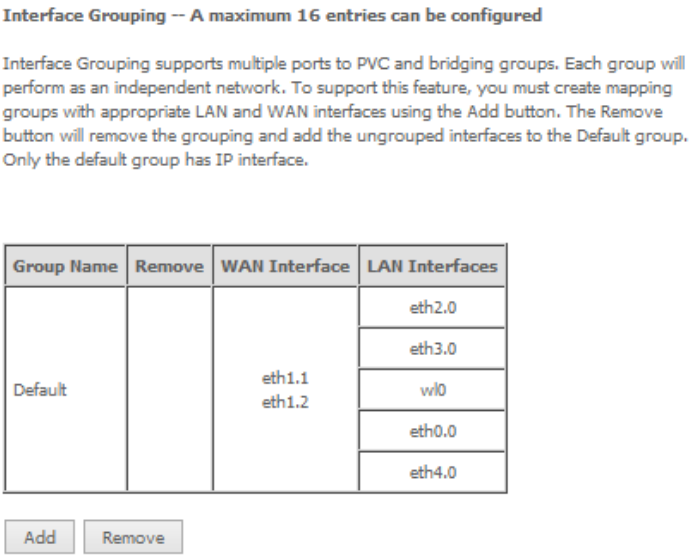
Adding an account allows the creation of specific user accounts with a password to further control access permissions. To add an account, click the **Add** button and then enter the desired username and password for the account.



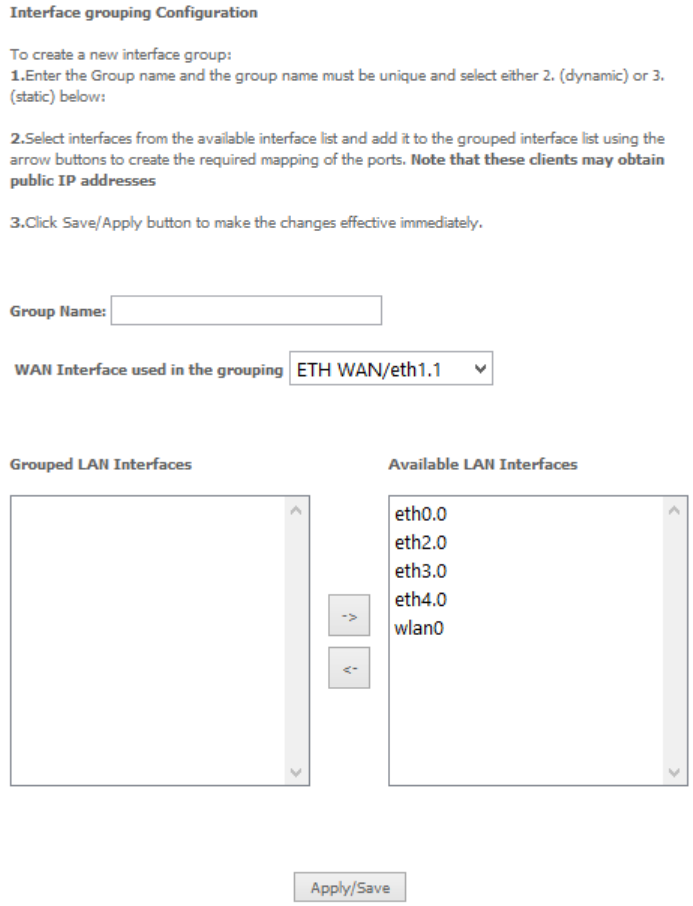
Interface Grouping

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

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



Click **Add** to create an Interface group.

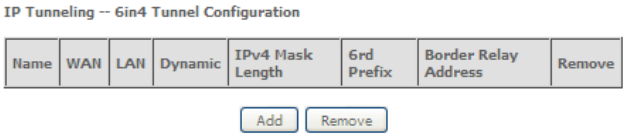


Enter a group name and then use the arrow buttons to select which interfaces you wish to group. Click **Apply/Save** to save the Interface grouping configuration settings.

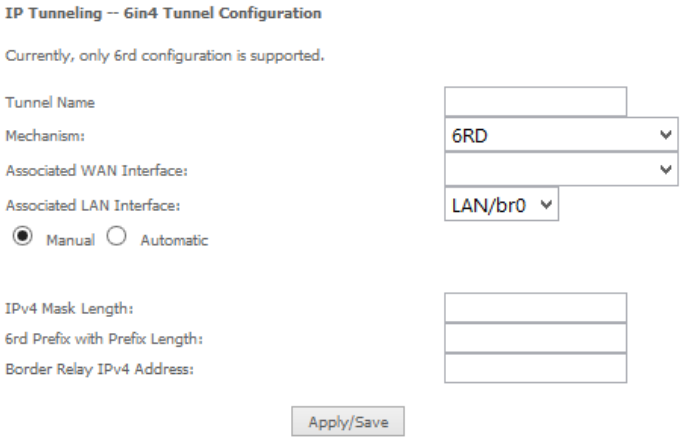
IP Tunnel

The IP Tunnelling feature allows you to configure tunnelling of traffic between IPv6 and IPv4 networks.

IPv6inIPv4

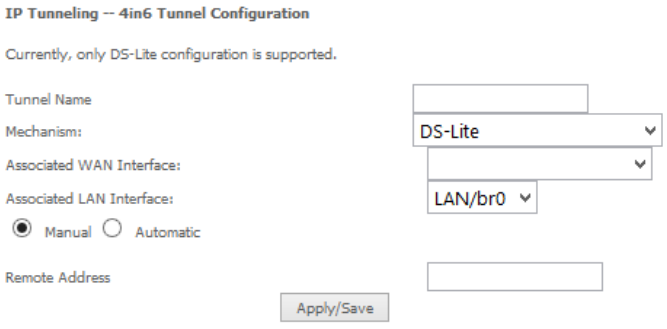


Click the **Add** button to add a new tunnel.



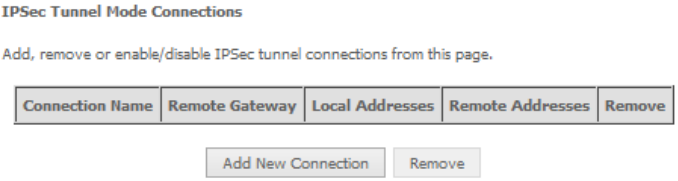
IPv4inIPv6

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



IPSec

The NF10WV offers IPSec VPN tunnel functionality. To delete an IPSec entry, click the Remove checkbox next to the selected IPSec tunnel entry and click **Remove**.



Click **Add** to create a new IPSec tunnel connection.

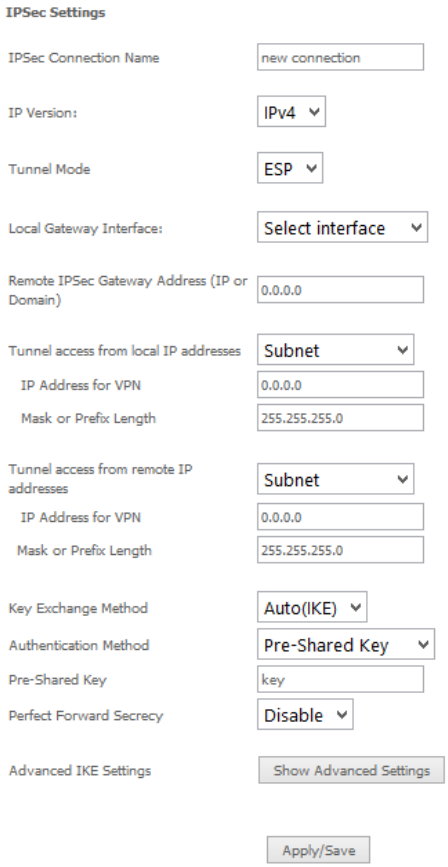


Figure 9: Advanced - IPSec

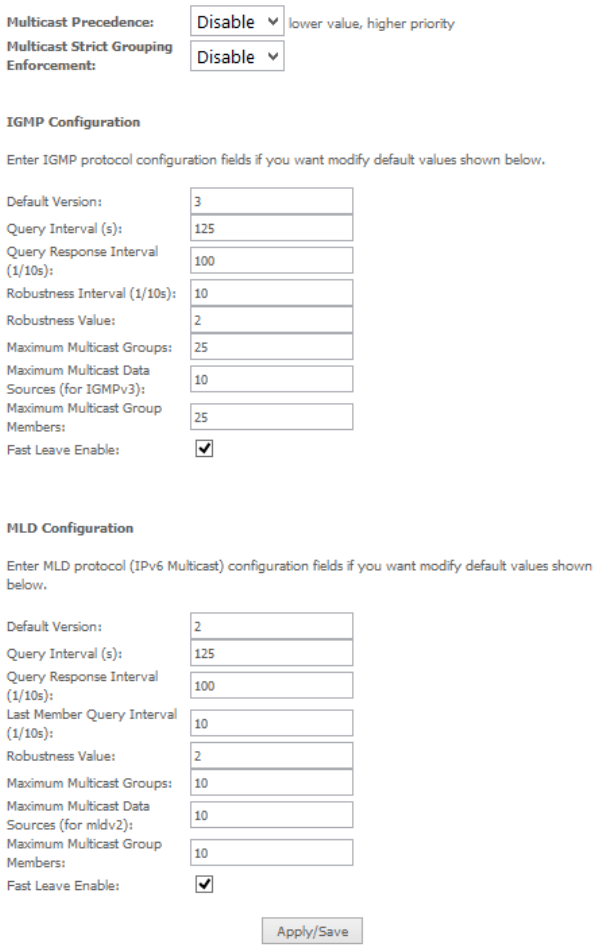
Enter the following parameters:

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
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

After entering the required IPSec tunnel service settings, click **Apply/Save** to save the new IPSec Tunnel configuration settings.

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.

