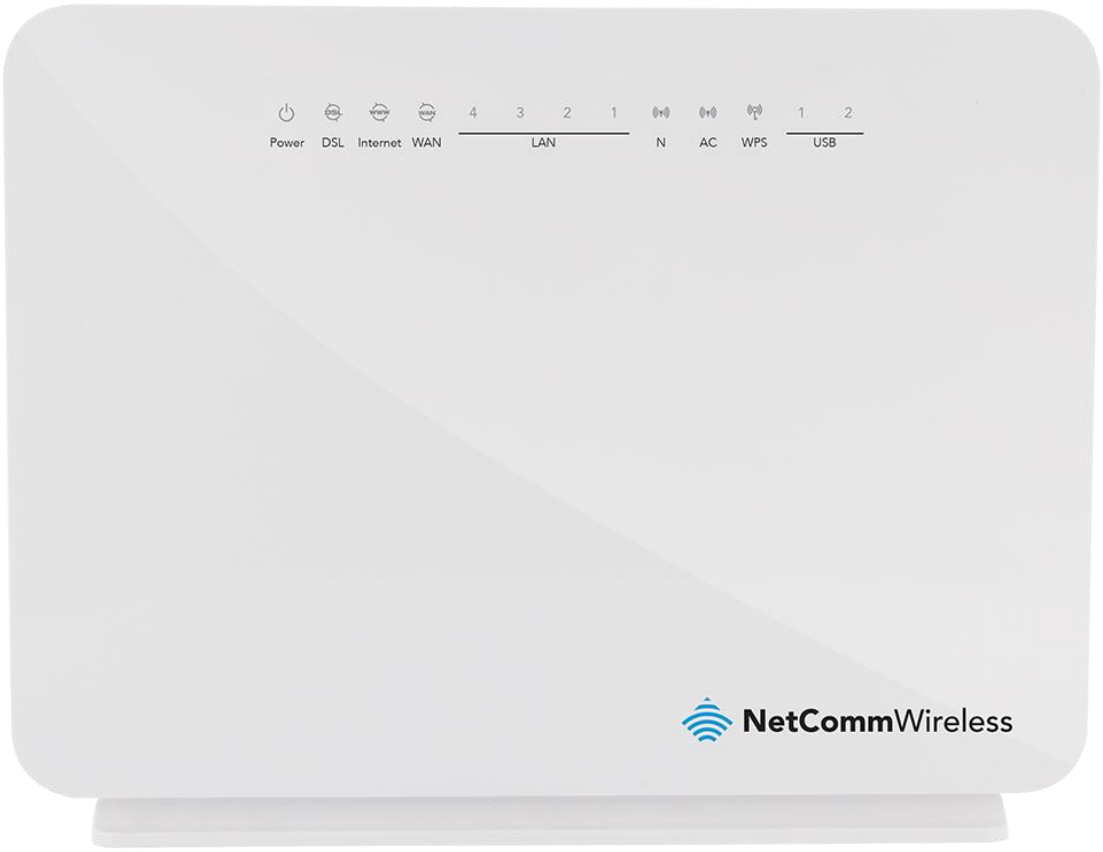
NetCommWireless

VDSL/ADSL AC1600 WiFi Gigabit Modem Router



NF8AC

USER GUIDE

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 NF8AC VDSL/ADSL AC1600 WiFi Gigabit Modem Router

DOCUMENT VERSION	DATE
1.0 - Initial document release	September 2014
1.1 – Added more QoS examples	25 November 2015

Table 1 - Document Revision History

NetCommWireless

Table of Contents

Overview

Introduction

This manual provides information related to the installation, operation, and use of the NF8AC.

Target Users

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 NF8AC, please confirm that you comply with the minimum system requirements below.

- An activated ADSL or configured WAN connection.
- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- A Web Browser such as Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari etc.
- Wireless Computer System Requirements:
  - Computer with a working 802.11b, 802.11g, 802.11n or 802.11ac wireless adapter.

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.

Product Introduction

Product Overview

- Fully featured VDSL2 / ADSL2+ Modem Router
- 1 x 10/100/1000 Gigabit Ethernet WAN port for connection to fibre services
- 4 x 10/100/1000 Gigabit Ethernet LAN ports for wired connections
- Wireless AC1600 Access Point for multiple high speed WiFi connections
- 2 x USB host ports – supports USB storage device for file sharing
- Built-in media server. Just add a USB hard drive
- NBN ready: carefully developed hardware and software features to ensure this device is optimised for use on the National Broadband Network:
  - Wireline Routing Speeds
  - IGMP Snooping
  - IPTV IGMP V1 V2 Pass through
  - QoS
- IPv6 ready for the next generation IP addressing
- WPS button for simple setup of your wireless network

Package Contents

The NF8AC package consists of:

- 1 x NetComm Wireless NF8AC VDSL/ADSL AC1600 WiFi Gigabit Modem Router
- 1 x Quick start guide
- 1 x 1.5m RJ-45 Ethernet cable
- 1 x WiFi security card
- 1 x Warranty card
- 1 x Power supply (12V/2A)
- 1 x RJ-11 Telephone cable

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 LAN Ethernet 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, smart phones, gaming consoles, tablets and PCs. The four Gigabit LAN 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, 802.11n and 802.11ac specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

.

Physical Dimensions and Indicators

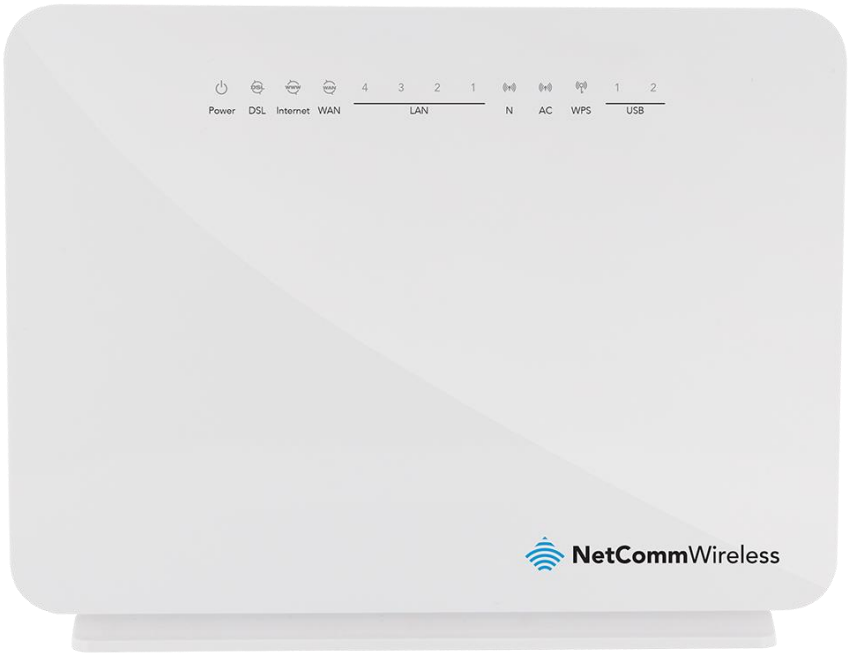
LED Indicators

The NF8AC 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 NF8AC 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 NF8AC is powered on and operating normally.
		Red	The NF8AC is starting up.
		Red Blinking	The firmware is being upgraded.
		Off	The power is off.
DSL		Off	No DSL signal detected.
		Green Blinking (Slow)	Data is being transferred over the DSL line.
		Green Blinking (Fast)	The NF8AC is attempting to connect to the xDSL service.
		Green	The DSL connection is established.
Internet		Green	The NF8AC is connected to an internet service.
		Red	Authentication on the broadband account has failed.
		Green Blinking	Data is being transmitted to or from the internet.
		Off	The NF8AC 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.
N		Green	2.4GHz WiFi is enabled.
		Green Blinking	Data is being transmitted to or from the 2.4GHz Wireless interface.
		Off	WiFi is disabled.
AC		Green	5GHz WiFi is enabled.
		Green Blinking	Data is being transmitted to or from the 5GHz Wireless interface.
		Off	WiFi is disabled.
WPS		Green	The client has successfully connected to the router.
		Green Blinking	The client is accessing the router via WPS.
		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

The following page lists the physical dimensions of the NF8AC.



190 mm (L) x 146 mm (W) x 33 mm

NF8AC DIMENSIONS	
Length	190 mm
Height	146 mm
Depth	33 mm
Weight	361 grams

NF8AC Default Settings

The following tables list the default settings for the NF8AC.

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

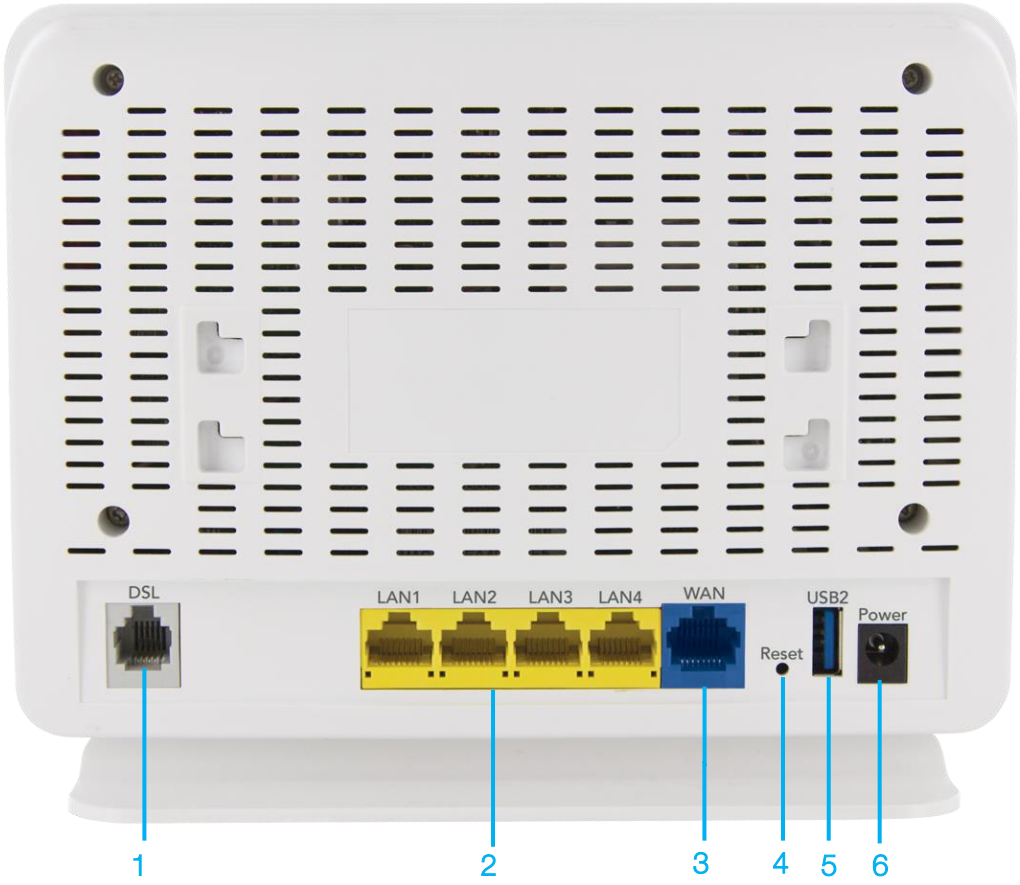
WIRELESS (WIFI)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA2-PSK (AES)
Security Key	(Refer to the included Wireless Security Card)

NF8AC WEB INTERFACE ACCESS	
Username	admin
Password	admin

Interfaces

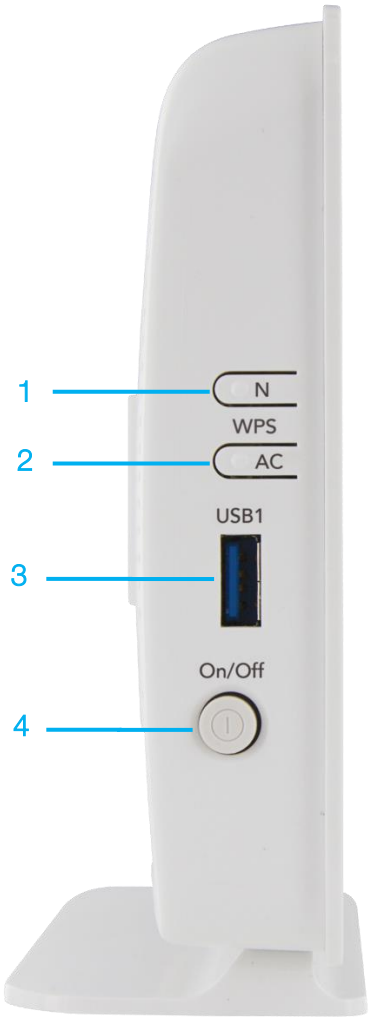
Rear

The following interfaces are available on the NF8AC:



NUMBER	INTERFACE	DESCRIPTION
1	DSL	Use the provided RJ-11 cable to connect the router to the telephone line operating your xDSL service.
2	Ethernet 1 - 4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
3	WAN	Gigabit WAN port for connection to a WAN network.
4	Reset button	Activate the Reset function by holding the Reset button down for 3 seconds.
5	USB 2	Connect an external USB hard drive here to use the NAS feature of the NF8AC.
6	Power	Connection point for the included power adapter. Connect the power supply here.

Left



NUMBER	INTERFACE	DESCRIPTION
1	WPS N	Activate the WPS function for the 2.4GHz network by holding the WPS button down for 3 seconds.
2	WPS AC	Activate the WPS function for the 5GHz network by holding the WPS button down for 3 seconds.
3	USB 1	Connect an external USB hard drive here to use the NAS feature of the NF8AC.
4	Power	Turns the NF8AC on or off.

Safety and Product Care

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water to avoid fire or shock hazard. For example, near a bathtub, kitchen sink, laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.

WARNING
Disconnect the power line from the device before servicing.

Transport and Handling

When transporting the NF8AC, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.

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 NF8AC

Placement of your NF8AC

The wireless connection between your NF8AC and your WiFi devices will be stronger the closer your connected devices are to your NF8AC. Your wireless connection and performance will degrade as the distance between your NF8AC and connected devices increases. 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 NF8AC 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 checklist may help.

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF8AC, please try the following steps:

- In multi-storey homes, place the NF8AC on a floor that is as close to the centre of the home as possible. This may mean placing the NF8AC on an upper floor.
- Try not to place the NF8AC near a cordless telephone that operates at the same radio frequency as the NF8AC (2.4GHz).

Avoid obstacles and interference

Avoid placing your NF8AC 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 NF8AC).

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 NF8AC 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 NF8AC.
- 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 NF8AC to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose 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. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

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 NF8AC.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF8AC to power up.

Connecting via a cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NF8AC.
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 NF8AC.

Connecting wirelessly

1. Ensure Wi-Fi 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 NF8AC.

Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF8AC

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF8AC.
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 NF8AC.

Web Based Configuration Interface

First-time Setup Wizard

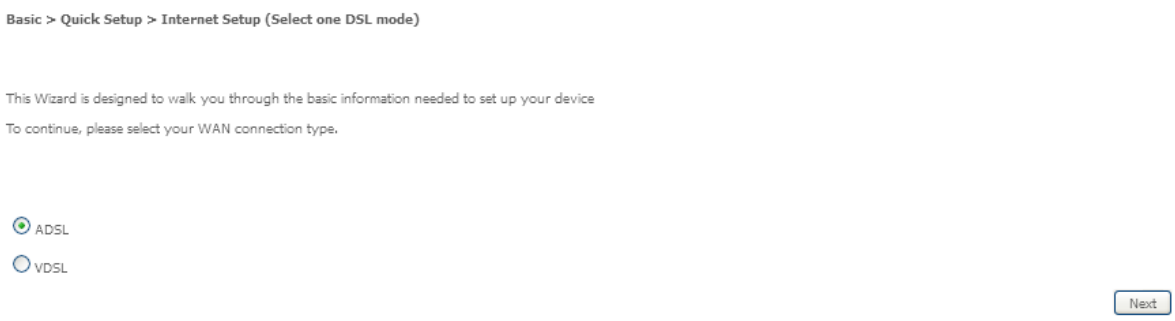
Please follow the steps below to configure your NF8AC Wireless router via the web based configuration wizard.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) 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.

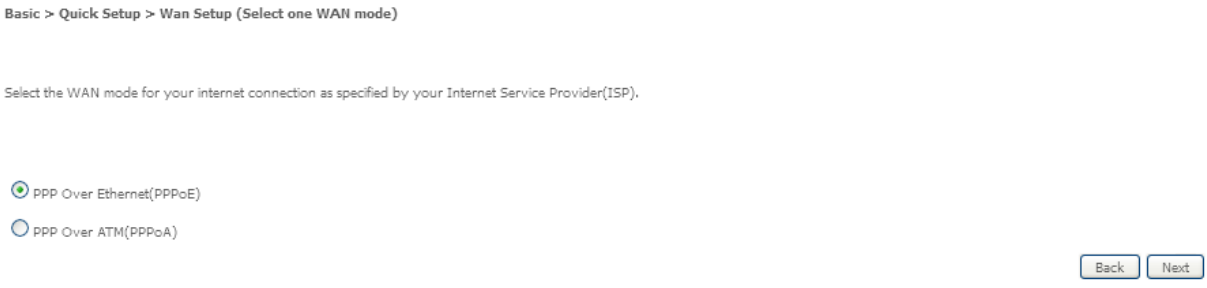
Note: `admin` is the default username and password for the unit.

