NF2 – DUAL BAND WIFI GIGABIT HUB

USER GUIDE

Copyright
Copyright©2012 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.

Please 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 NF2

DOCUMENT VERSION	DATE
1.0 - Initial document release	21/02/2011

Table 1 - Document Revision History

Table of Contents

Overview 5
Introduction 5
Target Users 5
Prerequisites 5
Notation 5
Product Introduction 6
Product Overview 6
Package Contents 6
Product Features 6
Physical Dimensions and Indicators 7
LED Indicators 7
Integrated Interfaces 7
NF2 Default Settings 9
Safety and Product Care 10
Transport and Handling 10
Installation and Configuration of the NetComm NF2 11
Placement of your NF2 and Mobile Broadband 11
Avoid obstacles and interference 11
Cordless Phones 11
Choose the “Quietest” Channel for your Wireless Network 11
Hardware installation 12
Connecting via an Ethernet cable 12
Connecting wirelessly 12
First Time Simple Configuration Wizard 13
Management Console Login Procedure 18
Management Console 19
Advanced Features 24
Network Setup 25
Network Setup 25
DHCP 27
Wireless 2.4 GHz 28
WDS Settings 29
WPS Setup 29
Wireless 5.0 GHz 30
VPN – IPSec 31
VPN-L2TP 33
VPN-PPTP Client 33
VPN – PPTP Server 34
Change Password 35
Forwarding Rules 36
Virtual Server 36
Special AP 37
Miscellaneous 37
Security Settings 38
Status 38
Packet Filtering 38
MAC Control 39
Domain Filter 40
URL Blocking 41
Miscellaneous 41
Advanced Settings 42
Status 42
System Log 42
Dynamic DNS 43
QoS (Quality of Service) 44
SNMP 44
Routing 45
System Time 46
Scheduling 46
IPV6 48
TR-069 49
VLAN 50
NAS Settings 51

Disk Utility 51
File Sharing 51
FTP Service Configuration 52
Access Control 53
iTunes Server 54
Download Assistant 55
Download Status 56
Web HDD 57
Toolbox 58
System Info 58
Restore Settings 59
Firmware Upgrade 59
Backup Settings 59
Reset to Default 60
Reboot 60
Startup Wizard 61
Miscellaneous 61
Logout 62
Additional Product Information 63
Establishing a wireless connection 63
Technical Data 64
Electrical Specifications 64
Environmental Specifications / Tolerances 64
FAQ 65
Appendix A: Tables 66
Legal & Regulatory Information 67
Intellectual Property Rights 67
Contact 69

Overview

Introduction

This manual provides information related to the installation, operation, and utilisation of the NetComm NF2.

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 NF2 Hub, please confirm that you comply with the minimum system requirements below.

- An activated fixed line Internet connection with a working modem attached (ADSL, Cable, Fibre) and/or a compatible 3G/4G USB modem.
- 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, Netscape Navigator, 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 utilised in this user manual:

-

The following note requires attention

-

The following note provides a warning

-

The following note provides relevant information

Product Introduction

Product Overview

- Wireless WAN (where network is available) - GPRS/EDGE/WCDMA/HSDPA/HSUPA/CDMA2000/EVDO/LTE.
- Ethernet WAN – PPPoE, DHCP client, Static IP, PPTP, L2TP
- 2 x USB 2.0 ports – for 3G/4G, USB storage.
- 2 x 3 internal WiFi antenna
- 1 x external WiFi antenna
- IPv6 Support – Dual Stack IPv6, Static IPv6, DHCPv6, PPPOE, 6 to 4, IPv6 to IPv4 tunnel
- 3 x 10/100/1000Mbps LAN Ethernet ports.
- 1 x 10/100/1000Mbps WAN Ethernet port for optional alternate Internet connectivity (ADSL/Cable/Satellite).
- 802.11n up to 900Mbps Wireless[1] (Backward compatible with 802.11b/g/a).
- 2.4GHz and 5.0GHz Concurrent WiFi.
- Supports auto Internet fallback from 3G to a fixed line WAN connection (ADSL/Cable/Satellite).
- WiFi Protected Setup (WPS) for wireless connectivity.
- Browser based interface for configuration and management.
- Wireless security options- WEP/WPA/WPA-PSK/WPA2/WPA2-PSK.
- VPN IPsec, VPN L2TPClient/Server, VPN PPTP Client/Server.

1. Speeds are dependent on network coverage. See your MBB provider coverage maps for more details. The total number of WiFi users can also affect data speeds. The maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. The actual wireless speed and coverage are dependent on network and environmental conditions including but not limited to the volume of network traffic, building materials and construction/layout.

