

# N300 WiFi Gigabit Router



NF7  
USER GUIDE

Copyright

Copyright©2013 NetComm Wireless Limited. All rights reserved.

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



Note: This document is subject to change without notice.

Save Our Environment

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

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

Please be responsible and protect our environment.

This manual covers the following products:

NetComm Wireless NF7 N300 WiFi Gigabit Router

DOCUMENT VERSION	DATE
1.0 – Initial document release	November 2013

# Table of Contents

<b>Overview</b> .....	<b>5</b>
Introduction.....	5
Target Users.....	5
Prerequisites.....	5
Notation.....	5
<b>Product Introduction</b> .....	<b>6</b>
Product Overview.....	6
Package Contents.....	6
Product Features.....	7
<b>Physical Dimensions and Indicators</b> .....	<b>8</b>
LED Indicators.....	8
Physical Dimensions.....	9
NF7 Default Settings.....	9
<b>Interfaces</b> .....	<b>10</b>
<b>Safety and Product Care</b> .....	<b>11</b>
<b>Transport and Handling</b> .....	<b>11</b>
<b>Installation and Configuration of the NF7</b> .....	<b>12</b>
Placement of your NF7.....	12
Avoid obstacles and interference.....	12
Cordless Phones.....	12
Choose the “Quietest” Channel for your Wireless Network.....	12
Hardware installation.....	13
Connecting via a cable.....	13
Connecting wirelessly.....	13
<b>Web Based Configuration Interface</b> .....	<b>14</b>
First-time Setup Wizard.....	14
Basic View.....	19
Status.....	19
Wireless.....	20
WAN.....	21
Advanced Configuration.....	22
Status.....	23
Network Setup.....	24
DHCP Server.....	29
Wireless.....	31
Change Password.....	32
Port Configuration.....	32
Forwarding Rules.....	33
Port Forwarding.....	33
Port Triggering.....	34
Miscellaneous.....	35
Security Settings.....	36
Status.....	36
Packet Filters.....	37
Domain Filters.....	39
URL Blocking.....	40
MAC Control.....	41
Miscellaneous.....	42
Advanced Settings.....	43
Status.....	43
System Log.....	44
Dynamic DNS.....	45
QoS.....	46
SNMP.....	51
Routing.....	52
System Time.....	53
Scheduling.....	54
IPv6.....	55
TR-069.....	56
VLAN.....	57

Toolbox.....	58
System Info .....	58
Routing Table.....	58
Restore Settings.....	58
Firmware Upgrade.....	59
Backup Settings.....	59
Reset to Default.....	59
Reboot.....	59
Startup Wizard .....	59
Logout .....	59
<b>Additional Product Information .....</b>	<b>60</b>
Establishing a wireless connection .....	60
Windows XP (Service Pack 3).....	60
Windows Vista.....	60
Windows 7 .....	60
Mac OSX 10.6.....	60
Troubleshooting.....	61
Using the indicator lights (LEDs) to Diagnose Problems.....	61
<b>Technical Data .....</b>	<b>62</b>
Electrical Specifications.....	62
Environmental Specifications / Tolerances.....	62
<b>Legal &amp; Regulatory Information.....</b>	<b>63</b>
Intellectual Property Rights.....	63
Customer Information .....	63
Consumer Protection Laws.....	63
Product Warranty .....	64
Limitation of Liability.....	64
<b>Contact.....</b>	<b>65</b>

# Overview

## Introduction






This manual provides information related to the installation, operation, and use of the NF7.

## Target Users

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

## Prerequisites

Before continuing with the installation of your NF7, please confirm that you comply with the minimum system requirements below.

-  A configured WAN connection.
-  Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
-  A web browser such as Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Safari etc.
-  Wireless computer system requirements:
  -  Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

## Notation

The following symbols are used in this manual:



Indicates a note requiring attention.



Indicates a note providing a warning.



Indicates a note providing useful information.

# Product Introduction

## Product Overview

- 📶 Gigabit WAN port for a fixed line connection. Perfect for a future NBN/Fibre connection
- 📶 Establish up to 4 high speed wired connections with the Gigabit LAN ports
- 📶 Create a WiFi network to share your connection with multiple WiFi devices at speeds of up to 300Mbps<sup>1</sup>
- 📶 Supports IPv6 for next generation IP addressing

## Package Contents

The NF7 package consists of:

- 📶 N300 WiFi Gigabit Router
- 📶 Quick Start Guide
- 📶 Power Supply Unit
- 📶 Ethernet Cable (RJ-45)
- 📶 Wireless Security Card
- 📶 Warranty Card

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>

---

<sup>1</sup> 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.

## Product Features

The NetComm Wireless NF7 is a future-ready WiFi router that connects the home or office to super-fast broadband. Simply connect your fixed line modem to the Gigabit WAN port for instant Internet access - perfect for NBN/Fibre connections

The advanced network sharing function gives multiple users the freedom to watch movies, download music, play online games and enjoy other bandwidth intensive activities such as IPTV streaming on a single broadband account. Enjoy extended WiFi coverage with high-speed WiFi, or connect up to four wired devices via the Gigabit Ethernet ports.





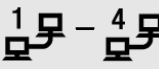
The NF7 is also kind to the environment with innovative green features for power conservation. With support for IPV6, be assured that your router will be able to continue to access websites when new web addressing starts becoming commonplace.

# Physical Dimensions and Indicators

## LED Indicators

The NF7 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 NF7 to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.



LED INDICATOR	ICON	STATUS	DEFINITION
Power		Off	The NF7 is powered off.
		On	The NF7 is powered on and operating normally.
		Flashing	The NF7 is starting up.
WWW		Off	Internet connection not configured.
		On	Internet connected.
		Flashing	Internet traffic is being sent and received.
WiFi		Off	WiFi is disabled on the NF7.
		On	WiFi is enabled on the NF7.
		Flashing	The NF7 is waiting for a WPS PBC connection.
WAN		Off	No device is connected to the Ethernet WAN port.
		On	A device is connected to the Ethernet WAN port.
LAN 1-4		Off	No device is connected to the Ethernet LAN port.
		On	A device is connected to the Ethernet LAN port.
		Flashing	Data is being sent or received via the Ethernet LAN port.



## Physical Dimensions

The following table lists the physical dimensions and weight of the NF7.

NF7 DIMENSIONS	
Length	119mm
Width	168mm
Height	27mm
Weight	217g

## NF7 Default Settings

The following tables list the default settings for the NF7.

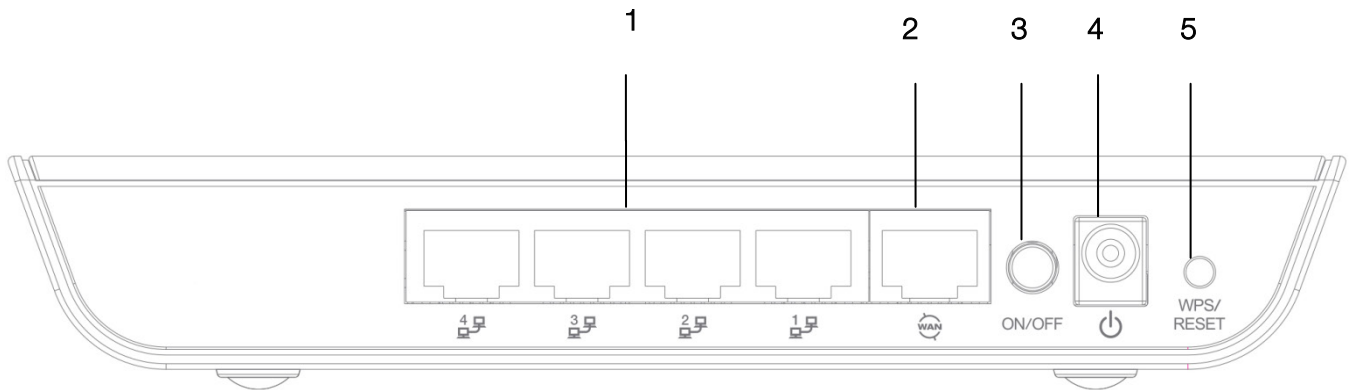
LAN (MANAGEMENT)	
Static IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1

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

NF7 WEB INTERFACE ACCESS	
Username	admin
Password	admin

# Interfaces




The following interfaces are available on the NF7:



NUMBER	INTERFACE	DESCRIPTION
1	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
2	WAN	Gigabit WAN port for connection to a WAN network.
3	Power button	Turns the NF7 on or off.
4	Power jack	Connection point for the included power adapter. Connect the power supply here.
5	WPS button	Activate the WiFi WPS function by press/hold the WPS/RESET button for 1-3 seconds Activate the RESET function by press/hold the WPS/RESET button for 10 seconds

# Safety and Product Care

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

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



## WARNING

Disconnect the power line from the device before servicing.

# Transport and Handling

When transporting the NF7, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.



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

# Installation and Configuration of the NF7

## Placement of your NF7

The wireless connection between your NF7 and your WiFi devices will be stronger the closer your connected devices are to your NF7. Your wireless connection and performance will degrade as the distance between your NF7 and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NF7 in order to see if distance is the problem.



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

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF7, please try the following steps:

- 📶 In multi-storey homes, place the NF7 on a floor that is as close to the centre of the home as possible. This may mean placing the NF7 on an upper floor.
- 📶 Try not to place the NF7 near a cordless telephone that operates at the same radio frequency as the NF7 (2.4GHz).

## Avoid obstacles and interference

Avoid placing your NF7 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 NF7).

## 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 NF7 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 NF7.
- 📶 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 NF7 to channel 11. See your phone's user manual for detailed instructions.
- 📶 If necessary, consider switching to a 900MHz or 5GHz cordless phone.

## Choose the "Quietest" Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

## Hardware installation

1. Connect the power adapter to the Power socket on the back of the NF7.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF7 to power up.

## Connecting via a cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NF7.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter <http://192.168.20.1> into the address bar and press enter.
5. Follow the steps to set up your NF7.

## Connecting wirelessly

1. Ensure WiFi is enabled on your device (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 NF7.



Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF7

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF7.
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 NF7.

# Web Based Configuration Interface

## First-time Setup Wizard

Please follow the steps below to configure your NF7 Wireless router via the web based configuration wizard.

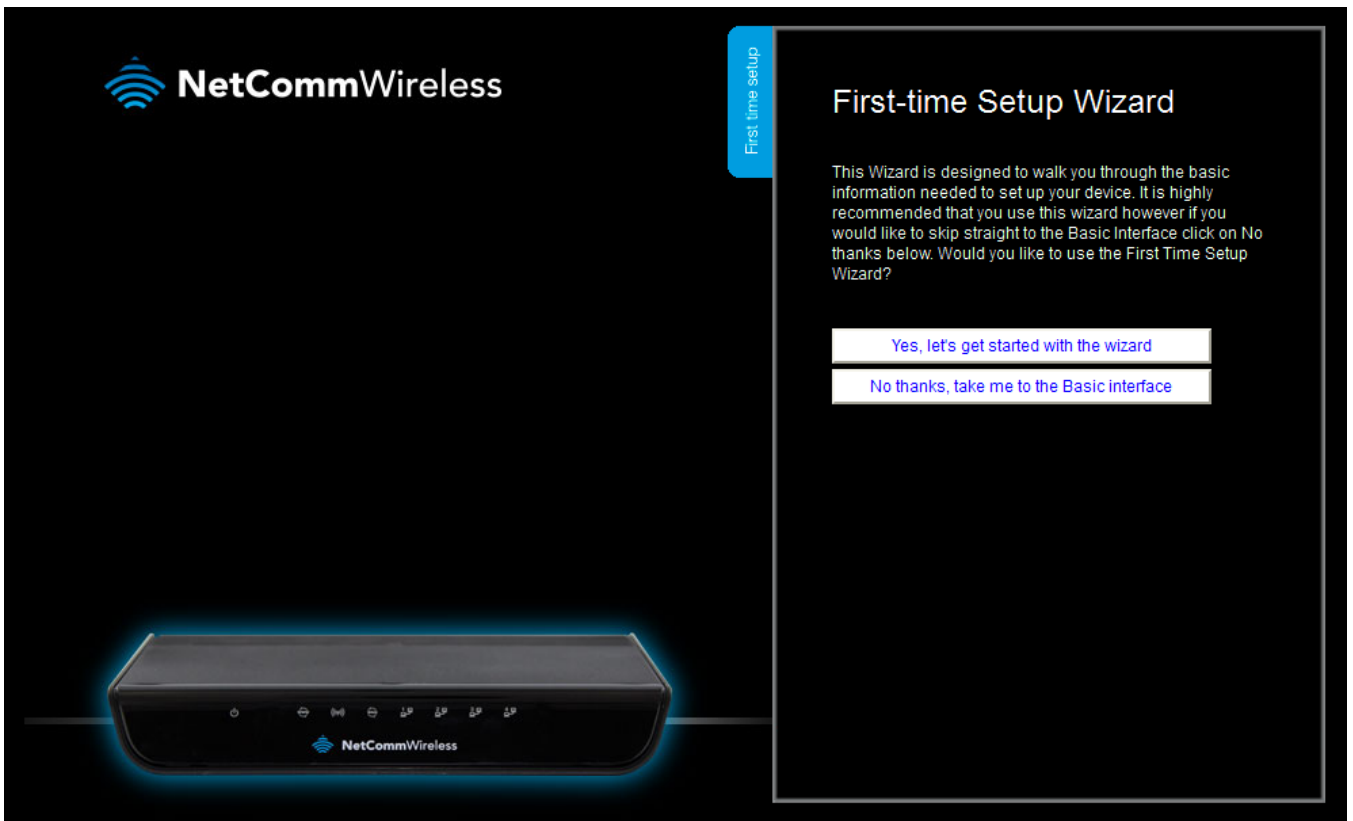
Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type <http://192.168.20.1/> into the address bar at the top of the window.