1. Click on **Basic Setup** on the left side of the screen. The wizard assists you in configuring the router and entering the information required to setup your Internet connection.
2. Select either **VDSL** or **ADSL** depending on your connection type and click **Next**.

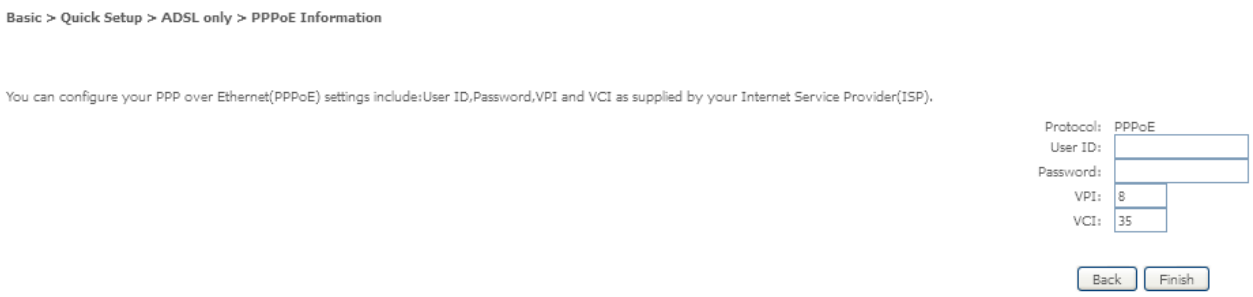


ADSL:

3. Select either **PPP over Ethernet (PPPoE)** or **PPP over ATM (PPPoA)** depending on your Internet Service Provider's requirements. Click **Next**.

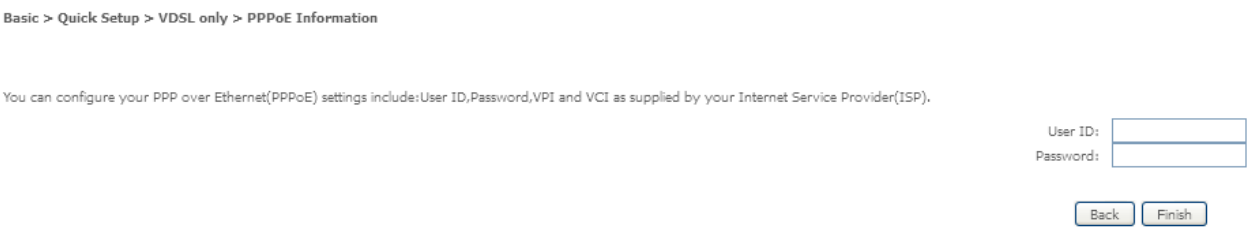


4. In the Username and Password fields, enter the username and password supplied to you by your Internet Service Provider (ISP). If required by your ISP, you may also adjust the VPI and VCI figures here. Click the **Finish** button when you have entered the required information.



VDSL:

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

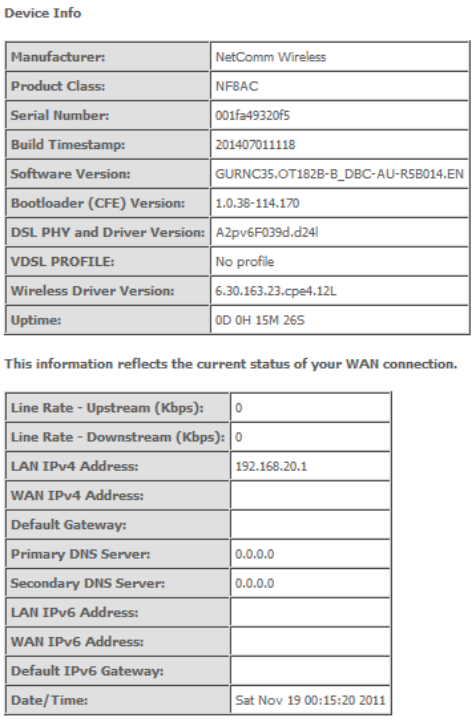


6. Click the **Finish** button when you have entered the required details.

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:	NF8AC
Serial Number:	001fa49320f5
Build Timestamp:	201407011118
Software Version:	GURNC35.OT182B-B_DBC-AU-R5B014.EN
Bootloader (CFE) Version:	1.0.38-114.170
DSL PHY and Driver Version:	A2pv6F039d.d24l
VDSL PROFILE:	No profile
Wireless Driver Version:	6.30.163.23.cpe4.12L
Uptime:	0D 0H 15M 26S

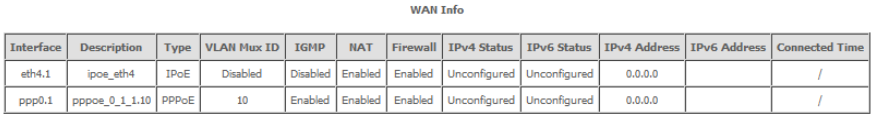
This information reflects the current status of your WAN connection.

Line Rate - Upstream (Kbps):	0
Line Rate - Downstream (Kbps):	0
LAN IPv4 Address:	192.168.20.1
WAN IPv4 Address:	
Default Gateway:	
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0
LAN IPv6 Address:	
WAN IPv6 Address:	
Default IPv6 Gateway:	
Date/Time:	Sat Nov 19 00:15:20 2011

ITEM	DEFINITION
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.
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.
WAN IPv4 Address	The current version 4 WAN IP address assigned to the router.
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 Address	The current IPv6 LAN IP address in use if assigned.
WAN IPv6 Address	The current IPv6 WAN 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

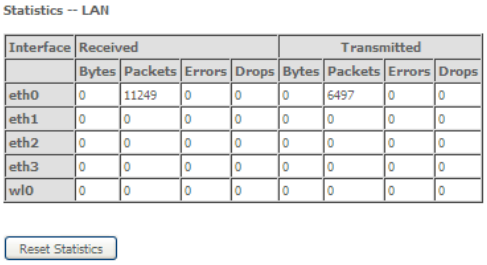
Interface	Description	Type	VLAN Mux ID	IGMP	NAT	Firewall	IPv4 Status	IPv6 Status	IPv4 Address	IPv6 Address	Connected Time
eth4.1	ipoe_eth4	IPoE	Disabled	Disabled	Enabled	Enabled	Unconfigured	Unconfigured	0.0.0.0		/
ppp0.1	pppoe_0_1_1.10	PPPoE	10	Enabled	Enabled	Enabled	Unconfigured	Unconfigured	0.0.0.0		/

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.
IGMP	Details the status of IGMP on each WAN connection. IGMP is only used with IP v4 connections.
NAT	The NAT status of the WAN connection.
Firewall	The status of the router firewall across the WAN connection.
IPv4 Status	The status of the IPv4 WAN connection.
IPv6 Status	The status of the IPv6 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

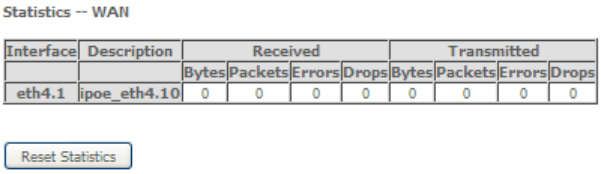
Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
eth0	0	11249	0	0	0	6497	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

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.



Statistics -- WAN

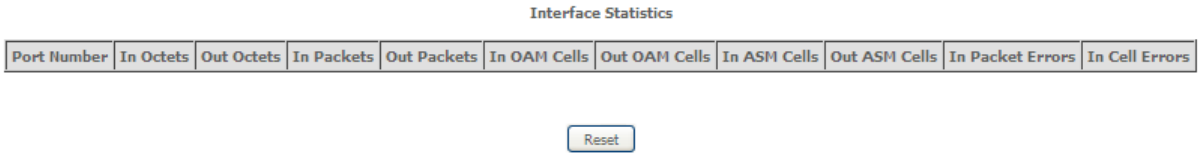
Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
eth4.1	ipoe_eth4.10	0	0	0	0	0	0	0	0

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 – xTM

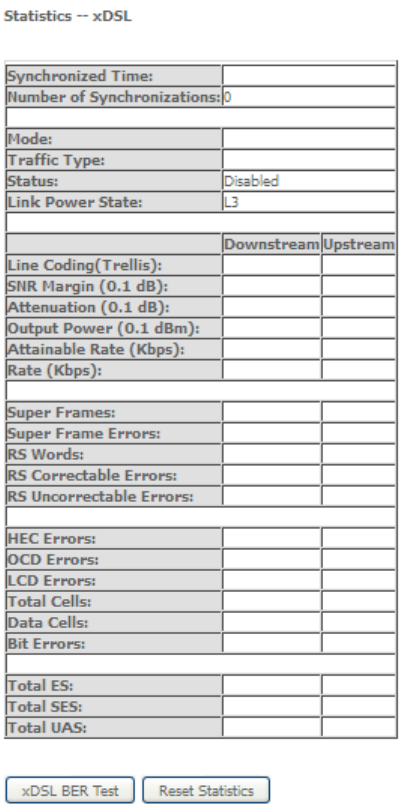
The Statistics – xTM page shows details related to the xTM interface of the router.



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.

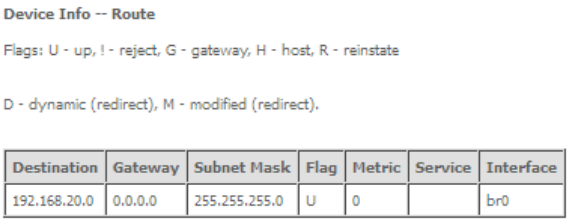
Statistics – xDSL

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



Route

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



Device Info -- Route

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

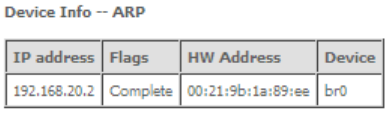
D - dynamic (redirect), M - modified (redirect).

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 ARP 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.

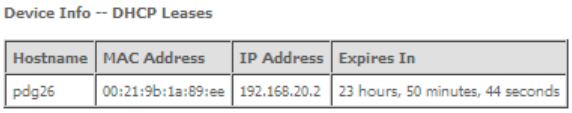


Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.20.2	Complete	00:21:9b:1a:89:ee	br0

DHCP

Click DHCP to display the DHCP information.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
pdg26	00:21:9b:1a:89:ee	192.168.20.2	23 hours, 50 minutes, 44 seconds

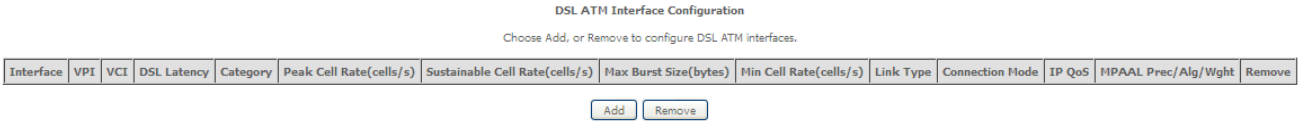
You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

Advanced Setup

Layer2 Interface

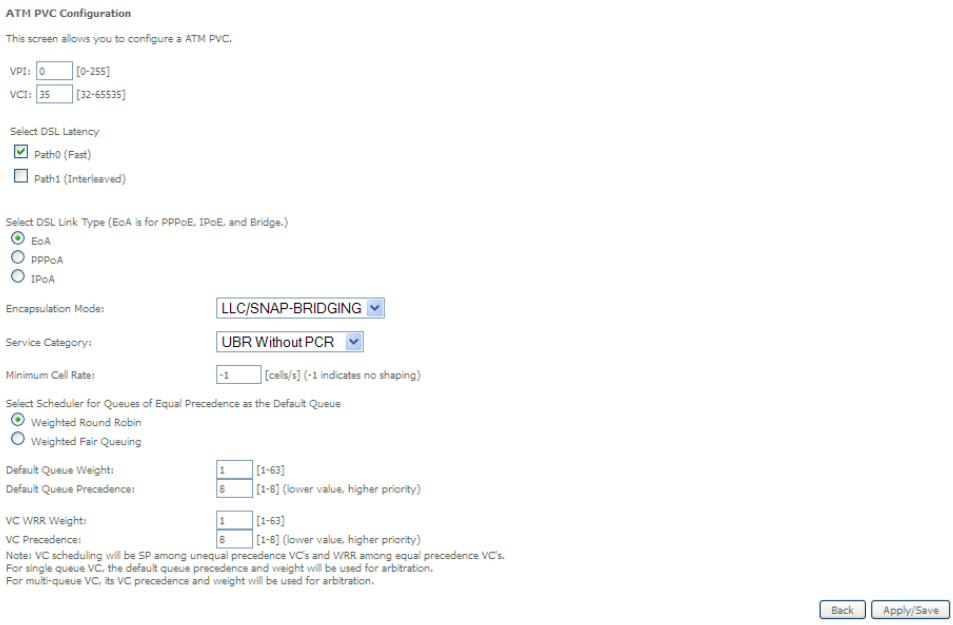
ATM Interface

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



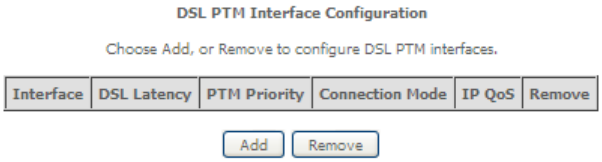
FIELD	DESCRIPTION
Interface	This field shows the interface name.
VPI	This field shows the Virtual Path Identifier (VPI) value. For most Australia connections the VPI is 8, for most new Zealand connections the VPI is 0.
VCI	This field shows the Virtual Channel Identifier (VCI) value. For most Australia connections the VCI is 35, for most new Zealand connections the VCI is 100.
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.

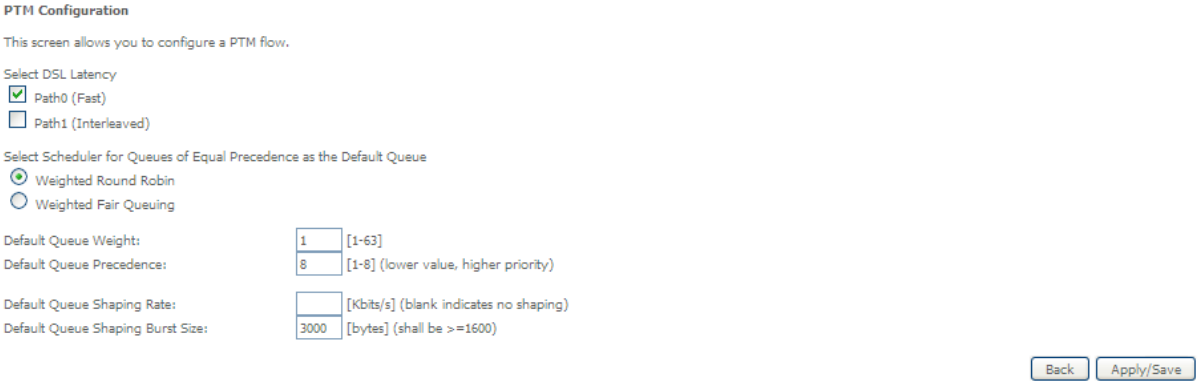


PTM Interface

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.

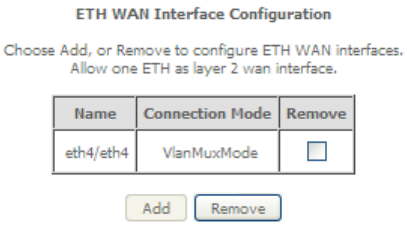


Click the **Add** button to create a new PTM interface. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.



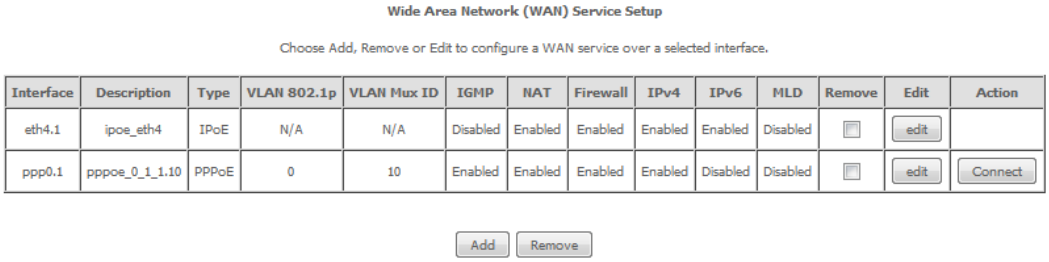
ETH Interface

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

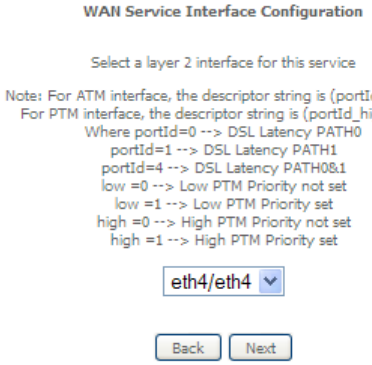


WAN Service

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.



