NetComm Wireless

VDSL/ADSL AC1600 WiFi Gigabit Modem Router

NF8AC USER GUIDE
Copyright
Copyright©2014 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless Limited.

⚠️ 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 Modern Router

<table>
<thead>
<tr>
<th>DOCUMENT VERSION</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 - Initial document release</td>
<td>September 2014</td>
</tr>
</tbody>
</table>

Table 1 - Document Revision History
# Table of Contents

Overview ...................................................................................................................... 5  
Introduction .................................................................................................................. 5  
Target Users .................................................................................................................. 5  
Prerequisites .................................................................................................................. 5  
Notation ....................................................................................................................... 6  
Product Introduction .................................................................................................... 6  
Product Overview ........................................................................................................ 6  
Package Contents ......................................................................................................... 6  
Product Features ......................................................................................................... 7  

Physical Dimensions and Indicators .......................................................................... 8  
LED Indicators ............................................................................................................. 8  
Physical Dimensions .................................................................................................. 9  
NF8AC Default Settings .............................................................................................. 9  
Interfaces .................................................................................................................... 10  
Rear .............................................................................................................................. 10  
Left ................................................................................................................................ 11  
Safety and Product Care .............................................................................................. 12  
Transport and Handling .............................................................................................. 12  
Installation and Configuration of the NF8AC ............................................................ 13  
Placement of your NF8AC .......................................................................................... 13  
Avoid obstacles and interference .............................................................................. 13  
Cordless Phones ........................................................................................................ 13  
Choose the “Quietest” Channel for your Wireless Network ...................................... 13  
Hardware installation ................................................................................................. 14  
Connecting via a cable ............................................................................................... 14  
Connecting wirelessly ............................................................................................... 14  
Web Based Configuration Interface ......................................................................... 15  
First-time Setup Wizard ............................................................................................. 15  
ADSL: .......................................................................................................................... 15  
VDSL: .......................................................................................................................... 16  
Device Info .................................................................................................................. 17  
Summary ..................................................................................................................... 17  
WAN ............................................................................................................................. 18  
Statistics ..................................................................................................................... 18  
Route ............................................................................................................................ 20  
ARP .............................................................................................................................. 20  
DHCP ........................................................................................................................... 20  
Advanced Setup ......................................................................................................... 21  
Layer2 Interface ......................................................................................................... 21  
WAN Service ............................................................................................................. 23  
LAN ............................................................................................................................. 26  
NAT ............................................................................................................................... 27  
Security ....................................................................................................................... 31  
Parental Control ......................................................................................................... 32  
Quality of Service ...................................................................................................... 33  
Routing ....................................................................................................................... 35  
DNS .............................................................................................................................. 37  
DSL ............................................................................................................................... 38  
UPnP ............................................................................................................................. 39  
DNS Proxy ................................................................................................................... 39  
DLNA ............................................................................................................................ 40  
Packet Acceleration ................................................................................................. 40  
Storage Service ......................................................................................................... 40  
Interface Grouping ..................................................................................................... 41  
IP Tunnel .................................................................................................................... 42  
IPSec ........................................................................................................................... 43  
Certificate .................................................................................................................... 44  
Power Management ................................................................................................. 44  
Multicast (IGMP Configuration) .............................................................................. 45  
Wireless ....................................................................................................................... 46
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.