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

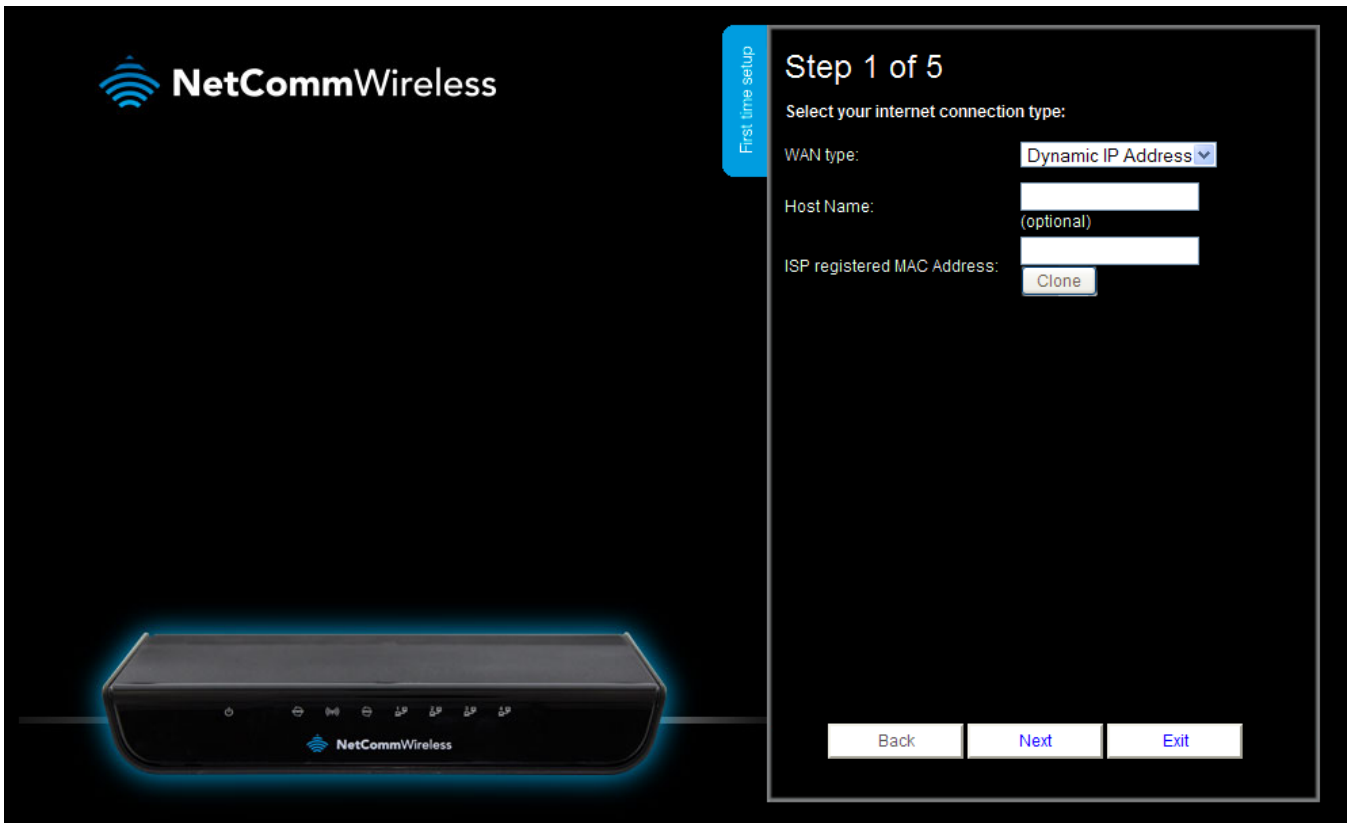


Note: **admin** is the default username and password for the unit.

1. Click on **Yes, let's get started with the wizard**.



The wizard assists you in configuring the router and entering the information required to setup your Internet connection.



2. Use the **WAN type** field to select the type of WAN connection:

#### Dynamic IP Address

- a. Enter the Host Name (Optional)
- b. Enter the MAC Address of your device which is registered with the ISP

#### Static IP Address

- a. Enter the Static IP Address
- b. Enter the Static Subnet Mask
- c. Enter the Static Gateway
- d. Enter the Static Primary and Secondary DNS.

#### PPP over Ethernet (or PPPoE)

Enter the PPPoE Username and Password supplied by your service provider.

#### PPTP

- a. Enter the Server IP Address/Name
- b. Enter the PPTP Account and PPTP Password.

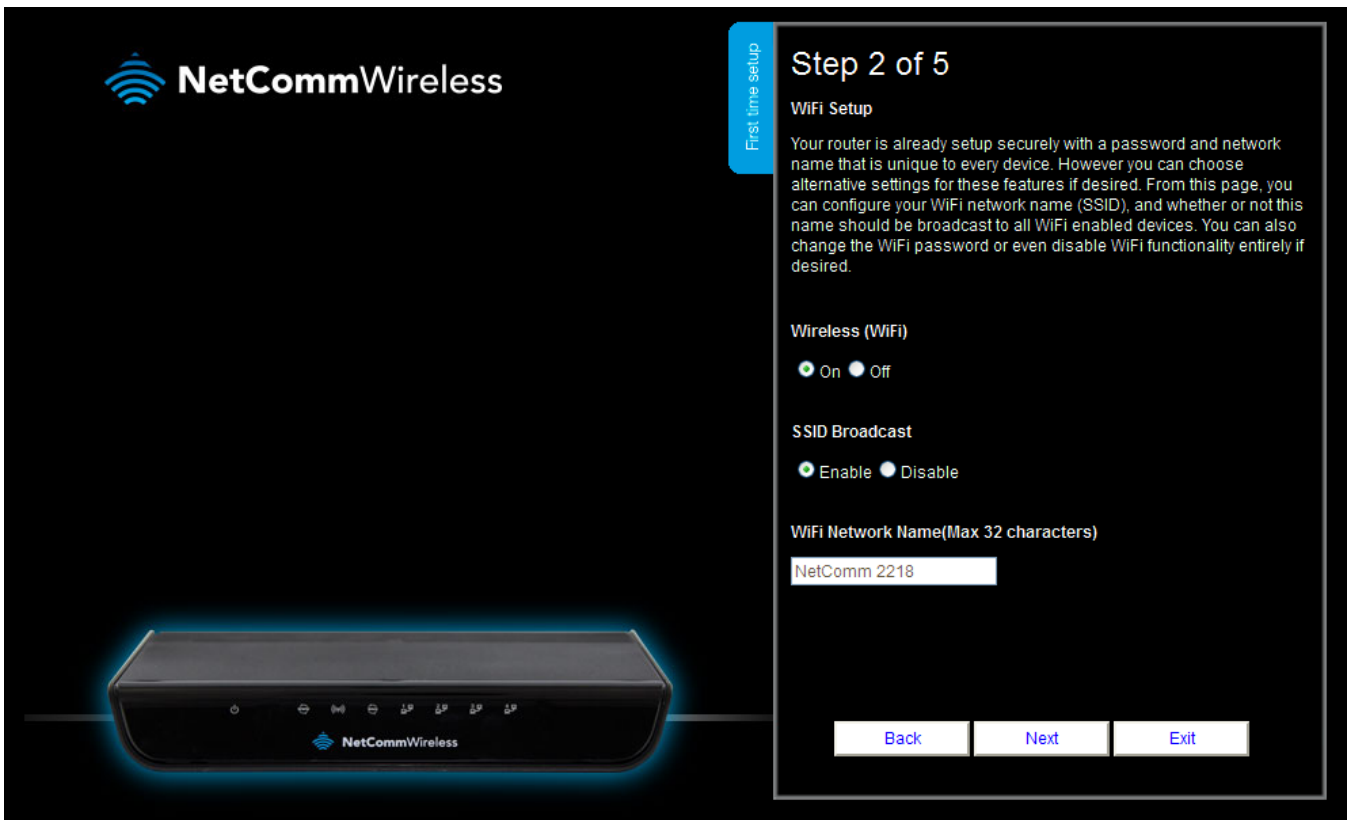
#### L2TP

- a. Enter the Server IP Address/Name
- b. Enter the PPTP Account and PPTP Password.

Click **Next** when you have entered the required details.

3. If you want to change the Wireless network settings, you can do so on this page. You can enable or disable the Wireless network, select whether to broadcast your SSID or not and change the Wireless network name. Change the settings as needed and click **Next**.

(If you wish to use the default settings, click **Next**)



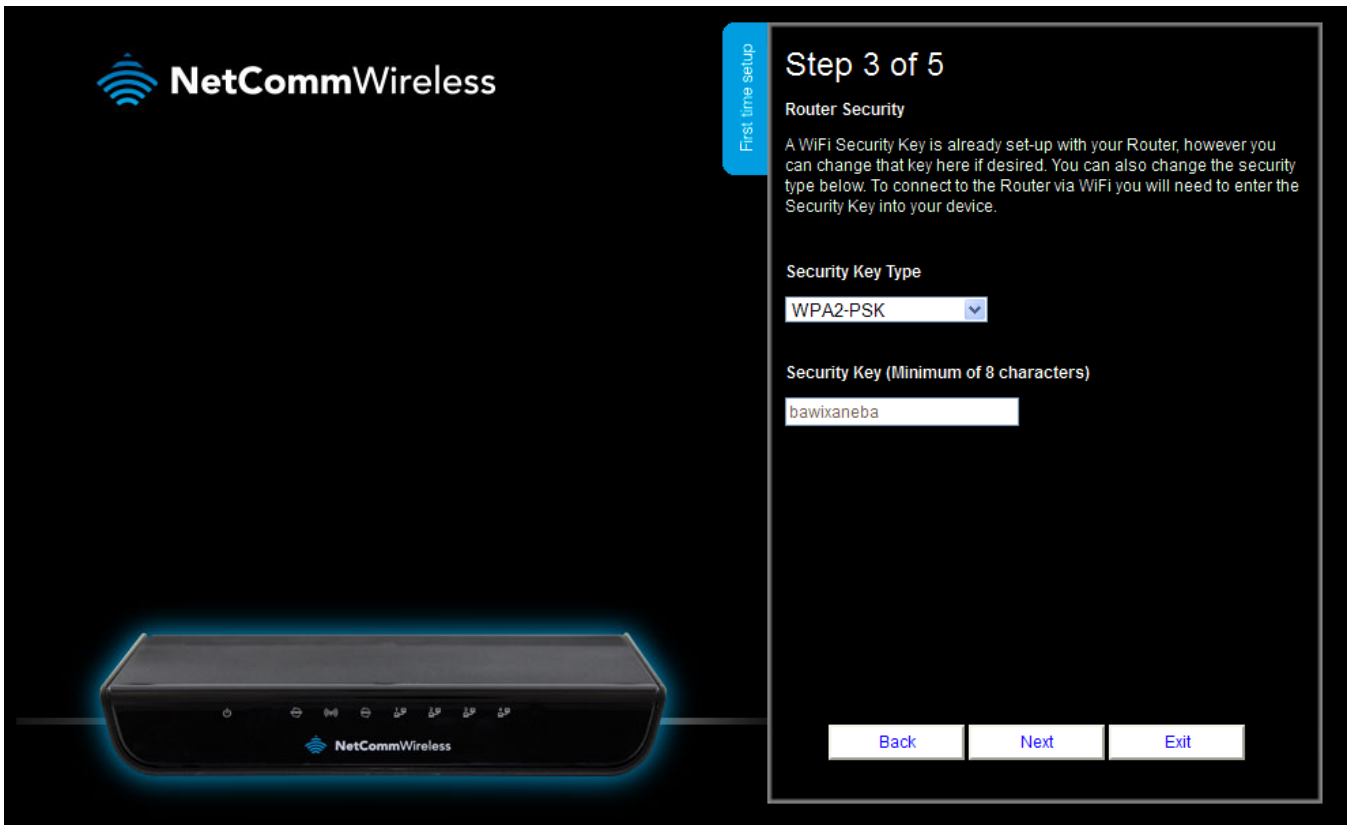
The screenshot shows the NetCommWireless router's first-time setup interface. On the left, there is a glowing blue image of the router. The main area is titled "Step 2 of 5" and "WiFi Setup". It contains the following settings:

- Wireless (WiFi):**  On  Off
- SSID Broadcast:**  Enable  Disable
- WiFi Network Name(Max 32 characters):** A text input field containing "NetComm 2218".