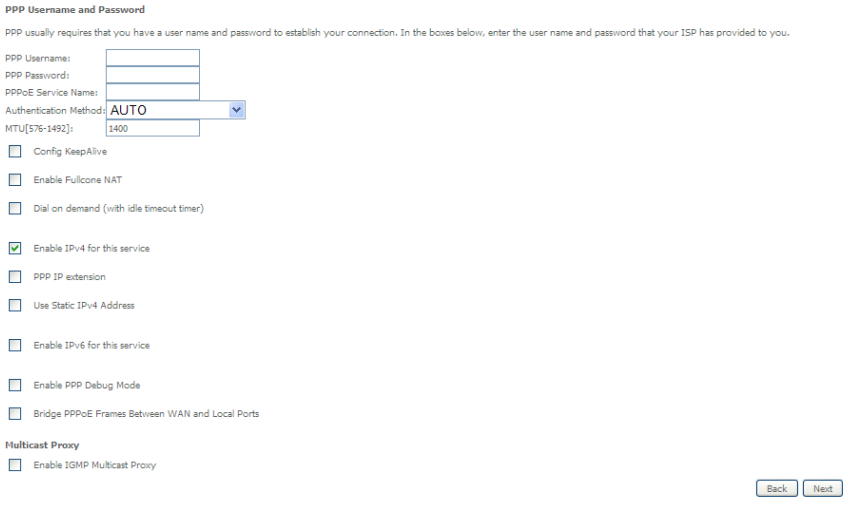
To add a WAN service, click the **Add** button. Use the drop down list to select the layer 2 interface to use for the WAN service and click the **Next** button.



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

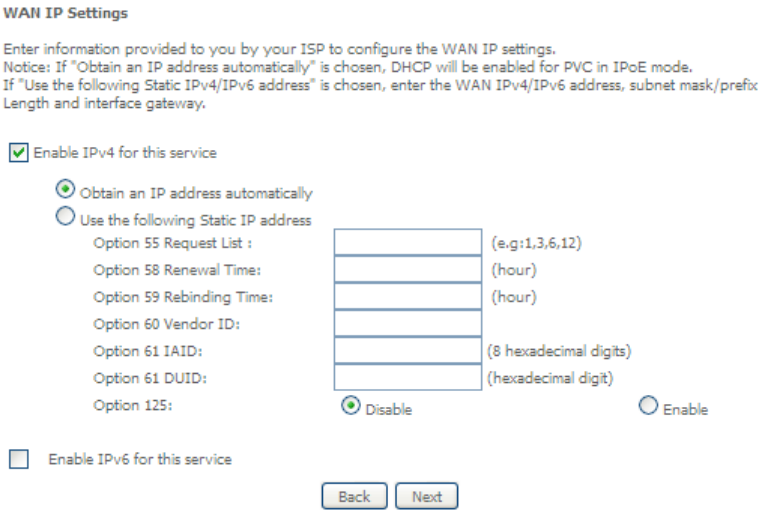
PPP over Ethernet

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

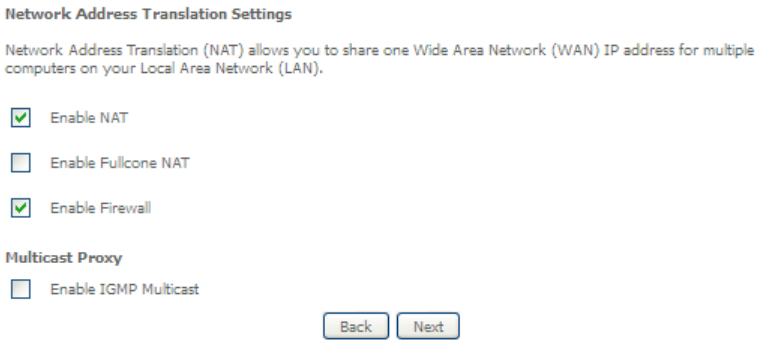


IP over Ethernet

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

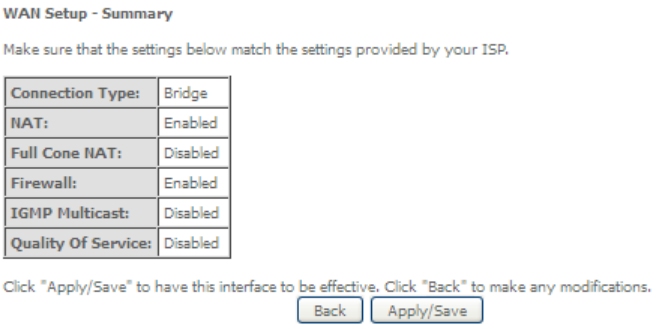


Select the NAT Translation settings as desired and click the **Next** button.

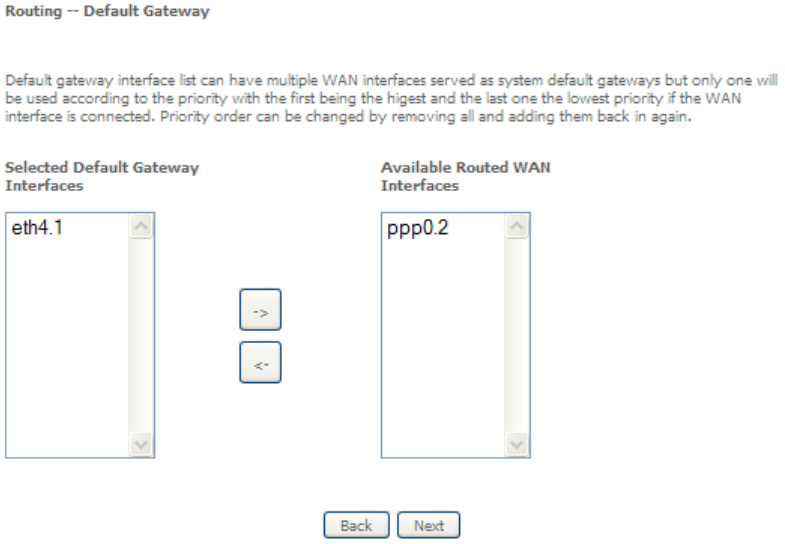


Bridging

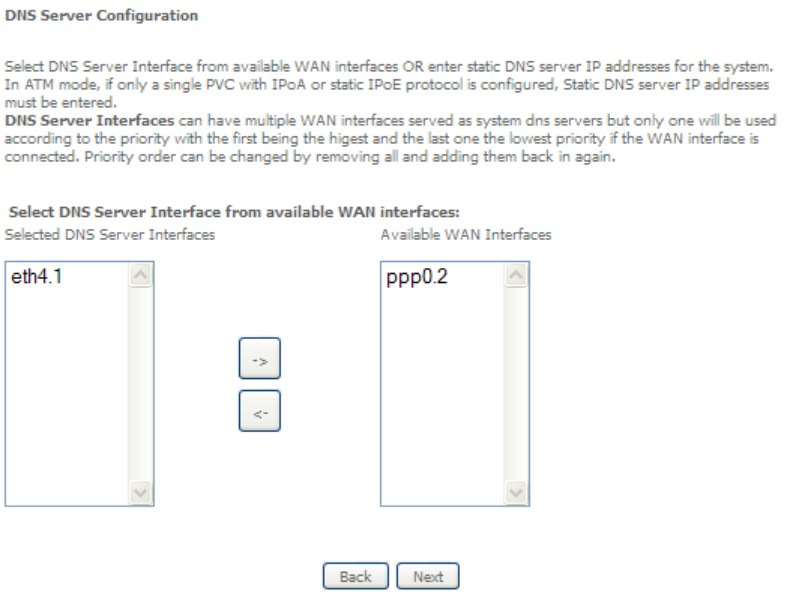
When you select bridging mode, a summary of the settings is displayed. Click **Apply/Save** to commit the settings.



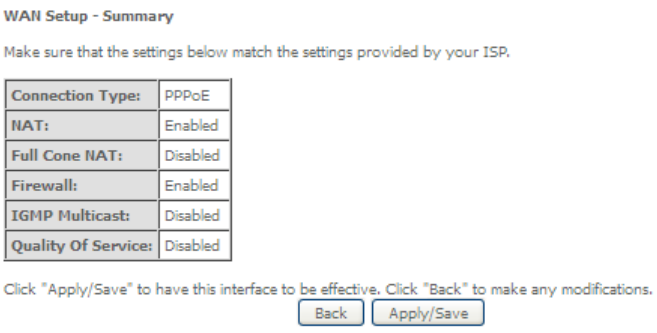
Use the arrow buttons to move the interfaces required to the list on the left. Click **Next**.



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.



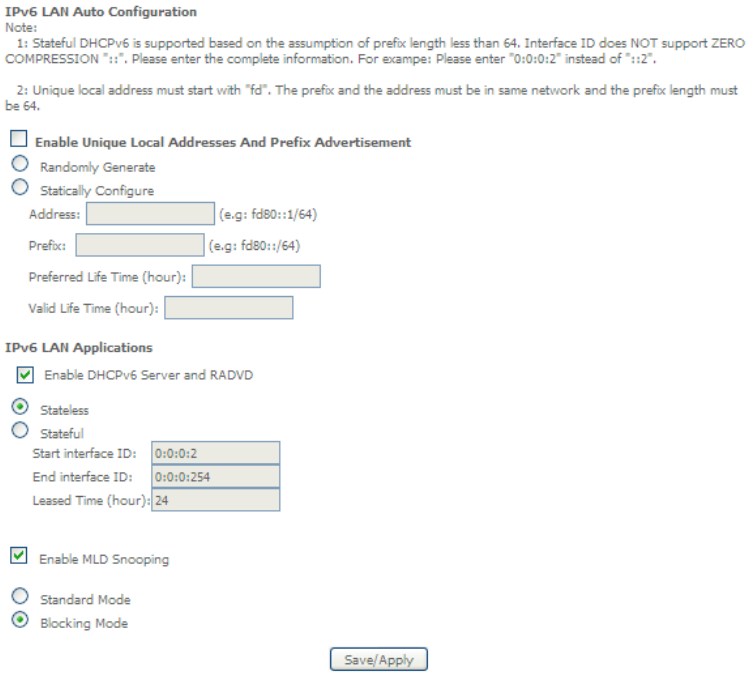
A summary of your settings is displayed. Click **Apply/Save** to commit your settings to the router.



LAN

IPv6 Autoconfig

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

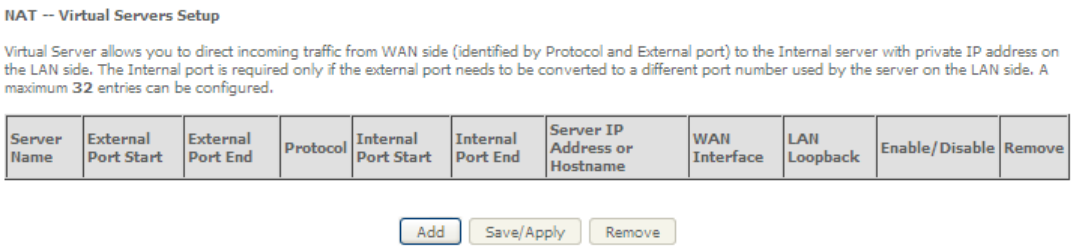


OPTION	DEFINITION
Enable Unique Local Addresses and Prefix Advertisement	Enable the use of unique local addresses. The router will advertise the IPv6 prefix to new devices on the network.
Randomly Generate	Randomly generates the unique local addresses and the prefix.
Statically Configure	Enter a static 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.

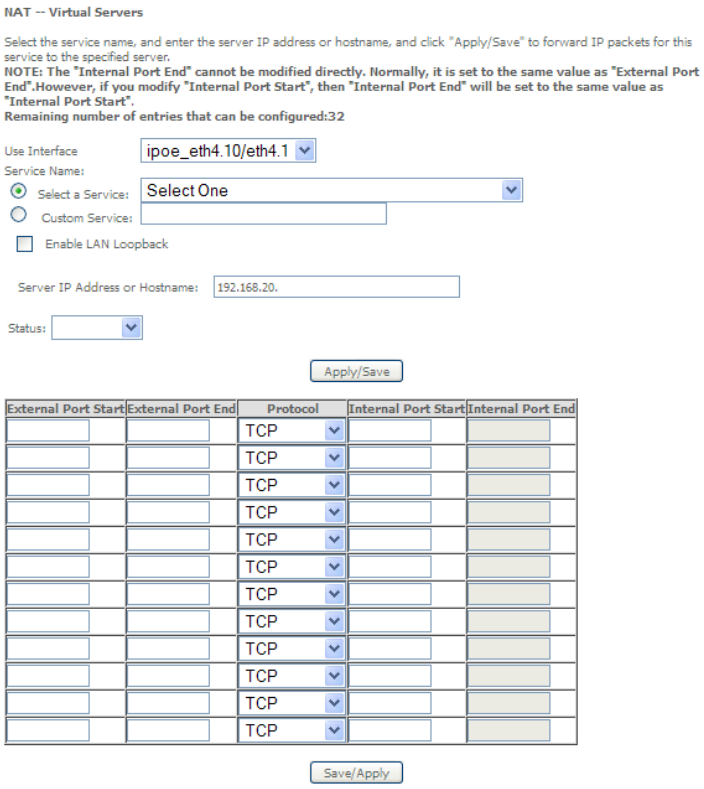
NAT

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.



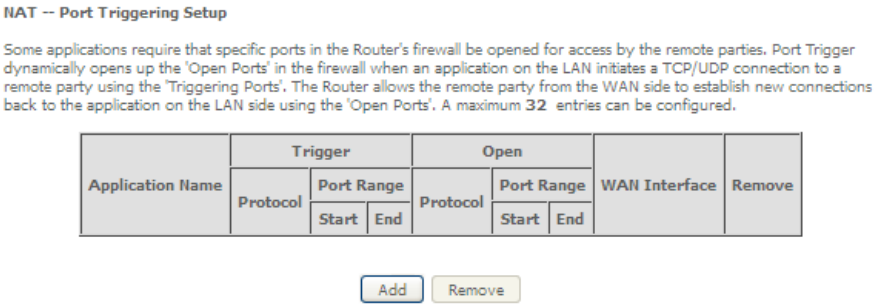
FIELD	DESCRIPTION
Select a Service or custom Server	Select a pre-configured port forwarding rule or choose custom server to create your own port forwarding rule.
Server IP Address	Enter the IP address of the local server.
External Port Start	Enter the starting external port number (when custom server 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.

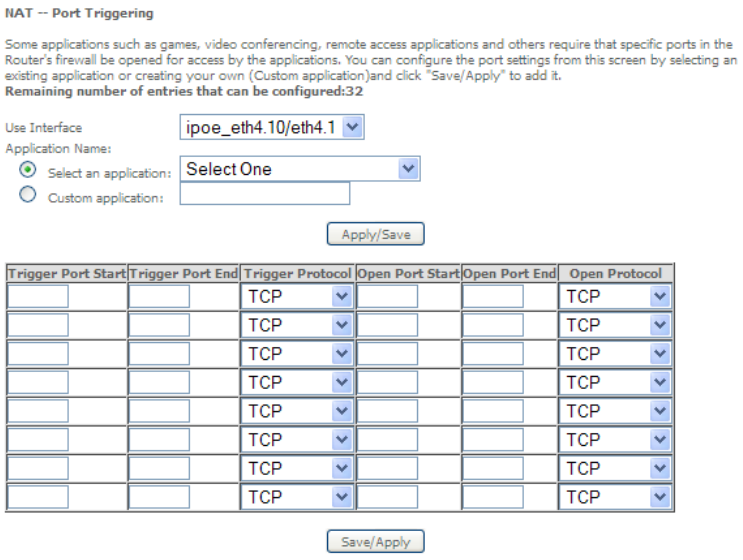
Port Triggering

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.

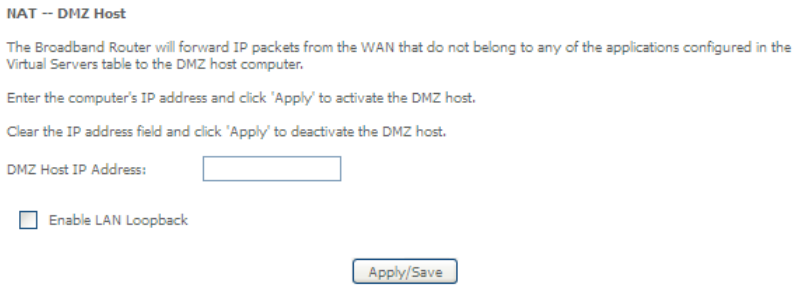


FIELD	DESCRIPTION
Select an Application or Custom Application	A user can select a pre-configured application from the list or select the Custom Application option to create custom application settings.
Trigger Port Start	Enter the starting trigger port number (when you select Custom Application). When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

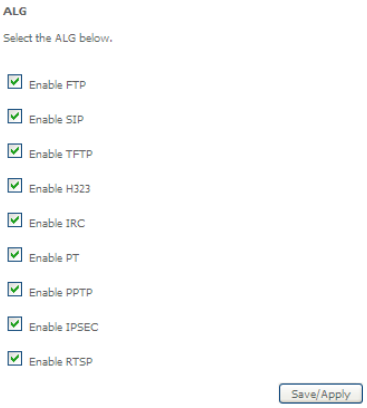
The NF8AC will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

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.



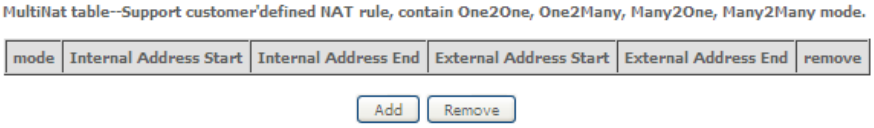
ALG

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.

