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 NF10W VDSL/ADSL WiFi Modem Router

<table>
<thead>
<tr>
<th>DOCUMENT VERSION</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 - Initial document release</td>
<td>28 September 2015</td>
</tr>
<tr>
<td>1.1 – Added more QoS examples</td>
<td>24 November 2015</td>
</tr>
</tbody>
</table>

Table 1 - Document Revision History
# Table of contents

Overview ....................................................................................................................... 5
Introduction .................................................................................................................... 5
Target audience ............................................................................................................. 5
Prerequisites .................................................................................................................. 5
Notation ......................................................................................................................... 5
Welcome ......................................................................................................................... 6
Product overview .......................................................................................................... 6
Package contents ......................................................................................................... 6
Product features ............................................................................................................ 7
Physical dimensions and indicators ............................................................................ 8
LED indicators ............................................................................................................... 8
Physical Dimensions .................................................................................................... 9
NF10W Default Settings .............................................................................................. 9
Interfaces ....................................................................................................................... 10
Rear ............................................................................................................................... 10
Top ............................................................................................................................... 11
Safety and product care ............................................................................................... 12
Transport and handling ............................................................................................... 12
Installation and configuration of the NF10W ............................................................. 13
   Placement of your NF10W ......................................................................................... 13
      Avoiding obstacles and interference ................................................................. 13
      Cordless phones ................................................................................................. 13
      Choosing the “quietest” channel for your wireless network ......................... 14
      Hardware installation ......................................................................................... 14
         Connecting a client via Ethernet cable ......................................................... 14
         Connecting a client wirelessly ..................................................................... 14
Web based configuration interface ............................................................................. 15
   First-time setup wizard ......................................................................................... 15
      ADSL ................................................................................................................... 15
      VDSL ............................................................................................................... 16
      Ethernet WAN ................................................................................................. 16
Device Info ................................................................................................................... 17
   Summary ................................................................................................................ 17
   WAN ....................................................................................................................... 19
   Statistics .............................................................................................................. 19
   Route ................................................................................................................... 22
   ARP ...................................................................................................................... 22
   DHCP .................................................................................................................. 22
Advanced Setup .......................................................................................................... 23
   Layer2 Interface ................................................................................................. 23
   WAN Service ..................................................................................................... 25
   LAN ..................................................................................................................... 29
   NAT .................................................................................................................... 31
   Security ............................................................................................................... 34
   Parental Control ................................................................................................. 37
Quality of Service ....................................................................................................... 39
Routing .......................................................................................................................... 41
   DNS .................................................................................................................... 43
   DSL ..................................................................................................................... 44
   UPnP ................................................................................................................... 45
   DNS Proxy ........................................................................................................ 45
   DLNA .................................................................................................................. 46
   Storage Service ................................................................................................. 46
   Interface Grouping ............................................................................................. 47
   IP Tunnel ........................................................................................................... 48
   IPSec .................................................................................................................. 49
   Multicast (IGMP Configuration) ....................................................................... 50
Wireless ....................................................................................................................... 51
   Basic .................................................................................................................. 51
   Diagnostics ...................................................................................................... 56
Diagnostics..........................................................56
Ethernet OAM......................................................57
Management.......................................................58
Settings...........................................................58
System Log.......................................................59
SNMP Agent.....................................................60
TR-069 Client....................................................60
Internet Time.....................................................61
Access Control..................................................61
Update Firmware...............................................62
Reboot............................................................62
Additional Product Information.................................63
Establishing a wireless connection.............................63
Windows 7 .......................................................63
Windows 8/8.1/10 ..............................................63
Mac OSX 10.6 ..................................................63
Troubleshooting................................................64
Using the indicator lights (LEDs) to Diagnose Problems........64
Appendix: Quality of Service Setup Example.....................65
Reserving IP addresses........................................65
QoS Configuration Settings....................................66
High Priority QoS Queue Configuration.....................67
Low Priority QoS Queue Configuration.....................68
High Priority QoS Classification...........................68
Low Priority QoS Classification............................70
Limiting the upstream rate..................................71
Limiting the downstream rate..............................72
Legal & Regulatory Information................................73
Intellectual Property Rights..................................73
Customer Information........................................73
Consumer Protection Laws..................................73
Product Warranty.............................................74
Limitation of Liability.......................................74
Contact..........................................................75
Overview

Introduction
This manual provides information related to the installation, operation, and use of the NF10W.