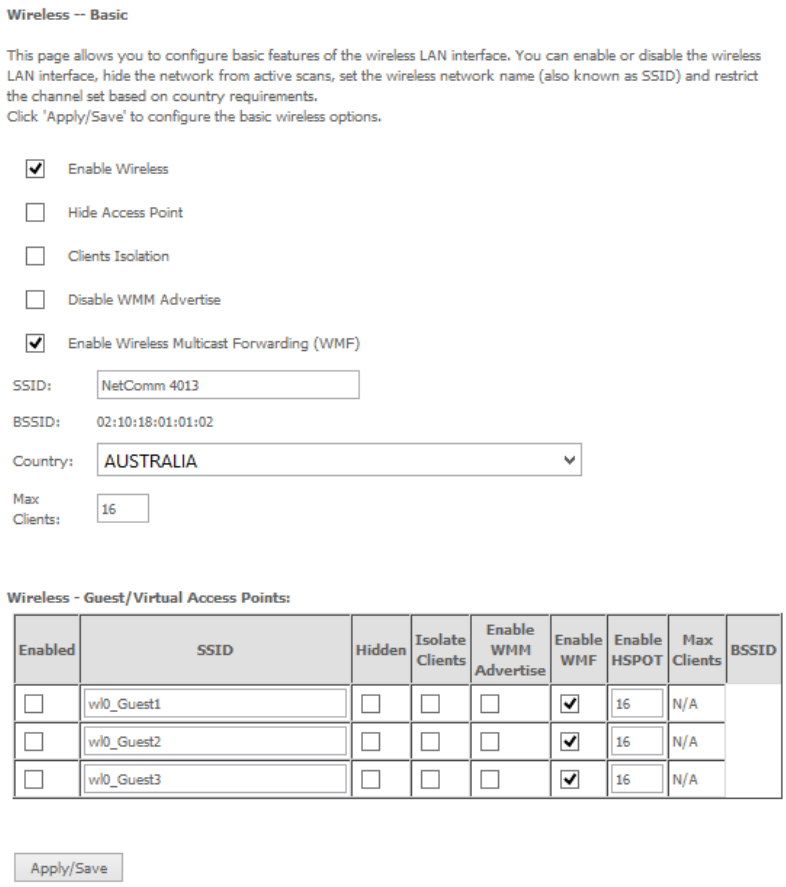


FIELD	DEFINITION
Default Version	The version IGMP in use by the router.
Query Interval	The hosts on the segment report their group membership in response to the router's queries. The query interval timer is also used to define the amount of time a router will store particular IGMP state if it does not 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 timer expires, the host replies with a report, provided that no other host has responded yet. This accomplishes two purposes: 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 a IGMP host.

Wireless

Basic

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



The following parameters are available:

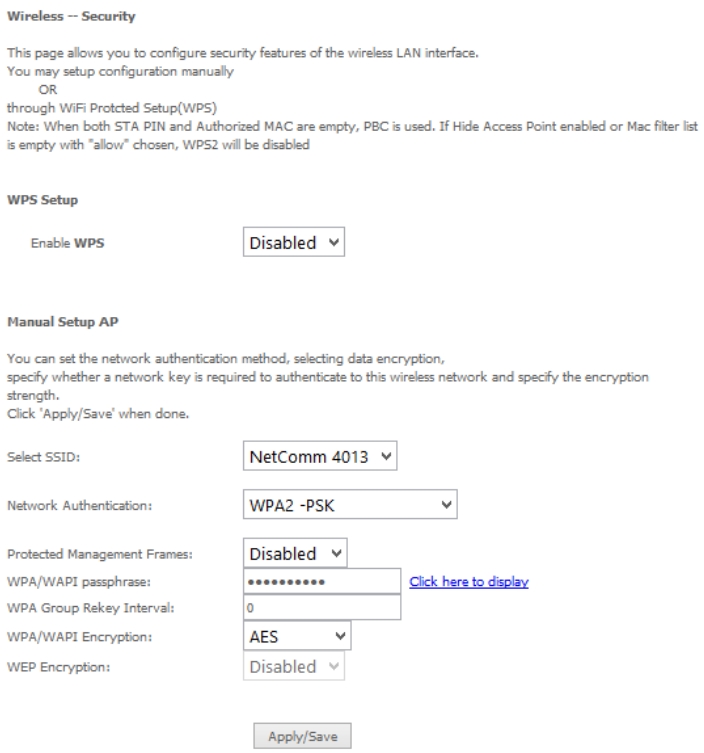
PARAMETER	DEFINITION
Enable Wireless	Select to enable or disable the wireless network function
Hide Access Point	Select to hide or display the wireless network when an SSID scan is performed
Clients Isolation	Select to prevent clients on the wireless network being able to access each other
Disable WMM Advertise	Select to prevent the NF10WV advertising its WMM function
Enable Multicast Forwarding (WMF)	Select to enable Wireless Multicast Forwarding. This 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 Network	Select to enable a separate Wireless Guest network, the same options are available for a Guest network as with the main system wireless network.

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, hiding a SSID is Security through obscurity.

Security

The NF10WV supports all encryptions within the 802.11 standard. The factory default is WPA2-PSK. The NF10WV also supports WPA, WPA-PSK, WPA2, WPA2-PSK. You can also select to enable WPS mode.



The following parameters are available:

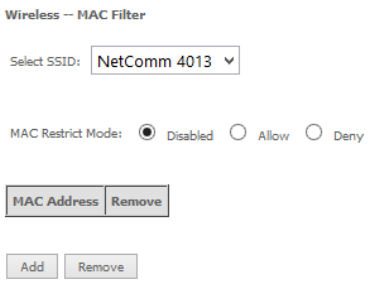
PARAMETER	DEFINITION
Enable WPS	Select to enable or disable the WPS function of the NF10WV.
Select SSID	Select the SSID to apply the security settings to.
Network Authentication	Select the Wireless security type to use with the wireless network.
WPA/WAPI passphrase	Enter the security key to use with 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.
WEP Encryption	Select to utilise WEP encryption on the wireless network connection.

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.

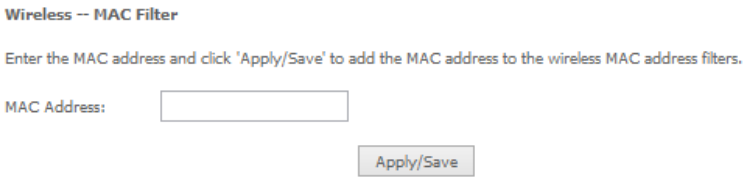
Click **Apply/Save** to save the new wireless security configuration settings.

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.



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

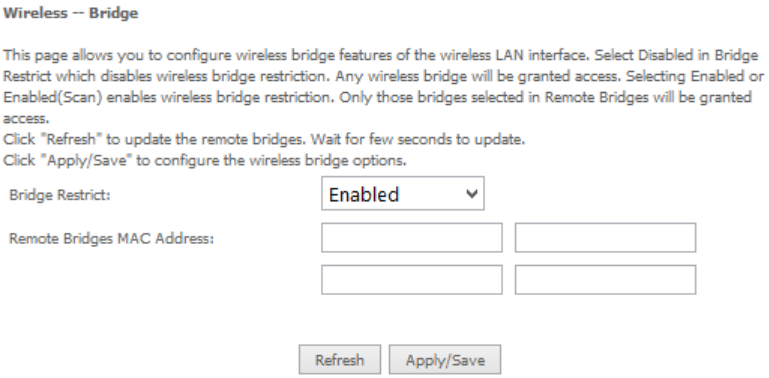


Enter the MAC Address to be filtered and click **Apply/Save** to save the new MAC Address filter settings.
To delete a MAC filter entry, click the Remove checkbox next to the selected filter entry and click Remove.

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 Bridge (Wireless Distribution Service)

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



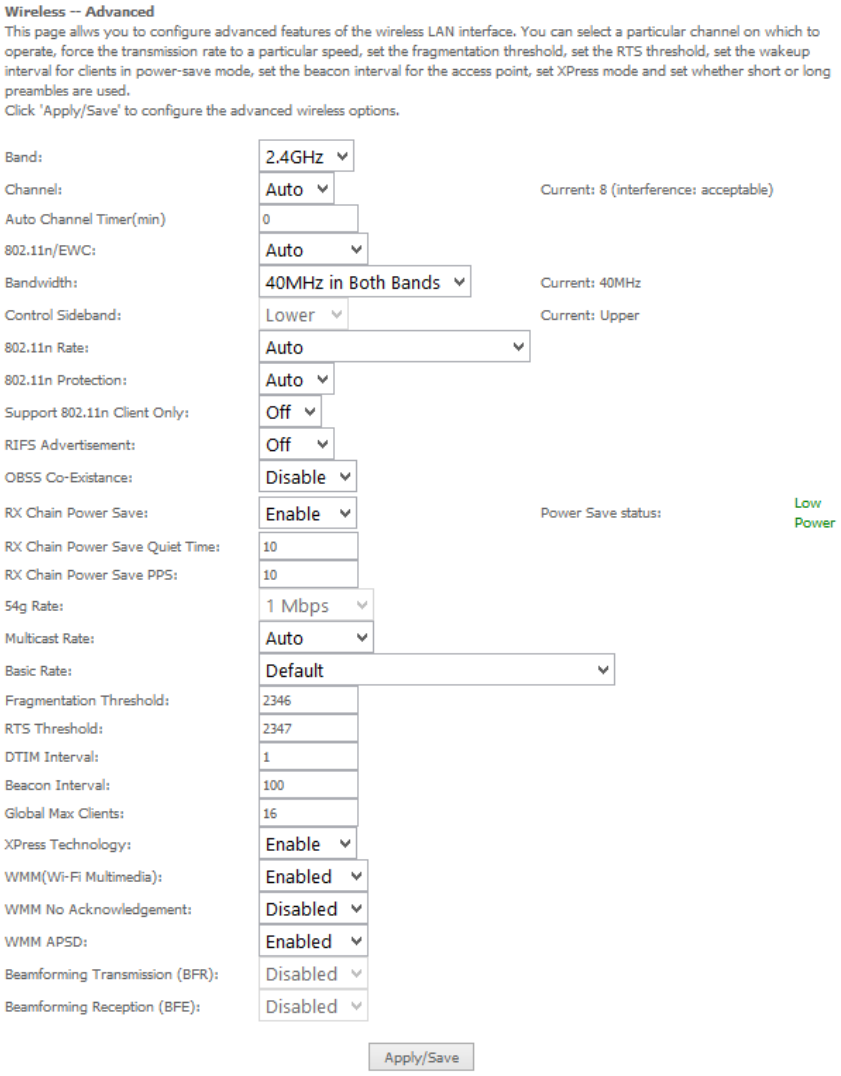
Select the mode for the Wireless Access Point built into the NF10WV. You can specify which wireless networks will be allowed to connect to the NF10WV by using the 'Bridge Restrict' option and then entering the applicable MAC Addresses of the other wireless access points.

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.

Advanced

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



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 channeling functionality.
Auto Channel Timer(min)	Specifies the timer of auto channelling.
802.11n/EWC	Select disable 802.11n or Auto.
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. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is 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 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 accelerating technology for IEEE802.11g. The default is Enabled.
WMM (Wi-Fi 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.

Station Info

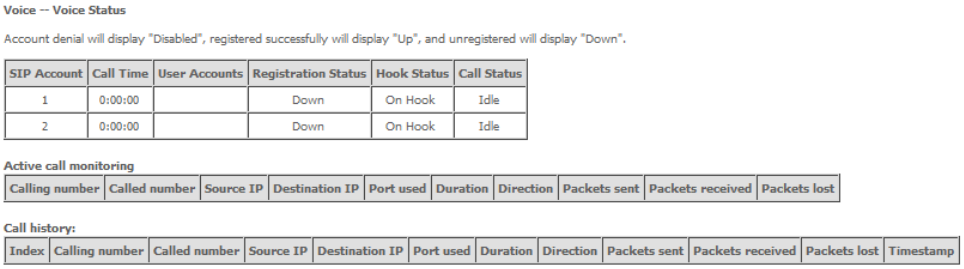
This page shows the MAC address of authenticated wireless stations that are connected to the NF10WV and their status

Voice

This section explains how to configure the VoIP settings of the NF10WV.