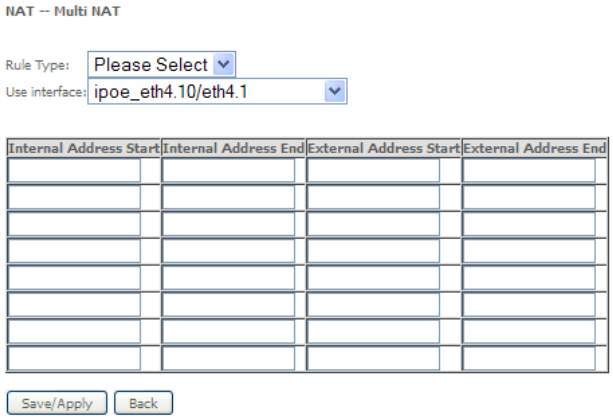


Multi Nat

The Multi NAT page allows you to configure your own custom NAT rules.



To add a new rule, click the **Add** button and enter the details of the rule as required.



1. Select the type of NAT to use from the Rule Type drop down menu.
2. Select the interface to which the NAT rule should apply.
3. Enter the appropriate Internal Address Start and Internal Address End
4. Enter the appropriate External Address Start and External Address End

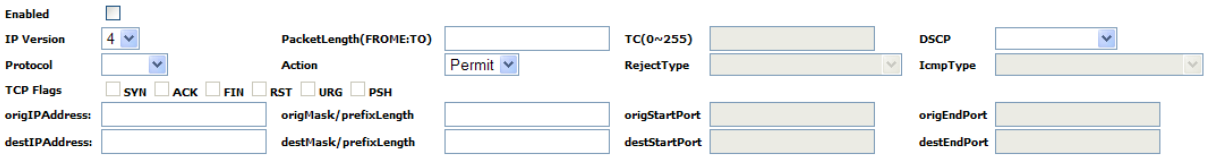
Click **Save/Apply** to save the new Multi NAT configuration settings.

Security

Firewall

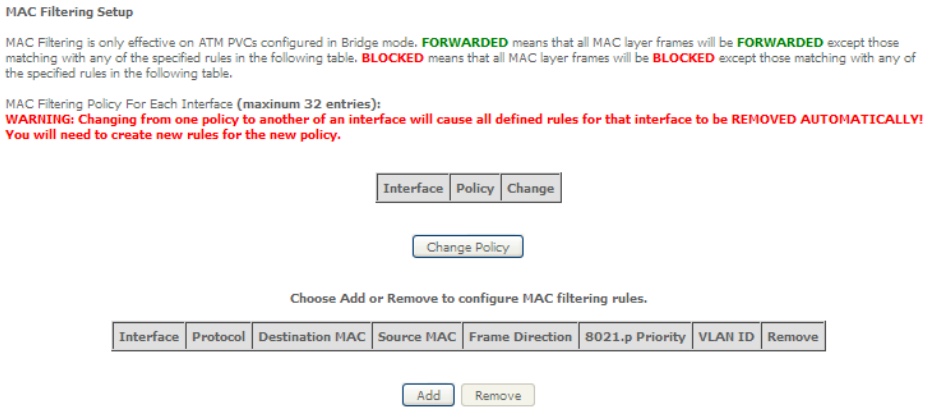
The NF8AC has a firewall function which helps to keep you secure while allowing you to configure rules allowing certain types of data through.

To use the firewall feature, begin by clicking the **Add Firewall** button to create a firewall. Then click the **Add Rule** button to create a rule for the firewall. Enter the rules that you require for the firewall and then click the **Save&Apply** button to commit the settings.

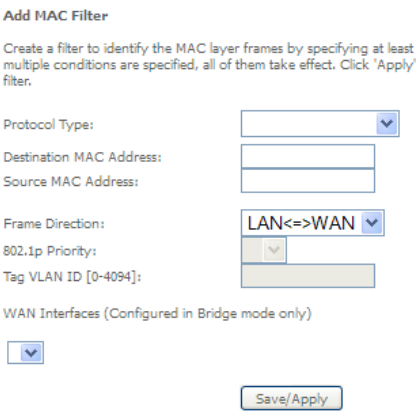


MAC Filtering

The NF8AC 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.

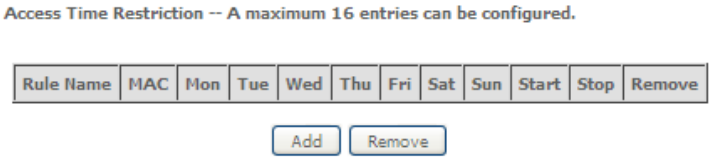


Figure 1: Advanced - Parental Control – Time Restriction

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

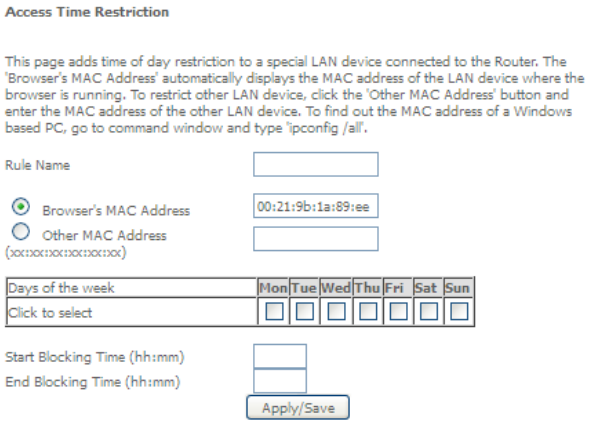


Figure 2: Advanced - Parental Control - Add Time Restriction

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 NF8AC.

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.

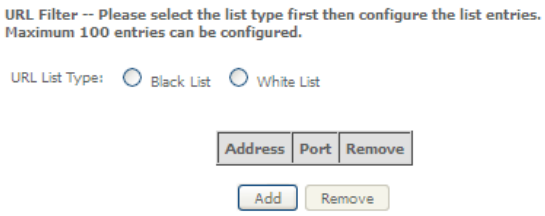


Figure 3: Advanced - Parental Control - URL Filter

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.

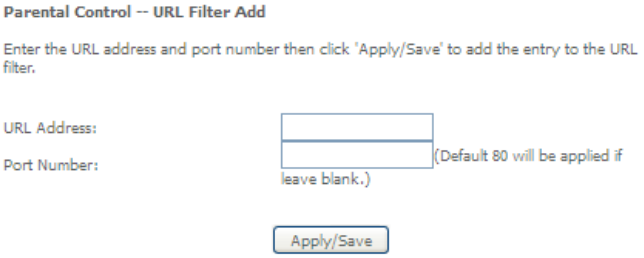


Figure 4: Advanced - Parental Control - Add URL Filter

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.

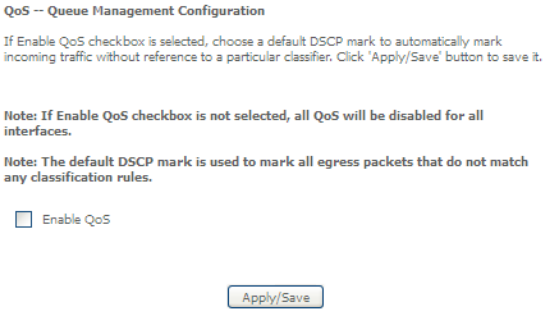
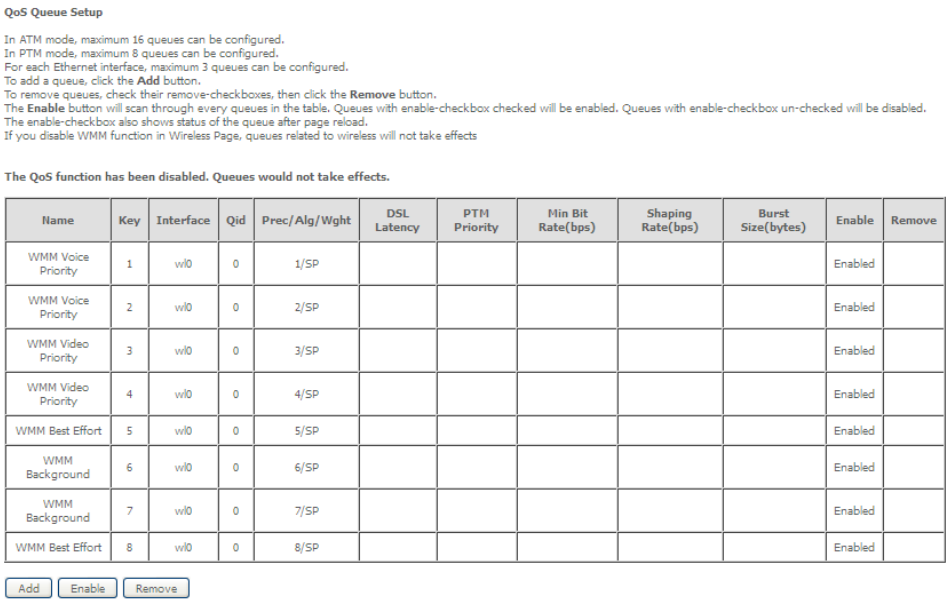


Figure 5: Advanced - Enable QoS

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



QoS Queue Setup

In ATM mode, maximum 16 queues can be configured.
In PTM mode, maximum 8 queues can be configured.
For each Ethernet interface, maximum 3 queues can be configured.
To add a queue, click the **Add** button.
To remove queues, check their remove-checkboxes, then click the **Remove** button.
The **Enable** button will scan through every queues in the table. Queues with enable-checkbox checked will be enabled. Queues with enable-checkbox un-checked will be disabled.
The enable-checkbox also shows status of the queue after page reload.
If you disable WMM function in Wireless Page, queues related to wireless will not take effects

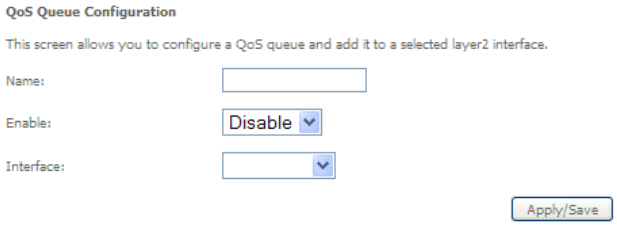
The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Qid	Prec/Alg/Wght	DSL Latency	PTM Priority	Min Bit Rate(bps)	Shaping Rate(bps)	Burst Size(bytes)	Enable	Remove
WMM Voice Priority	1	wl0	0	1/SP						Enabled	
WMM Voice Priority	2	wl0	0	2/SP						Enabled	
WMM Video Priority	3	wl0	0	3/SP						Enabled	
WMM Video Priority	4	wl0	0	4/SP						Enabled	
WMM Best Effort	5	wl0	0	5/SP						Enabled	
WMM Background	6	wl0	0	6/SP						Enabled	
WMM Background	7	wl0	0	7/SP						Enabled	
WMM Best Effort	8	wl0	0	8/SP						Enabled	

Add Enable Remove

Figure 6: Advanced - QoS Queue Setup

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



QoS Queue Configuration

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

Name:

Enable: Disable

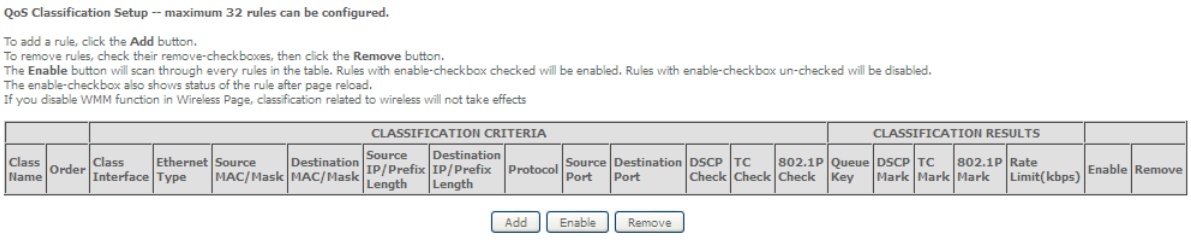
Interface:

Apply/Save

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.

QoS Classification



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

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

		CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS						
Class Name	Order	Class Interface	Ethernet Type	Source MAC/Mask	Destination MAC/Mask	Source IP/Prefix Length	Destination IP/Prefix Length	Protocol	Source Port	Destination Port	DSCP Check	TC Check	802.1P Check	Queue Key	DSCP Mark	TC Mark	802.1P Mark	Rate Limit(kbps)	Enable	Remove

Add Enable Remove

Figure 8: Advanced - QoS Classification Setup

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

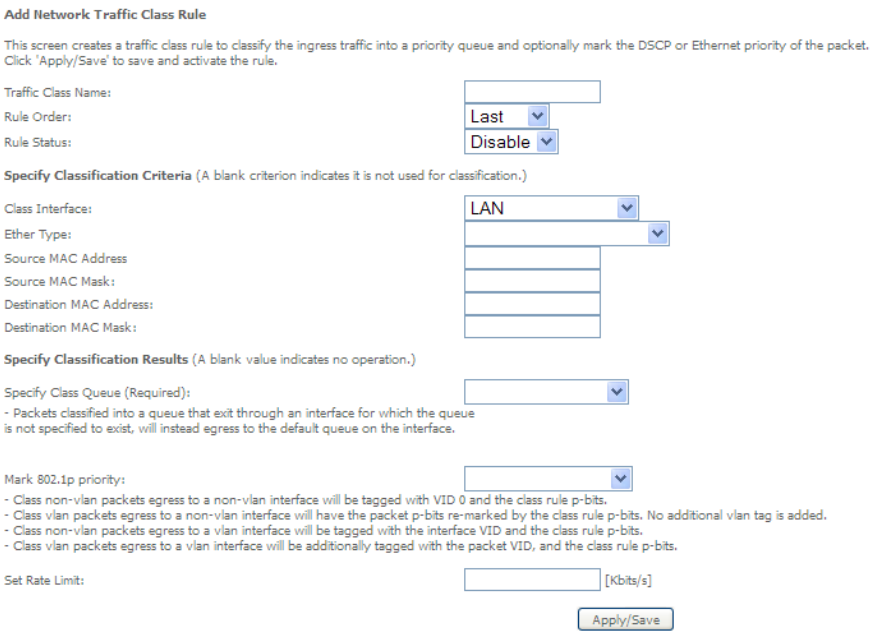


Figure 9: Advanced - Add QoS Network Traffic Classification

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.

Figure 10: Advanced - Routing - Default Gateway

Static Route

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

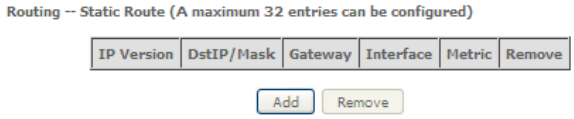


Figure 11: Advanced - Routing - Static Route

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

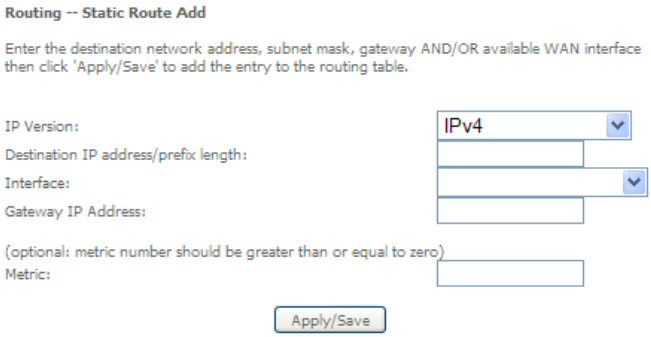


Figure 12: Advanced - Routing - Add Static Route

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.

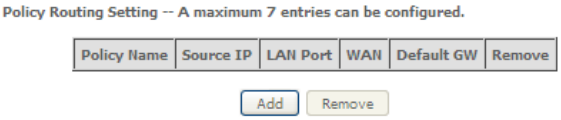


Figure 13: Advanced - Routing - Policy Routing

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

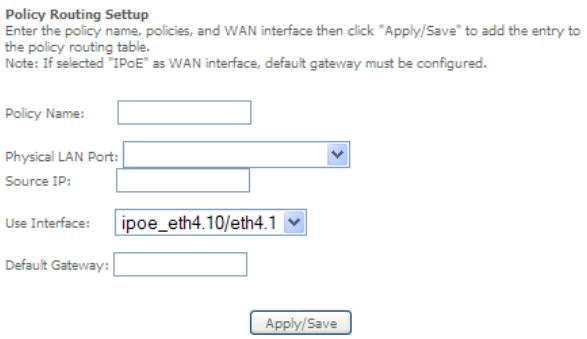


Figure 14: Advanced - Routing - Add Policy Route

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.

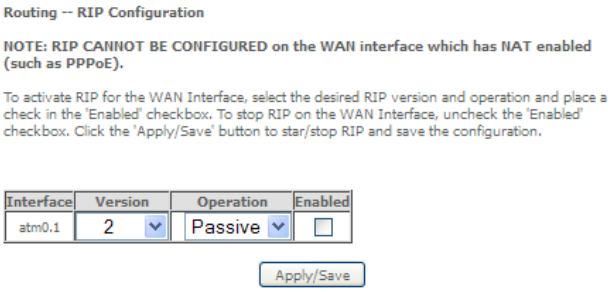


Figure 15: Advanced - Routing - RIP

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.