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

Prerequisites
Before continuing with the installation of your NF10W, please confirm that you meet the minimum system requirements below.

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

Notation
The following symbols are used in this manual:

⚠ Indicates a note requiring attention.

⚠ Indicates a note providing a warning.

ℹ Indicates a note providing useful information.
Welcome

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

Product overview

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

Package contents

The NF10W package consists of:

- 1 x NetComm Wireless NF10W VDSL/ADSL WiFi Modem Router
- 1 x Quick Start Guide
- 1 x 1.5m RJ45 Ethernet cable
- 1 x RJ11 Telephone cable
- 1 x WiFi security card
- 1 x Warranty card
- 1 x Power supply (12V/1.5A)

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

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

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

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

Note: Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g, and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.
Physical dimensions and indicators

LED indicators

The NF10W 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 NF10W 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>Power</td>
<td></td>
<td>Green</td>
<td>The NF10W is powered on and operating normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>The power is off.</td>
</tr>
<tr>
<td>DSL</td>
<td></td>
<td>Off</td>
<td>No DSL signal detected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Synching</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green</td>
<td>DSL synchronized.</td>
</tr>
<tr>
<td>Internet</td>
<td></td>
<td>Green</td>
<td>The NF10W is connected to an internet service.</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 NF10W is not connected to the internet.</td>
</tr>
<tr>
<td>WAN</td>
<td></td>
<td>Green</td>
<td>A device is connected to the Ethernet WAN port.</td>
</tr>
<tr>
<td></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>LAN 1-4</td>
<td></td>
<td>Green</td>
<td>A device is connected to the Ethernet LAN port.</td>
</tr>
<tr>
<td></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>WiFi</td>
<td></td>
<td>Green</td>
<td>WiFi is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>Data is being transmitted to or from the Wireless interface.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>WiFi is disabled.</td>
</tr>
<tr>
<td>WPS</td>
<td></td>
<td>Green</td>
<td>WPS is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Green Blinking</td>
<td>WPS pairing is triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Off</td>
<td>WPS is disabled.</td>
</tr>
<tr>
<td>USB 1 - 2</td>
<td></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 NF10W. The length and width measurements were taken at the base where the dimensions are slightly larger.

Weight: approximately 260 grams

NF10W Default Settings
The following tables list the default settings for the NF10W.

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

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

### NF10W WEB INTERFACE ACCESS
- Username: admin
- Password: admin
## Interfaces

### Rear

The following interfaces are available on the NF10W:

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power supply jack</td>
<td>Connection point for the included power adapter. Connect the power supply here.</td>
</tr>
<tr>
<td>2</td>
<td>Power button</td>
<td>Press this button to turn the NF10W on or off.</td>
</tr>
<tr>
<td>3</td>
<td>Reset button</td>
<td>Reset unit to Default by holding the Reset button down for 3 seconds.</td>
</tr>
<tr>
<td>4</td>
<td>USB 2</td>
<td>Connect an external USB hard drive here to use the NAS feature of the NF10W.</td>
</tr>
<tr>
<td>5</td>
<td>Ethernet 1 - 4</td>
<td>Fast Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.</td>
</tr>
<tr>
<td>6</td>
<td>WAN</td>
<td>Gigabit capable WAN port for connection to a WAN network.</td>
</tr>
<tr>
<td>7</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>
</tbody>
</table>
### Top

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>USB 1</td>
<td>Connect an external USB hard drive here to use the NAS feature of the NF10W.</td>
</tr>
<tr>
<td>2</td>
<td>WPS / WiFi buttons</td>
<td>Press the WPS button to activate the WPS pairing function. Press the WiFi button to turn the WiFi radio on or off. When the WiFi radio is off, the WiFi LED on the front panel turns off. WPS feature is Disabled by default, to enabled refer to wireless setup.</td>
</tr>
</tbody>
</table>
Safety and product care

Your router is an electronic device that sends and receives radio signals. Please take the time to read this list of precautions that should be taken when installing and using the router.

- Do not disassemble the router. There are no user-serviceable parts.
- Do not allow the router to come into contact with liquid or moisture at any time. To clean the device, wipe it with a damp cloth.
- Do not restrict airflow around the device. This can lead to the device overheating.
- Do not place the device in direct sunlight or in hot areas.