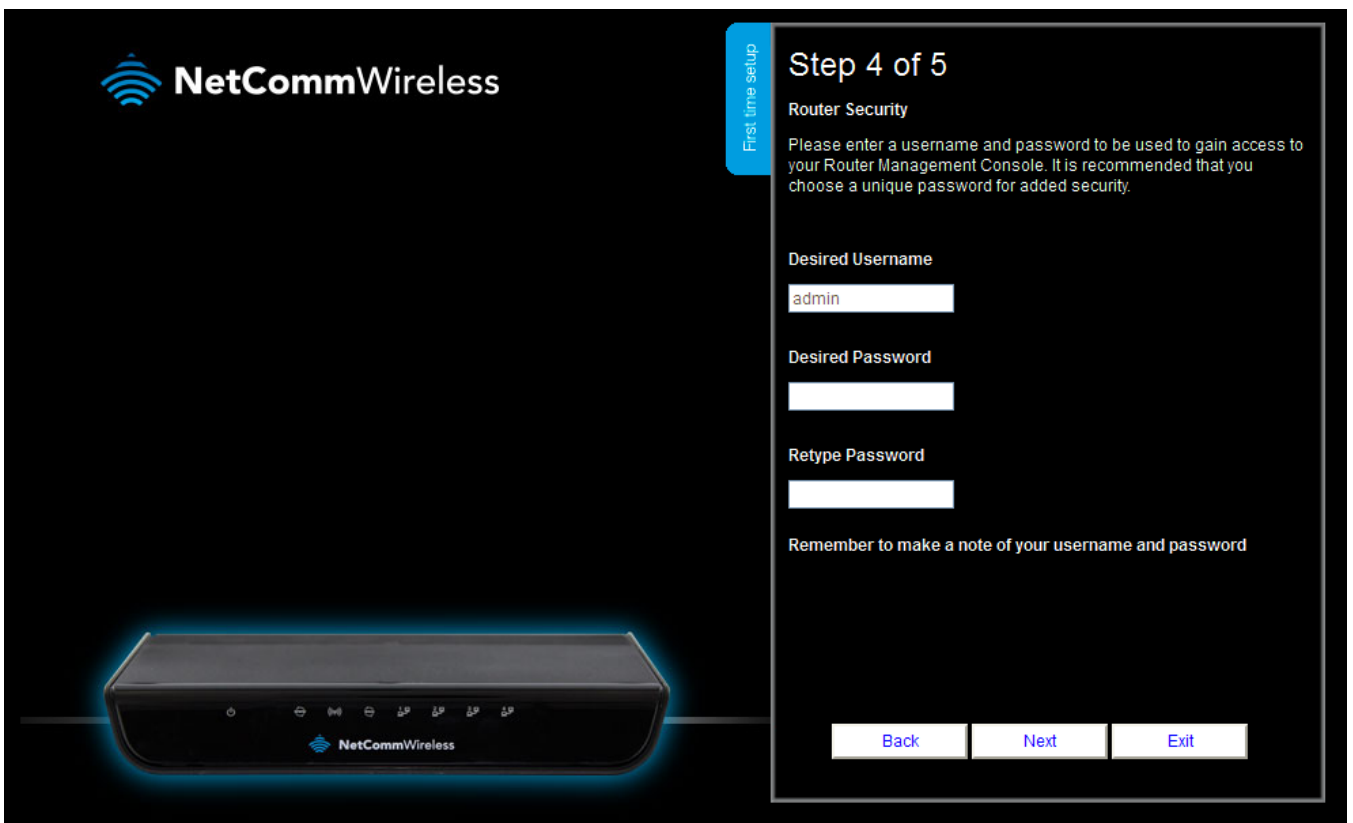
At the bottom right, there are three buttons: "Back", "Next", and "Exit".



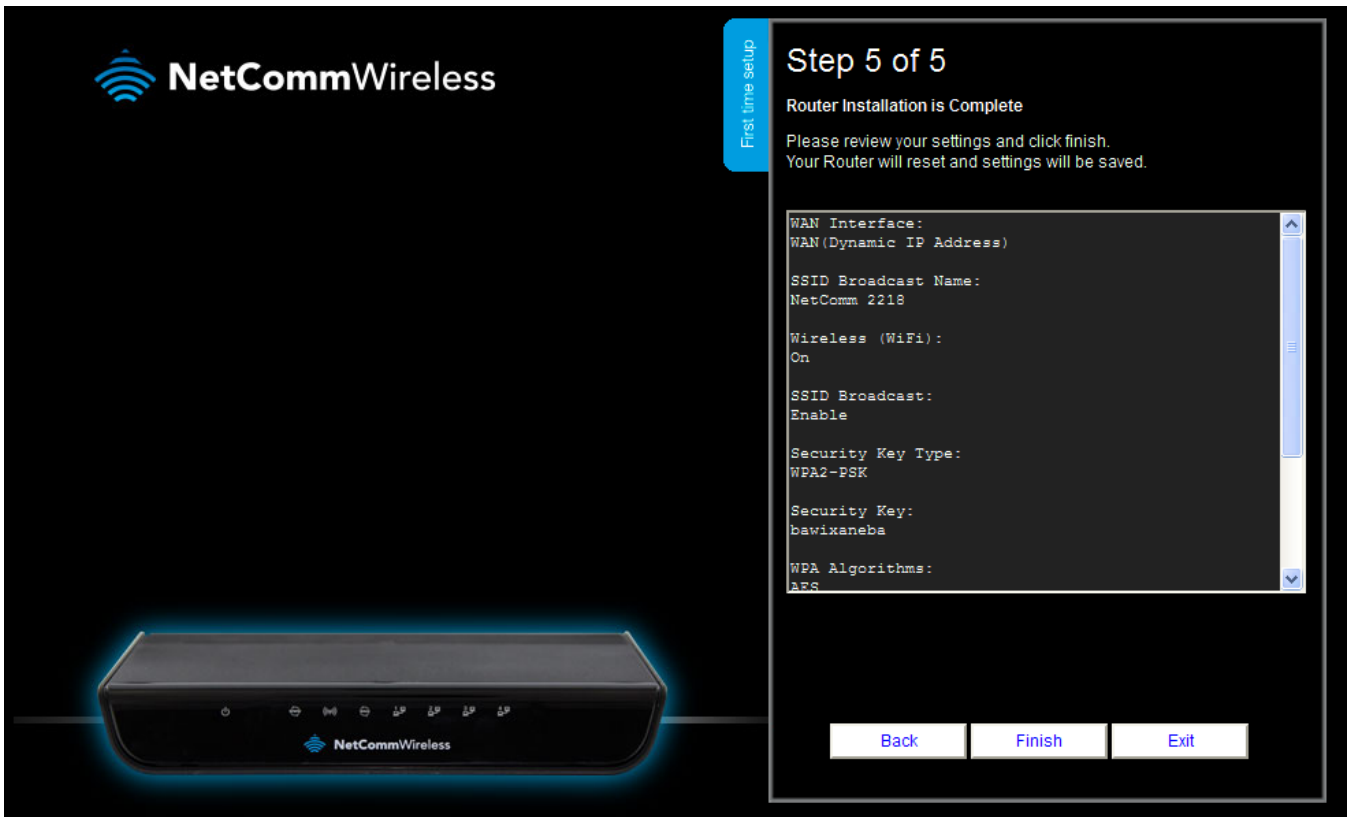
- You can change the WiFi security key if you wish by using the **Security Key Type** drop down list and then typing in a new security key in the **Security Key** field. The Security key must be at least 8 characters long. Click **Next** to continue.



- If you want to change the system username or password, enter the new username in the **Desired Username** field and then enter the new password into both the **Desired Password** and **Retype Password** fields and then click **Next**. (If you do not wish to change the password, leave the fields blank and click **Next**).



6. Confirm the setup information and click **Finish** if everything is correct. You can also click **Back** to go back and change any of the previously configured settings.







When you click Finish, the wizard applies your settings and the Advanced Status view is displayed. Your WiFi Gigabit Router is ready to use.

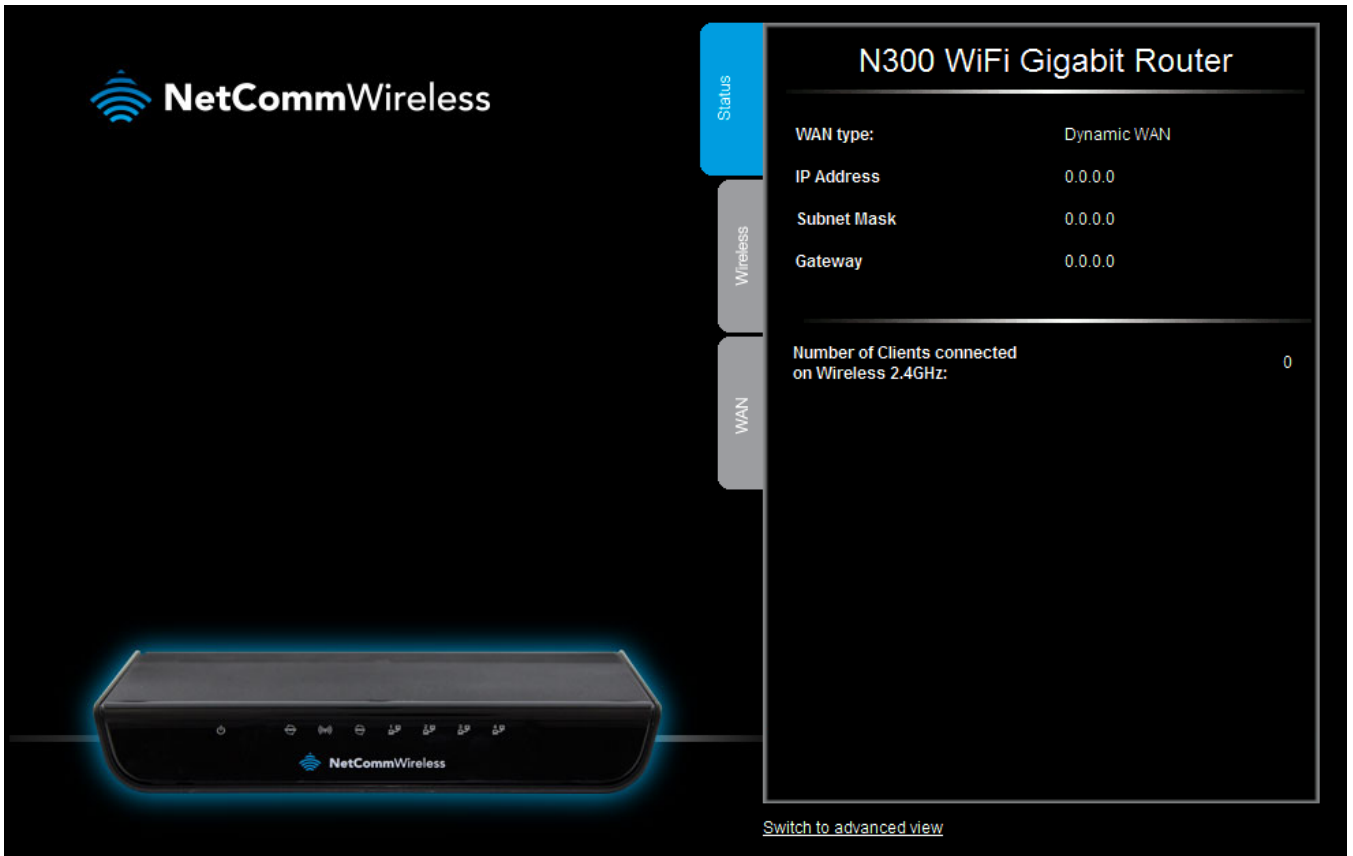
## Basic View

When you log in to the router, the Basic View is displayed. Basic View gives you the most important information at a glance.