VoIP Status

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



Voice -- Voice Status

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

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

Active call monitoring

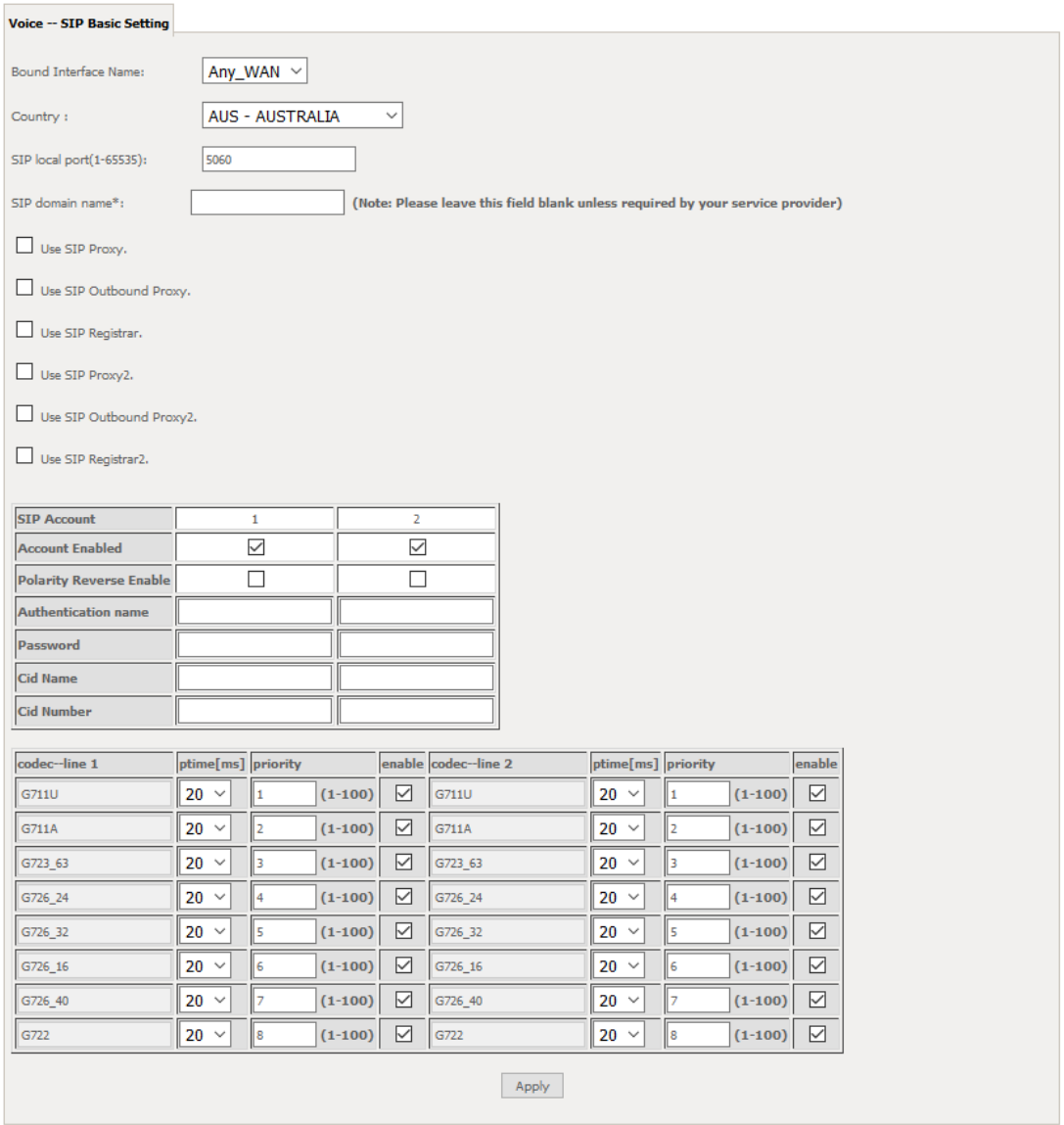
Calling number	Called number	Source IP	Destination IP	Port used	Duration	Direction	Packets sent	Packets received	Packets lost

Call history:

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

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.



Voice -- SIP Basic Setting

Bound Interface Name: Any_WAN

Country : AUS - AUSTRALIA

SIP local port(1-65535): 5060

SIP domain name*: (Note: Please leave this field blank unless required by your service provider)

- Use SIP Proxy.
- Use SIP Outbound Proxy.
- Use SIP Registrar.
- Use SIP Proxy2.
- Use SIP Outbound Proxy2.
- Use SIP Registrar2.

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

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

Apply

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

OPTION	DEFINITION
Bound Interface Name	Select the Interface that the VoIP account will use to make a connection to the VoIP Service Provider.
SIP Local Port	Set the SIP local port of the gateway, the default value is 5060. SIP local port is the SIP UA (user agent) port.
SIP domain name	Enter the SIP domain name or IP address of your VoIP Service Provider here.
Use SIP Proxy	Select the checkbox of Use SIP Proxy, if your DSL router uses a SIP proxy. SIP proxy allows other parties to call DSL router through it. When it is selected, the following fields appear.
SIP Proxy	The IP address of the proxy.
SIP Proxy port	The port that this proxy is listening on. By default, the port value is 5060.
Use SIP Outbound Proxy	Some network service providers require the use of an outbound proxy. This is an additional proxy, through which all outgoing calls are directed. In some cases, the outbound proxy is placed alongside the firewall and it is the only way to let SIP traffic pass from the internal network to the Internet. When it is selected, the following fields appear.
SIP Outbound Proxy	The IP address of the outbound proxy.
SIP Outbound Proxy port	The port that the outbound proxy is listening on. By default, the port value is 5060.
Use SIP Registrar	Select this option if required by your VoIP Service Provider. Enter the SIP Proxy Domain Name and SIP Proxy Port which is typically 5060.
SIP Registrar	The IP address of the SIP registrar.
SIP Registrar port	The port that SIP registrar is listening on. By default, the port value is 5060.
Account Enabled	If it is unselected, the corresponding account is disabled. You can not 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 millisecond, packets improve the voice quality. Because of the packet loss, less information is lost, but more loads on the network traffic.
Priority	The priority of codec is declined from up to down. Codecs define the method of relaying voice data. Different codecs have different characteristics, such as data compression and voice quality. For Example, G723 is a codec that uses compression, therefore, it is good for use where the bandwidth is limited but its voice quality is not good as other codecs, such as the G711. If you specify none of the codecs, using the default value showed in the above figure, the DSL router chooses the codec automatically.

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.

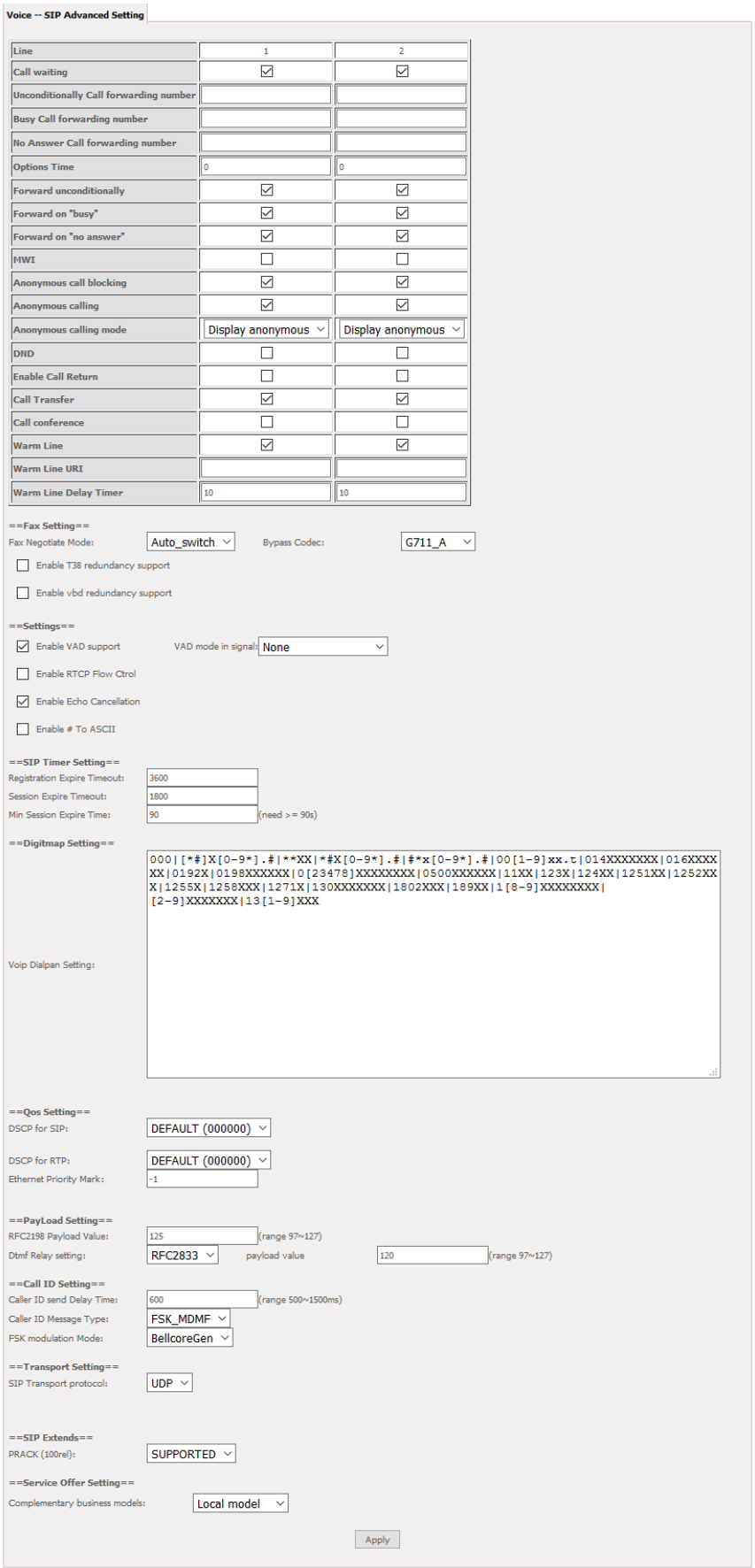


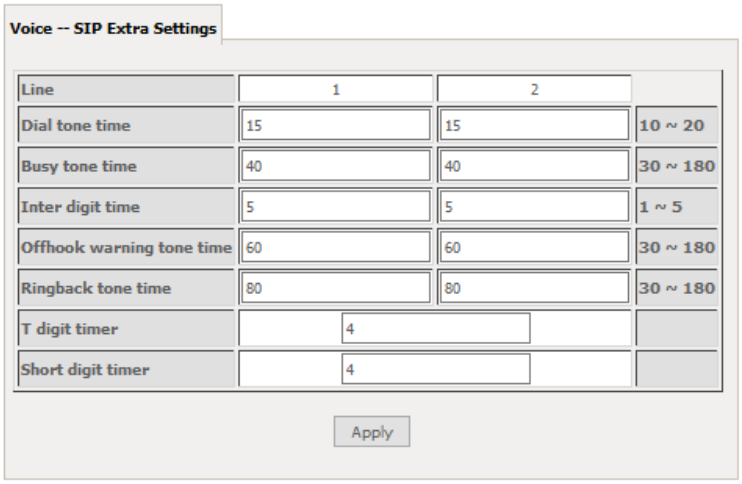
Figure 10: VoIP - Advanced - Service Provider