Transport and handling

When transporting the NF10W, it is recommended to return the product in the original packaging. This ensures that the product will not be damaged.

Note: In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.
Installation and configuration of the NF10W

Placement of your NF10W

The wireless connection between your NF10W and your WiFi devices will be strong when they are in close proximity and have direct line of sight. As your client device moves further away from the NF10W or solid objects block direct line of sight to the router, your wireless connection and performance may degrade. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network’s performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NF10W in order to see if distance is the problem.

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this check list may help.

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF10W, please try the following steps:

- In multi-storey homes, place the NF10W on a floor that is as close to the centre of the home as possible. This may mean placing the NF10W on an upper floor.
- Try not to place the NF10W near a cordless telephone that operates at the same radio frequency as the NF10W (2.4GHz).

Avoiding obstacles and interference

Avoid placing your NF10W near devices that may emit radio “noise,” such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows
- If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal’s path (between your devices and the NF10W).

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 NF10W 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 NF10W.
- 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 NF10W to channel 11. See your phone’s user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.
Choosing the “quietest” channel for your wireless network
In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Your wireless adapter may include a utility to assist in scanning for the least congested network, otherwise you may be able to find another piece of software that can be used. These tools display a graphical representation of the wireless networks in range and the channels on which they are operating. Try to find a channel which is not as busy and does not overlap with another one. Channels 1, 6 and 11 are the only channels which do not overlap with one another and you should ideally choose one of these channels. Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

Hardware installation
1. Connect the power adapter to the Power socket on the back of the NF10W.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF10W to power up.

Connecting a client via Ethernet cable
4. Connect the yellow Ethernet cable provided to one of the ports marked ‘LAN’ at the back of the NF10W.
5. Connect the other end of the yellow Ethernet cable to your computer.
6. Wait approximately 30 seconds for the connection to establish.
7. Open your Web browser, and enter http://192.168.20.1 into the address bar and press enter.
8. Follow the steps to set up your NF10W.

Connecting a client wirelessly
1. Ensure WiFi is enabled on your device (e.g. computer/laptop/smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NF10W.

Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF10W

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF10W.
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 NF10W.
Web based configuration interface

First-time setup wizard
Please follow the steps below to configure your NF10W Wireless router via the web based configuration wizard.

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

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

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

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

ADSL

   a) Select ADSL and click the Next button.

   b) Select either the PPPoE or PPPoA for your internet connection as specified by your Internet Service Provider (ISP). Click the Next button.
c) In the **User ID** and **Password** fields, enter the username and password assigned to you by your Internet Service Provider (ISP). Click the **Finish** button.

The account settings are saved and the NF10W connects to the internet.

**VDSL**

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

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

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

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

**Ethernet WAN**

a) Connect an RJ45 Ethernet cable to the WAN port on the NF10W. Connect the other end of the cable to your WAN service.
b) Select **Ethernet WAN** then click the **Next** button.
b) Select the WAN mode for your internet connection as specified by your Internet Service Provider (ISP). Click the Next button.

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

**IP over Ethernet (IPoE)**
If your ISP has supplied a static IP address, select **Use the following Static IP address** and enter the details, otherwise select **Obtain an IP address automatically**. Click the Next button.

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

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

<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 driver version of the on-board DSL chip.</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>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>
</tbody>
</table>

**WAN connection**

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<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>Service connection type</td>
<td>Displays whether the WAN connection is ADSL/VDSL or Ethernet WAN.</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 is use.</td>
</tr>
<tr>
<td>LAN IPv6 ULA Address</td>
<td>The current IPv6 LAN 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>
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 Pxy</td>
<td>Details the status of IGMP on each WAN connection. IGMP is only used with IP v4 connections. IGMP proxy enables the router to issue IGMP host messages on behalf of hosts that the router discovered through standard IGMP interfaces, allowing NAT transversal of Multicast traffic.</td>
</tr>
<tr>
<td>IGMP Src Enbl</td>
<td>Shows the status of the Multicast Listener Discovery protocol when IPv6 is in use. Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router discovered through standard MLD interfaces.</td>
</tr>
<tr>
<td>MLD Pxy</td>
<td>Shows the status of the Multicast Listener Discovery protocol when IPv6 is in use. Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router discovered through standard MLD interfaces.</td>
</tr>
<tr>
<td>MLD Src Enbl</td>
<td>Details the status of MLD Src on each WAN connection. MLD Sources function can send a membership report that includes a list of MLD source addresses.</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>Status</td>
<td>The status of the 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.