### Status

The Status tab displays the following information:

-  The selected WAN type
-  The current WAN IP Address and Subnet Mask
-  The WAN Gateway Address
-  The number of clients connected on the 2.4GHz wireless network



**NetCommWireless**

**N300 WiFi Gigabit Router**





WAN type:	Dynamic WAN
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0

Number of Clients connected on Wireless 2.4GHz: 0

[Switch to advanced view](#)

## Wireless

The wireless tab displays the following options:

-  Turn Wireless (WiFi) on or off
-  Turn SSID Broadcast on or off
-  Set the SSID (WiFi Network Name)
-  Set the Wireless Security Key

If you make any changes to the Wireless configuration, Click the **Save and apply the changes** button to make these changes active.








The screenshot displays the NetCommWireless web interface. On the left, there is a sidebar with three tabs: 'Status', 'Wireless' (highlighted in pink), and 'WAN'. Below the sidebar is an image of the NetCommWireless router. The main content area shows the following configuration options:

- Wireless (WiFi)**:  On  Off
- SSID Broadcast**:  Enable  Disable
- WiFi Network Name**:   
(This is the name of your personal wireless network and will appear when you search for wireless networks to connect to.)
- Security Key**:

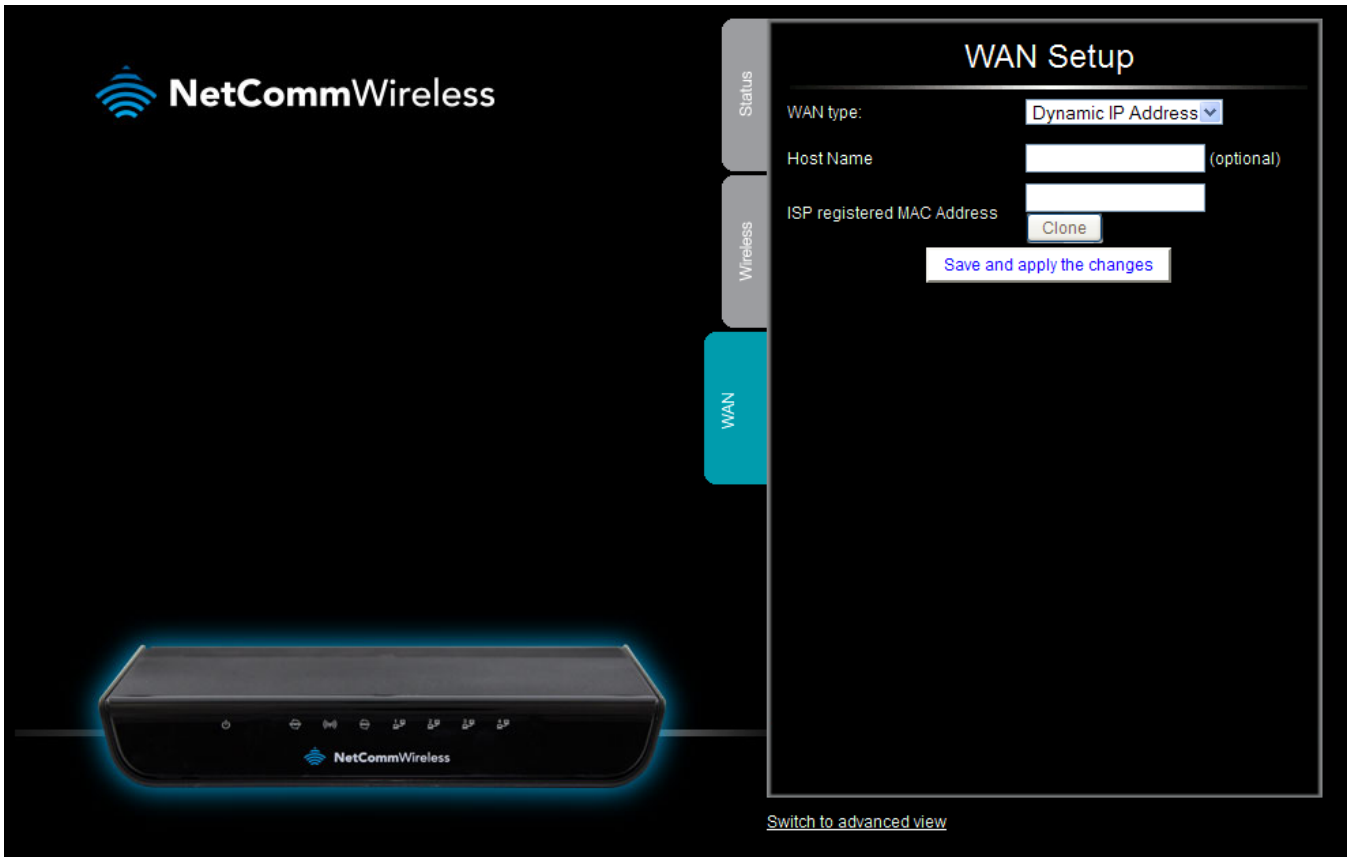
At the bottom of the configuration area, there is a button labeled **Save and apply the changes**. At the bottom right of the interface, there is a link labeled [Switch to advanced view](#).

## WAN

The WAN tab provides configuration options for your WAN connection. The available WAN types are:

-  Dynamic IP Address
-  Static IP Address
-  PPP over Ethernet
-  PPTP
-  L2TP

Select the correct WAN type and enter the appropriate information in the fields provided. When you have finished, click **Save and apply the changes** to make them active.



Note: Saving any configuration changes on this page will make the xDSL connection the primary method of connecting to the Internet and disable the ADSL connection.

## Advanced Configuration

To access the advanced configuration options of your NF7, you need to log in to the web configuration and change to Advanced view.

To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari), type <http://192.168.20.1/> into the address bar at the top of the window and press the Enter key.

At the login screen, type **admin** in the Username and Password field and click the Login button.



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



**NetCommWireless**

### N300 WiFi Gigabit Router

WAN type:	Dynamic WAN
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0


Number of Clients connected on Wireless 2.4GHz: 0

Click on the Switch to Advanced View link

Switch to advanced view

Click on the **Switch to Advanced View** link at the bottom of the page. The Advanced Status page is displayed.

N300 WiFi Gigabit Router - NF7


NetComm Wireless
Switch to basic view

Status

[Network Setup](#)
[Forwarding Rules](#)
[Security Settings](#)
[Advanced Settings](#)
[Toolbox](#)

// IPv4 System Status

Item	WAN Status	Sidenote
Remaining Lease Time	-	<a href="#">Renew</a>
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Gateway	0.0.0.0	
Domain Name Server	0.0.0.0, 0.0.0.0	

// IPv6 System Status

Item	WAN Status	Sidenote
WAN Link-Local Address		Dynamic IPv6
Global IPv6 Address	/64	
LAN IPv6 Link-Local Address		
Link Status		<a href="#">Connect</a>

// Wireless Status

Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	NetComm2218	
Channel	Auto	
Security	WPA2-PSK	(AES)

// Statistics Information

Statistics of WAN	Inbound	Outbound
Octets	0	0
Unicast packets	0	0
Multicast packets	0	0

[View Log...](#)
[Clients List...](#)
[NAT Status...](#)
[Refresh](#)

Device Time: Thu, 01 Jan 2009 10:34:05 +1000

ITEM	DESCRIPTION
<b>IPv4 System Status</b>	
Remaining Lease Time	The period remaining for the IPv4 address lease.
IP Address	The IP Address assigned to the router.
Subnet Mask	The Subnet Mask of the router.
Gateway	The router's gateway.
Domain Name Server	The IP addresses of the primary and secondary Domain Name Servers.
<b>IPv6 System Status</b>	
WAN Link-Local Address	The link-local address assigned to the router on the WAN side. The router will process packets destined to link-local addresses but will not forward them to other links.
Global IPv6 Address	The publicly routable and reachable IPv6 internet address.
LAN IPv6 Link-Local Address	The link-local address assigned to the router on the LAN side. The router will process packets destined to link-local addresses but will not forward them to other links.
Link Status	The current status of the IPv6 link.
<b>Wireless Status</b>	
Wireless mode	The status of the wireless radio.
SSID	The SSID of the wireless network.
Channel	The channel number in use by the wireless radio.
Security	The form of encryption in use on the router for the wireless network.
<b>Statistics Information</b>	
Octets	The number of data packets which have passed into and out of the router.
Unicast packets	The number of unicast packets which have passed into and out of the router.
Multicast packets	The number of multicast packets which have passed into and out of the router.






## Network Setup

### Network Setup

This page allows you to configure the Ethernet WAN (Wide Area Network) connection settings on the NF7.

#### Ethernet WAN

**WAN Type:** You can select from the following WAN types:-

-  Dynamic IP
-  Static IP
-  PPP over Ethernet
-  PPTP
-  L2TP

#### Dynamic IP Address

Item	Setting
WAN Interface	WAN <input type="button" value="v"/>
WAN Type	Dynamic IP Address <input type="button" value="v"/>
Host Name	<input type="text"/> (optional)
ISP registered MAC Address	<input type="text"/> <input type="button" value="Clone"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable <input type="button" value="v"/>
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="2"/> (range: 1~4094)
VLAN PRI	<input type="text" value="0"/> <input type="button" value="v"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
WAN Interface	The interface to configure.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Host Name	Set the hostname for your connection <i>(Optional - Refer to your ISP for more information).</i>
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.
VLAN PRI	The priority of the VLAN



## Static IP Address

Item	Setting
WAN Interface	WAN
WAN Type	Static IP Address
WAN IP Address	<input type="text"/>
WAN Subnet Mask	<input type="text"/>
WAN Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Auto
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="2"/> (range: 1~4094)
VLAN PRI	0

OPTION	DEFINITION
WAN Interface	The interface to configure.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
WAN IP Address	The static IP address assigned to you by your internet service provider.
WAN Subnet Mask	The subnet mask of the IP address assigned to you by your internet service provider.
WAN Gateway	The WAN Gateway provided to you by your internet service provider.
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.
VLAN PRI	The priority of the VLAN

## PPP over Ethernet

Item	Setting
WAN Interface	WAN
WAN Type	PPP over Ethernet
IPv6 Dualstack	<input type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Connection Control	Auto Reconnect (always-on)
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	0 (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="2"/> (range: 1~4094)
VLAN PRI	<input type="text" value="0"/>

OPTION	DEFINITION
WAN Interface	The interface to configure.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP.
Primary DNS	This feature allows you to manually assign a Primary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server <i>(Optional - Refer to your ISP for more information).</i>
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: <b>Connect-on-demand:</b> detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. <b>Auto-reconnect (always-on):</b> automatically reconnects the connection when it drops so that the internet connection is always on. <b>Manually:</b> Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Service Name	Enter the service name if your ISP requires it <i>(Optional - Refer to your ISP for more information).</i>
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which VLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.
VLAN PRI	The priority of the VLAN

## PPTP

Item	Setting
WAN Interface	WAN
WAN Type	PPTP
IP Mode	Dynamic IP Address
Server IP Address/Name	<input type="text"/>
PPTP Account	<input type="text"/>
PPTP Password	<input type="text"/>
Connection ID	<input type="text"/> (optional)
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)
MPPE	<input type="checkbox"/>
Multicast	Auto
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="2"/> (range: 1~4094)
VLAN PRI	<input type="text" value="0"/>