OPTION	DEFINITION
Line	Displays the line number 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. Additionally, you must activate the feature using the handset to dial *78. DND is deactivated automatically if the handset is put in the off-hook position.
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.
Enable RTCP Flow Control	Select this checkbox to use the feature.
Enable Echo Cancellation	Select this checkbox to use the feature.
Enable # To ASCII	Select this checkbox to use the feature.
Enable Reinjection Function	Select this checkbox to use the feature.
RFC2198 Payload Value (range 97-127)	Enter the RFC2198 payload value that the valid range is 96 ~ 127.
Registration Expire Timeout	Enter the registration expire timeout.
Session Expire Time	The interval of dialog refreshing time.
Min Session Expire Time	The minimum interval of dialog refreshing time.
VoIP DialPlan Setting	Set the VoIP dial plan. If user-dialed number matches it, the number is processed by the DSL router immediately.
DSCP for SIP	Set the DSCP for SIP. You can select it from the drop-down list.
DSCP for RTP	Set the DSCP for RTP. You can select it from the drop-down list.
Ethernet Priority Mark	This is the priority marking as per the 802.1p standard. Priority markings are carried in the VLAN tag. The following priority markings are valid settings: Background = 0 (lowest) Best Effort = 1 Excellent Effort = 2 Critical Applications = 3 Video < 100ms latency and jitter = 4 Voice < 10ms latency and jitter = 5 Internetwork control = 6 Network control = 7 (highest)
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 signaling. Note that the SIP proxy and registrar 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 can not be set by the telephone set.

Table 4: VoIP - Advanced - Service Provider

SIP Extra Setting

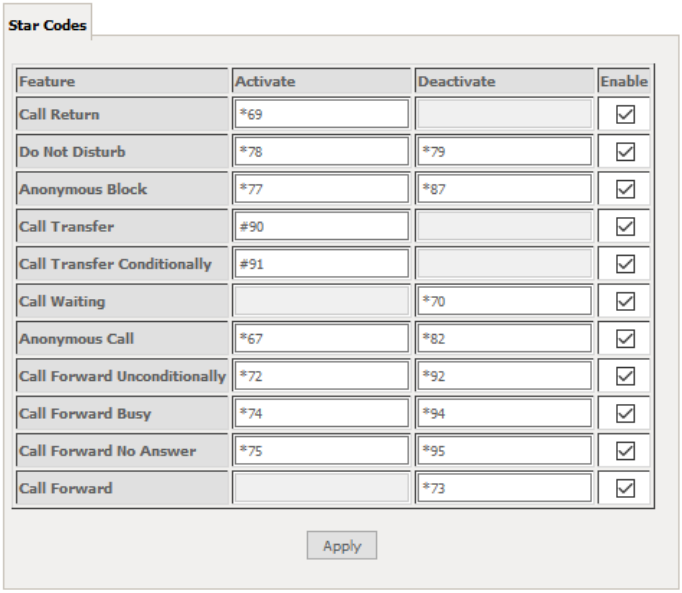
This page displays additional settings related to the SIP service.



PARAMETER	DEFINITION
Dial tone time	Dial tone duration.
Busy tone time	Busy tone duration.
Inter digit time	The valid range is 1 ~ 5.
Offhook warning tone time	Offhook warning tone duration.
Ringback tone time	Ringback tone duration.

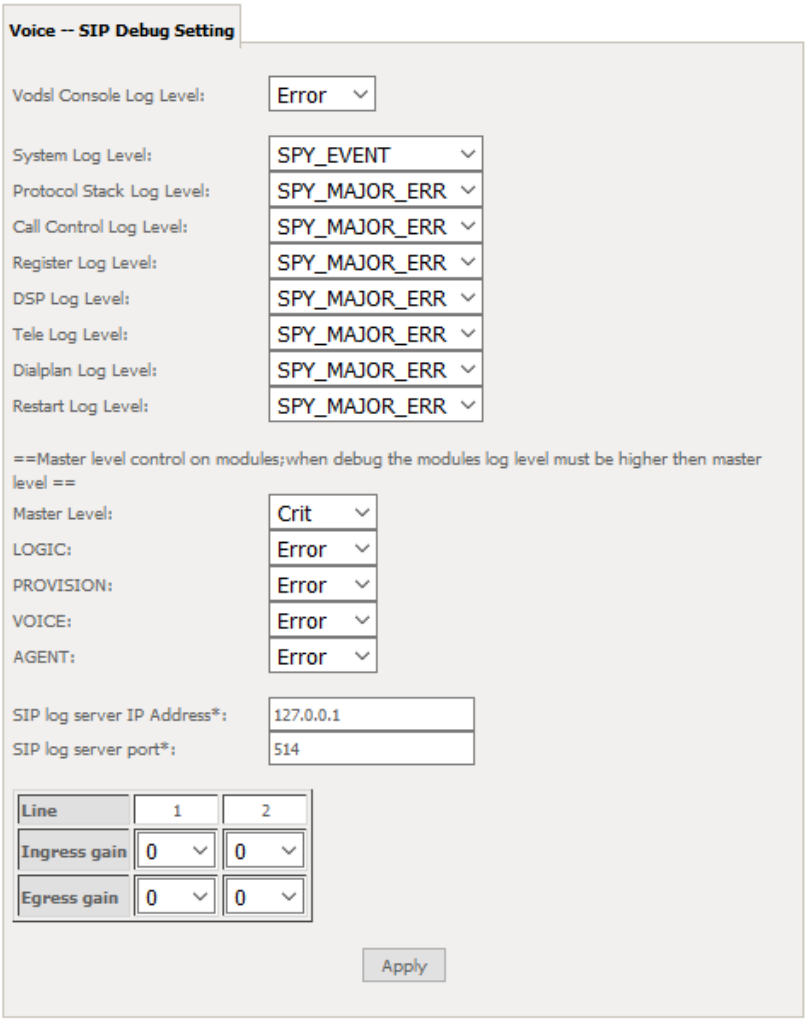
SIP Star Code Setting

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.



SIP Debug Setting

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



OPTION	DEFINITION
SIP Log Server IP Address	Enter the IP address where the SIP Log data for the router's currently saved VoIP account settings will be sent to.
SIP Log Server port	Enter the port to be used for transmitting the SIP Log data for the router's currently saved VoIP account settings.
Ingress Gain	The incoming signal amplitude can be controlled with this field. Combined with the Egress gain a ratio can be expressed of input to output. The Ingress Gain setting can help improve the quality of the VoIP line, and can influence call volumes and help eliminate echoes.
Egress Gain	The outgoing signal amplitude can be controlled with this field. Combined with the Ingress gain a ratio can be expressed of input to output. The Egress Gain setting can help improve the quality of the VoIP line, and can influence call volumes and help eliminate echoes.

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 signaling 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 dialing, 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 whom you are.

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.

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.

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 dialed the whole number.

Call Hold

Call hold enable you to put a call to a pending state, and pick it up in future.

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.

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.

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.

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.

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.

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.

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.

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.

T38 Faxing

To make T38 faxing, enable T38 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 T38 mode, and use it as the transmit approach.

Pass-Through Faxing

If T38 support is disabled, faxing uses normal voice codec as its coding approach. Therefore, this mode is more like normal phone calls.

Diagnostics

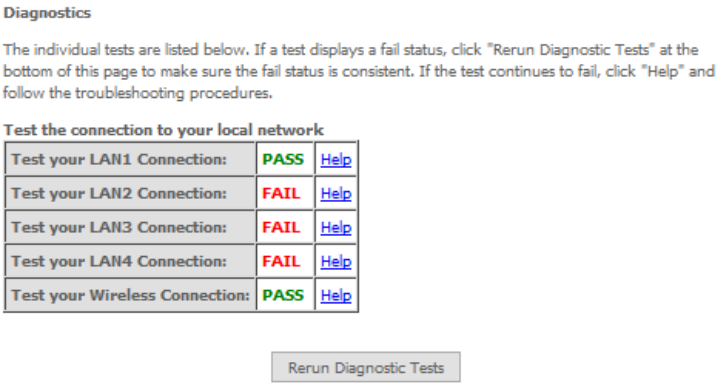
This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click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