Package Contents

The NF2 Hub package consists of:

- 1 x NF2 WiFi Router.
- 1 x 12VDC~1.5A Power Adapter.
- 1 x External Antenna.
- 1 x RJ-45 LAN Cable.
- Quick Setup Guide.
- Wireless Security Card.
- Warranty Card.

If any of these items are missing or damaged, please contact your dealer immediately.

Product Features

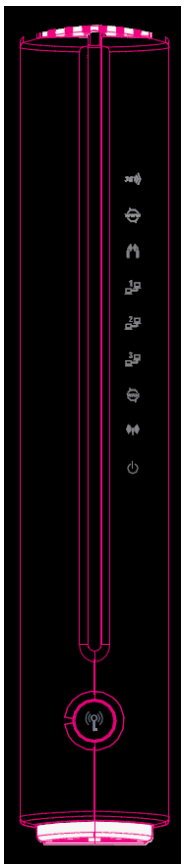
The NetComm NF2 creates a secure WiFi network, providing Internet access for up to 15 users. Simply plug the NF2 into a power outlet then insert a Mobile Broadband (MBB) dongle into the USB port on the side panel to access a high speed Internet connection within minutes.

The NetComm NF2 incorporates a WLAN 802.11b/g/n access point, three 10/100/1000Mbps Gigabit Ethernet ports and one 10/100Mbps Ethernet WAN port. It features the latest security options such as WPA and WPA2 data encryption, SPI (Stateful Packet Inspection) Firewall and VPN pass through.

Physical Dimensions and Indicators

LED Indicators

The NetComm NF2 has been designed to be placed on a desktop. All of the cables exit from the rear for better organization. The display is visible on the front of the NF2 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	DEFINITION
3G		A solid blue light indicates the NF2 is connected via 4G. The 4G LED will flash on data traffic throughput.
WWW		A solid blue light will appear when the WWW connection is established.
WDS		When the NF2 is connected via wireless to another access point this LED will be lit up.
LAN		The LAN LEDs will be a solid blue light when a specific LAN connection is established. The LED flashes on LAN port traffic throughput.
WAN		WAN mode: The WAN LED lights up when the router is connected to the internet via a fixed line WAN connection.
WWW		A solid blue light appears when the WWW connection is established.
WiFi		The LED will show a solid blue light when WLAN is enabled. The LED flashes on traffic throughput (data transfer).
Power		The power LED will be a solid blue light when the device is powered on. The power LED will flash during the device start up process.

Table 2 - LED Indicators

Integrated Interfaces

The following integrated interfaces are available on the rear of the NetComm NF2:

INTERFACE	FUNCTION
WiFi Antenna	Attach the wireless antenna turning it in a clockwise direction.
WAN	The WAN Ethernet port for a Fixed Line (ADSL/Cable/Satellite) connection to the internet.
On/Off	The power button for the NF2. Press once to switch the unit on or off.
LAN 1	The LAN 1 Port for wired Ethernet clients (Computers, Laptops, etc).
LAN 2	The LAN 2 Port for wired Ethernet clients (Computers, Laptops, etc).
LAN 3	The LAN 3 Port for wired Ethernet clients (Computers, Laptops, etc).
Power	The power connector designed for use with a DC 12V 1.5A Power Adapter.
Reset	Hold this button down for over 10 seconds to reset the router to factory default settings.
3G	Connect a 3G/4G USB modem here
USB Storage	Connect a USB based storage device here

Table 3 – Integrated Interface

NF2 Default Settings

The following tables list the default settings for the NF2 Hub.

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

Table 3: LAN Management Default Settings

WAN (INTERNET)	
WAN mode:	Dynamic IP

Table 4: WAN Port Default Settings

WIRELESS (WIFI)	
SSID:	(Refer to the included wireless security card)
Security:	WPA-PSK/WPA2-PSK
Security Key:	(Refer to the included wireless security card)

Table 5: WiFi Default Settings

For security purposes, each NF2 comes with a unique SSID that varies by a 4 digit number at the end. e.g. SSID: "NetComm Wireless XXXX"

NF2™ HUB WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Table 6: Web Interface Default Settings

Safety and Product Care

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

- To avoid fire or shock hazard do not use or install this product near water. 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 NetComm NF2, 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 NetComm NF2

Placement of your NF2 and Mobile Broadband

Just like your mobile phone, the NF2's location will affect its signal strength to the MBB (Mobile Broadband) Provider's Mobile Base Station (Cell Tower). The data speed achievable from the NF2 is relative to this signal strength, which is affected by many environmental factors. Please keep in mind that the NF2 will need adequate signal strength in order to provide Internet connectivity whilst choosing a location to place your NF2.