OPTION	DEFINITION
WAN Interface	The interface to configure.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the PPTP IP Address, PPTP Subnet Mask and PPTP Default gateway in use for the connection <i>(Refer to your PPTP administrator for more information).</i>
Server IP Address/Name	Enter the PPTP server name or IP Address.
PPTP Account	Enter the PPTP username supplied by your PPTP administrator.
PPTP Password	Enter the PPTP password supplied by your PPTP administrator.
Connection ID	Enter an Optional name to identify the PPTP connection.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: <b>Connect-on-demand:</b> detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. <b>Auto-reconnect (always-on):</b> automatically reconnects the connection when it drops so that the internet connection is always on. <b>Manually:</b> Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the PPTP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.
VLAN PRI	The priority of the VLAN

## L2TP

Item	Setting
WAN Interface	WAN
WAN Type	L2TP
IP Mode	Dynamic IP Address
Server IP Address/Name	<input type="text"/>
L2TP Account	<input type="text"/>
L2TP Password	<input type="text"/>
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)
MPPE	<input type="checkbox"/>
Multicast	Auto
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text" value="2"/> (range: 1~4094)
VLAN PRI	<input type="text" value="0"/>

OPTION	DEFINITION
WAN Interface	The interface to configure.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the L2TP IP Address, L2TP Subnet Mask and L2TP Default gateway in use for the connection <i>(Refer to your PPTP administrator for more information).</i>
Server IP Address/Name	Enter the L2TP server name or IP Address.
L2TP Account	Enter the L2TP username supplied by your L2TP administrator.
L2TP Password	Enter the L2TP password supplied by your L2TP administrator.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: <b>Connect-on-demand:</b> detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. <b>Auto-reconnect (always-on):</b> automatically reconnects the connection when it drops so that the internet connection is always on. <b>Manually:</b> Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the L2TP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.
VLAN PRI	The priority of the VLAN

## DHCP Server

This page allows you to change the Dynamic Host Configuration Protocol (DHCP) server settings on the NF7. The DHCP Server enables computers or devices connecting to the NF7 to automatically obtain their network configuration settings. By default, the DHCP server is enabled.

The **LAN IP Address** and **Subnet Mask** fields offer the ability to configure the IP address of the router locally and the subnet mask.

Item	Setting
DHCP Server	DHCP <input type="radio"/> Disable <input checked="" type="radio"/> Enable
LAN IP Address	<input type="text" value="192.168.20.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="200"/>
Lease Time	<input type="text" value="86400"/> Seconds
Domain Name	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Primary WINS	<input type="text"/>
Secondary WINS	<input type="text"/>
Gateway	<input type="text"/> (optional)

OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
LAN IP Address	The local IP address of the NF7. <i>(The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.)</i>
Subnet Mask	Enter the subnet mask for use on the local network. This would usually be set to 255.255.255.0.
IP Pool Starting/Ending Address	Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
Lease Time	Length of the DHCP lease time
Domain Name	Optional, this information will be passed to the client
Primary DNS	Optional, this information will be passed to the client
Secondary DNS	Optional, this information will be passed to the client
Primary WINS	Optional, this information will be passed to the client
Secondary WINS	Optional, this information will be passed to the client
Gateway	Optional, this information will be passed to the client

When you have finished configuring the DHCP Server settings, click **Save** to save your settings. If you want to cancel any changes you have made before saving them, click the **Undo** button.

Use the **Clients List** button to check the DHCP client list. The **Fixed Mapping** button allows you to map a specific IP address to a specific MAC address. The following pages describe these features in more detail.

### DHCP Client List

This is the list of currently connected devices using DHCP.

IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.20.100	computer_name	00-40-F4-CE-FA-1E	Wired	23:34:40	<input type="checkbox"/>

If you wish to set a permanent IP address for a particular DHCP client (or device), select the appropriate DHCP client by clicking in the "Select" box. This will ensure the clients current IP address is always assigned to it.

### DHCP Fixed Mapping

DHCP Fixed Mapping allows you to reserve a specific IP address for a specific device.

DHCP clients -- select one --  ID --

ID	MAC Address	IP Address	Enable
1	<input type="text" value="00:40:F4:CE:FA:1E"/>	<input type="text" value="192.168.20.100"/>	<input checked="" type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

The DHCP Server will reserve a specific IP for a device based on that device's unique MAC address.

You can enter a new fixed mapping by entering the MAC address of the device and the IP address you wish to allocate to it.

Select the **Enable** checkbox to activate the DHCP fixed mapping entry.

## Wireless

The Wireless page allows you to configure the options related to the wireless network of the router.

Item	Setting
Wireless Module	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	<input type="text" value="NetComm 2218"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="B/G/N mixed"/>
Authentication	<input type="text" value="WPA2-PSK"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	<input type="text" value="AES"/>
Pre-shared Key	<input type="text" value="bawixaneba"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

OPTION	DEFINITION
Wireless Module	Select to enable or disable the 2.4GHz Wireless network function of the NF7.
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. <i>(Please refer to the included Wireless Security Card insert for your default SSID)</i>
SSID Broadcast	The router will broadcast the SSID so that wireless clients can find the wireless network.
Channel	The wireless radio channel in use by your network.
Wireless Mode	Choose B/G Mixed, B only, G only, and N only, G/N Mixed or B/G/N mixed. <i>(The factory default setting is B/G/N mixed)</i>
Authentication	<p>You may select from the following authentication types to secure your wireless network:</p> <ul style="list-style-type: none"> <li>▪ Open</li> <li>▪ Shared</li> <li>▪ Auto</li> <li>▪ WPA</li> <li>▪ WPA-PSK</li> <li>▪ WPA2</li> <li>▪ WPA2-PSK</li> <li>▪ WPA/WPA2</li> <li>▪ WPA-PSK/WPA2-PSK.</li> </ul> <p>WPA-PSK/WPA2-PSK is a newer type of security. This type of security gives a more secure network compared to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK.</p> <p>Please enter the key in the "Preshare Key". The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers.</p> <p><i>(Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)</i></p>
802.1X	When Authentication is set to <b>Open</b> , you can enable 802.1X which enables Extensible Authentication Protocol (EAP) over wired or wireless networks.
Encryption	Select the type of encryption for your network. These options vary depending on the type of Authentication selected.



**Note:** The configuration for WPA-PSK and WPA2-PSK is identical

After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security. Please refer to your wireless adapter user guide for more information.

It is strongly recommended that you set up wireless security such as WPA-PSK (when the wireless client supports WPA) in order to secure your network.

Click **Save** to save these settings or click **Undo** to cancel.

## Change Password

This page allows you to change the NF7 web configuration password.

Item	Setting
Username	<input type="text" value="admin"/> (*Change this if you need to change Username.)
Old Password	<input type="password"/>
New Password	<input type="password"/>
Reconfirm	<input type="password"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Type in the old password (the factory default username and password is **admin**) and then type in the new password. Re-enter the new password in the **Reconfirm** field and click **Save**.

## Port Configuration

The port configuration page allows you to configure the mode of each of the Ethernet ports on the rear of the device. By default they are all set to **Auto** which means they can automatically detect and select the highest speed common to both connected devices. If you require to restrict the speed of any of the ports, you may use the drop down lists for the appropriate port to select **100Mbps / Full Duplex**, **10Mbps / Full Duplex**, **100Mbps / Half Duplex** or **10Mbps / Half Duplex** as required.

Item	Setting
WAN	<input type="text" value="Auto"/> ▼
LAN1	<input type="text" value="Auto"/> ▼
LAN2	<input type="text" value="Auto"/> ▼
LAN3	<input type="text" value="Auto"/> ▼
LAN4	<input type="text" value="Auto"/> ▼
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

When you have finished configuring the ports, click the **Save** button to confirm the settings.






## Forwarding Rules

The Forwarding Rules page allows you to configure the port forwarding management on the router. Click on any of the menu items on the left to access the respective settings page.

Forwarding rules are a necessary feature as by default NAT (Network Address Translation) will automatically block incoming traffic from the Internet to the LAN unless a specific port mapping exists in the NAT translation table. Because of this, NAT provides a level of protection for computers that are connected to your LAN.

However this also creates a connectivity problem when you want to make LAN resources available to Internet clients. For example, to play network games or host network applications.

There are three ways to work around NAT and to enable certain LAN resources available from the Internet:

-  Port Forwarding
-  Port Triggering
-  DMZ Host

### Port Forwarding

A virtual server is defined as a Service Port, and all requests to this port will be redirected to the computer specified by the Server IP.

Port Forwarding can also work with Scheduling Rules, and give you more flexibility on Access control.



Note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide

Well known services -- select one -- Copy to ID --

Item	Setting			
Port Forwarding Mode	Single Mode <span>▼</span>			
ID	Service Ports	Server IP	Enable	Use Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
17	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
18	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
19	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>
20	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	(0) Always <span>▼</span>

Save Undo

For example, if you have an FTP server (the default port is 21) at 192.168.1.10, a Web server (the default port is 80) at 192.168.20.40, and a VPN server (the default port is 1723) at 192.168.20.60, then you would need to specify the following virtual server mappings:



Note: At any given time, only one IP address can be bound to a particular Service Port.

SERVICE PORT	SERVER IP	ENABLE	USE RULE#
21	12.168.1.10	✓	(0) Always
80	192.168.20.40	✓	(0) Always
1723	192.168.20.60	✓	(0) Always

Click **Save** to save the settings or **Undo** to cancel.

## Port Triggering

Some applications like online games, video conferencing and Internet telephony require multiple connections to the internet. As such, these applications cannot work with a pure NAT router such as the NF7.

Popular applications -- select one -- Copy to ID --

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Save
Undo

The Port Triggering feature allows some of these applications to work with this router.



Note: If this fails to make the application work, try to configure that computer as the DMZ host instead.

(For further instructions on setting up a DMZ host, please refer to the “Miscellaneous” section below)

OPTION	DEFINITION
Trigger	The outbound port number that will be triggered by the application..
Incoming Ports	When the trigger packet is detected, the inbound packets sent to the specified port numbers will be allowed to pass through the firewall.
Enable	Select to enable or disable the configured special application entry.

The NF7 also provides predefined settings for some popular applications.

To use the predefined settings, select your application from the **Popular applications** drop down list, select an unused ID from the list and then click **Copy to**. The predefined settings will then be added to the list.

Click **Save** to save the settings or **Undo** to cancel.

## Miscellaneous

A Demilitarised Zone (DMZ) Host is a computer without the protection of firewall. It allows that particular computer to be exposed to unrestricted 2-way communication to the internet. It is mostly used for Internet games, Video conferencing, Internet telephony and other special applications.

Item	Setting	Enable
DMZ Mode	Single Mode ▼	
IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
UPnP setting		<input checked="" type="checkbox"/>

To enable DMZ, enter the IP address of the computer you want to be live on the internet and select the **Enable** option.



Note: This feature should be used only when required as it exposes the selected machine to the greater Internet without security.

OPTION	DEFINITION
DMZ Mode	Select from Single Mode or Multi Mode. Single Mode uses the currently active connection type for the DMZ host while Multi Mode allows you to specify which connection type should be placed in the DMZ.
IP Address of DMZ Host	Enter the IP address of the computer you wish to put in the DMZ.
UPnP Setting	The device also supports uPnP. If the DMZ host operating system supports this function enable it to automatically configure the required network settings.

Click **Save** to save the settings or **Undo** to cancel.

## Security Settings

The Security Settings page allows you to configure the security management on the router such as Packet filters and MAC Control. The following pages describe the various security options available

### Status

The Status page lists any currently configured filtering for the Outbound, Inbound and Domain filters.

Item	Status		
Outbound Filter	Disable		
Local Client	Only Deny Remote Host	Service	Working Time
Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time
Item	Status		
Domain Filter	Disable		
Domain	Access		
All other Domains	Yes		
<input type="button" value="Refresh"/>			

## Packet Filters

The Packet Filter enables you to control what packets are allowed to pass through the router. There are two types of packet filter, Outbound Packet Filter which applies to all outbound packets and the Inbound Packet Filter which only applies to packets that are destined for a Virtual Server or DMZ host only.





Note: For further instructions on setting up MAC Level Filtering, please refer to the “MAC Control” section below

### Outbound Filter:




To enable an Outbound Filter, tick the **Enable** tick box at the top of the page.

Item		Setting		
Outbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
<input type="button" value="First page"/> <input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Last page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/>				

There are two types of filtering policies:

-  Allow all data traffic to pass except those that match the specified rules.
-  Deny all data traffic to pass except those that match the specified rules.