<table>
<thead>
<tr>
<th>LED INDICATOR</th>
<th>ICON</th>
<th>COLOUR</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power</strong></td>
<td>![Power Icon]</td>
<td>Green</td>
<td>The NF8AC is powered on and operating normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>The NF8AC is starting up.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red Blinking</td>
<td>The firmware is being upgraded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The power is off.</td>
</tr>
<tr>
<td><strong>DSL</strong></td>
<td>![DSL Icon]</td>
<td>Off</td>
<td>No DSL signal detected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking (Slow)</td>
<td>Data is being transferred over the DSL line.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking (Fast)</td>
<td>The NF8AC is attempting to connect to the xDSL service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>The DSL connection is established.</td>
</tr>
<tr>
<td><strong>Internet</strong></td>
<td>![Internet Icon]</td>
<td>Green</td>
<td>The NF8AC is connected to an internet service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Red</td>
<td>Authentication on the broadband account has failed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the internet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The NF8AC is not connected to the internet.</td>
</tr>
<tr>
<td><strong>WAN</strong></td>
<td>![WAN Icon]</td>
<td>Green</td>
<td>A device is connected to the Ethernet WAN port.</td>
</tr>
<tr>
<td>LAN 1-4</td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the WAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No device is connected to the Ethernet WAN port.</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td>![LAN Icon]</td>
<td>Green</td>
<td>A device is connected to the Ethernet LAN port.</td>
</tr>
<tr>
<td>1-4</td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the Ethernet LAN port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No device is connected to the Ethernet LAN port.</td>
</tr>
<tr>
<td><strong>N</strong></td>
<td>![N Icon]</td>
<td>Green</td>
<td>2.4GHz WiFi is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the 2.4GHz Wireless interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>WiFi is disabled.</td>
</tr>
<tr>
<td><strong>AC</strong></td>
<td>![AC Icon]</td>
<td>Green</td>
<td>5GHz WiFi is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the 5GHz Wireless interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>WiFi is disabled.</td>
</tr>
<tr>
<td><strong>WPS</strong></td>
<td>![WPS Icon]</td>
<td>Green</td>
<td>The client has successfully connected to the router.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>The client is accessing the router via WPS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>WPS is disabled.</td>
</tr>
<tr>
<td><strong>USB 1 - 2</strong></td>
<td>![USB Icon]</td>
<td>Green</td>
<td>A USB hard drive is connected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted through the USB interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>No USB hard drive is connected to the USB interface.</td>
</tr>
</tbody>
</table>
Physical Dimensions

The following page lists the physical dimensions of the NF8AC.

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

<table>
<thead>
<tr>
<th>NF8AC DIMENSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
</tr>
<tr>
<td>Height</td>
</tr>
<tr>
<td>Depth</td>
</tr>
<tr>
<td>Weight</td>
</tr>
</tbody>
</table>

NF8AC Default Settings

The following tables list the default settings for the NF8AC.

<table>
<thead>
<tr>
<th>LAN (MANAGEMENT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Default Gateway</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WIRELESS (WIFI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
</tr>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Security Key</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NF8AC WEB INTERFACE ACCESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
</tr>
<tr>
<td>Password</td>
</tr>
</tbody>
</table>
Interfaces

Rear

The following interfaces are available on the NF8AC:

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DSL</td>
<td>Use the provided RJ-11 cable to connect the router to the telephone line operating your xDSL service.</td>
</tr>
<tr>
<td>2</td>
<td>Ethernet 1 - 4</td>
<td>Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.</td>
</tr>
<tr>
<td>3</td>
<td>WAN</td>
<td>Gigabit WAN port for connection to a WAN network.</td>
</tr>
<tr>
<td>4</td>
<td>Reset button</td>
<td>Activate the Reset function by holding the Reset button down for 3 seconds.</td>
</tr>
<tr>
<td>5</td>
<td>USB 2</td>
<td>Connect an external USB hard drive here to use the NAS feature of the NF8AC.</td>
</tr>
<tr>
<td>6</td>
<td>Power</td>
<td>Connection point for the included power adapter. Connect the power supply here.</td>
</tr>
<tr>
<td>NUMBER</td>
<td>INTERFACE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>WPS N</td>
<td>Activate the WPS function for the 2.4GHz network by holding the WPS button down for 3 seconds.</td>
</tr>
<tr>
<td>2</td>
<td>WPS AC</td>
<td>Activate the WPS function for the 5GHz network by holding the WPS button down for 3 seconds.</td>
</tr>
<tr>
<td>3</td>
<td>USB 1</td>
<td>Connect an external USB hard drive here to use the NAS feature of the NF8AC.</td>
</tr>
<tr>
<td>4</td>
<td>Power</td>
<td>Turns the NF8AC on or off.</td>
</tr>
</tbody>
</table>
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 device 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.
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.