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

Diagnostics

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

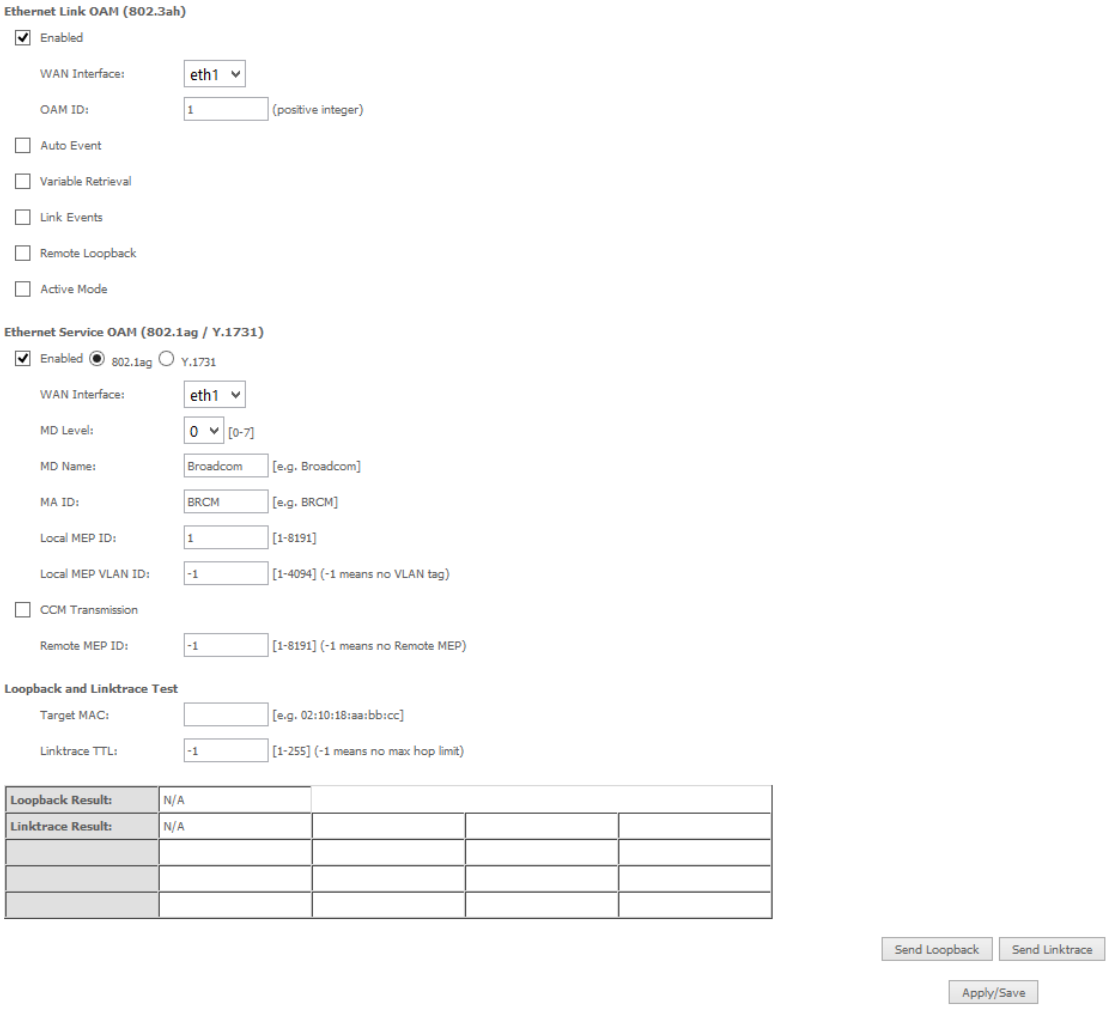
1. Click on the **Help** link and follow the troubleshooting procedures in the Help screen that appears.
2. Now click **Rerun Diagnostic Tests** at the bottom of the screen to re-test and confirm the error.
3. If the test continues to fail, contact Technical Support.



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.
Test your Wireless Connection	Pass: Indicates that the wireless card is switched ON. Fail: Indicates that the wireless card is switched OFF.

Ethernet OAM

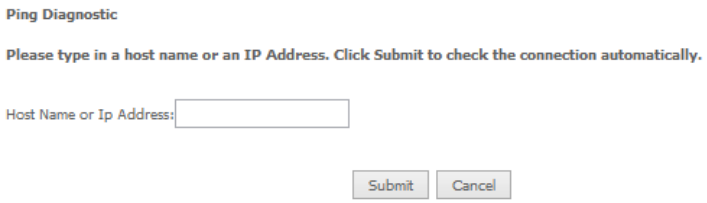
The Ethernet OAM page provides administrators with operation, administration and management features.



Diagnostics

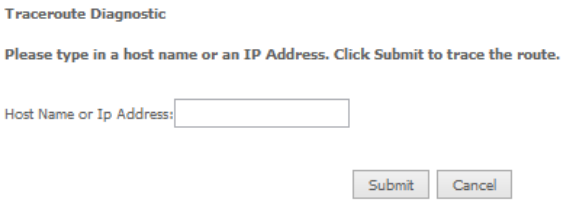
Ping

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



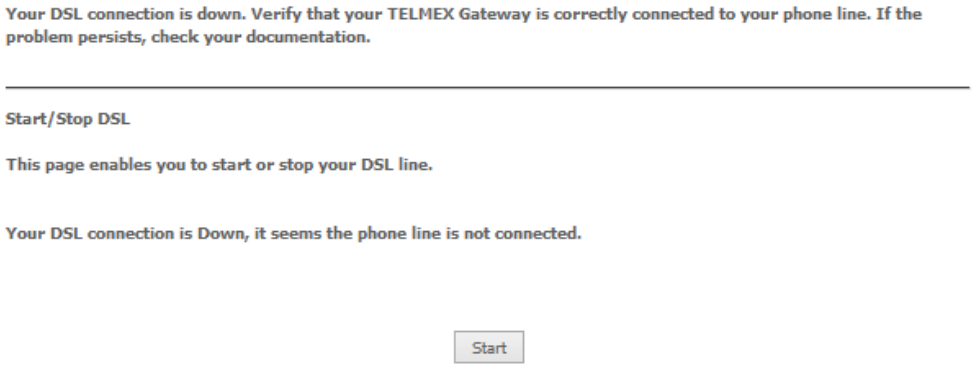
Traceroute

The Traceroute page lets you perform a trace route to a remote IP address or host name.



Start/Stop DSL

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



Management

Settings

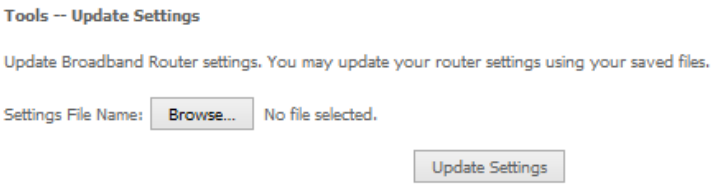
The Settings screens allow you to back up, retrieve and restore the default settings of your Router. It also provides a function for you to update your router's firmware.

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.

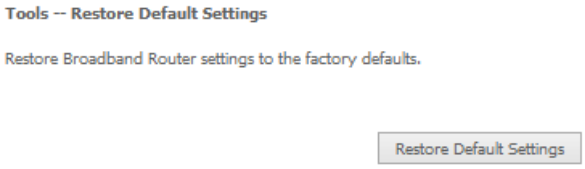
Update Settings

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



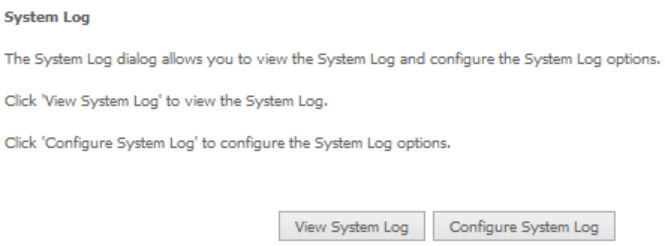
Factory Reset

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.

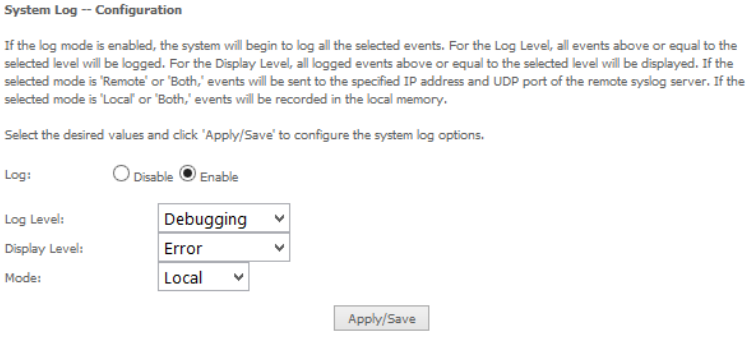


System Log

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.



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.

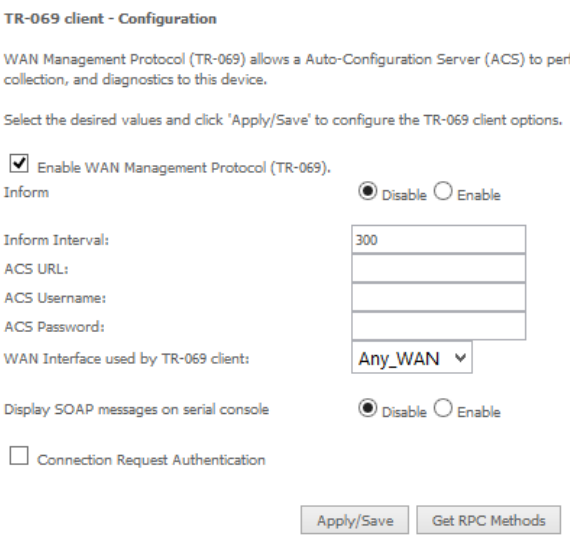


SNMP Agent

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 NF1ADV (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.

TR-069 Client

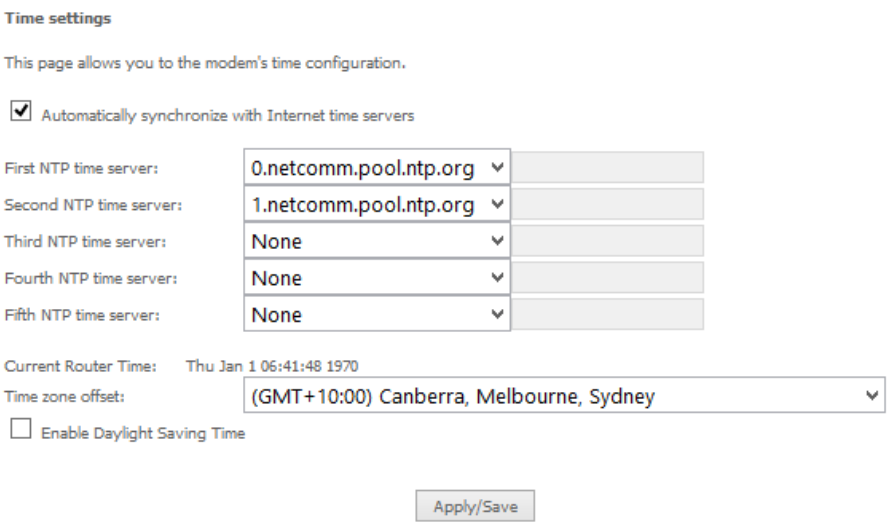
TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router if supported by your Internet Service Provider (ISP).



FIELD	DESCRIPTION
Inform	Set to enable to activate TR-069 client settings.
Inform interval	Time in seconds that 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 connection used to send and receive data to the ACS server.

Internet Time

The Internet Time page allows you to configure NTP time servers that the NF10WV router synchronises with in order to keep accurate time.



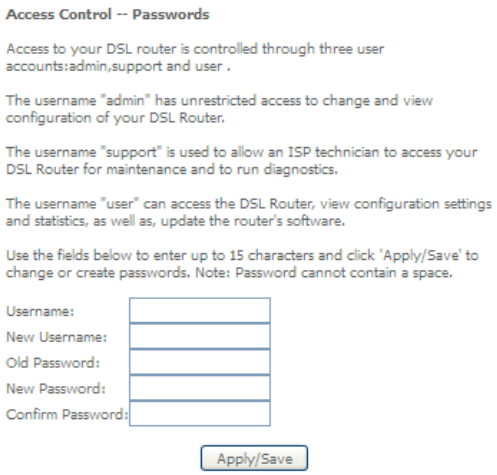
Access Control

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

- Passwords
- Services Control

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

Access Controls – Passwords



Usernames – The Username used determines the level of access to the device.
There are three usernames and three levels of access:

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

The username **admin** can be changed. Your new 'admin' username can contain up to 15 characters and cannot contain spaces. The usernames **support** and **user** cannot be changed.