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

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

<table>
<thead>
<tr>
<th>INTERFACE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received/Transmitted</td>
<td>Rx/Tx (receive/transmit) packets in bytes.</td>
</tr>
<tr>
<td>Rx</td>
<td>Rx/Tx (receive/transmit) packets.</td>
</tr>
<tr>
<td>Tx</td>
<td>Rx/Tx (receive/transmit) packets with errors.</td>
</tr>
<tr>
<td>Drops</td>
<td>Rx/Tx (receive/transmit) packets with drops.</td>
</tr>
</tbody>
</table>

Statistics – xTM

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

<table>
<thead>
<tr>
<th>Mode:</th>
<th>Downstream</th>
<th>Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Type:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status:</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Link Power State:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Line Coding (Trellis):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNR Margin (0.1 dB):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attenuation (0.1 dB):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Output Power (0.1 dB):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attainable Rate (Kbps):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rate (Kbps):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Super Frames:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Super Frame Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS Words:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS Correctable Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS Uncorrectable Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HEC Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VCC Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCD Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Cells:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Del Cells:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bit Errors:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Ils:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total SES:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total UAS:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

xDSL BER Test  Reset Statistics
Route
The Route page displays any routes that the router has created.

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

DHCP
Click DHCP to display the DHCP lease information.
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

Layer 2 Interface

ATM Interface

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

### ATM Interface Configuration

<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. Please refer to your ISP for correct value.</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. Please refer to your ISP for correct value.</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 is used for VDSL connections.

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

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

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

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

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

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

IP over Ethernet
Enter the details as required by your Internet Service Provider and click the **Next** button.
Select the NAT Translation settings as desired and click the **Next** button.

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

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

A summary of your settings is displayed. Click Apply/Save to commit your settings to the router.
LAN
IPv4 Autoconfig
The LAN window allows you to modify the settings for your local area network (LAN).

The following options are available to configure:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the Local IP Address to use for the NF10W.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask of the Local Network.</td>
</tr>
<tr>
<td>Enable IGMP Snooping</td>
<td>Enable IGMP Snooping and select the IGMP Snooping mode to use. Standard: allow all multicast traffic to LAN clients. Blocking: only allow multicast subscribed clients to receive multicast packets.</td>
</tr>
<tr>
<td>Enable LAN side Firewall</td>
<td>Enable the LAN side firewall to restrict traffic between LAN hosts.</td>
</tr>
<tr>
<td>Enable DHCP Server</td>
<td>Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.</td>
</tr>
<tr>
<td>Enable DHCP Server Relay</td>
<td>Disabled DHCP server, and relay all request to external server specified by the IP address.</td>
</tr>
<tr>
<td>Configure the second IP Address</td>
<td>This option enables you to set a secondary IP Address for the NF10W</td>
</tr>
</tbody>
</table>

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

DHCP Static IP Lease
Enter the Mac address and Static IP address then click Apply/Save.
To set a DHCP reservation, enter the MAC Address of the chosen host and IP to use and then click **Apply/Save**. The NF10W enables you to set the DHCP options which are provided to hosts attempting to connect to the DHCP server. These options should not normally need to be set or changed. Click **Apply/Save** to save the new LAN configuration settings.

### IPv6 Autoconfig

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

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

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

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

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

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

**Port Triggering**

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

The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the ‘Open Ports’. A maximum 32 entries can be configured.

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

The NF10W will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer’s IP address and click **Apply** to activate the DMZ host. To deactivate the DMZ Host function clear the IP address field and press the Save/Apply button.