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

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.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturer</td>
<td>Indicates that NetComm Wireless is the manufacturer of this product.</td>
</tr>
<tr>
<td>Product Class</td>
<td>The model of the product.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The unique set of numbers assigned to the routers for identification purposes.</td>
</tr>
<tr>
<td>Build Timestamp</td>
<td>The date and time that the software running on the router was published.</td>
</tr>
<tr>
<td>Software Version</td>
<td>The current firmware version installed on the router.</td>
</tr>
<tr>
<td>Bootloader (CFE) Version</td>
<td>The current boot loader installed on the router.</td>
</tr>
<tr>
<td>DSL PHY and Driver Version</td>
<td>The current boot loader installed on the router.</td>
</tr>
<tr>
<td>VDSL PROFILE</td>
<td>The VDSL profile in use. Supports 8a, 8b, 12a and 17a VDSL profiles.</td>
</tr>
<tr>
<td>DSL PHY and Driver Version</td>
<td>The current line driver installed on the router.</td>
</tr>
<tr>
<td>Wireless Driver Version</td>
<td>The current wireless driver installed on the router.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The number of days, hours and minutes that the router has been running.</td>
</tr>
<tr>
<td>Line Rate – Upstream (Kbps)</td>
<td>The current upstream speed of the DSL connection in Kbps.</td>
</tr>
<tr>
<td>Line Rate – Downstream (Kbps)</td>
<td>The current upstream speed of the DSL connection in Kbps.</td>
</tr>
<tr>
<td>LAN IPv4 Address</td>
<td>The current version 4 LAN IP address assigned to the router.</td>
</tr>
<tr>
<td>WAN IPv4 Address</td>
<td>The current version 4 WAN IP address assigned to the router.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The current default gateway of the WAN interface.</td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td>The current primary DNS server in use.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>The current secondary DNS server in use.</td>
</tr>
<tr>
<td>LAN IPv6 Address</td>
<td>The current IPv6 LAN IP address in use if assigned.</td>
</tr>
<tr>
<td>WAN IPv6 Address</td>
<td>The current IPv6 WAN IP address in use if assigned.</td>
</tr>
<tr>
<td>Default IPv6 Gateway</td>
<td>The current IPv6 default gateway if assigned.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>The current date and time set on the router.</td>
</tr>
</tbody>
</table>
WAN

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

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The Interface of the WAN connection.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the WAN connection.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of WAN connection.</td>
</tr>
<tr>
<td>VLAN Mux ID</td>
<td>Details the status of VLAN Mux ID if used.</td>
</tr>
<tr>
<td>IGMP</td>
<td>Details the status of IGMP on each WAN connection. IGMP is only used with IP v4 connections.</td>
</tr>
<tr>
<td>NAT</td>
<td>The NAT status of the WAN connection.</td>
</tr>
<tr>
<td>Firewall</td>
<td>The status of the router firewall across the WAN connection.</td>
</tr>
<tr>
<td>IPv4 Status</td>
<td>The status of the IPv4 WAN connection.</td>
</tr>
<tr>
<td>IPv6 Status</td>
<td>The status of the IPv6 WAN connection.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The current IP v4 address of the WAN connection.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The current IP v6 address of the WAN connection.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received/Transmitted</td>
<td>Bytes</td>
</tr>
<tr>
<td></td>
<td>Packets</td>
</tr>
<tr>
<td></td>
<td>Errors</td>
</tr>
<tr>
<td></td>
<td>Drops</td>
</tr>
</tbody>
</table>

Statistics – WAN Service

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

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received/Transmitted</td>
<td>Bytes</td>
</tr>
<tr>
<td></td>
<td>Packets</td>
</tr>
<tr>
<td></td>
<td>Errors</td>
</tr>
<tr>
<td></td>
<td>Drops</td>
</tr>
</tbody>
</table>
The Statistics – xTM page shows details related to the xTM interface of the router.

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

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.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Subnet Mask</th>
<th>Flag</th>
<th>Metric</th>
<th>Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>b/0</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Flags</th>
<th>HW Address</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.2</td>
<td>Complete</td>
<td>00:21:80:1d:89:aa</td>
<td>b/0</td>
</tr>
</tbody>
</table>

DHCP
Click DHCP to display the DHCP information.