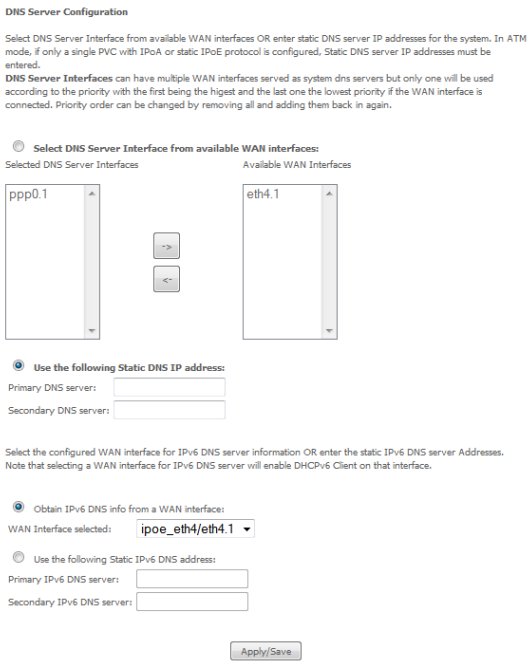


Figure 16: Advanced - DNS Server

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.

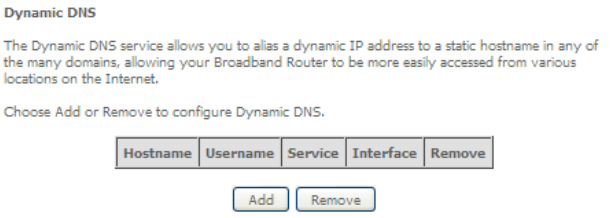


Figure 17: Advanced - DNS - Dynamic DNS

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.

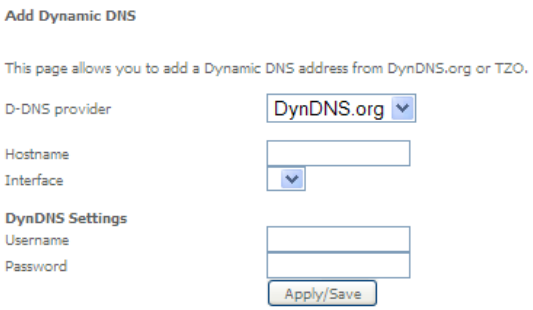


Figure 18: Advanced - DNS - Add Dynamic DNS Account

FIELD	DESCRIPTION
D-DNS Provider	Select the dynamic DNS provider from the list.
Host Name	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.

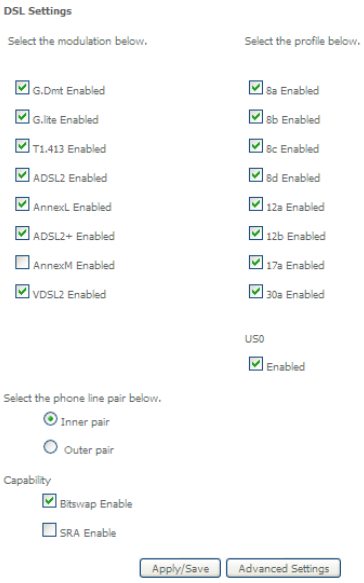


Figure 19: Advanced – DSL

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

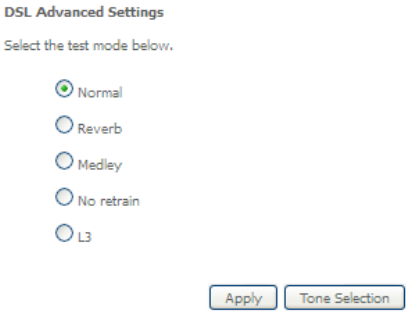


Figure 20: Advanced - DSL - Advanced DSL Settings

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.

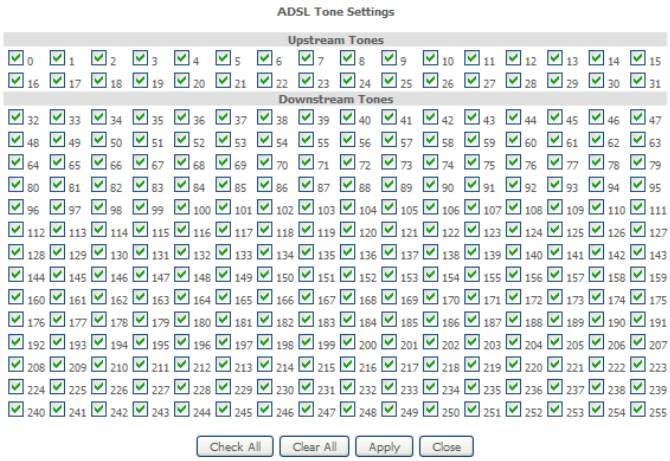


Figure 21: Advanced - DSL - ADSL Tone Settings

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.

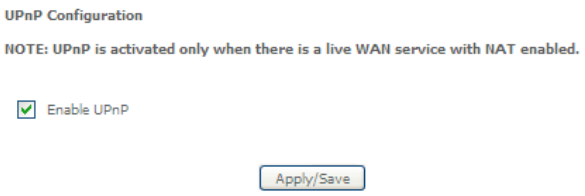


Figure 22: Advanced – UPnP

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.

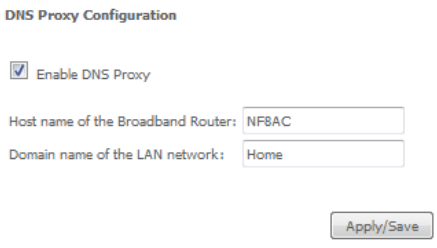


Figure 23: Advanced - DNS Proxy

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.

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 NF8AC and the router will make it accessible to other devices on your network.

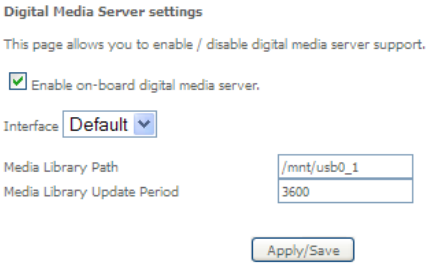


Figure 24: Advanced - DLNA

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.

Packet Acceleration

Packet acceleration uses a number of methods to try and reduce the latency experienced on some DSL services. These can range from utilising locally terminated TCP connections to Fast Connection Setup.

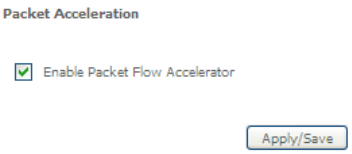


Figure 25: Advanced - Packet Acceleration

Select to enable or disable Packet Acceleration and click **Apply/Save** to save the new packet acceleration configuration settings.

Storage Service

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

Storage Device Info

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

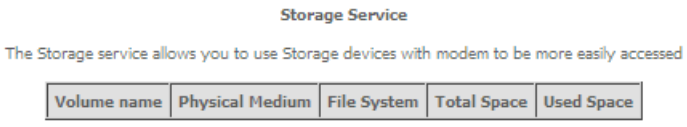


Figure 26: Advanced – Storage Service

User Accounts

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

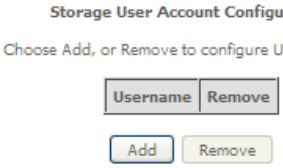


Figure 27: Advanced – Storage Service – Storage User Account Configuration

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

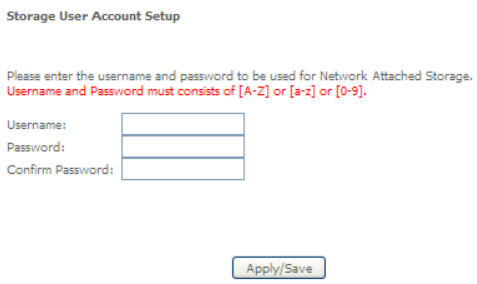


Figure 28: Advanced – Storage Service – Storage User Account Setup

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.

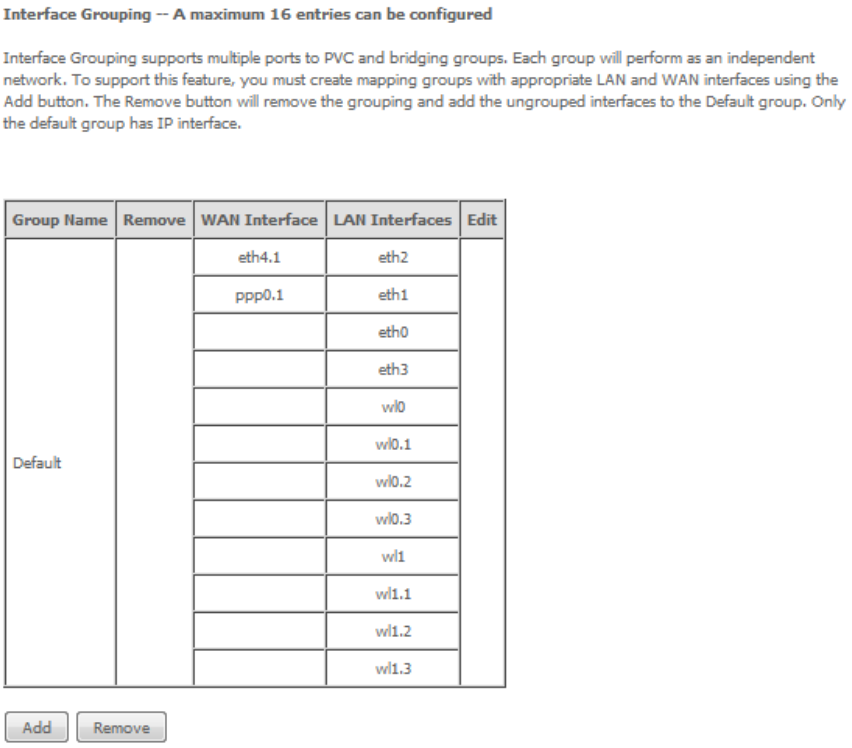
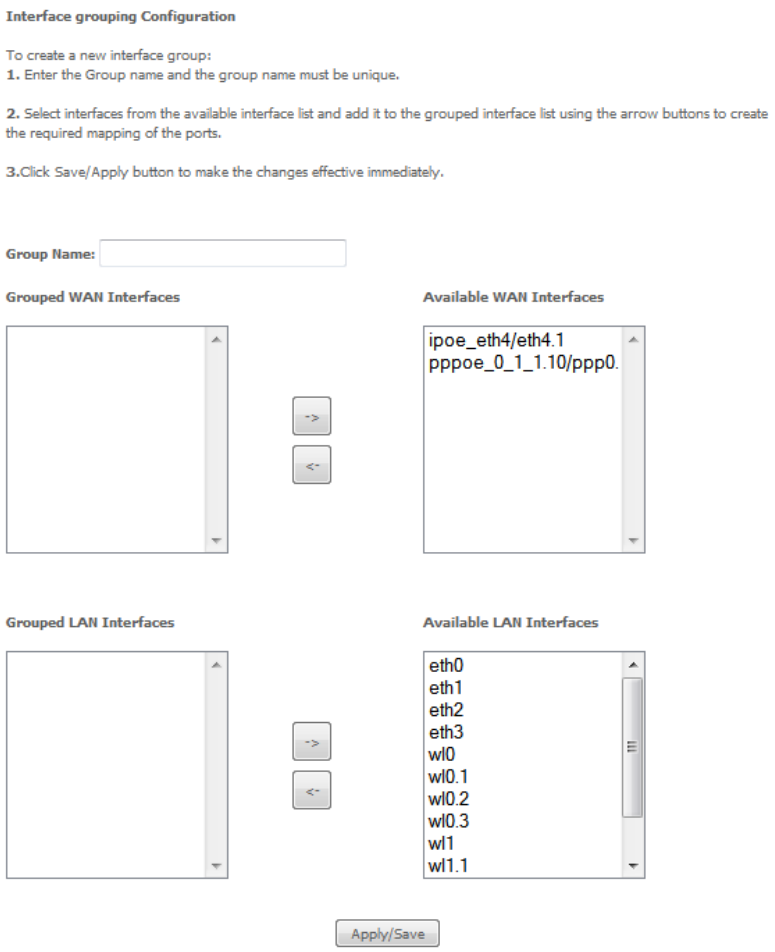


Figure 29: Advanced - Interface Grouping

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

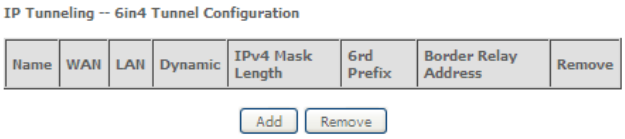


Figure 30: Advanced - IP Tunnel - IPv6inIPv4

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

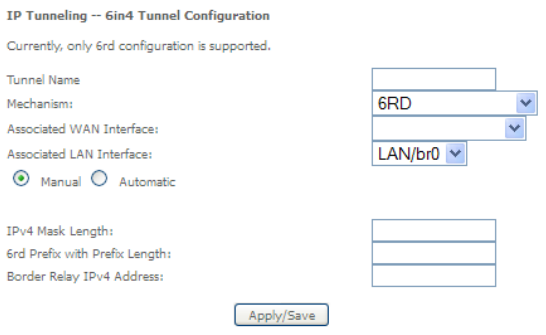


Figure 31: Advanced - IP Tunnel - IPv6inIPv4 - 6in4 Tunnel Configuration

IPv4inIPv6

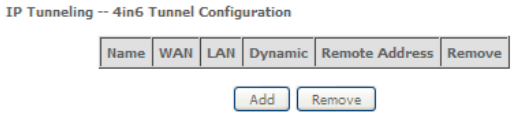


Figure 32: Advanced - IP Tunnel – IPv4inIPv6

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

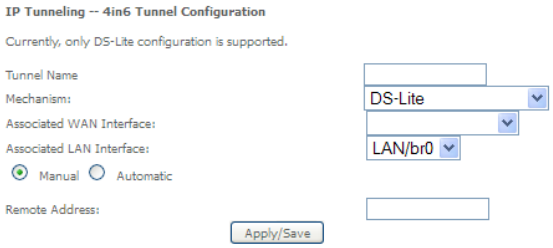


Figure 33: Advanced - IP Tunnel – IPv4inIPv6 - 4in6 Tunnel Configuration

IPSec

The NF8AC 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.

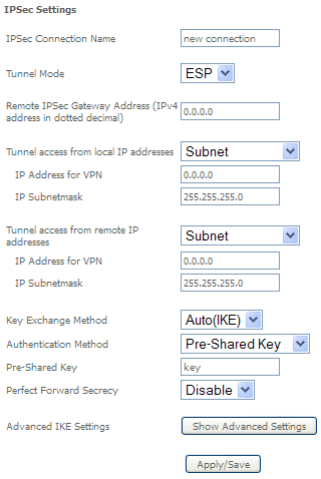


Figure 34: Advanced - IPSec

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.

Certificate

Local

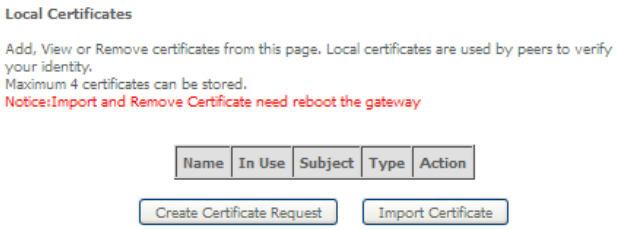


Figure 35: Advanced – Certificate - Local

Trusted CA

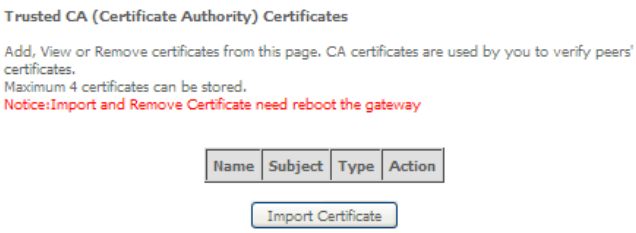


Figure 36: Advanced – Certificate – Trusted CA

Power Management

The power management page enables you to control the green aspects of the NF8AC.

You can enable or disable the power management features by selecting or unselecting the different power management functions as necessary and then click **Apply** to save these settings.