Passwords – Initially the Password for each type of Username is the same word as the initial Username:

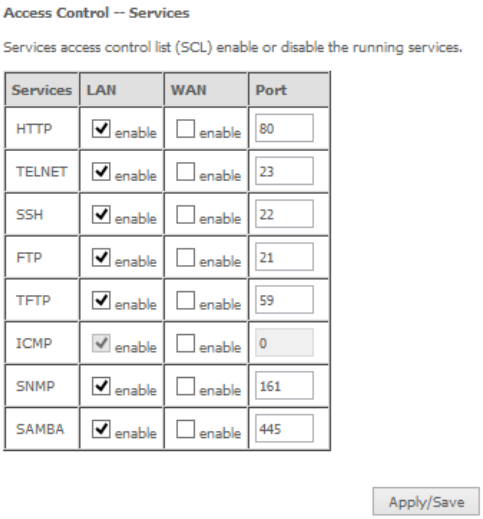
INITIAL USERNAME	INITIAL PASSWORD
admin	admin
support	support
user	user

The Password for each type of Username can be changed.
Passwords must be 15 characters or less with no spaces.
To change the password for a username:

1. Enter the current Username into both the **Username** and **New Username** fields (for the **admin** username only you can enter a different **New Username**).
2. Enter the **Old Password**
3. Enter the **New Password** (it must be 15 characters or less with no spaces).
4. Enter the same password into the **Confirm Password** field.
5. Click the **Apply/Save** button

Access Controls -- Services

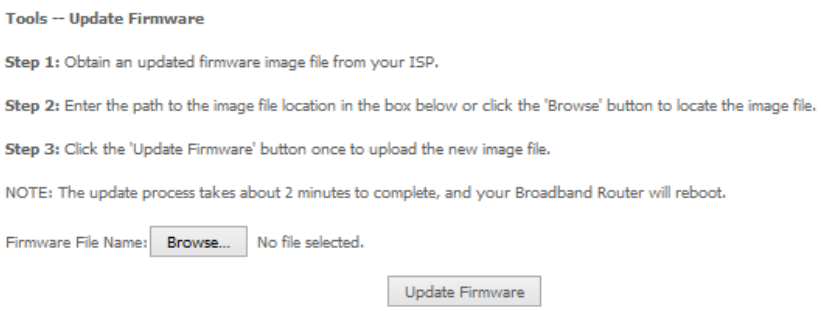
The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP. Click the **Apply/Save** button after making any changes to continue.



Update Firmware

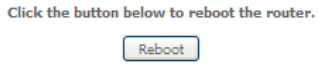
The following screen appears when selecting the Update Software option from the **Management** menu. By following this screen's steps, you can update your modem's firmware. Manual device upgrades from a locally stored file can also be performed using the following screen.

1. Obtain an updated software image file.
2. Enter the path and filename of the firmware image file in the Software File Name field or click the **Browse** button to locate the image file.
3. Click the **Update Software** button once to upload and install the file.



Reboot

This option reboots the NF10WV.



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.

NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 7 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 NF10WV 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 NF10WV 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 wireless adapter documentation for instructions on establishing a wireless connection.

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NF10WV 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 NF10WV and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF10WV off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

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 NF10WV'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 holding the reset button down for 7 seconds or until the LEDs turn off. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

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. (Steps may vary depending on the version of your Internet browser.)

Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Hold the Reset button down for 7 seconds or until all the LEDs turn off. The NF10WV restarts with factory default settings. 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.

WLAN Interface

I cannot access the NF10WV from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the Wi-Fi 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 NF10WV and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

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 NF10WV 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 NF10WV 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 NF10WV 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.

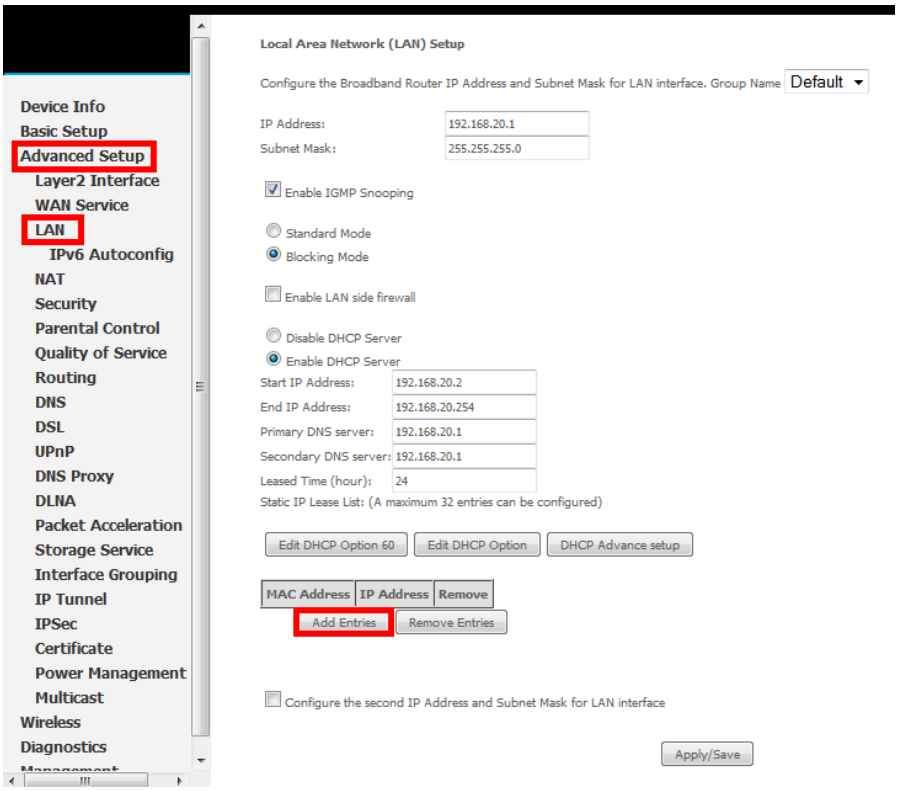
Reserving IP addresses

It is necessary to reserve an IP address for each of the devices connecting to the NF10WV router so that QoS settings can be managed for each device.

a) Navigate to http://192.168.20.1 in a web browser.

b) When prompted, enter `admin` as both the username and password.

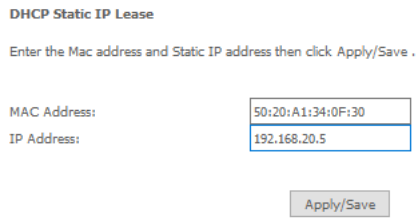
c) Select **Advanced Setup > LAN**



d) Click the **Add Entries** button.

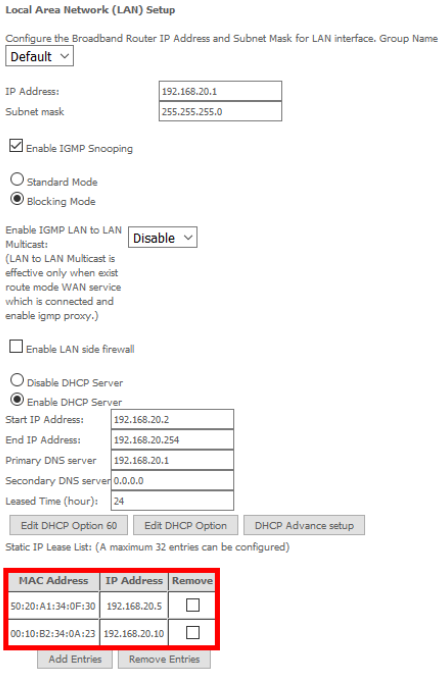
e) Enter the MAC address of the computer/device you are connecting to the router. The MAC address is a 12 character set of numbers and letters (A-F), with every 2 characters separated by a colon.

f) 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.



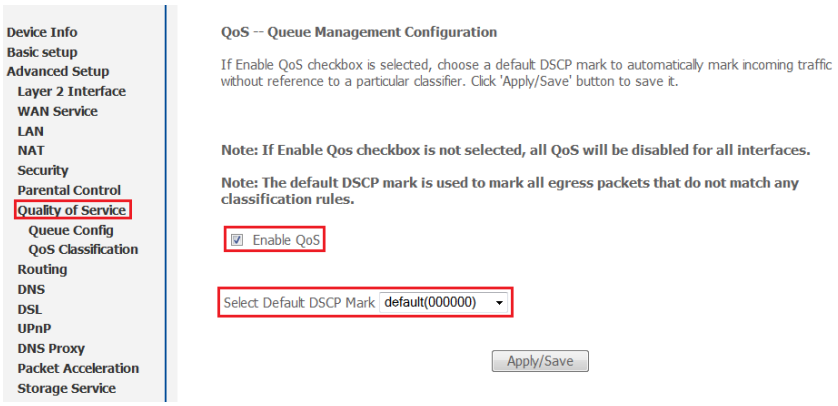
g) Click the **Apply/Save** button.

h) Complete steps d) through g) for each device connected to the NF10WV router. Each entry will be listed in the Static IP Lease List as shown below.



QoS Configuration Settings

a) Select **Advanced Setup > Quality of Service**



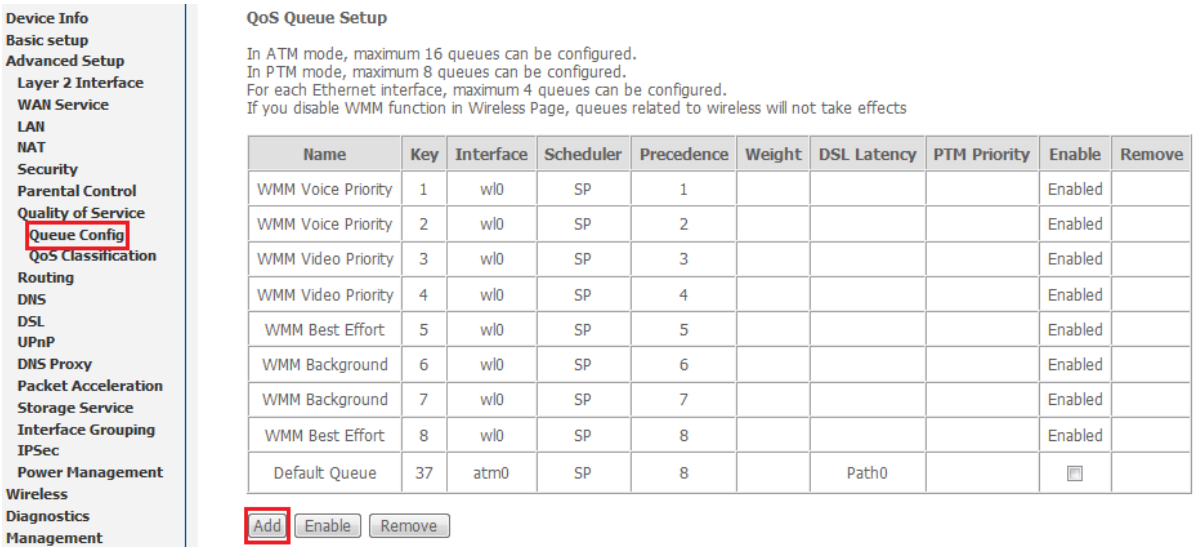
b) Select the **Enable QoS** option.

c) Select the **Default DSCP Mark** as **default(000000)**.