<table>
<thead>
<tr>
<th>Hostname</th>
<th>MAC Address</th>
<th>IP Address</th>
<th>Expires In</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdg26</td>
<td>00:21:80:1d:89:aa</td>
<td>192.168.20.2</td>
<td>23 hours, 80 minutes, 44 seconds</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>This field shows the interface name.</td>
</tr>
<tr>
<td>VPI</td>
<td>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.</td>
</tr>
<tr>
<td>VCI</td>
<td>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.</td>
</tr>
<tr>
<td>DSL Latency</td>
<td>The value of the DSL Latency.</td>
</tr>
<tr>
<td>Category</td>
<td>This field shows the ATM service classes.</td>
</tr>
<tr>
<td>Peak Cell Rate (cell/s)</td>
<td>The maximum number of cells that may be transferred per second over the ATM interface.</td>
</tr>
<tr>
<td>Sustainable Cell Rate (cell/s)</td>
<td>An average, long-term cell transfer rate on the ATM interface.</td>
</tr>
<tr>
<td>Max Burst Size (bytes)</td>
<td>The maximum allowable burst size of cells that can be transmitted contiguously on the ATM interface.</td>
</tr>
<tr>
<td>Min Cell Rate (cell/s)</td>
<td>The minimum allowable rate at which cells may be transferred on the ATM interface.</td>
</tr>
<tr>
<td>Link Type</td>
<td>This field shows the type of link in use.</td>
</tr>
<tr>
<td>Connection Mode</td>
<td>This field shows the selected mode of connection.</td>
</tr>
<tr>
<td>IP QoS</td>
<td>This field shows the status of the Quality of Service (QoS) function.</td>
</tr>
<tr>
<td>MPAAL Prec/Alg/Wght</td>
<td>This displays data related to load balancing.</td>
</tr>
<tr>
<td>Remove</td>
<td>Select this field to remove the ATM configuration.</td>
</tr>
</tbody>
</table>

To add an ATM interface, click the **Add** button. Enter the details as required by your Internet Service Provider and click the **Apply/Save** button.
PTM Interface
The router can also establish DSL connections using PTM (Packet Transfer Mode). This page shows you an overview of the PTM interfaces and allows you to add or remove them.

![PTM Interface Configuration](image)

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.

![ETH Interface Configuration](image)
WAN Service

The WAN Service page displays the current Wide Area Network service setup and allows you to configure the router to connect to a larger network for Internet access.

![WAN Service Interface Configuration](image)

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.

WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPv4 mode.
If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix length and interface gateway.

- Enable IPv4 for this service
- Obtain an IP address automatically
- Use the following Static IP address
  - Option 55 Request List
  - Option 60 Vendor ID
  - Option 59 Rebinding Times
  - Option 58 Renewal Time
  - Option 61 TADC
  - Option 61 DUOD
  - Option 128

- Enable IPv6 for this service

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

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

- Enable NAT
- Enable FUPena NAT
- Enable Firewall

Multicast Proxy
- Enable IGMP Multicast

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.

Routing – Default Gateway

Use the arrow buttons to move the interfaces required as DNS Server interfaces to the left. The interface highest on the list has the highest priority as a DNS server. Click Next to continue.

DNS Server Configuration

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.

### IPv6 LAN Auto Configuration

**Note:**
1. Stateless DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION format. Please enter the complete information. For example: Please enter "60::20" instead of "60:20:20".
2. Unique local address must start with "fe". The prefix and the address must be in same network and the prefix length must be 64.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Unique Local Addresses and Prefix Advertisement</td>
<td>Enable the use of unique local addresses. The router will advertise the IPv6 prefix to new devices on the network.</td>
</tr>
<tr>
<td>Randomly Generate</td>
<td>Randomly generates the unique local addresses and the prefix.</td>
</tr>
<tr>
<td>Statically Configure</td>
<td>Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider.</td>
</tr>
<tr>
<td>IPv6 LAN Applications</td>
<td>Enable IPv6 DHCP server</td>
</tr>
<tr>
<td>Enable DHCPv6 Server and RADVD</td>
<td>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.</td>
</tr>
<tr>
<td>Stateless</td>
<td>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.</td>
</tr>
<tr>
<td>Stateful</td>
<td>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.</td>
</tr>
<tr>
<td>Enable MLD Snooping</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

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.

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

### DMZ Host

<table>
<thead>
<tr>
<th>DMZ Host IP Address</th>
<th>Enable LAN Loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

### ALG

- Enable FTP
- Enable SIP
- Enable TFTP
- Enable M32
- Enable IRC
- Enable POP
- Enable SMTP
- Enable RTSP

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

### Multi Nat

<table>
<thead>
<tr>
<th>mode</th>
<th>Internal Address Start</th>
<th>Internal Address End</th>
<th>External Address Start</th>
<th>External Address End</th>
</tr>
</thead>
</table>

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.

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.