### ALG

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

#### ALG

Select the ALG below:

- [ ] FTP Enabled
- [ ] SIP Enabled
- [ ] TFTP Enabled
- [ ] H323 Enabled
- [ ] IPX Enabled
- [ ] Port Triggering Enabled
- [ ] RTSP Enabled
- [ ] NPSC Enabled
- [ ] RTP Enabled

Click **Save/Apply**.
Security

IP Filtering

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

Outgoing IP Filtering

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

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

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

![Add IP Filter-Outgoing](image)

Enter the following parameters:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Enter a name to identify the filtering rule.</td>
</tr>
<tr>
<td>IP Version</td>
<td>Select the IP version to apply the filter to.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol type to block</td>
</tr>
<tr>
<td>Source IP Address/Subnet Mask</td>
<td>Enter the IP Address of the PC on the LAN to block</td>
</tr>
<tr>
<td>Source Port</td>
<td>Enter the port number used by the application to block</td>
</tr>
<tr>
<td>Destination IP Address/Subnet Mask</td>
<td>Enter the IP Address of the Remote Server to which connections should be blocked</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the destination port number used by the application to block</td>
</tr>
</tbody>
</table>

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

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

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

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

Enter the following parameters:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Name</td>
<td>Enter a name to identify the filtering rule</td>
</tr>
<tr>
<td>IP Version</td>
<td>Select the IP version to apply the filter to</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the protocol type to allow</td>
</tr>
<tr>
<td>Source IP Address/Subnet Mask</td>
<td>Enter the IP Address of the Remote Server from which to allow connections</td>
</tr>
<tr>
<td>Source Port</td>
<td>Enter the port number used by the application to allow</td>
</tr>
<tr>
<td>Destination IP Address/Subnet Mask</td>
<td>Enter the IP Address of the PC on the LAN to which connections should be allowed</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Enter the destination port number used by the application to allow</td>
</tr>
<tr>
<td>WAN Interface</td>
<td>Select the WAN Interface to apply the filter to</td>
</tr>
</tbody>
</table>

Click Save/Apply to take effect the settings. The new rule will then be displayed in the Incoming IP Filtering table list.
MAC Filtering
The NF10W offers the ability to use MAC Address filtering on ATM PVCs. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow connections which match the criteria.

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

1. Enter the Protocol type to which the filter should apply.
2. Enter the Source and Destination MAC Address
3. Enter the direction of the traffic to filter
4. Select the WAN interface to which the filter should apply.

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

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

Time Restriction

This Parental Control function allows you to restrict access from a Local Area Network (LAN) connected device to an outside network through the router on selected days and at certain times. Make sure to activate the Internet Time server synchronization as described in the SNTP section, so that the scheduled times match your local time.

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>
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 NF10W. 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

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

The above screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately.

NOTE: Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority.
The QoS Wlan Queue page displays a summary of the QoS configuration.

### QoS Classification

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

Click the **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.

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

Enter the Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. Then click Apply/Save to add the entry to the routing table.
Policy Routing
This function allows you to add policy rules to certain situations.

![Policy Routing Setting](image)

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

![Advanced - Routing - Add Policy Route](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.
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
Select DNS Server Interface from available WAN Interfaces OR enter static DNS server IP address for the system. In XTM mode, if only a single PVC with IPv4 or static IPv6 protocol is configured, static DNS server IP address must be entered.

DNS Server Interface can have multiple WAN interfaces served as system DNS server but only one will be used according to the priority. The first being the highest and the last one the lowest priority. If the WAN interface is connected, priority order can be changed by removing all and adding them back in again.

- Select DNS Server Interface from available WAN interfaces:
  - eth1.2

- Use the following static DNS IP address:
  - Primary DNS server:
  - Secondary DNS server:

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

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

Choose Add or Remove to configure Dynamic DNS.

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.
Add Dynamic DNS

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

<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>Hostname</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 3: Advanced - DNS - Add Dynamic DNS Account Settings

DSL

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

For advanced DSL options press the Advanced Settings button.

The DSL advanced settings relate to test mode settings. The default selection is ‘Normal’.
ADSL Tone Settings
For ADSL Tone Settings select the ‘Tone Selection’ button on the DSL Advanced Settings page.

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125kHz apart. With each tone carrying separate data, the technique operates as if 256 separate routers were running in parallel. The tone range is from 0 to 31 for upstream traffic and from 32 to 255 for downstream traffic. Do not change these settings unless you are directed by your Internet Service Provider.

UPnP
Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, WiFi access points and mobile phones to automatically detect each other’s presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP allow automatic port forwarding configuration form your UPnP devices.