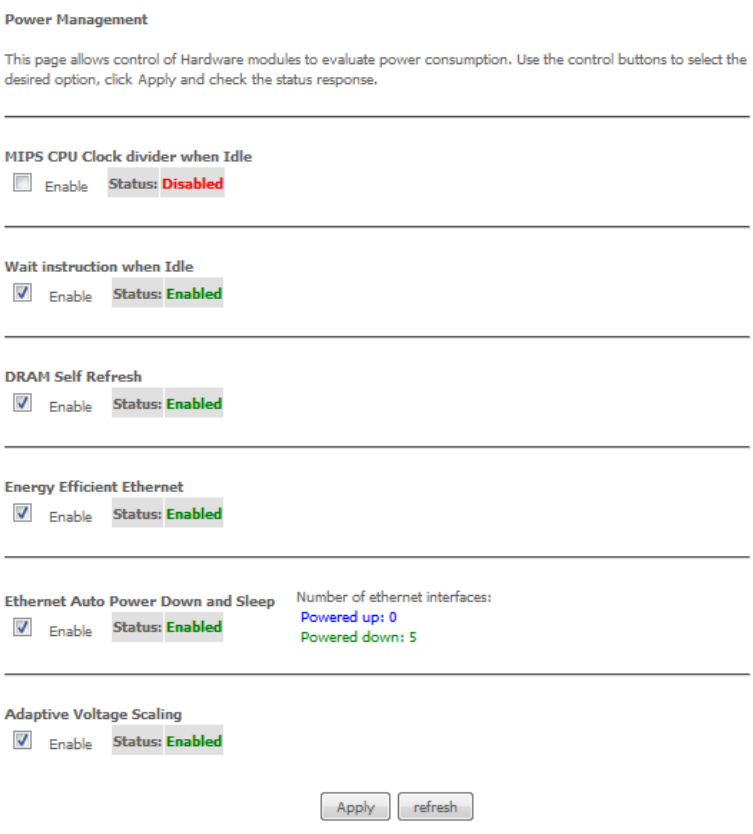


Figure 37: Advanced – Power Management

Multicast (IGMP Configuration)

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

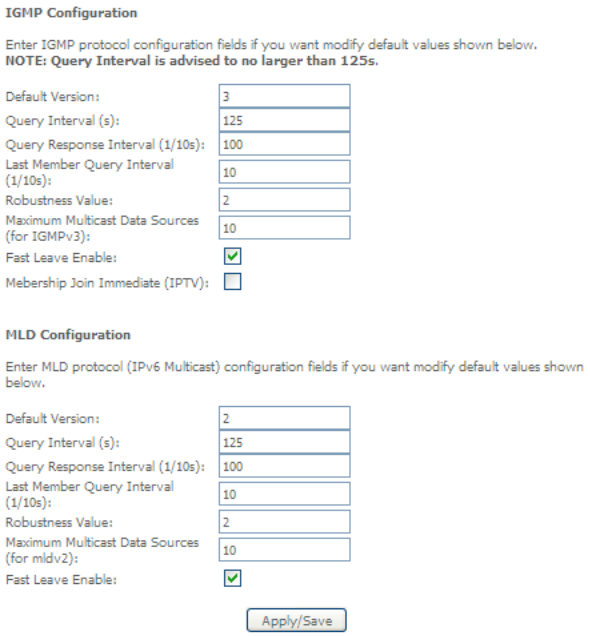


Figure 38: Advanced - IGMP Configuration

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

WiFi 2.4GHz / WiFi 5GHz

Basic

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

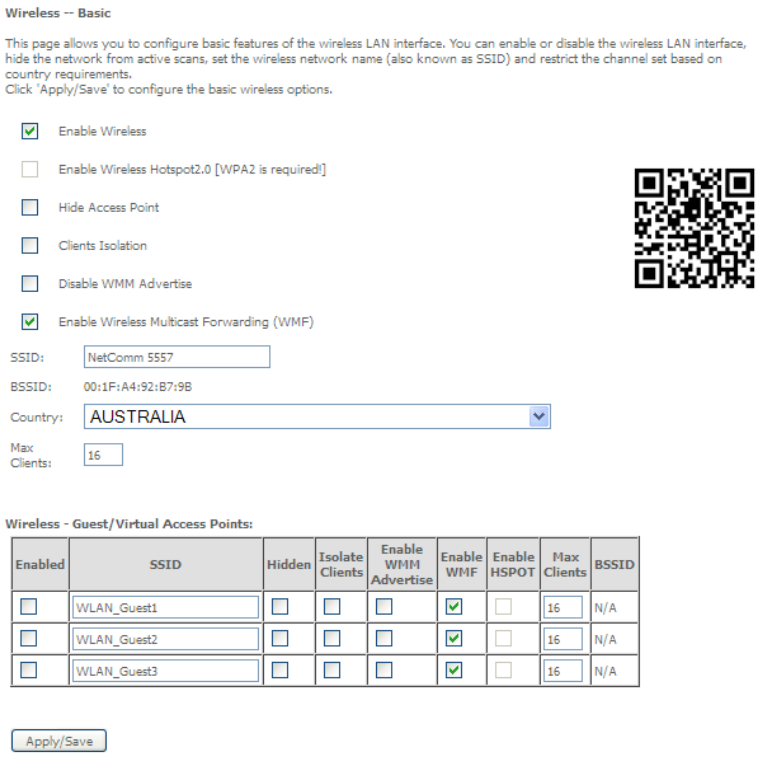


Figure 39: Wireless - Basic

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 NF8AC 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.

Security

The NF8AC supports all encryptions within the 802.11 standard. The factory default is WPA2-PSK. The NF8AC also supports WPA, WPA-PSK, WPA2, WPA2-PSK. You can also select to enable WPS mode.

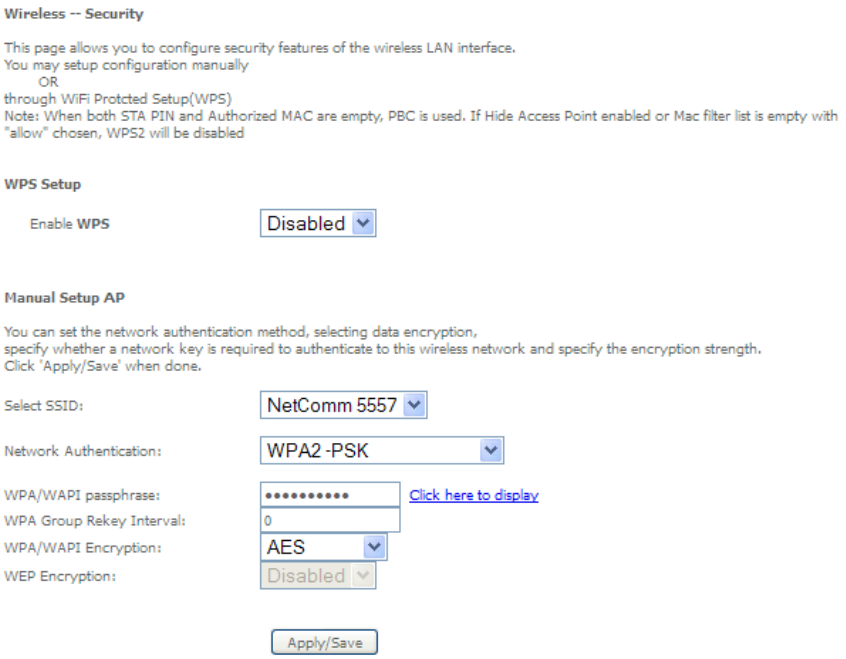


Figure 40: Wireless - Security

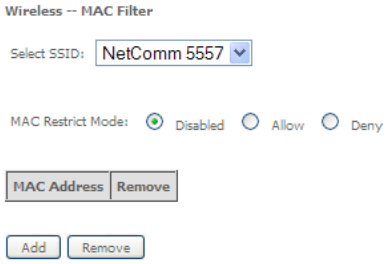
The following parameters are available:

PARAMETER	DEFINITION
Enable WPS	Select to enable or disable the WPS function of the NF8AC.
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.

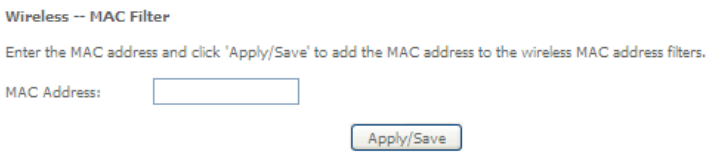
Click **Apply/Save** to save the new wireless security configuration settings.

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.



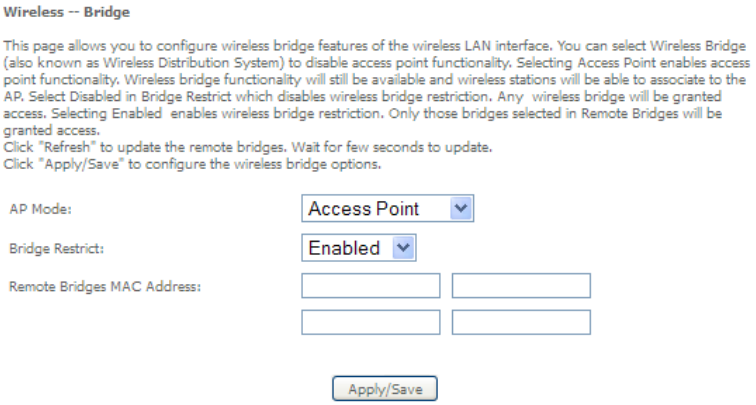
Click **Add** to add a MAC Address Filter.



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.

Wireless Bridge

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

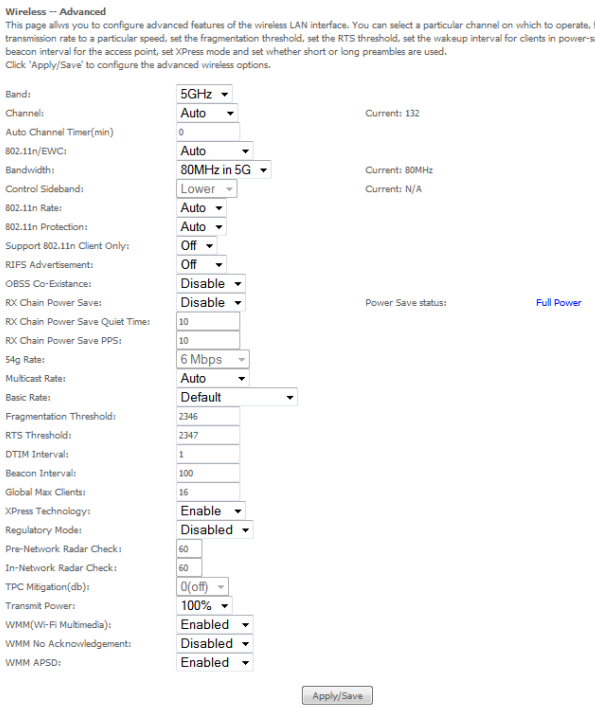


Select the mode for the Wireless Access Point built into the NF8AC. You can specify which wireless networks will be allowed to connect to the NF8AC by using the 'Bridge Restrict' option and then entering the applicable MAC Addresses of the other wireless access points.

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.

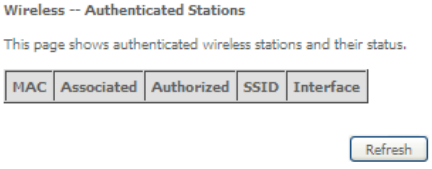


Click **Apply/Save** to save any changes to the wireless network settings configuration.

PARAMETER	DEFINITION
Band	You can select 2.4GHz or 5GHz.
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. The 80MHz in 5G option appears only on the 5GHz WiFi settings and is the bandwidth that should be selected for 802.11ac speeds.
Control Sideband	If you select 20MHz in Both Bands or 20MHz in 2.4G Band and 40MHz in 5G Band, the service of control sideband does not work. When you select 40MHz in Both Bands as the bandwidth, the following page appears. 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 defaule is Disabled.
Transmit Power	Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
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 NF8AC and their status



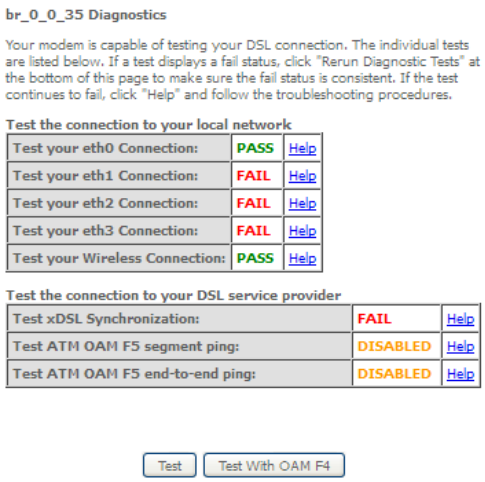
Diagnostics

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.

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:

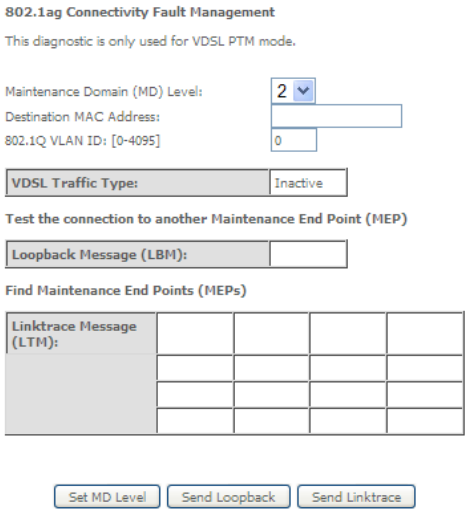
1. Click on the **Help** link and follow the troubleshooting procedures in the Help screen that appears.
2. Now click **Rerun Diagnostic Tests** at the bottom of the screen to re-test and confirm the error.
3. If the test continues to fail, contact Technical Support.



FIELD	DESCRIPTION
eth 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.

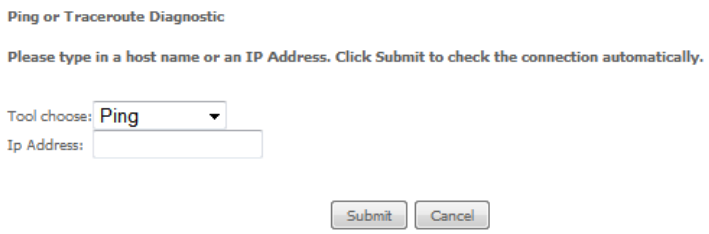
Fault Management

The Fault Management page allows you to perform diagnostics for VDSL PTM mode.



Ping Test

The ping test page lets you perform basic diagnostics like performing a ping or traceroute to a remote IP address or hostname.



Management

Settings

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

Backup

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings. You will be prompted for the location to save the backup file to on your PC.

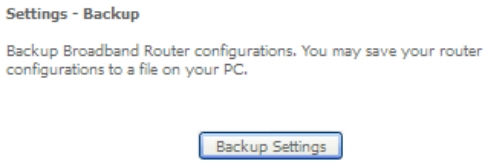
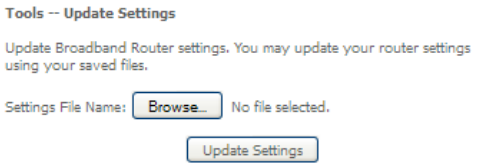


Figure 41: Management - Device Settings – Backup

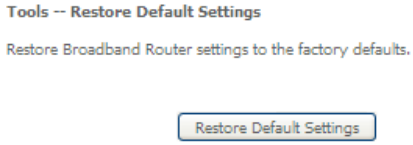
Update Settings

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.



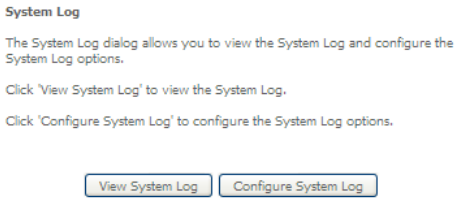
Restore Default

The following screen appears when selecting Restore Default from the Settings submenu. By clicking on the Restore Default Settings button, you can restore your Routers default firmware settings. To restore system settings, reboot your Router.

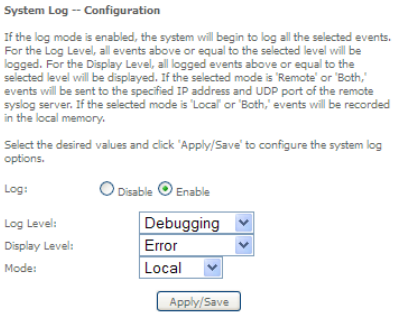


System Log

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.

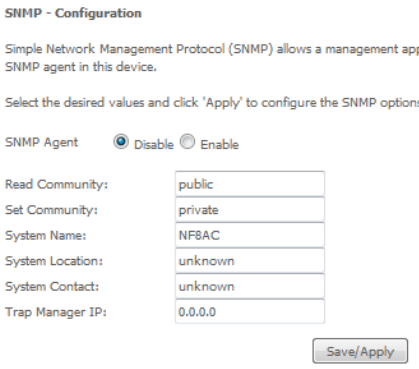


To configure the system log, click the Configure System Log button.



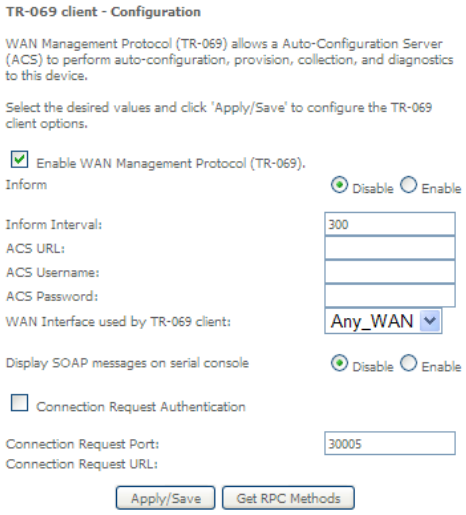
SNMP Agent

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

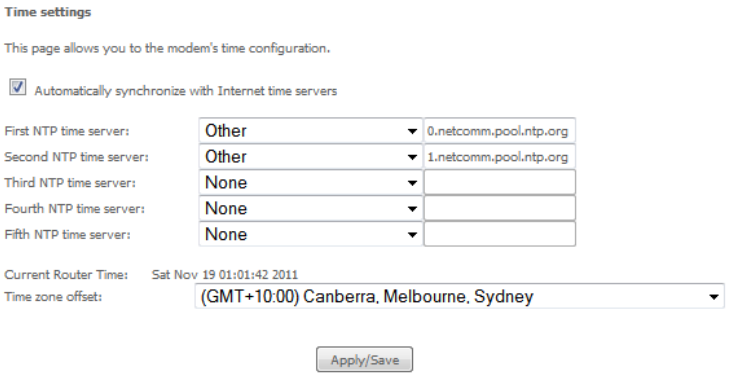
TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router if supported by your Internet Service Provider (ISP).