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

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

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>A user defined name for the time restriction rule.</td>
</tr>
<tr>
<td>Browser’s MAC Address</td>
<td>The MAC address of the network card of the computer running the browser.</td>
</tr>
<tr>
<td>Other MAC Address</td>
<td>The MAC address of a second LAN device or network card.</td>
</tr>
<tr>
<td>Days of the Week</td>
<td>The days of the week for which the rules apply.</td>
</tr>
<tr>
<td>Start Blocking Time</td>
<td>The time of day when the restriction starts.</td>
</tr>
<tr>
<td>End blocking time</td>
<td>The time of day when the restriction ends.</td>
</tr>
</tbody>
</table>

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.

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.

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.

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 2 queues can be configured.
To add a queue, click the Add button.
To remove queues, check the remove checkboxes, then click the Remove button.
The Enable button will turn on/off every queue in the table. Queue with enable-checkbox checked will be enabled. Queue with enable-checkbox un-checked will be disabled.
If you disable WMM function in Wireless page, queues related to wireless will not take effects.

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 22 rules can be configured.

To add a rule, click the Add button.
To remove rule, check their remove checkboxes, then click the Remove button.
The Enable button will turn on/off every rule in the table. Rule with enable-checkbox checked will be enabled. Rule with enable-checkbox un-checked will be disabled.
If you disable WMM function in Wireless page, classification related to wireless will not take effects.

Figure 8: Advanced - QoS Classification Setup

Click the Add button to configure network traffic classes.
The above screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte. A rule consists of a class name and at least one condition. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

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

### Routing

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

**Default Gateway**

Select your preferred WAN interface from the available options.
Static Route
The Static Route screen displays the configured static routes. Click the **Add** or **Remove** buttons to change settings.

![Static Route Screen](image)

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

![Add Static Route Screen](image)

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.

![Policy Routing Screen](image)

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

![Add Policy Route Screen](image)

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

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>A user defined name for the policy route.</td>
</tr>
<tr>
<td>Physical LAN Port</td>
<td>The LAN port to be used for the policy.</td>
</tr>
<tr>
<td>Source IP</td>
<td>The IP address of the LAN device involved with the policy.</td>
</tr>
<tr>
<td>Use Interface</td>
<td>Select the Interface that the policy will employ.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the gateway address.</td>
</tr>
</tbody>
</table>
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.

![RIP Configuration](image)

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.

![DNS Server Configuration](image)

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.

![Dynamic DNS](image)

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.
Advanced DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

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

![Figure 18: Advanced - DNS - Add Dynamic DNS Account](image)

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-DNS Provider</td>
<td>Select the dynamic DNS provider from the list.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The name of the dynamic DNS provider.</td>
</tr>
<tr>
<td>Interface</td>
<td>Select the interface from the list.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the Dynamic DNS account username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Dynamic DNS account password.</td>
</tr>
</tbody>
</table>

![Table 2: Advanced - DNS - Add Dynamic DNS Account Settings](image)

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](image)

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

![Figure 20: Advanced - DSL - Advanced DSL Settings](image)
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](image)

**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](image)

**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](image)

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.

![Digital Media Server Settings](image)

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.

![Packet Acceleration](image)

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.

![Storage Service](image)

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.

![Storage User Account Configuration](image)

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

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

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

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

**IP Tunnel**

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

IPv6inIPv4

Click the **Add** button to add a new tunnel.
IPv4inIPv6

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

**IPSec**

The 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.

Enter the following parameters:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Connection Name</td>
<td>Enter a name to identify the IPSec tunnel</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>Select the applicable IPSec tunnel mode</td>
</tr>
<tr>
<td>Remote IPSec Gateway</td>
<td>Enter the IP Address of the IPSec server to connect to</td>
</tr>
<tr>
<td>Tunnel access from Local</td>
<td>Select which remote addresses local IPSec connections are able to access</td>
</tr>
<tr>
<td>IP Address from VPN</td>
<td>Enter the IP Address to be used locally for the IPSec tunnel</td>
</tr>
<tr>
<td>Subnet mask for VPN</td>
<td>Enter the subnet mask to be used locally for the IPSec tunnel</td>
</tr>
<tr>
<td>Tunnel Access from Remote</td>
<td>Select which local addresses remote IPSec connections are able to access</td>
</tr>
<tr>
<td>IP Address for VPN</td>
<td>Enter the IP Address to be used on the remote end for the IPSec tunnel</td>
</tr>
<tr>
<td>Subnet mask for VPN</td>
<td>Enter the subnet mask to be used on the remote end for the IPSec tunnel</td>
</tr>
<tr>
<td>Key Exchange Method</td>
<td>Select the type of IPSec exchange to be used on the IPSec tunnel</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Select the applicable authentication for the IPSec tunnel</td>
</tr>
<tr>
<td>Perfect Forward Secrecy</td>
<td>Select to use Perfect Forward Secrecy during key exchange for the IPSec tunnel</td>
</tr>
<tr>
<td>Advanced IKE Settings</td>
<td>Configure advanced IKE settings for the IPSec tunnel such as the encryption method or key life time</td>
</tr>
</tbody>
</table>