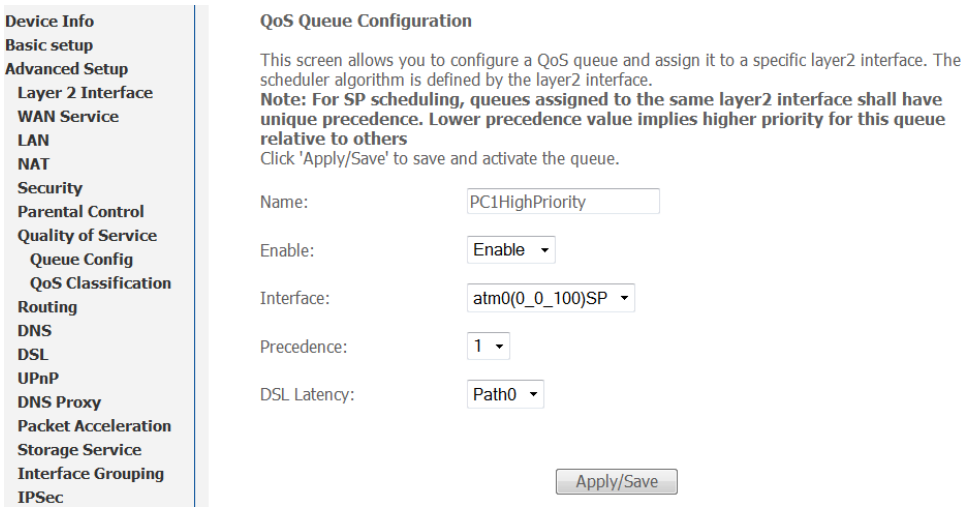
d) Click the **Apply/Save** button.

High Priority QoS Queue Configuration

a) Select **Advanced > Quality of Service > Queue Config**.



b) Click the **Add** button.



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

d) Set the Enable option to **Enable**.

e) Set the Interface (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0)100)**).

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

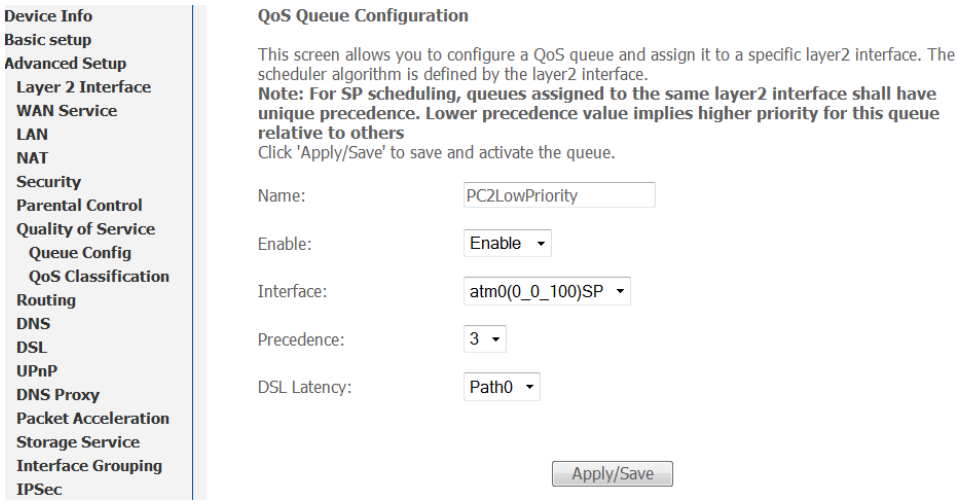
g) Set the **DSL Latency** as **Path0**.

h) Click the **Save/Apply** button.

Low Priority QoS Queue Configuration

a) Select **Advanced > Quality of Service > Queue Config**.

b) Click the **Add** button.



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

d) Set the Enable option to **Enable**.

e) Set the Interface (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0)100)**).

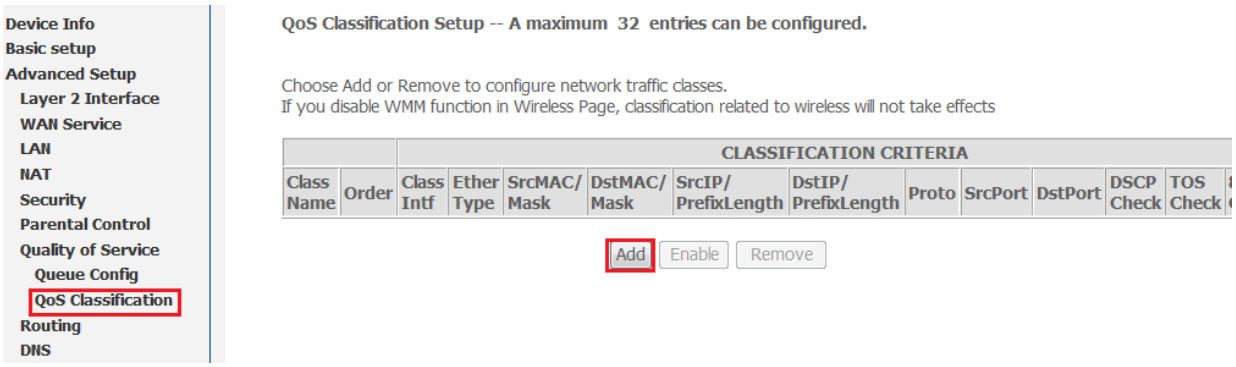
f) Enter a **Precedence**. For the lowest priority, set it to **3**. For the highest priority use **1**.

g) Set the **DSL Latency** as **Path0**.

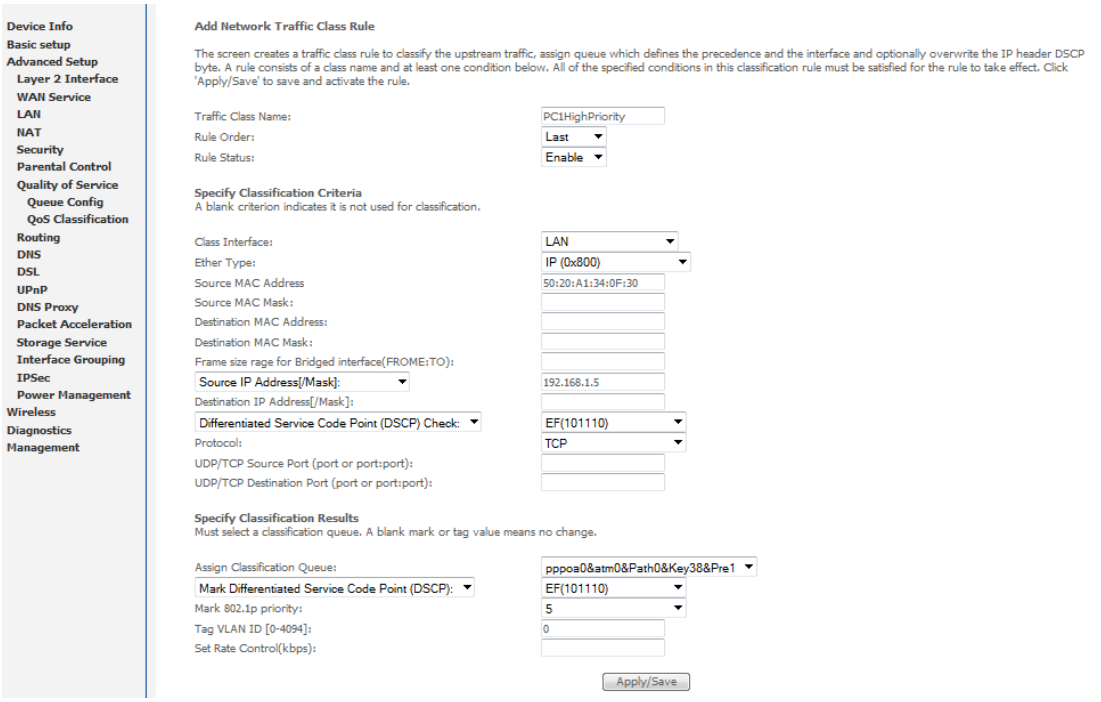
h) Click the **Save/Apply** button.

High Priority QoS Classification

a) Select **Advanced > Quality of Service > QoS Classification**.



b) Click the **Add** button.



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

d) Leave the **Rule Order** as **Last**.

e) Set the **Rule Status** to **Enable**.

f) 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**.

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

h) 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.

i) 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.

j) 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.

k) 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.

l) 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.

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

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

o) 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.

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

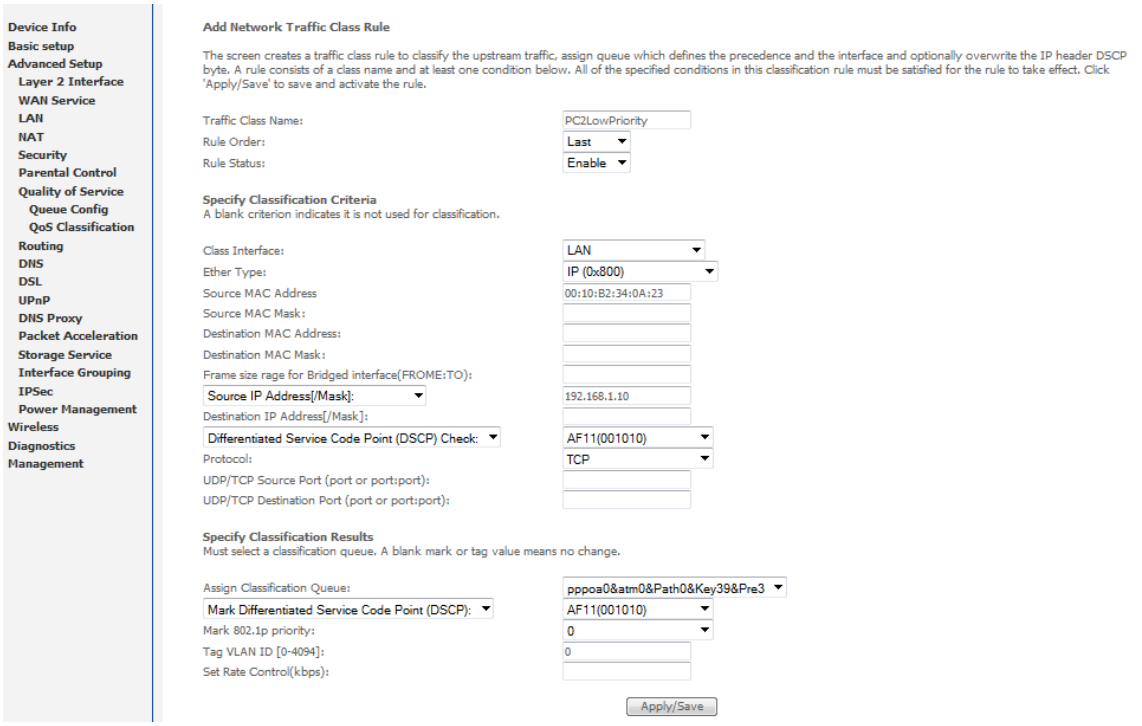
q) Set **Mark 802.1p Priority** as **5**. In the scale 0-7, 0 is best effort, 6 and 7 are reserved for networking performance so set 5 as the highest priority.

r) Click the **Apply/Save** button.