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 NF8AC 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

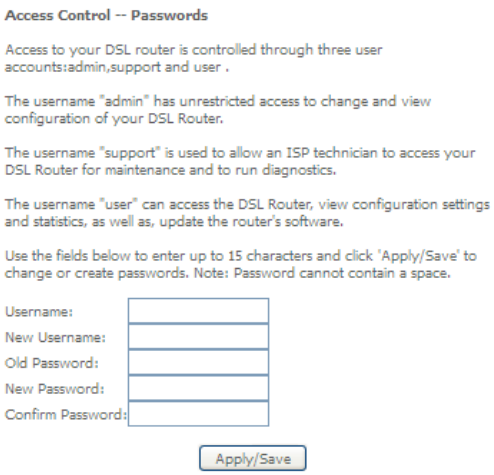
Access Control is used to control local and remote management settings for your router.

Passwords

The Passwords option configures your account access password for your modem. Access to the device is limited to the following three user accounts:

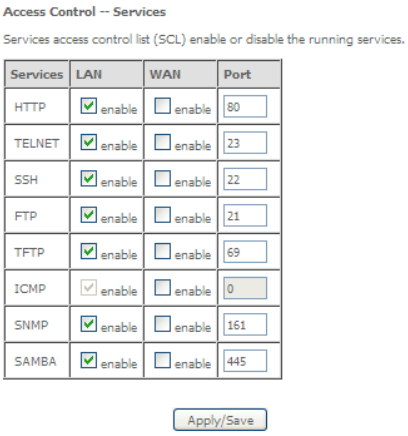
- admin is to be used for local unrestricted access control
- support is to be used for remote maintenance of the device
- user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click the Apply/Save button after making any changes to continue.



Services

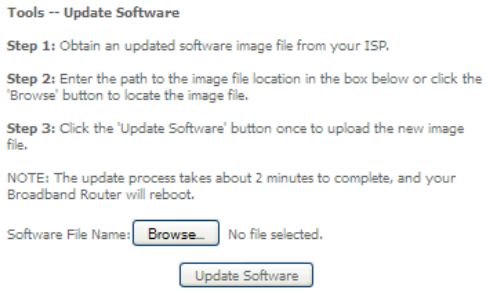
The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP. Click the **Apply/Save** button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



Update Software

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 NF8AC.

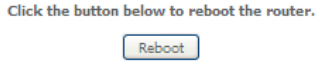


Figure 42: Management - Reboot

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

NOTE 2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 3 seconds to restore default settings.

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 3)

1. Open the Network Connections control panel (Start -> Control Panel -> Network Connections):
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks:
3. Select the wireless network listed on your included wireless security card and click Connect.
4. Enter the network key *(*refer to the included wireless security card for *the default wireless network key)*.
5. The connection will show Connected.

Windows Vista

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
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. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

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 NF8AC with "Connected" next to 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 NF8AC 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 NF8AC and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF8AC 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	Make sure you are using the correct IP address of the NF8AC. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NF8AC'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.
4	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.
5	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for 3 seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NF8AC restarts. 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	Press the Reset button for 3 seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF8AC restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN Interface

I cannot access the NF8AC 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 NF8AC 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 NF8AC 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 NF8AC router to provide different priorities to different applications, users or data flows or to guarantee a certain level of performance to a data flow.

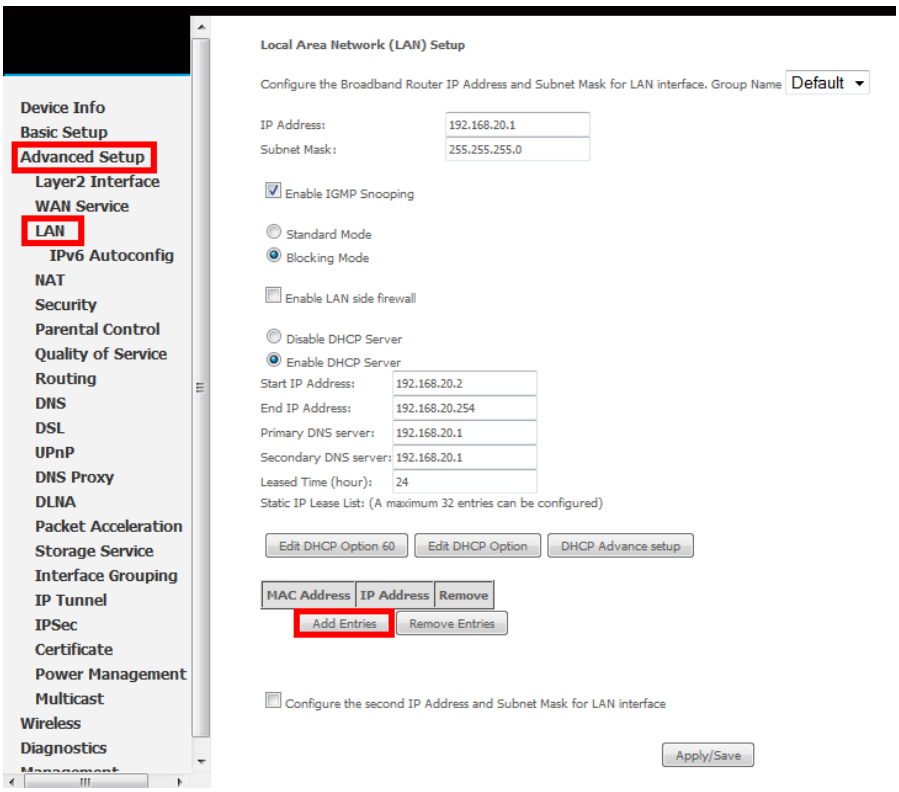
In this implementation, QoS employs DSCP (Differentiated Services Code Point), a computer networking architecture that specifies a simple, scalable and course-grained mechanism for classifying and managing network traffic.

This example guide sets up QoS with two devices (PC and laptop) connecting via Ethernet cable to an NF8AC 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

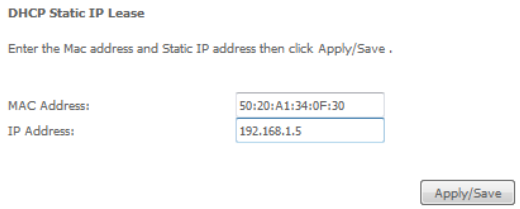
It is necessary to reserve an IP address for each of the devices connecting to the NF8AC router so that QoS settings can be managed for each device.

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

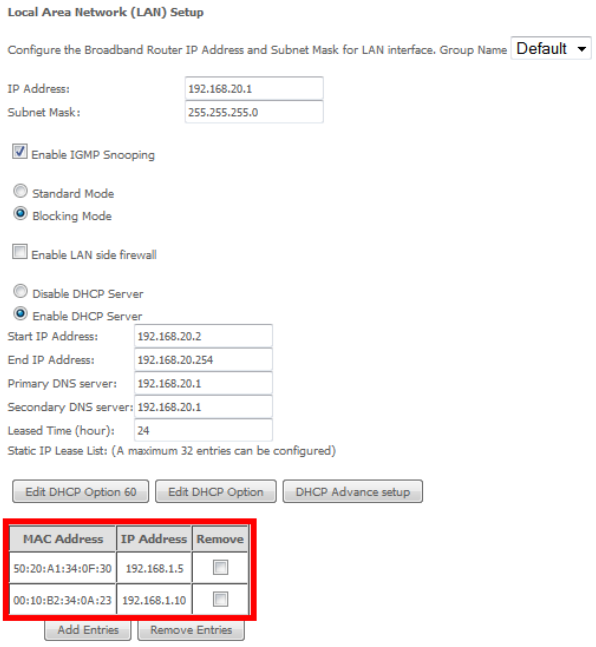


4. Click the **Add Entries** button.

5. Enter the MAC address of the computer/device you are connecting to the router. The MAC address os a 12 character set of numbers and letters (A-F), with every 2 characters separated by a colon.
6. Enter the IP address of the computer/device. This is the local address in the range of 192.168.1.x where x = a number between 2 and 254.

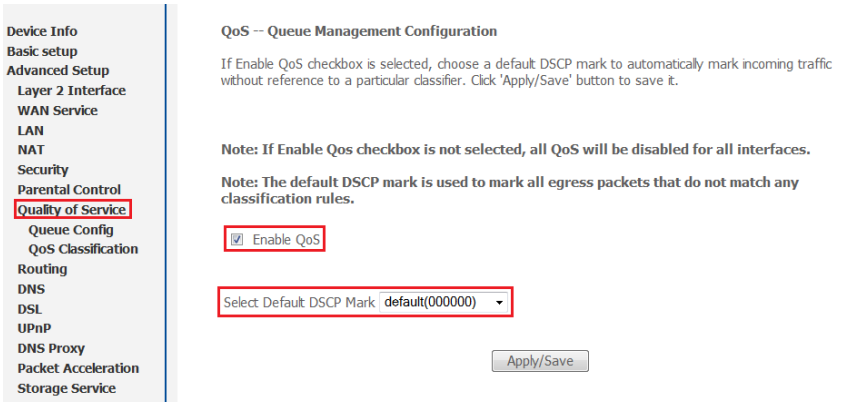


7. Click the **Apply/Save** button.
8. Complete steps 4 through 7 for each device connected to the NF8AC router. Each entry will be listed in the Static IP Lease List as shown below.



QoS Configuration Settings

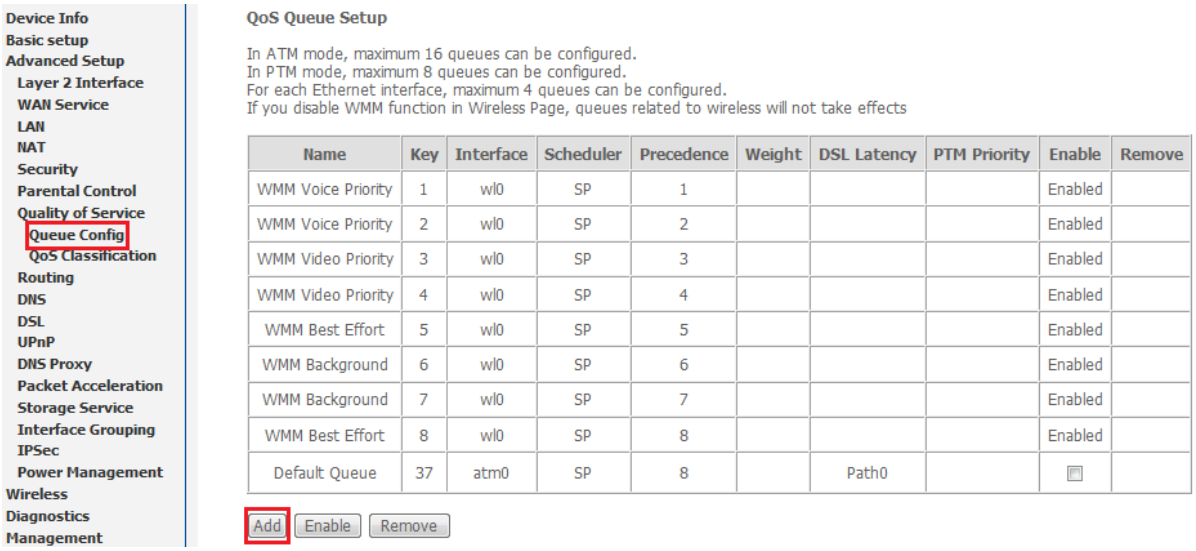
9. Select **Advanced Setup > Quality of Service**



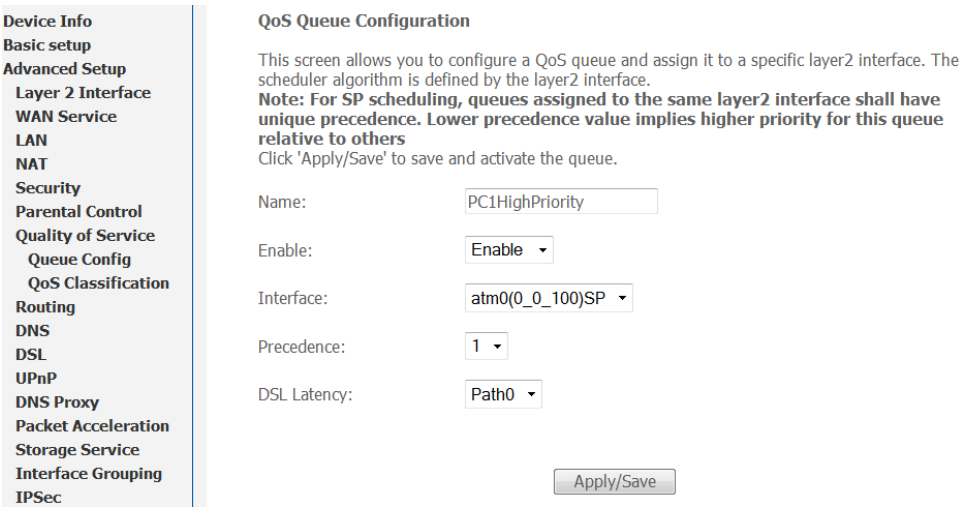
10. Select the **Enable QoS** option.
11. Select the **Default DSCP Mark** as **default(000000)**.
12. Click the **Apply/Save** button.

High Priority QoS Queue Configuration

13. Select **Advanced > Quality of Service > Queue Config**.



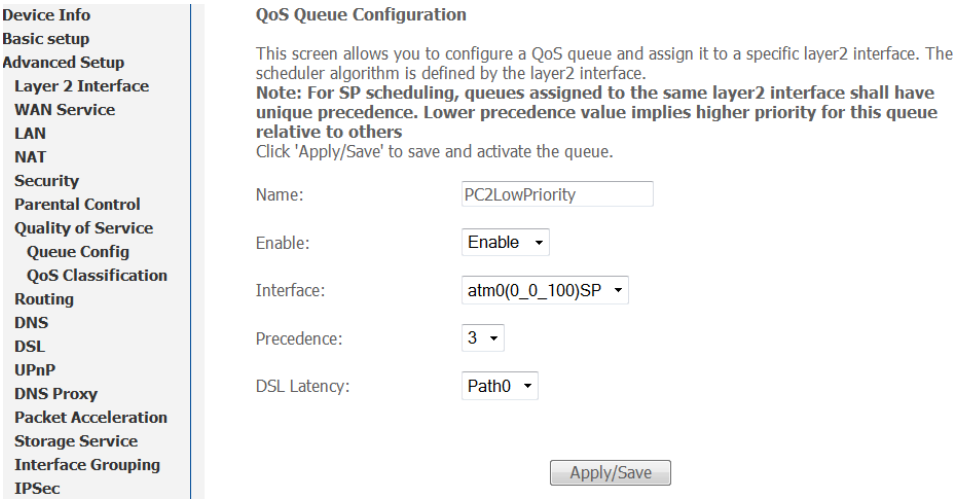
14. Click the **Add** button.



15. Enter a name of 15 characters or less to reflect the device that will have high priority QoS, e.g. PC1HighPriority.
16. Set the Enable option to **Enable**.
17. Set the Interface (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0)100)**).
18. Enter a **Precedence**. For the highest priority, set it to **1**. For the lowest priority use **3**.
19. Set the **DSL Latency** as **Path0**.
20. Click the **Save/Apply** button.

Low Priority QoS Queue Configuration

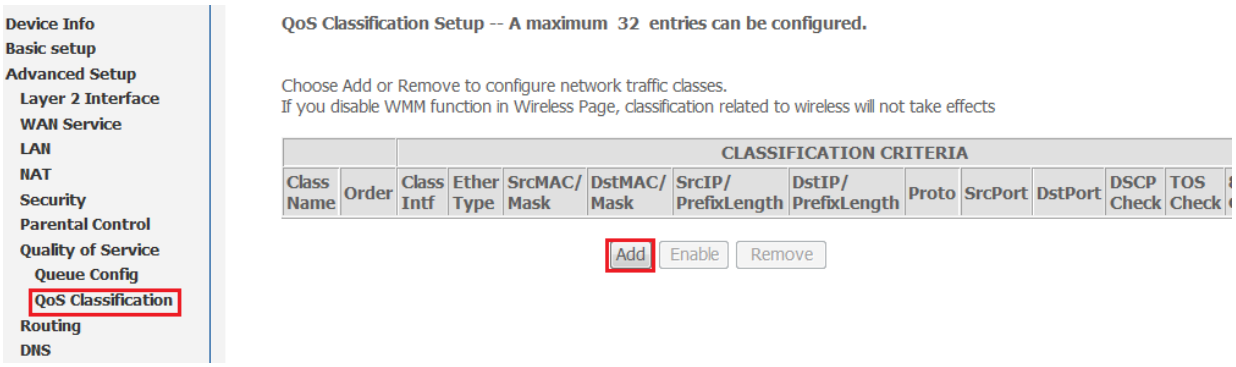
21. Select **Advanced > Quality of Service > Queue Config**.
22. Click the **Add** button.