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

Local

Local Certificates
Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.
Notice: Import and Remove Certificate need reboot the gateway

<table>
<thead>
<tr>
<th>Name</th>
<th>In Use</th>
<th>Subject</th>
<th>Type</th>
<th>Action</th>
</tr>
</thead>
</table>

Figure 35: Advanced – Certificate - Local

Trusted CA

Trusted CA (Certificate Authority) Certificates
Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.
Notice: Import and Remove Certificate need reboot the gateway

<table>
<thead>
<tr>
<th>Name</th>
<th>Subject</th>
<th>Type</th>
<th>Action</th>
</tr>
</thead>
</table>

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.

Power Management
This page allows control of Hardware modules to evaluate power consumption. Use the control buttons to select the desired option, click Apply and check the status response.

- MIPS CPU Clock divider when Idle
  - Enable Status: Enabled

- Wait instruction when Idle
  - Enable Status: Enabled

- DRAM Self Refresh
  - Enable Status: Enabled

- Energy Efficient Ethernet
  - Enable Status: Enabled

- Ethernet Auto Power Down and Sleep
  - Enable Status: Enabled

- Adaptive Voltage Scaling
  - Enable Status: Enabled

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.

![IGMP Configuration](image)

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Version</td>
<td>The version IGMP in use by the router.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Query Response Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Last Member Query Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Robustness Value</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum Multicast Groups</td>
<td>The maximum number of multicast groups that the router can control at any one time.</td>
</tr>
<tr>
<td>Maximum Multicast Data Sources</td>
<td>The maximum number of data sources a multicast group can have.</td>
</tr>
<tr>
<td>Maximum Multicast Group Members</td>
<td>The maximum number of hosts a multicast group can have.</td>
</tr>
<tr>
<td>Fast Leave Enable</td>
<td>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.</td>
</tr>
</tbody>
</table>
Wireless
WiFi 2.4GHz / WiFi 5GHz

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

![Wireless Basic Page](image)

The following parameters are available:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Wireless</td>
<td>Select to enable or disable the wireless network function</td>
</tr>
<tr>
<td>Hide Access Point</td>
<td>Select to hide or display the wireless network when an SSID scan is performed</td>
</tr>
<tr>
<td>Clients Isolation</td>
<td>Select to prevent clients on the wireless network being able to access each other</td>
</tr>
<tr>
<td>Disable WMM Advertise</td>
<td>Select to prevent the NF8AC advertising its WMM function</td>
</tr>
<tr>
<td>Enable Multicast Forwarding (WMP)</td>
<td>Select to enable Wireless Multicast Forwarding. This can reduce latency and improve throughput for wireless clients</td>
</tr>
<tr>
<td>Max Clients</td>
<td>Enter the maximum number of wireless clients able to connect to the wireless network</td>
</tr>
<tr>
<td>Wireless Guest Network</td>
<td>Select to enable a separate Wireless Guest network, the same options are available for a Guest network as with the main system wireless network.</td>
</tr>
</tbody>
</table>

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.

The following parameters are available:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable WPS</td>
<td>Select to enable or disable the WPS function of the NF8AC.</td>
</tr>
<tr>
<td>Select SSID</td>
<td>Select the SSID to apply the security settings to.</td>
</tr>
<tr>
<td>Network Authentication</td>
<td>Select the Wireless security type to use with the wireless network.</td>
</tr>
<tr>
<td>WPA/WAP passphrase</td>
<td>Enter the security key to use with the wireless network.</td>
</tr>
<tr>
<td>WPA Group Rekey Interval</td>
<td>Enter the group rekey interval. This should not need to change.</td>
</tr>
<tr>
<td>WPA/WAPI Encryption</td>
<td>Select the type of encryption to use on the wireless network.</td>
</tr>
<tr>
<td>WEP Encryption</td>
<td>Select to utilise WEP encryption on the wireless network connection.</td>
</tr>
</tbody>
</table>

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.