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

The Host name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the user interface of the router with a local name rather than by using the router IP address. Eg. You can access your router by entering http://NF10W into your web browser.
DLNA
The DLNA page allows you to enable or disable and configure the digital media server. This means you can have digital media stored on an external USB hard drive connected to the NF10W 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.

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 Device Info](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.

![Storage User Account Setup](image)
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.

IPv6 in IPv4

Click the Add button to add a new tunnel.

IPv4 in IPv6

Click the Add button to add a new tunnel.
IPSec

The NF10W 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>Pre-Shared Key</td>
<td>Enter the pre-shared key (if applicable) to grant access to 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.
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.

<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

Basic

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

Enable Wireless
Select to enable or disable the wireless network function.

Hide Access Point
Select to hide or display the wireless network when an SSID scan is performed.

Clients Isolation
Select to prevent clients on the wireless network from accessing each other.

Disable WMM Advertisement
Select to prevent the NF10W from advertising its WMM function.

Enable Multicast Forwarding (WMF)
Select to enable Wireless Multicast Forwarding. This can reduce latency and improve throughput for wireless clients.

Max Clients
Enter the maximum number of wireless clients able to connect to the wireless network.

Wireless Guest Network
Select to enable a separate Wireless Guest network. The same options are available for a Guest network as with the main system wireless network.

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

**Note:** Hiding the network may lead to potential connection problems, a non-broadcast network is not undetectable, hiding a SSID is Security through obscurity.
Security
The NF10W supports all encryptions within the 802.11 standard. The factory default is WPA2-PSK. The NF10W 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 NF10W.</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/WAPI 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>

Note: WPA with TKIP and Open WEP are no longer considered secure. WPA2 with AES is the most secure option. Mixed WPA2/WPA (TKIP+AES) will provide maximum compatibility with legacy devices.

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

MAC Filter
MAC Filter allows you to add or remove the MAC Address of devices which will be allowed or denied access to the wireless network. First use the **Select SSID** drop down list to select the wireless network you wish to configure, then select to either allow or deny access to the MAC addresses listed.
Click **Add** to add a MAC Address Filter.

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

**Note:** While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC and then spoofing one's own MAC into a validated one, using MAC Filtering may lead to a false sense of security.

**Wireless Bridge (Wireless Distribution Service)**

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

Select the mode for the Wireless Access Point built into the NF10W. You can specify which wireless networks will be allowed to connect to the NF10W by using the 'Bridge Restrict' option and then entering the applicable MAC Addresses of the other wireless access points.

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

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

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

Click **Apply/Save** to save any changes to the wireless network settings configuration.
<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band</td>
<td>Shows your current frequency band.</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. In high wireless activity/interference environment, reduce band to 20MHz for better stability.</td>
</tr>
<tr>
<td>Control Sideband</td>
<td>If you select 20MHz in Both Bands you cannot select sideband does not work as you are not utilizing side bands. When you select 40MHz in Both Bands as the bandwidth and manual select channel, the following options will appear. Then you can select Lower or Upper as the value of sideband. As the control sideband, when you select Lower, the channel is 1<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 “speaking” 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>DTIM Interval</td>
<td>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 Enabled.</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 VoIP, 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 NF10W 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.

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

Diagnostics

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

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

<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>
### Ethernet OAM

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

#### Ethernet Link OAM (802.3ah)
- **Selected** option
- **WAN Interface:** `eth1`
- **OAM ID:** `1` (positive integer)

#### Ethernet Service OAM (802.1ag / Y.1731)
- **Selected** option
- **WAN Interface:** `eth1`
- **MD Level:** `0` (`0-7`)
- **M/G Name:** `Broadcom` [exp. Broadcom]
- **MA ID:** `[BCH]` [exp. BCH]
- **Local MEP ID:** `1`
- **Remote MEP VID:** `-1` [1-4094] (1 means no VLAN tag)
- **COI Transmission:**
- **Remote MEP ID:** `1` [1-4094] (1 means no Remote MEP)

#### Loopback and Linktrace Test
- **Target MAC:** [exp. 50-50-50-50-50-50] [exp. 50-50-50-50-50-50]
- **Linktrace TTL:** `1` [1-255] (1 means no max hop limit)

<table>
<thead>
<tr>
<th>Loopback Result</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linktrace Result</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Diagnostics

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

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

Host Name or Ip Address:
Submit  Cancel

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

Traceroute Diagnostic
Please type in a host name or an IP Address. Click Submit to trace the route.