You can specify up to 48 filtering rules for each direction (Inbound or Outbound). For each rule you will need to define the following:

-  Source IP address
-  Source port
-  Destination IP address
-  Destination port
-  Protocol: TCP or UDP or both.
-  Use Schedule Rule#

For source or destination IP address, you can define a single IP address (192.168.1.1) or a range of IP addresses (192.168.1.100-192.168.20.200). Leaving these fields empty implies all IP addresses are matched.

For source or destination port, you can also define a single port (80) or a range of ports (1000-1999). Use the prefix "T" or "U" to specify either the TCP or UDP protocol e.g. T80, U53, U2000-2999. No prefix indicates both TCP and UDP are defined. Leaving this field empty implies all ports are matched.

The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.



Note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide

Click **Save** to save the settings or **Undo** to cancel.

### Inbound Filter

To access the Inbound Packet Filter page, click on the **Inbound Filter** button on the bottom of the Outbound Filter page. All the settings on this page are the same as those for the Outbound Filter shown on the previous page.

Item		Setting		
Inbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
<input type="button" value="First page"/> <input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Last page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Outbound Filter..."/> <input type="button" value="MAC Level..."/>				

Click **Save** to save the settings or **Undo** to cancel.

## Domain Filters

Domain Filters enable you to prevent users from accessing specific domain addresses.

To enable the Domain Filter, select the **Enable** tick box at the top of the page.

Item	Setting
Domain Filter	<input type="checkbox"/> Enable
Log DNS Query	<input type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text"/> To <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

OPTION	DEFINITION
Domain Filter	Select to enable or disable domain filtering.
Log DNS Query	Enable this if you want to log when someone accesses filtered URLs.
Privilege IP Addresses Range	Set a group of computers that has unrestricted access to the internet

To set a Domain Filter, you need to specify the following:

OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx.com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this access.
Enable	Select to enable the rule.

Click **Save** to save the settings or **Undo** to cancel.

## URL Blocking

URL Blocking blocks LAN computers from connecting to a pre-defined website. The major difference between the Domain Filter and URL Blocking is that Domain Filtering requires you to input a suffix (e.g. xxx.com, yyy.net) while URL Blocking only requires you to input a keyword.

To enable URL Blocking, select the **Enable** option at the top of the page.

Item		Setting	
URL Blocking		<input type="checkbox"/> Enable	
ID	URL	Enable	
1	<input type="text"/>	<input type="checkbox"/>	
2	<input type="text"/>	<input type="checkbox"/>	
3	<input type="text"/>	<input type="checkbox"/>	
4	<input type="text"/>	<input type="checkbox"/>	
5	<input type="text"/>	<input type="checkbox"/>	
6	<input type="text"/>	<input type="checkbox"/>	
7	<input type="text"/>	<input type="checkbox"/>	
8	<input type="text"/>	<input type="checkbox"/>	
9	<input type="text"/>	<input type="checkbox"/>	
10	<input type="text"/>	<input type="checkbox"/>	
<input type="button" value="Save"/> <input type="button" value="Undo"/>			

To set a URL Blocking rule, you need to specify the following:

OPTION	DEFINITION
URL	If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

Click **Save** to save the settings or **Undo** to cancel.



## MAC Control

MAC Control allows you to assign different access rights for different users and to assign a specific IP address to a specific MAC address.

To enable MAC Address Control, select the **Enable** option at the top of the page.

Item	Setting		
MAC Address Control	<input type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <b>allow</b> unspecified MAC addresses to connect.		
<input type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <b>allow</b> unspecified MAC addresses to associate.		
DHCP clients <b>-- select one --</b> <input type="button" value="Copy to"/> ID <b>--</b>			
ID	MAC Address	C	A
1	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value=" &lt;&lt; Previous"/> <input type="button" value=" Next &gt;&gt;"/> <input type="button" value=" Save"/> <input type="button" value=" Undo"/>			

Two types of MAC Control are available:

OPTION	DEFINITION
Connection control (C column)	Use this to control which clients (wired and wireless) can connect to the unit. If a client is denied access to connect to this device, it means the client cannot access the Internet either. Choose to allow or deny clients with MAC addresses that are not in the list to connect to this device.
Association control (A column)	Check Association Control to control which wireless client can associate with the unit. If a client is denied access to associate with the unit, it means the client cannot send or receive any data via this device. Choose to allow or deny the clients with MAC addresses that are not in the list to associate to the wireless LAN.



Note: Click the "Next Page" or the "Previous Page" buttons to see the entire list

Click **Save** to save the settings or **Undo** to cancel.

## Miscellaneous

This page allows you to change various security settings on the unit.

Item	Setting	Enable
Administrator Time-out	<input type="text" value="300"/> seconds (0 to disable)	
Remote Administration	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
Discard PING from WAN side		<input checked="" type="checkbox"/>
DoS Attack Detection		<input checked="" type="checkbox"/>
Keep WAN in stealth mode		<input type="checkbox"/>


OPTION	DEFINITION
Administrator Time-out	The period of time with no activity in the web configuration page to logout automatically, set this to zero to disable this feature.
Remote Administrator Host/Port	Normally only Intranet users can browse the built-in web pages to perform administration tasks. This feature enables you to perform administration tasks from a remote host. If this feature is enabled, only the specified IP address can perform remote administration.
Discard PING from WAN side	When this feature is enabled, your router will not respond to ping requests from remote hosts.
DoS Attack Detection	When this feature is enabled, the router will detect and log where the DoS attack comes from on the Internet.
Keep WAN in stealth mode	When enabled, the router protects you by ignoring port scans. Port scans are often performed by attackers as a means of finding which services are running on your network in order to find an entry point.



Note: If the specified IP address is 0.0.0.0, any host can connect to the router to perform administration tasks. You can also use a subnet mask (/nn) to specify a group of trusted IP addresses for example, "10.1.2.0/24".

When Remote Administration is enabled, the web server port will be shifted to 80.

You can also change the web server port. When enabled, the router can detect the following (and more) DoS attack types:

-  SYN Attack
-  WinNuke
-  Port Scan
-  Ping of Death
-  Land Attack

Click **Save** to save the settings or **Undo** to cancel.

## Advanced Settings

The Advanced Settings page allows you to configure the advanced settings on the router such as the System log, Dynamic DNS and SNMP options.

### Status

The Status page displays the current System time, and lists any configured Dynamic DNS (DDNS) accounts, any Static or Dynamic Routes added or any Quality of Service (QoS) rules in place.

Item	Status			
System Time	Thu, 01 Jan 2009 14:05:16 +1000			
Item	Status			
DDNS	Disable			
Provider	-			
Item	Status			
Dynamic Routing	Disable			
Static Routing	Disable			
Destination	Subnet Mask	Gateway	Hop	
Item	Status			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time

## System Log

This enables you to set up the system log features of the router. You can also choose to send the system log to a remote syslog server (via a UDP connection) or email a copy to a recipient.

Item	Setting	Enable
IP address for syslog server	<input type="text"/>	<input type="checkbox"/>
Email address to send syslog to		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the "Enable" checkbox to enable this function.
SMTP Server : port	Enter the IP address or fully qualified domain name (FQDN) and port for the selected email server.
SMTP Username	The SMTP username required to send email <i>(if required)</i> .
SMTP Password	The SMTP password required to send email <i>(if required)</i> .
Email Addresses	Enter the email addresses to send a copy of the current syslog to.
Email Subject	Enter the email subject to show on any sent emails.
View Log...	View the current system log.
Email Log Now	Email the current syslog to the entered email addresses.

## Dynamic DNS




The Dynamic DNS feature enables users to set a static domain name for their internet connection even when the ISP only provides a dynamic IP address.

By mapping the host name to the current public IP address of the router, users who want to connect to the router or any services behind the router from the internet can just use the Dynamic DNS hostname instead of the IP Address which might change every time the router connects to the Internet.

Before you can use a Dynamic DNS service, you need to register an account on one of the many supported Dynamic DNS providers such as DynDNS.org, TZO.com or dhs.org.

Item	Setting
DDNS	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Provider	<input type="text" value="DynDNS.org(Dynamic)"/>
Host Name	<input type="text"/>
Username / E-mail	<input type="text"/>
Password / Key	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

After registering the account, the Dynamic DNS provider will provide you with the following details:

-  Host Name
-  Username/Email
-  Password/Key

To enable the Dynamic DNS feature on the unit, select the **Enable** option, choose the appropriate Dynamic DNS Provider and enter the details supplied by your Dynamic DNS provider.

Click **Save** to save the settings or **Undo** to cancel.

## QoS

Quality of Service (QoS) is a collection of network technologies which allow configuration of different priorities for different applications, users or data flows in order to guarantee a certain level of performance. The ultimate goal of QoS is to guarantee that the network delivers predictable results for availability, throughput, latency and error rate. QoS is especially important in ensuring the smooth operation of real-time streaming applications such as Voice over IP (VoIP), IPTV and online games.

As part of a strategy to provide Quality of Service, the NF7 supports Type of Service (ToS), the Differentiated Services (DiffServ) architecture and IEEE P802.1p priority tags (specified in the IEEE 802.1Q standard). DiffServ is a mechanism for classifying and managing network traffic by marking each packet on the network with a Differentiated Services Code Point (DSCP) which is a field in an IP packet used for classification purposes and operates at the IP layer. The NF7 also supports 802.1p priority tags which operate at the media access control (MAC) level. ToS, like DSCP, is a field in the header of IP packets that marks packets with different types of service such as minimize delay, maximize throughput, maximize reliability, minimize cost or normal service.

Item	Setting
QoS	Disable ▾
WAN Interface	Ethernet WAN ▾
QoS Mode	Smart-QoS ▾
Bandwidth of Upstream	<input type="text"/> Kbps (Kilobits per second)
Bandwidth of Downstream	<input type="text"/> Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable ▾

Item	Select	Setting
Game	<input type="checkbox"/>	<input type="text" value="0"/> %
Chat	<input type="checkbox"/>	<input type="text" value="0"/> %
VoIP	<input type="checkbox"/>	<input type="text" value="0"/> %
P2P	<input type="checkbox"/>	<input type="text" value="0"/> %
Video	<input type="checkbox"/>	<input type="text" value="0"/> %
Web	<input type="checkbox"/>	<input type="text" value="0"/> %

OPTION	DEFINITION
QoS	Use the drop down list to Enable or Disable QoS.
WAN Interface	Use the drop down list to select the interface to which QoS should apply.
QoS Mode	Use the drop down list to select the type of QoS to apply. Smart-QoS lets the router decide on the best settings based on the types of service you select below and the percentage setting assigned to each type of service. Higher percentages give a higher quality of service for that service type.
Bandwidth of Upstream	Enter the upstream bandwidth in Kilobits per second of your connection so that the router can calculate the best QoS settings.
Bandwidth of Downstream	Enter the downstream bandwidth in Kilobits per second of your connection so that the router can calculate the best QoS settings.
Flexible Bandwidth Management	<p>In Smart-QoS mode, when Flexible Bandwidth Management is enabled, you are able to select certain types of traffic to prioritise. The bandwidth allocated to each type of traffic is automatically divided by the number of types selected, for example, if you select "Game", "VoIP" and "Video", the router reserves 10% of bandwidth for other types of traffic and splits the remaining 90% of bandwidth equally among the 3 selected types, allowing each type 30% of bandwidth when each type of traffic is concurrently in use. If, for example, only two types of that traffic are in use, the 30% bandwidth allocated to the type of traffic not in use is re-distributed to other applications.</p> <p>When Flexible Bandwidth Management is disabled, you are able to manually specify the percentage of bandwidth to allocate to each type of traffic, however, you must still allow for 10% of bandwidth to be reserved for other types of traffic.</p>

### Basic QoS configuration

To configure QoS:

1. Set the **QoS** item to **Enable**.
2. The **WAN Interface** item displays the current WAN interface in use by the router and therefore to which interface the configuration applies.
3. Use the **QoS Mode** drop down list to set the QoS mode to **Smart-QoS**.
4. In the **Bandwidth of Upstream** field, enter the total upstream bandwidth of your broadband connection in Kilobits per second.
5. In the **Bandwidth of Downstream** field, enter the total downstream bandwidth of your broadband connection in Kilobits per second.
6. The **Flexible Bandwidth Management** option, when enabled, stipulates that you would like the router to manage the prioritisation of the selected traffic types on your behalf. When it is disabled, you have a greater degree of control by specifying a percentage of bandwidth that should be dedicated to a particular type of traffic. Choose whether you want it enabled or disabled and then select the types of traffic you want to give priority to. If you chose to disable flexible bandwidth management, in the **Setting** column you must also specify the percentage of bandwidth you wish to allocate for each type of traffic.