**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.
<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band</td>
<td>You can select 2.4GHz or 5GHz.</td>
</tr>
<tr>
<td>Channel</td>
<td>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.</td>
</tr>
<tr>
<td>Auto Channel Timer(min)</td>
<td>Specifies the timer of auto channeling.</td>
</tr>
<tr>
<td>802.11n/EWC</td>
<td>Select disable 802.11n or Auto.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>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.</td>
</tr>
<tr>
<td>Control Sideband</td>
<td>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<del>7. When you select Upper, the channel is 5</del>11.</td>
</tr>
<tr>
<td>802.11n Rate</td>
<td>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.</td>
</tr>
<tr>
<td>802.11n Protection</td>
<td>The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without &quot;speaking&quot; at the same time.</td>
</tr>
<tr>
<td>Support 802.11n Client Only</td>
<td>Only stations that are configured in 802.11n mode can associate.</td>
</tr>
<tr>
<td>54g Rate</td>
<td>Allows you to specify the maximum bandwidth of the 802.11g network.</td>
</tr>
<tr>
<td>Multicast Rate</td>
<td>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.</td>
</tr>
<tr>
<td>Basic Rate</td>
<td>Select the basic transmission rate ability for the AP.</td>
</tr>
<tr>
<td>Fragmentation Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>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.</td>
</tr>
<tr>
<td>D TIM Interval</td>
<td>(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.</td>
</tr>
<tr>
<td>Beacon Interval</td>
<td>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.</td>
</tr>
<tr>
<td>XPress Technology</td>
<td>Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default is Disabled.</td>
</tr>
<tr>
<td>Transmit Power</td>
<td>Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.</td>
</tr>
<tr>
<td>WMM (Mi-Fi Multimedia)</td>
<td>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.</td>
</tr>
<tr>
<td>WMM No Acknowledgement</td>
<td>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.</td>
</tr>
<tr>
<td>WMM APSD</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETH Connection</td>
<td>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.</td>
</tr>
<tr>
<td>Test your Wireless Connection</td>
<td>Pass: Indicates that the wireless card is switched ON. Fail: Indicates that the wireless card is switched OFF.</td>
</tr>
</tbody>
</table>

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.

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).

### TR-069 Client - Configuration
- **WAN Management Protocol (TR-069)**: Allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to the device.
- **Inform**: Select the desired values and click 'Apply/Save' to configure the TR-069 client options.
- **Enable WAN Management Protocol (TR-069)**: Set to enable or disable.
- **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.

### TABLE
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inform</td>
<td>Set to enable to activate TR-069 client settings.</td>
</tr>
<tr>
<td>Inform interval</td>
<td>Time in seconds that data is sent to the Auto-Configuration Server (ACS).</td>
</tr>
<tr>
<td>ACS URL</td>
<td>The address where the ACS server is located.</td>
</tr>
<tr>
<td>ACS User Name</td>
<td>The user name to access the ACS server.</td>
</tr>
<tr>
<td>ACS Password</td>
<td>The password to access the ACS server.</td>
</tr>
<tr>
<td>WAN Interface used by TR-069 Client</td>
<td>The connection used to send and receive data to the ACS server.</td>
</tr>
</tbody>
</table>

### 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.

### Time settings
This page allows you to configure the Internet time settings:
- **First NTP Time Server**: Other (netcomm.pool.ntp.org)
- **Second NTP Time Server**: Other (netcomm.pool.ntp.org)
- **Third NTP Time Server**: None
- **Fourth NTP Time Server**: None
- **Fifth NTP Time Server**: None
- **Current Router Time**: Sun Nov 19 03:42:14 2011 (GMT+10.00) Canberra, Melbourne, Sydney
- **Time Zone Offset**: (GMT+10.00) Canberra, Melbourne, Sydney

**Apply/Save**
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.

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.
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.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Check that the NF8AC and the power source are both turned on and device is receiving sufficient power.</td>
</tr>
<tr>
<td>3</td>
<td>Turn the NF8AC off and on.</td>
</tr>
<tr>
<td>4</td>
<td>If the error persists, you may have a hardware problem. In this case, you should contact technical support.</td>
</tr>
</tbody>
</table>

Web Configuration

I cannot access the web configuration pages.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer’s IP address matches it.</td>
</tr>
<tr>
<td>3</td>
<td>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.</td>
</tr>
<tr>
<td>4</td>
<td>If you have changed the device’s IP address, then enter the new one as the URL you enter into the address bar of your web browser.</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
</tr>
</tbody>
</table>