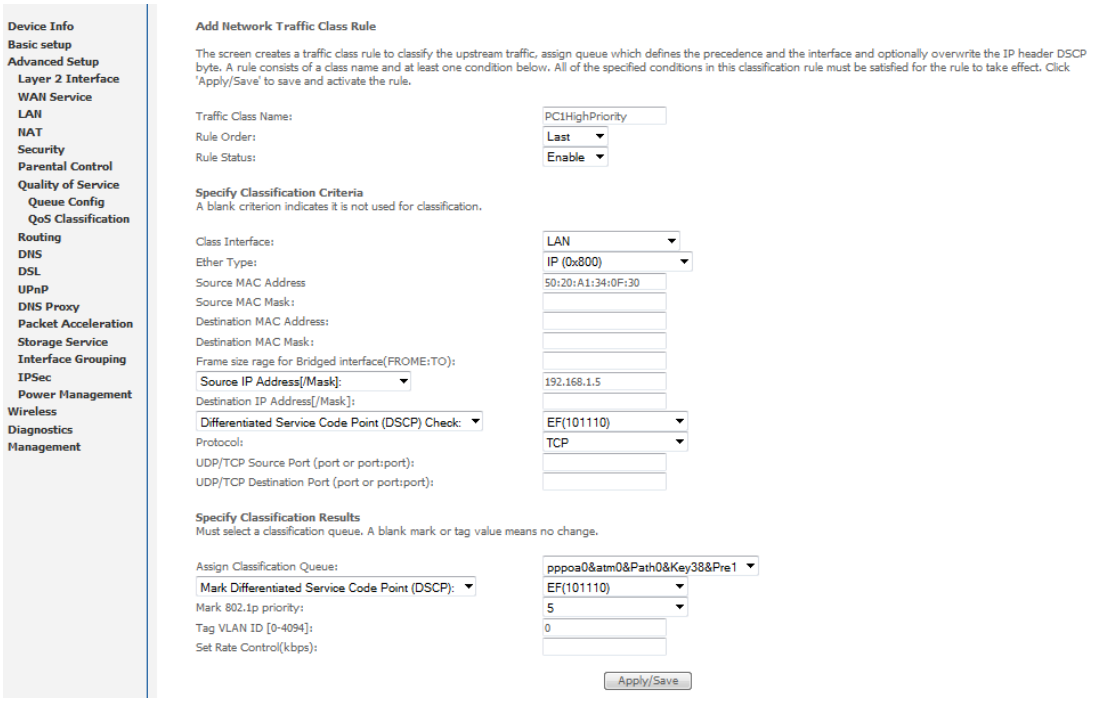
23. Enter a name of 15 characters or less to reflect the device that will have low priority QoS e.g. PC2LowPriority.
24. Set the Enable option to **Enable**.
25. Set the Interface (Australian customers use **atm0(0_8_35)**, NZ customers use **atm0(0)0)100)**).
26. Enter a **Precedence**. For the lowest priority, set it to **3**. For the highest priority use **1**.
27. Set the **DSL Latency** as **Path0**.
28. Click the **Save/Apply** button.

High Priority QoS Classification

29. Select **Advanced > Quality of Service > QoS Classification**.



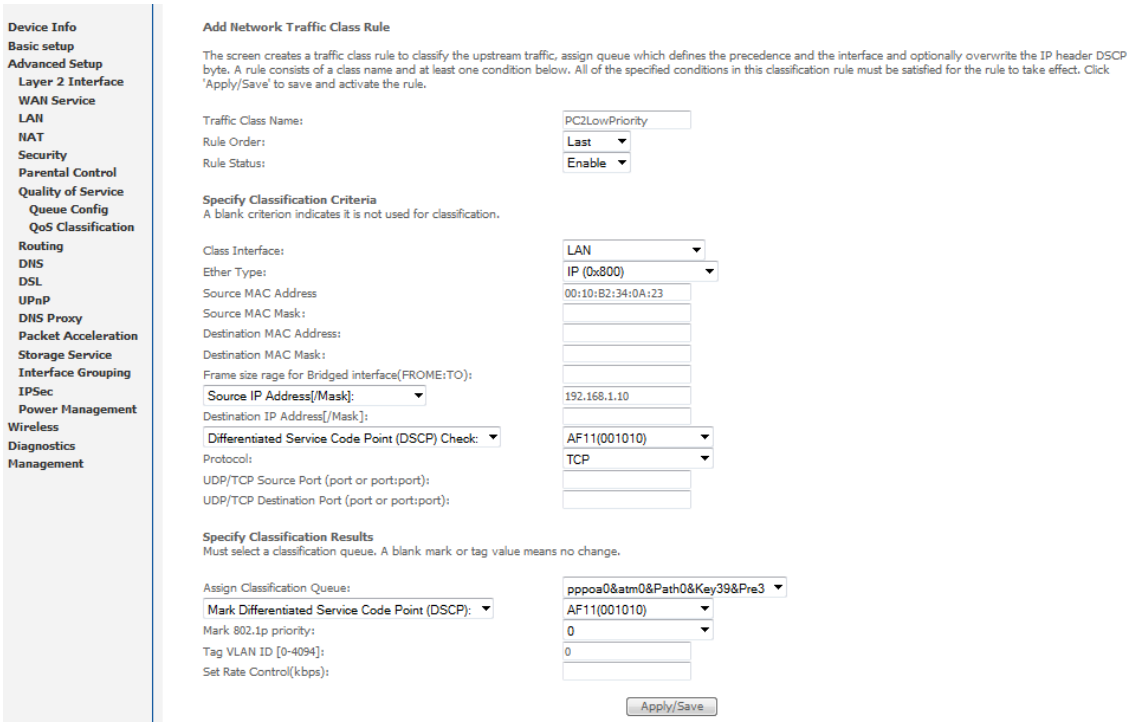
30. Click the **Add** button.



31. Enter a **Traffic Class Name** reflecting the High Priority QoS rule, e.g. PC1HighPriority.
32. Leave the **Rule Order** as **Last**.
33. Set the **Rule Status** to **Enable**.
34. 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**.
35. Set the **Ether Type** to **IP(0x800)**. Other options include ARP(0x8086), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100).
36. 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.
37. 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.
38. 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.
39. 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.
40. 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.
41. Set the **Differentiated Service Code Point** (DSCP) Check to **EF(101110)**.
42. Set the **Protocol** to **TCP**. Other options include UDP, ICMP or IGMP.
43. 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.
44. Set **Mark Differentiated Service Code Point** (DSCP) as **EF(101110)**.
45. 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.
46. Click the **Apply/Save** button.

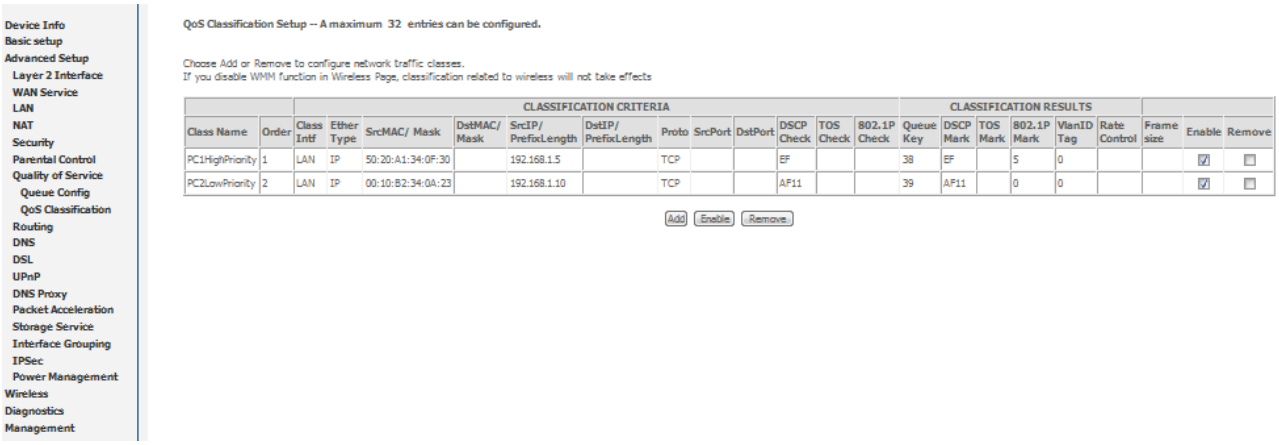
Low Priority QoS Classification

47. Select **Advanced > Quality of Service > QoS Classification.**
48. Click the **Add** button.



49. Enter a **Traffic Class Name** reflecting the High Priority QoS rule; eg. **PC2LowPriority.**
50. Leave the **Rule Order** as **Last**.
51. Set the **Rule Status** to **Enable**.
52. 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**.
53. Set the **Ether Type** to **IP(0x800)**. Other options include ARP(0x8086), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100).
54. 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.
55. 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.
56. 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.
57. 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.
58. 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.
59. Set the **Differentiated Service Code Point (DSCP)** Check to **AF11(001010).**
60. Set the **Protocol** to **TCP**. Other options include UDP, ICMP or IGMP.
61. 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.
62. Set **Mark Differentiated Service Code Point (DSCP)** as **AF11(001010).**
63. 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.
64. Click the **Apply/Save** button.

65. You now have 2 Quality of Service rules implemented for 2 devices connecting to the NF8AC router.



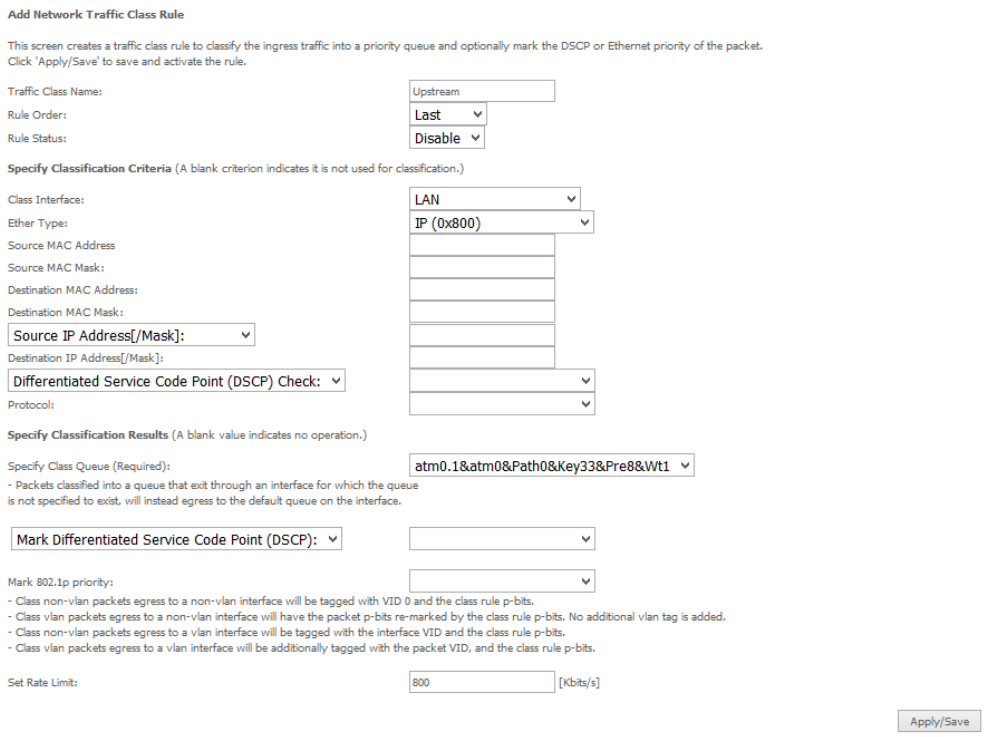
66. Select **Management** > **Reboot**. Click the **Reboot** button to restart the router and save the new settings.
67. To test your Quality of Service settings try running speed-tests (http://speedtest.net) on both PCs/devices **simultaneously**.

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.

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

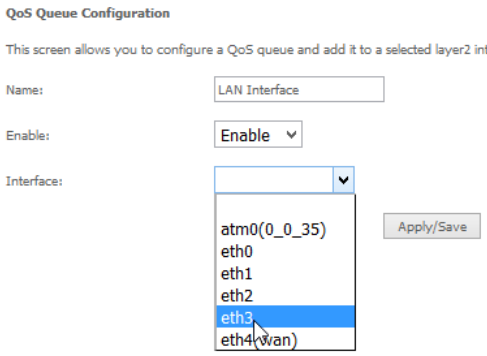
Classification Criteria:
Class Interface: LAN
Ether type: IP
Classification Results:
Class Queue: the queue that was enabled in Step 1
Set rate-limit: set according to your preference



c) Click **Apply/Save.**

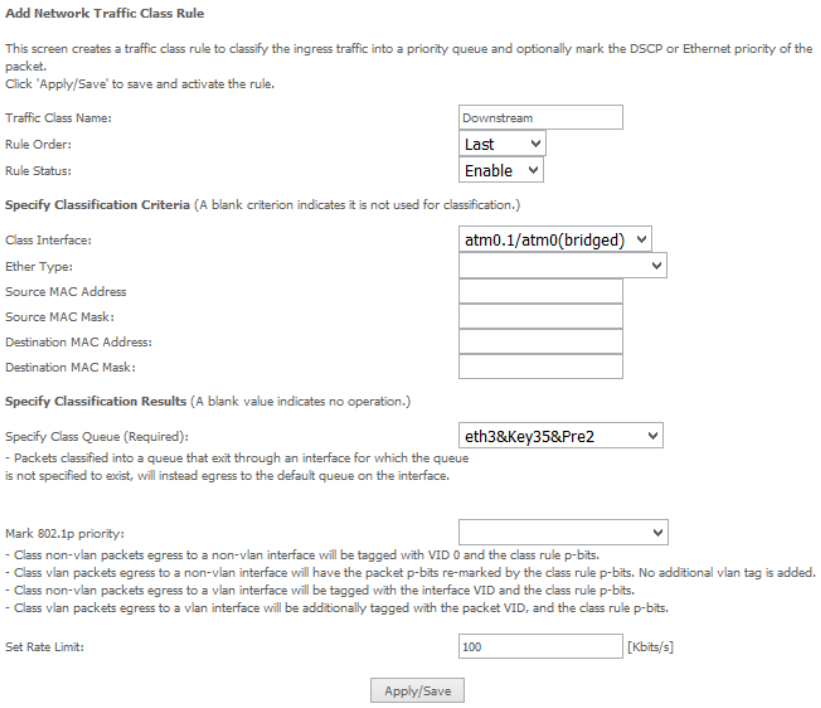
Limiting the downstream rate

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



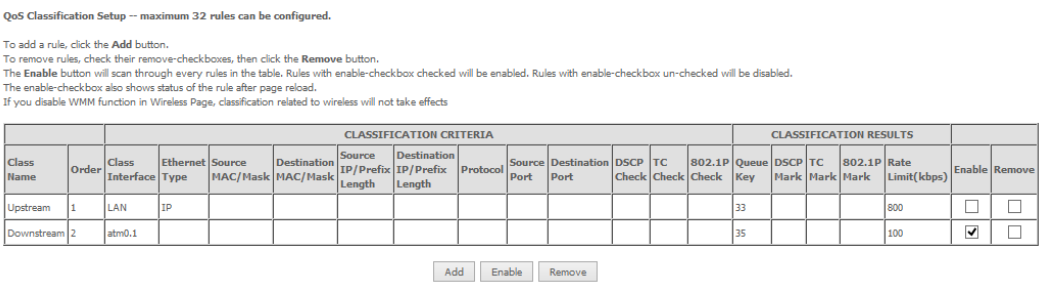
b) On the QoS Classification page, add a rule to limit the downstream rate, for example:

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:



Technical Data

The following table lists the hardware specifications of the NF8AC.

MODEL	NF8AC
ADSL Compliance	G.992.1 (T1.413) G.992.2 (G.dmt), G.lite G.992.3 (G.bis/ADS L2) G.992.5 (ADSL2+) Annex A Annex L (Reach Extended ADSL2) Supports ATM forum UNI3.0, 3.1 and 4.0 permanent virtual circuits (PVCs) Supports CBR, UBR, VBR-rt, VBR-nrt Supports multiple PVCs Supports ITU-T i.610F4/F5 OAM
VDSL Compliance	ITU-T G.993.2 Supports 8a, 8b, 12a, 12b and 17a profile
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	4 x 10/100/1000 Mbps, 1 x RJ-11 ADSL, 1 x WLAN
LED Indicators	Power, ADSL, WWW, LAN 1-4, WAN, WiFi.
Operating Temperature	Operating temperature: 0˚C - 40˚C, Humidity: 10%-90% non-condensing Storage temperature: -10˚C - 60˚C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 2A
Dimensions & Weight	190 mm (L) x 146 mm (H) x 33 mm (D) 361 grams
Regulatory Compliance	RCM, Telepermit

Electrical Specifications

It is recommended that the NF8AC be powered by the supplied 12V DC, 2A power supply. A replacement power supply is available from the NetComm Wireless Online shop.

Environmental Specifications / Tolerances

The NF8AC housing enables it to operate over a wide variety of temperatures from 0˚C - 40˚C (operating temperature).

Legal & Regulatory Information

Intellectual Property Rights

Customer Information

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

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

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the Consumer Protection Laws). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.
If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

Product Warranty

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

1. the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;
2. the Product Warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. the customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. the cost of transporting product to and from NetComm's nominated premises is your responsibility;
5. NetComm Wireless Limited does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and
6. the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm Wireless Limited recommends that you enable these features to enhance your security.

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

1. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;
2. the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm Wireless Limited; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitation of Liability

This clause does not apply to New Zealand consumers. Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the Consumer Protection Laws Section above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.
If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm Wireless's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm Wireless's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Wireless Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.
To the extent NetComm Wireless Limited is unable to limit its liability as set out above, NetComm Wireless Limited limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM WIRELESS LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
Phone: +61(0)2 9424 2070
Fax: +61(0)2 9424 2010
Email: sales@netcommwireless.com techsupport@netcommwireless.com