Note: The Setting column's percentage figures must add up to 90%. The remaining 10% of bandwidth is reserved for other types of network traffic.

### Advanced QoS configuration

To configure QoS:

1. Set the **QoS** item to **Enable**.
2. The **WAN Interface** item displays the current WAN interface in use by the router and therefore to which interface the configuration applies.
3. Use the **QoS Mode** drop down list to select **User-defined QoS Rule** to display the QoS rules table.

Item	Setting
QoS	Disable ▾
WAN Interface	Mobile Broadband ▾
QoS Mode	User-defined QoS Rule ▾
Bandwidth of Upstream	<input type="text"/> Kbps (Kilobits per second)
Bandwidth of Downstream	<input type="text"/> Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable ▾
<input type="button" value="Save"/>	
QoS Rules Table	
<input type="button" value="Add A New Rule..."/>	
<input type="button" value="Restart"/> <input type="button" value="Reset"/>	

4. In the **Bandwidth of Upstream** field, enter the total upstream bandwidth of your broadband connection in Kilobits per second.
5. In the **Bandwidth of Downstream** field, enter the total downstream bandwidth of your broadband connection in Kilobits per second.
6. The **Flexible Bandwidth Management** option, when enabled, stipulates that you would like the router to manage the prioritisation of the selected traffic types automatically. When it is disabled, you have a greater degree of control by specifying a percentage of bandwidth that should be dedicated to a particular type of traffic. Choose whether you want it enabled or disabled and then select the types of traffic you want to give priority to. If you chose to disable flexible bandwidth management, in the **Setting** column you must also specify the percentage of bandwidth you wish to allocate for each type of traffic.



Note: The Setting column's percentage figures must add up to 90%. The remaining 10% of bandwidth is reserved for other types of network traffic.

7. Click the **Add A New Rule** button. A new screen to configure a QoS rule is displayed.

Item	Setting
Rule	<input type="checkbox"/> Enable
Class	IP
Class Info - IP	
IP mask	
Protocol	All
DiffServ CodePoint	Default
Function	PRI
Function data - Priority	
Direction	In
Schedule	(0) Always
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

8. For the **Rule** item, check the **Enable** option. Use the descriptions in the table below to complete the rest of the settings for the rule. When the Class field is set to TCP/PORT, UDP/PORT, MAC, TOS or VLANPRI, you are able to add a conjunction rule. Click the **Add A Conjunction (AND) Rule** button that appears at the bottom of the page to add a conjunction rule.

OPTION	DEFINITION
Rule	Select to enable or disable the QoS rule.
Class	Select the class of traffic you would like to prioritise. This may be IP, TCP Port, UDP Port, MAC address, DSCP, ToS or VLAN Priority field.
Class Info	This field is only displayed when you select the Class field to be IP, TCP/PORT, UDP/PORT, MAC or VLANPRI. Enter the appropriate details for the class you have chosen e.g. an IP address, a TCP or UDP port number, a MAC address or a VLAN Priority flag.
IP mask	Only displayed when Class is set to IP. Enter the subnet mask of the IP address specified in the Class Info – IP field.
Protocol	Use the drop down list to select the protocol to which the rule should apply. This may be TCP, UDP or ICMP.
DiffServ CodePoint	Use the drop down list to select the DiffServ CodePoint that will be marked in the header of IP packets. There are 7 IP Precedence classes which are used in Type of Service headers but are also backwards compatible with DiffServ routers. The IP Precedence codes mark priority traffic. Assured Forwarding (AF) marks are also available. AF marks assign a drop precedence to each packet which defines the likelihood that a packet is dropped if traffic exceeds the subscribed rate. The last type of code is the Expedited Forwarding (EF) code. Packets marked EF have the properties of low delay, low loss and low jitter. This makes EF packets desirable for real-time streaming services for voice and video.
Service Type	This field is only displayed when the Class field is set to DSCP. The Service Type field specifies the type of packets to which the rule should apply. Use the drop down list to select the service type. The TCP/UDP port numbers are listed in brackets after each item.
Type of Service	The Type of Service field is only displayed when Class is set to TOS. Use the Type of Service drop down list to specify whether the QoS rule should minimize delay, maximize throughput, maximize reliability, minimize cost or just provide normal service.
Function	Select the function of the rule. You can select from Priority, Marking, Max Rate, Min Rate, Session, Drop, Log or Alert.
Function data	This field changes depending on the selected function. When Function is set to PRI (Priority), the Function data field should contain a priority value from 1 to 6 with 1 being the highest priority. When Function is set to MARKING, the Function data field allows you to specify a DiffServ Code Point marking for the packets. When the Function field is set to MAXR (Max Rate) or MINR (Minimum Rate), the Function data field should contain a data transfer rate in either Kilobits per second (KBps) or Megabits per second (MBps). This represents the minimum or maximum rate that the packet should expect to achieve on the network. When the Function field is set to SESSION, the Function data field should contain an integer representing the maximum number of sessions.
Direction	Select the direction of traffic to prioritise. Available options include In, Out or Both.
Schedule	Select a schedule for the new rule to apply. Previously created schedules are visible here or you can select the rule to always apply.
And Rule – Class	This field is displayed only when you have selected to add a conjunction rule. A conjunction rule allows you to add a second set of criteria with which the packets will be marked. Use the drop down list to select a second class of traffic for the rule. The only classes that will show up are MAC, TCP/PORT, UDP/PORT, TOS or VLANPRI.
And Rule – Class Info	This field is only displayed when you select to add a conjunction rule. Enter the appropriate details for the class you have chosen e.g. a MAC address, a TCP or UDP port number, a Type of Service or a VLAN Priority flag.



Note: For further instructions on scheduling rules, please refer to the “Scheduling” section later in this guide



Click on **Save** to store your setting or **Undo** to discard your changes.

### QoS configuration examples

Example 1.

To limit downstream bandwidth on LAN port 1 (IP address 192.168.20.2) to 100 KBps:

Item	Setting
QoS	Enable
WAN Interface	Ethernet WAN
QoS Mode	User-defined QoS Rule
Bandwidth of Upstream	1000 Kbps (Kilobits per second)
Bandwidth of Downstream	5000 Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable

QoS Rules Table	
<input type="button" value="Add A New Rule..."/>	
<input type="button" value="Restart"/> <input type="button" value="Reset"/>	

Click the **Add a New Rule** button. Enter the settings as below. When the direction is set to “IN”, the QoS function checks packets coming from the WAN side to the LAN side.

Item	Setting
Rule	<input checked="" type="checkbox"/> Enable
Class	IP
Class Info - IP	192.168.20.2
IP mask	255.255.255.0
Protocol	All
DiffServ CodePoint	Default
Function	MAXR
Function data - Rate	100 (KBps)
Direction	In
Schedule	(0) Always

The QoS rule is displayed in the QoS Rules Table at the bottom of the screen. The machine on LAN port 1 is now always restricted to a maximum download speed of 100 KBps at all times.

QoS Rules Table						
<input checked="" type="checkbox"/>	1.	<input checked="" type="checkbox"/> IP / 255.255.255.0 / All	: 192.168.20.2	Set MAXR Rate	: 100 KBps	(In) (Always)

To disable the rule, remove the check from the checkbox on the left. To delete the rule, click the X in the box after the rule number.

Example 2

To limit the number of sessions (per port) that can be made in an outbound direction from the machine on LAN port 1 (192.168.20.2) to 4 sessions:

Item	Setting
QoS	Enable
WAN Interface	Ethernet WAN
QoS Mode	User-defined QoS Rule
Bandwidth of Upstream	1000 Kbps (Kilobits per second)
Bandwidth of Downstream	5000 Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable

Save

QoS Rules Table						
<input checked="" type="checkbox"/>	1.	<input checked="" type="checkbox"/> IP / 255.255.255.0 / All	: 192.168.20.2	Set MAXR Rate	: 100 KBps	(In) (Always)

Add A New Rule...

Restart    Reset

Click the **Add a New Rule** button. Enter the settings as below. When the direction is set to “OUT”, the QoS function checks packets going from the LAN side to the WAN side.

Item	Setting
Rule	<input checked="" type="checkbox"/> Enable
Class	IP
Class Info - IP	192.168.20.2
IP mask	255.255.255.0
Protocol	All
DiffServ CodePoint	Default
Function	SESSION
Function data - Session	4 (Session)
Direction	Out
Schedule	(0) Always

Save    Undo

The QoS rule is displayed in the QoS Rules Table at the bottom of the screen. The machine on LAN port 1 will not be able to make more than 4 simultaneous outbound connections to a server.

QoS Rules Table						
<input checked="" type="checkbox"/>	1.	<input checked="" type="checkbox"/> IP / 255.255.255.0 / All	: 192.168.20.2	Set MAXR Rate	: 100 KBps	(In) (Always)
<input checked="" type="checkbox"/>	2.	<input checked="" type="checkbox"/> IP / 255.255.255.0 / All	: 192.168.20.2	Set SESSION Session	: 4 (Session)	(Out) (Always)

Add A New Rule...

Restart    Reset

To disable the rule, remove the check from the checkbox on the left. To delete the rule, click the X in the box after the rule number.

## SNMP

SNMP (Simple Network Management Protocol) is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

Item	Setting
Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	<input type="text"/>
Set Community	<input type="text"/>
IP 1	<input type="text"/>
IP 2	<input type="text"/>
IP 3	<input type="text"/>
IP 4	<input type="text"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
WAN Access IP Address	<input type="text"/>

OPTION	DEFINITION
Enable SNMP	You must check Local, Remote or both to enable SNMP function. If Local is checked, this device will only respond to requests from LAN connected hosts. If Remote is checked, this device will respond to requests from the WAN connection.
Get Community	Sets the community string your device will respond to for Read-Only access.
Set Community	Sets the community string your device will respond to for Read/Write access.
IP 1, IP 2, IP 3, IP 4	Input your SNMP Management host IP here. You will need to configure the address where the device should send SNMP Trap messages to.
SNMP Version	Please select proper SNMP Version that your SNMP Management software supports.
WAN Access IP Address	You can limit remote access to a specific IP address by entering it here.



Note: If "Remote" access is enabled, the default setting of 0.0.0.0 means any IP obtain SNMP protocol Information.

Click the **Save** button to store your setting or the **Undo** button to discard your changes.

## Routing

Routing tables allow you to determine which physical interface address to use for outgoing IP data. If you have more than one router and subnet, you will need to configure the routing table to allow packets to find the proper routing path and allow different subnets to communicate with each other.

These settings are used to setup the static and dynamic routing features of the NF7.

Item		Setting			
Dynamic Routing		<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2			
Static Routing		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

### Dynamic Routing:

Routing Information Protocol (RIP) will exchange information about different host destinations for working out routes throughout the network.



Note: Only select RIPv2 if you have a different subnet in your network. Otherwise, select RIPv1.

### Static Routing:

For static routing, you can specify up to 8 routing rules.

You need to enter the **destination IP address**, **subnet mask**, **gateway**, and **hop** for each routing rule, then enable the rule by selecting the **Enable** checkbox.

Click the **Save** button to store your setting or the **Undo** button to discard your changes.

## System Time

This page allows you to change the System time setting on the NF7.

Item	Setting															
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney															
Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org															
Enable Daylight Saving	<input checked="" type="radio"/> Disable <input type="radio"/> Enable															
Daylight Saving Dates	<table border="0"> <tr> <td></td> <td>Month</td> <td>Week</td> <td>Day of Week</td> <td>Time</td> </tr> <tr> <td>DTS Start</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> <tr> <td>DTS End</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> </table>		Month	Week	Day of Week	Time	DTS Start	Jan	1st	Sun	1am	DTS End	Jan	1st	Sun	1am
	Month	Week	Day of Week	Time												
DTS Start	Jan	1st	Sun	1am												
DTS End	Jan	1st	Sun	1am												
<input type="button" value="Save"/> <input type="button" value="Undo"/>																
<input type="button" value="Sync with Time Server"/> <input type="button" value="Sync with my PC (Wed April 24, 2013 10:13:55)"/>																

OPTION	DEFINITION
Time Zone	Select the time zone where this device is located.
Auto-Synchronization	Select the "Enable" checkbox to enable this function.
Enable Daylight Saving	Enables or disables the router's automatic daylight saving adjustment feature.
Daylight Savings Dates	Use the drop down lists to select a daylight saving start and end date and time.
Time Server	Select a NTP time server to obtain the current UTC time from.
Sync with Time Server	Select if you want to set Date and Time by NTP Protocol.
Sync with my PC	Select if you want to set Date and Time using your computers Date and Time

Click **Save** to save the settings or **Undo** to cancel.