Host Name or Ip Address:
Submit  Cancel

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

Management

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

Backup
The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings. You will be prompted for the location to save the backup file to on your PC.
Update Settings
The following screen appears when selecting Update from the Settings submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings button to upload the selected file. Please allow up to 5 minutes for system updates.

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

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

To configure the system log, click the Configure System Log button. You can sent system log to remote server via selecting both, or remote under “Mode” option.
SNMP Agent
The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NF1ADV (if SNMP is enabled). An SNMP ‘community’ performs the function of authenticating SNMP traffic. A ‘community name’ acts as a password that is typically shared among SNMP agents and managers.

```
SNMP - Configuration
Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.
Select the desired values and click 'Apply' to configure the SNMP options.

SNMP Agent: [ ] Disable [ ] Enable
Read Community: public
Set Community: private
System Name: NF10W
System Location: unknown
System Contact: unknown
Trap Manager IP: 0.0.0.0

Save/Apply
```

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

[ ] Enable WAN Management Protocol (TR-069)
Inform
Inform Interval: 300
ACS URL:
ACS Username:
ACS Password:
WAN Interface used by TR-069 client: [ ] Any WAN
Display SNMP messages on serial console: [ ] Enable
[ ] Connection Request Authentication

Apply/Save | Get RPC Methods
```

<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 NF10W router synchronises with in order to keep accurate time.

![Time settings](image)

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.

![Access Control - Passwords](image)
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.

![Services Access Control List](image)

Update Firmware

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

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

Reboot

This option reboots the NF10W.

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

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

Establishing a wireless connection

Windows 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 NF10W with "Connected" next to it.

Windows 8/8.1/10
1. Open the Network and Sharing Centre (Click on Start, Type "Network and Sharing Centre")
2. Click on "Change adapter settings" on the left hand column.
3. Right-click on Wireless Network Adaptor and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
6. After clicking on this, you should see an entry matching the SSID of your NF10W with "Connected" under it.

Mac OSX 10.6
1. Click on the Airport icon on the top right menu.
2. Select the wireless network listed on your included wireless security card and click Connect.
3. On the new window, select "Show Password", type in the network key (refer to the included wireless security card for the default wireless network key) in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.

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

Using the indicator lights (LEDs) to Diagnose Problems
The LEDs are useful aides for finding possible problem causes.

Power LED
The Power LED does not light up.

<table>
<thead>
<tr>
<th>STEP</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Make sure that the NF10W 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 NF10W and the power source are both turned on and device is receiving sufficient power.</td>
</tr>
<tr>
<td>3</td>
<td>Turn the NF10W 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>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>2</td>
<td>Your computer’s and the NF10W’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>3</td>
<td>If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.</td>
</tr>
<tr>
<td>4</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 NF10W 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 NF10W 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 NF10W 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 NF10W 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 NF10W 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 NF10W 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 coarse-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 NF10W 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 NF10W router so that QoS settings can be managed for each device.


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

c) Select Advanced Setup > LAN

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

f) Enter the IP address of the computer/device. This is the local address in the range of 192.168.1.x where x = a number between 2 and 254.

![DHCP Static IP Lease](image1)

- **MAC Address:** 5C-3D:16:07:3C
- **IP Address:** 192.168.1.1.5

![Apply/Save button](image2)

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

h) Complete steps 4 through 7 for each device connected to the NF10W router. Each entry will be listed in the Static IP Lease List as shown below.

![Local Area Network (LAN) Setup](image3)

- **IP Address:** 192.168.20.1
- **Subnet Mask:** 255.255.255.0

![Enable IGMP Snooping](image4)

- Enable IGMP Snooping
- Standard Mode
- Blocking Mode
- Enable LAN side firewall
- Disable DHCP Server
- **Enable DHCP Server**
- **Start IP Address:** 192.168.20.2
- **Default IP Address:** 192.168.20.2
- **Default DNS Servers:** 192.168.20.2
- **Secondary DNS Servers:** 192.168.20.3
- **Leased Time (hour):** 24

- **MAC Address:** 00:20:0a:07:3C
- **IP Address:** 192.168.1.1.5

![Static IP Lease List](image5)

QoS Configuration Settings

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

![QoS Configuration](image6)

- **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. Click **Apply/Save** button to save.