Low Priority QoS Classification

a) Select **Advanced > Quality of Service > QoS Classification.**

b) Click the **Add** button.



c) Enter a **Traffic Class Name** reflecting the High Priority QoS rule; eg. **PC2LowPriority.**

d) Leave the **Rule Order** as **Last**.

e) Set the **Rule Status** to **Enable**.

f) 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**.

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

h) 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.

i) 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.

j) 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.

k) 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.

l) 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.

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

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

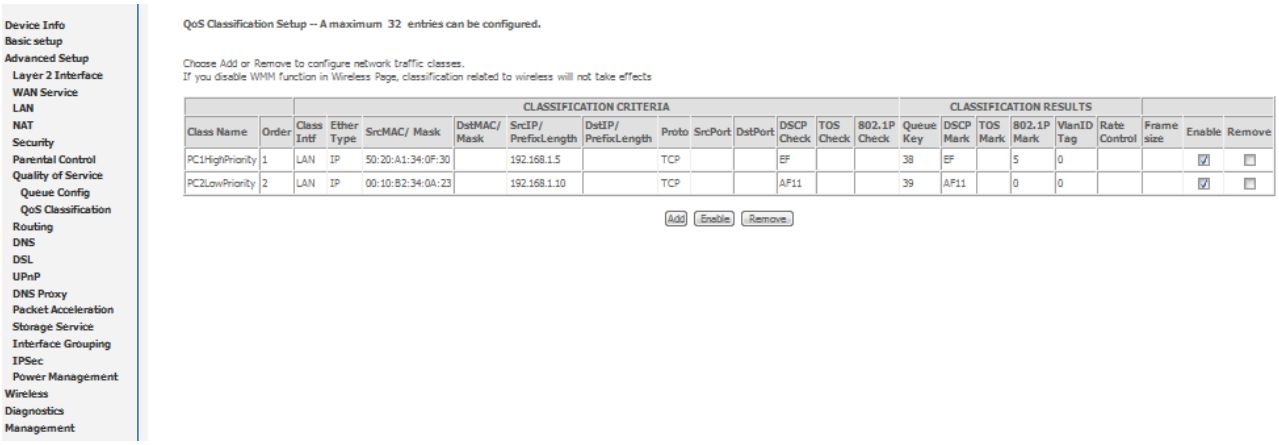
o) Set "**Assign Classification Queue**" to Priority 3 (in the example above pppoa0&atm0&Path0&Key39&Pre3). Other options are priority 1 and 2. Priority 1 gives the highest priority with priority 3 being the lowest.

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

q) 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.

r) Click the **Apply/Save** button.

s) You now have 2 Quality of Service rules implemented for 2 devices connecting to the NF10WV router.



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

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

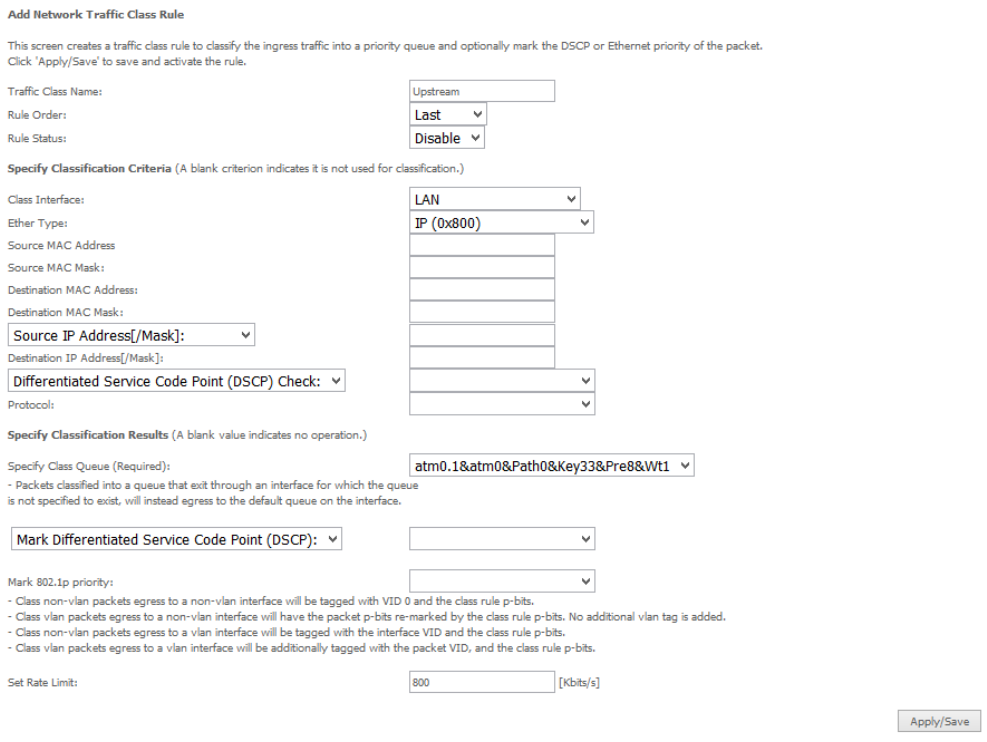
Limiting the upstream rate

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

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

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

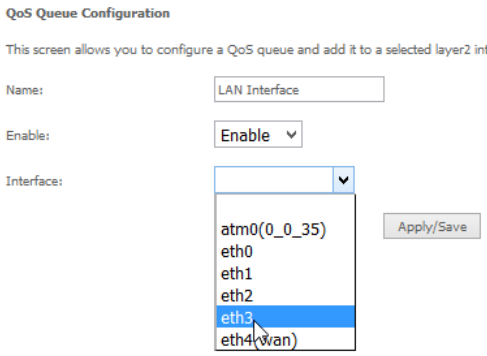
Classification Criteria:
Class Interface: LAN
Ether type: IP
Classification Results:
Class Queue: the queue that was enabled in Step 1
Set rate-limit: set according to your preference



c) Click **Apply/Save.**

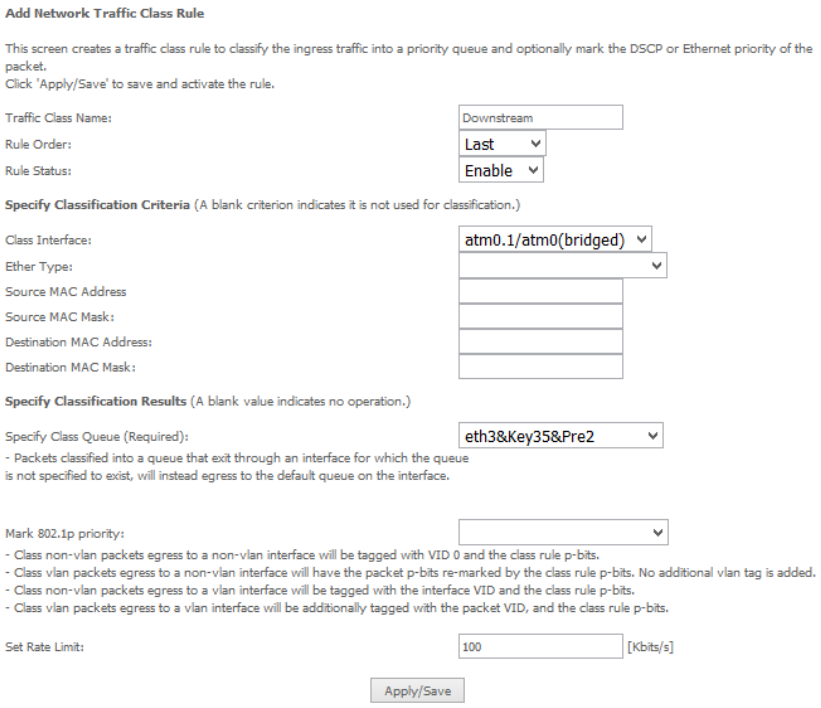
Limiting the downstream rate

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



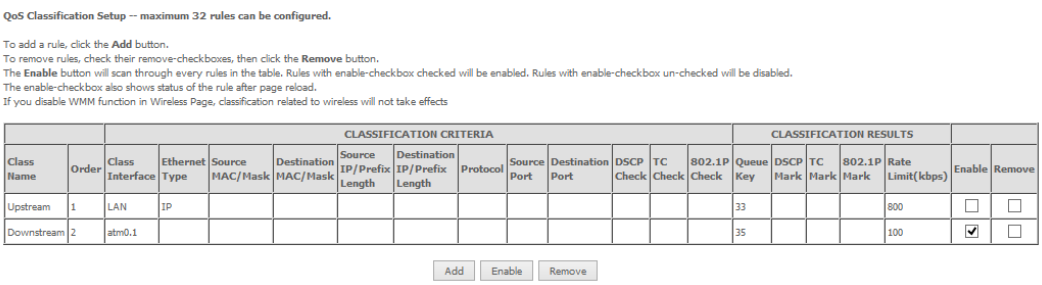
b) On the QoS Classification page, add a rule to limit the downstream rate, for example:

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



c) Click **Apply/ Save**

The QoS Classification table looks like this:



Legal & Regulatory Information

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out this Manual are owned by and vest in NetComm Wireless (ACN 002490486) (NetComm Wireless Limited) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited's (or its licensors') intellectual property rights to you.
You are permitted to use this Manual for the sole purpose of using the NetComm Wireless product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Wireless Limited.
NetComm, NetComm Wireless and NetComm Wireless Limited are a trademark of NetComm Wireless Limited. All other trademarks are acknowledged to be the property of their respective owners.

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