## Scheduling

You can use scheduling to enable or disable a service at a specific time or on a specific day.

Item		Setting
Schedule		<input type="checkbox"/> Enable
Rule#	Rule Name	Action
1		<input type="button" value="Add New"/>
2		<input type="button" value="Add New"/>
3		<input type="button" value="Add New"/>
4		<input type="button" value="Add New"/>
5		<input type="button" value="Add New"/>
6		<input type="button" value="Add New"/>
7		<input type="button" value="Add New"/>
8		<input type="button" value="Add New"/>
9		<input type="button" value="Add New"/>
10		<input type="button" value="Add New"/>
<input type="button" value=" &lt;&lt; Previous"/> <input type="button" value=" Next &gt;&gt;"/> <input type="button" value=" Save"/> <input type="button" value=" Add New Rule..."/>		

Select **Enable** and then click the **Add New Rule** button.

Item		Setting	
Name of Rule 1		<input type="text"/>	
Policy		<input type="button" value="Inactivate"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
2	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
3	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
4	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
5	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
6	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
7	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
8	<input type="button" value="-- choose one --"/>	<input type="text"/>	<input type="text"/>
<input type="button" value=" Save"/> <input type="button" value=" Undo"/> <input type="button" value=" Back"/>			

Select a name for the rule and enter the details such as the day, start time or end time and click the **Save** button

In the example below, the rule is called "Work Hours" and it is only active between 08:00 and 17:30.

You are then able to select the scheduling rule name specified from the Packet Filter configuration section to perform the configured filtering at the scheduled time as per the screenshot below.

Item		Setting	
Name of Rule 1		<input type="text" value="Work Hours"/>	
Policy		<input type="button" value="Inactivate"/> except the selected days and hours below.	
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	<input type="button" value="Every Day"/>	<input type="text" value="08:00"/>	<input type="text" value="17:30"/>

This example would prevent any access to the IP address 66.102.11.104 from any device connected to the router, 7 days a week, only between the hours of 08:00 and 17:30.

Click the **Save** button to save the settings or the **Undo** button to cancel.

## IPv6

The IPv6 page enables you to configure the settings used for an IPv6 connection (if supported by your Internet Service Provider).

Item	Setting
IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Interface	<input type="text" value="Ethernet"/>
IPv6 Connection	<input type="text" value="DHCPv6"/>
DNS Setting	<input checked="" type="radio"/> Obtain DNS Server address Automatically <input type="radio"/> Use the following DNS address
Primary DNS Address	<input type="text"/>
Secondary DNS Address	<input type="text"/>
LAN IPv6 Address	<input type="text"/> /64
LAN IPv6 Link-Local Address	
Autoconfiguration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Autoconfiguration Type	<input type="text" value="Stateless"/>
Router Advertisement Lifetime	<input type="text" value="200"/> Seconds
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

OPTION	DEFINITION
IPv6	Select to enable or disable IPv6 functionality.
IPv6 Interface	The IPv6 interface you wish to configure.
IPv6 Connection	Select the type of IPv6 connection to utilise for your service. You can select from: <ul style="list-style-type: none"> <li>▪ Static IPv6</li> <li>▪ DHCPv6</li> <li>▪ PPPoE</li> <li>▪ 6 to 4</li> <li>▪ IPv6 in IPv4 Tunnel</li> <li>▪ PPPoA</li> </ul> Select the type of connection as required by your Internet Service Provider for their IPv6 service.
DNS Setting	Select whether to automatically obtain DNS Server addresses or use the ones you manually specify.
Primary DNS Address	Enter the Primary DNS Address for the IPv6 connection.
Secondary DNS Address	Enter the Secondary DNS Address for the IPv6 connection.
LAN IPv6 Address	The IP Address to use for the IPv6 service connection.
LAN IPv6 Link-Local Address	The current local LAN IPv6 address of the NF7.
Autoconfiguration	Select to enable or disable IPv6 auto configuration (if supported by your Internet Service Provider).
Autoconfiguration Type	Select the appropriate type of auto configuration mode as required by your Internet Service Provider for their IPv6 service.
Router Advertisement Lifetime	Enter the length of time between the router advertising its availability on the IPv6 connection.

## TR-069

The TR-069 client allows the NF7 to be automatically configured from a TR-069 server. Enter the applicable configuration options to enable the router to contact the TR-069 server and retrieve any configuration options.

Item	Setting
TR-069	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
ACS URL	<input type="text"/>
ACS Username	<input type="text"/>
ACS Password	<input type="text"/>
Connection Request Port	<input type="text" value="8099"/>
Connection Request Username	<input type="text"/>
Connection Request Password	<input type="text"/>
Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Interval	<input type="text" value="900"/> seconds

OPTION	DEFINITION
TR-069	Select to enable or disable the TR-069 automatic configuration function.
ACS URL	Enter the URL of the ACS server for automatic configuration.
ACS User Name	The username required to login to the ACS server.
ACS Password	The password required to login to the ACS server.
Connection Request Port	The port number the ACS server is running on.
Connection Request Username	The username to use when a connection request is made to the CPE.
Connection Request Password	The password to use when a connection request is made to the CPE.
Inform	Select to enable or disable the Inform function for ACS connections.
Interval	Select the interval between Inform requests if Inform has been enabled.

Click the **Save** button to store any changes to the settings.



## VLAN

The VLAN page provides you with the ability to create Virtual Local Area Networks (VLANs). A VLAN is layer-2 network which has been partitioned to create multiple distinct broadcast domains. The purpose of this is to isolate packets so that they may only pass between these broadcast domains via one or more routers.

Ethernet	WAN/LAN	VID	Tx TAG
Port1	WAN	<input type="text" value="3"/>	<input type="checkbox"/>
Port1	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port2	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port3	LAN	<input type="text" value="1"/>	<input type="checkbox"/>
Port4	LAN	<input type="text" value="1"/>	<input type="checkbox"/>

VLAN ID on LAN	LAN/Wireless LAN(Interface)	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port3, Port4	No	NAT	0

OPTION	DEFINITION
Ethernet	The number of the physical port on the rear of the router for which the VLAN will be created.
WAN/LAN	The function of the port. Port 1 only functions as a WAN port.
VID	The Virtual LAN ID you want to assign to the VLAN.
Tx TAG	Selecting this option will tag packet headers with the VLAN ID.

To adjust advanced WAN VLAN settings for a particular VID, click the **WAN VLAN Settings** button. The following window is displayed:

Item	Setting
VID	<input type="text" value="1"/>
Routing Type	<input type="text" value="NAT"/>
DHCP Setting	DHCP

OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
DHCP Setting	Displays the current DHCP setting.

Setting **Routing Type** to **Bridge** displays further options:

Item	Setting
VID	<input type="text" value="1"/>
Routing Type	<input type="text" value="Bridge"/>
WAN type	<input type="text" value="Ethernet"/>
WAN Map VLAN ID	<input type="text" value="0"/> (0 is untag)

OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
WAN type	Use the drop down list to select which WAN type the VLAN uses.
WAN Map VLAN ID	Enter the VLAN ID to tag packets on the WAN interface.

## Toolbox

The toolbox menu provides access to various settings and maintenance functions of the router.

### System Info

The System Info screen displays the general settings on the router, such as the WAN type, the date and time, the log types and the log data.

Item	Setting
WAN Type	Dynamic IP Address
Display time	Thu, 01 Jan 2009 10:41:07 +1000
Time	Log

Page: 1/0 (Log Number: 0)

### Routing Table

The Routing table displays the current routes in place on the router.

Routing Table				
Destination	Netmask	Gateway	Flags	Interface
192.168.20.0	255.255.255.0	0.0.0.0		br0
239.0.0.0	255.0.0.0	0.0.0.0		br0
127.0.0.0	255.0.0.0	0.0.0.0		lo

Total numbers of routes :3  
 Flags Meaning : G:Gateway D:Dynamic H:Host

Click the **Refresh** button to update this list.

### Restore Settings

The Restore settings page allows you to restore a previously saved configuration of the router. This is handy for reverting to a working configuration when making changes to the router's settings.

Config Filename
<input data-bbox="667 1507 751 1534" type="button" value=" Browse... "/> No file selected.
Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.
<input data-bbox="719 1626 804 1653" type="button" value=" Restore "/> <input data-bbox="815 1626 900 1653" type="button" value=" Cancel "/>

To restore the router configuration, click the **Browse** button, select the saved configuration file and then click the **Restore** button.

## Firmware Upgrade

This page lets you upgrade the firmware of the router. The firmware is the system running on the router. New firmware updates are regularly made available and can fix bugs and add new features.

Firmware Filename
<input type="button" value="Browse..."/> No file selected. Current firmware version is <b>NCNU0.1004_10281915</b> .  Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.
<input type="button" value="Upgrade"/> <input type="button" value="Cancel"/>

## Backup Settings

Click the **Backup Settings** menu item to save the current configuration of the router to a file for safe-keeping.

## Reset to Default

Click the **Reset to Default** menu item to set the configuration of the router to the factory default settings.



Note: This will erase all configuration settings. Ensure you have a backup of your configuration before proceeding to reset to default settings.

## Reboot

Click the **Reboot** menu item to restart the router.

## Startup Wizard

Click the **Startup Wizard** menu item if you want to run the initial wizard that showed the first time you installed your router.

## Miscellaneous

The miscellaneous page provides options to send a Wake-on-LAN packet to a specified IP, ping a specified domain name or IP address and brighten or dim the front LEDs of the router.

Item	Setting
MAC Address for Wake-on-LAN	<input type="text"/> <input type="button" value="Wake up"/>
Domain Name or IP address for Ping Test	<input type="text"/> <input type="button" value="Ping"/>
LED Settings	<input checked="" type="radio"/> Manual <input type="radio"/> By Schedule <input type="button" value="Brighten LEDs"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

## Logout

The **Logout** menu item logs you out of the router.

# Additional Product Information

## Establishing a wireless connection

### Windows XP (Service Pack 3)

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

### Windows Vista

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

### Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for *the default wireless network key*).
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NF7 with "Connected" next to it.

### Mac OSX 10.6

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



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

## Troubleshooting

### Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

#### Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NF7 power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NF7 and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF7 off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

#### Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NF7. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NF7's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.
5	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for ten seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NF7 restarts. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

#### Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for ten seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF7 restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

#### WLAN Interface

I cannot access the NF7 from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NF7 and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

# Technical Data

The following table lists the hardware specifications of the NF7.

MODEL	NF7
Wireless WAN	PPP (for WCDMA / HSPA)
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	1 x 10/100/1000 Mbps WAN, 4 x 10/100/1000 Mbps LAN, 1 x WLAN.
LED Indicators	Power, WWW, WiFi, WAN, LAN 1-4.
Operating Temperature	Operating temperature: 0°C - 40°C, Humidity: 10%-90% non-condensing Storage temperature: -10°C - 70°C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 1A
Dimensions & Weight	168 mm (L) x 119 mm (W) x 27 mm (H) 217 grams
Regulatory Compliance	RCM

## Electrical Specifications

It is recommended that the NF7 be powered by the supplied 12V DC, 1A power supply. A replacement power supply is available from the NetComm Wireless Online shop.

## Environmental Specifications / Tolerances

The NF7 housing enables it to operate over a wide variety of temperatures from 0°C - 40°C (operating temperature).

# Legal & Regulatory Information

## Intellectual Property Rights

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

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

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

## Customer Information

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

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

## Consumer Protection Laws

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

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

## Product Warranty

All NetComm Wireless products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a Product Warranty). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Wireless Limited within 30 days of the original purchase date by registering online via the NetComm Wireless web site at [www.netcommwireless.com](http://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](mailto:sales@netcommwireless.com) [techsupport@netcommwireless.com](mailto:techsupport@netcommwireless.com)