  - **Note:** If Enable QoS checkbox is not selected, all QoS will be disabled for all interfaces.
  - **Note:** The default DSCP mark is used to mark all egress packets that do not match any classification rules.

![Select Default DSCP Mark](image7)

- **Select Default DSCP Mark:** default(0x0000)

![Apply/Save button](image8)
b) Select the **Enable QoS** option.

**High Priority QoS Queue Configuration**

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Key Interface</th>
<th>Scheduler</th>
<th>Precedence</th>
<th>Weight</th>
<th>DSL Latency</th>
<th>PTH Priority</th>
<th>Enable</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMM Voice Priority 1</td>
<td>wb</td>
<td>SP</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Voice Priority 2</td>
<td>wb</td>
<td>SP</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Video Priority 3</td>
<td>wb</td>
<td>SP</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Video Priority 4</td>
<td>wb</td>
<td>SP</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Best Effort 5</td>
<td>wb</td>
<td>SP</td>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Background 6</td>
<td>wb</td>
<td>SP</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Background 7</td>
<td>wb</td>
<td>SP</td>
<td>7</td>
<td>7</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>WMM Best Effort 8</td>
<td>wb</td>
<td>SP</td>
<td>8</td>
<td>8</td>
<td></td>
<td></td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td>Default Queue</td>
<td>atm0</td>
<td>SP</td>
<td>8</td>
<td></td>
<td>Path0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b) Click the **Add** button.

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

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

e) Set the Interface (Australian customers use atm0(0_8_35), NZ customers use atm0(0_100)).

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

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

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

Low Priority QoS Queue Configuration

a) Select **Advanced > Quality of Service > Queue Config.**
b) Click the **Add** button.

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

High Priority QoS Classification

a) Select **Advanced > Quality of Service > QoS Classification**.
b) Click the **Add** button.

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

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

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

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

g) Set the **Ether Type** to **IP(0x800)**. Other options include **ARP(0x806)**, **Ipv6(0x86DD)**, **PPPoE_DISC(0x8863)**, **8865(0x8865)**, **8866(0x8866)**, **8021Q(0x8100)**.

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

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

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

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

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

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

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

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

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

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

r) Click the **Apply/Save** button.
Low Priority QoS Classification

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

b) Click the Add button.

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

d) Leave the Rule Order as Last.

e) Set the Rule Status to Enable.

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

g) Set the Ether Type to IP(0x800). Other options include ARP(0x806),Ipv6(0x86DD), PPPoE_DISC(0x8863), 8865(0x8865), 8866(0x8866), 8021Q(0x8100).

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

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

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

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

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

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

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

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

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

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

r) Click the Apply/Save button.
s) You now have 2 Quality of Service rules implemented for 2 devices connecting to the NF10W router.

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

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

Limiting the upstream rate

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

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

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

c) Click Apply/Save.
Limiting the downstream rate

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

![QoS Queue Configuration](image)

- Names: LAN Interface
- Enable: [Enable]
- Interfaces: eth0, eth1, eth2, eth3

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

**Classification Criteria:**
- Class Interface: the appropriate WAN interface
- Class Queue: the queue that was created on Step 1

**Classification Results:**
- Set rate-limit: set according to your preference

![QoS Classification Table](image)

The QoS Classification table looks like this:

<table>
<thead>
<tr>
<th>Classification Criteria</th>
<th>Classification Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Interface</td>
<td>Class Queue</td>
</tr>
<tr>
<td>Class Interface</td>
<td>eth3&amp;Loy35&amp;Pre2</td>
</tr>
<tr>
<td>Eth2 Priority</td>
<td></td>
</tr>
<tr>
<td>Source MAC Address</td>
<td></td>
</tr>
<tr>
<td>Destination MAC Address</td>
<td></td>
</tr>
<tr>
<td>Source MAC Mask</td>
<td></td>
</tr>
<tr>
<td>Destination MAC Mask</td>
<td></td>
</tr>
<tr>
<td>Set Rate Limit</td>
<td>100</td>
</tr>
</tbody>
</table>

Click **Apply/Save**

The QoS Classification table looks like this:
Legal & Regulatory Information

Intellectual Property Rights
All intellectual property rights (including copyright and trademark 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