The web configuration does not display properly.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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.)</td>
</tr>
</tbody>
</table>

Login Username and Password

I forgot my login username and/or password.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>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).</td>
</tr>
<tr>
<td>2</td>
<td>It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.</td>
</tr>
</tbody>
</table>

WLAN Interface

I cannot access the NF8AC from the WLAN or ping any computer on the WLAN.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.</td>
</tr>
<tr>
<td>2</td>
<td>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.</td>
</tr>
</tbody>
</table>
Appendix: Quality of Service Setup Example

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

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 is 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.

```
DHCP Static IP Lease

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

```
MAC Address: 00:20:A3:09:01:00
IP Address: 192.168.1.1
```

```
Apply/Save
```

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
```

```
QoS – Queue Management Configuration

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. The Apply/Save button will save it.

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

QoS Classification: (Egress)
DSCP
DSCP Priority
Access Class
Packet Acceleration
Storage Service
```

```
Select Default DSCP Mark default(000000)  
Apply/Save
```
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_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(0x806), 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.**
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(0x806), Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 802.1Q(0x8868), 802.1Q(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.
Technical Data

The following table lists the hardware specifications of the NF8AC.

<table>
<thead>
<tr>
<th>MODEL</th>
<th>NF8AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSL Compliance</td>
<td>G.992.1 (T1.413)</td>
</tr>
<tr>
<td></td>
<td>G.992.2 (G.dmt), G.lite</td>
</tr>
<tr>
<td></td>
<td>G.992.3 (G.bis/ADS L2)</td>
</tr>
<tr>
<td></td>
<td>G.992.5 (ADSL2+)</td>
</tr>
<tr>
<td></td>
<td>Annex A</td>
</tr>
<tr>
<td></td>
<td>Annex L (Reach Extended ADSL2)</td>
</tr>
<tr>
<td></td>
<td>Supports ATM forum UNI3.0, 3.1 and 4.0 permanent virtual circuits (PVCs)</td>
</tr>
<tr>
<td></td>
<td>Supports CBR, UBR, VBR-rt, VBR-nrt</td>
</tr>
<tr>
<td></td>
<td>Supports multiple PVCs</td>
</tr>
<tr>
<td></td>
<td>Supports ITU-T.L.610/4/5.67/69.6</td>
</tr>
<tr>
<td>VDSL Compliance</td>
<td>ITU-T G.993.2</td>
</tr>
<tr>
<td></td>
<td>Supports 8a, 8b, 12a, 12b and 17a profile</td>
</tr>
<tr>
<td>Ethernet WAN</td>
<td>1 x Gigabit WAN port (10/100/1000 Mbps)</td>
</tr>
<tr>
<td>Connectivity</td>
<td>.4 x 10/100/1000 Mbps, 1 x R-J 11 ADSL, 1 x WLAN</td>
</tr>
<tr>
<td>LED Indicators</td>
<td>Power, ADSL, WWW, LAN 1-4, WAN, WiFi</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>Operating temperature: 0°C - 40°C, Humidity: 10%-90% non-condensing</td>
</tr>
<tr>
<td></td>
<td>Storage temperature: -10°C - 60°C, Humidity: 0%-95% non-condensing</td>
</tr>
<tr>
<td>Power Input</td>
<td>12V DC - 2A</td>
</tr>
<tr>
<td>Dimensions &amp; Weight</td>
<td>190 mm (L) x 146 mm (H) x 33 mm (D)</td>
</tr>
<tr>
<td></td>
<td>361 grams</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>RCM, Telepermit</td>
</tr>
</tbody>
</table>

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

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out this Manual are owned by and vest in NetComm Wireless (ACN 002490486) (NetComm Wireless Limited) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited’s (or its licensors’) intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless product to which it relates. Otherwise no part of this Manual may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Wireless Limited.

NetComm, NetComm Wireless and NetComm Wireless Limited are a trademark of NetComm Wireless Limited. All other trademarks are acknowledged to be the property of their respective owners.

Customer Information

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

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.

2. This equipment incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.

3. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
   i. Change the direction or relocate the receiving antenna.
   ii. Increase the separation between this equipment and the receiver.
   iii. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
   iv. Consult an experienced radio/TV technician for help.

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

Consumer Protection Laws

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

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

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

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

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

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

Limitation of Liability

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

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

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

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