Similarly, the wireless connection between your NF2 and your WiFi devices will be stronger the closer your connected devices are to your NF2. Your wireless connection and performance will degrade as the distance between your NF2 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 NF2™ Hub in order to see if distance is the problem.

Please 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. Please ensure that your NF2 WiFi external antenna is positioned vertically (toward the ceiling).

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF2, please try the following steps:

- In multi-storey homes, place the NF2 on a floor that is as close to the centre of the home as possible. This may mean placing the NF2 on an upper floor.
- Try not to place the NF2™ Hub near a cordless telephone that operates at the same radio frequency as the NF2 (2.4GHz).

Avoid obstacles and interference

Avoid placing your NF2 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 wireless devices and the NF2).

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 NF2 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 NF2.
- 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 NF2 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. Attach the supplied antenna to the antenna port. [This should be attached in a clockwise direction.]
2. Insert your MBB (Mobile Broadband) Dongle into the USB slot.
3. Connect the power adapter to the Power socket on the back of the NF2.
4. Plug the power adapter into the wall socket and switch on the power.
5. Wait approximately 60 seconds for the NF2 to power up.

Connecting via an Ethernet cable

1. Connect the Ethernet cable provided to the port marked LAN at the back of the NF2.
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 type http://192.168.20.1 into the address bar and press enter.
5. Enter “admin” (without quotations) for both the Username and Password and click on the Login button.
6. Follow the steps of the start-up wizard to set up your NF2.
7. After the setup process is completed, you will be connected to the Internet.

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 found on the Wireless Security Card (included in the box).

Figure 1: Included Security Card

Please note: For security purposes, each NF2 has a unique SSID (such as NetComm-WirelessXXXX) and Wireless Security Key. The included Wireless Security Card lists these fields instead of the xxxxx’s as shown in the screenshot above.

3. When prompted for your wireless security settings, enter the wireless security key listed on your Wireless Security Card.
4. Wait approximately 30 seconds for the connection to be established.
5. Open your Web browser and type http://192.168.20.1 into the address bar and press enter.
6. Enter “admin” (without quotations) as both the Username and Password and press the Login button.
7. Follow the steps to set up your NF2.
8. After the setup process is completed, you will be connected to the Internet.
9. To connect additional devices via WiFi, repeat steps 1 through 4.

First Time Simple Configuration Wizard

When you log in to your NF2 for the first time, you will be presented with the NF2 “Set-up Wizard” as shown in the screenshot below. This wizard can be skipped by clicking on the link shown on the screenshot below. You can re-run the Setup Wizard again anytime after first use by selecting the “Setup Wizard” option under the “Toolbox” tab in the Advanced View of the management console.

Figure 2: Setup Wizard - Start

Figure 2: Setup Wizard Step 1 –WAN Interface

Select your WAN interface preference – Ethernet WAN, 3G or Ethernet WAN with 3G backup. The example above shows an Ethernet WAN connection with 3G backup. Press the Next button to continue the setup wizard.

Figure 3: Setup Wizard Step 2 - 2.4 GHz WiFi Setup

This page allows you to customize the 2.4GHz wireless setting of the NF2.

Wireless (WiFi):

WiFi is set to “On” by default. Changing this option to “Off” will turn off the wireless feature and you will not be able to connect to your NF2 via 2.4 GHz WiFi.

SSID Broadcast:

Select ‘Disable’ to hide the SSID of the NF2. If disabled, other people will not be able scan and detect your NF2’s SSID.

SSID Broadcast Name (Max 32 Characters):

The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless network so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.

Click “Next” to continue.

Figure 4 - Setup Wizard Step 3 – 2.4 GHz WiFi Security Settings

This page allows you to configure the 2.4 GHz WiFi security settings for the NF2. Setting a strong wireless security level (such as WPA-PSK - AES) can prevent unauthorized access to your wireless network. Please enter the Security Key that you wish to use, or leave this field unchanged to use the default Security Key. Click “Next” to continue.

Figure 7: Setup Wizard Step 4 - 5.0 GHz WiFi Setup

This page allows you to customize the 5.0 GHz wireless setting of the NF2.

Wireless (WiFi):

WiFi is set to “On” by default. Changing this option to “Off” will turn off the wireless feature and you will not be able to connect to your NF2 via 5.0 GHz WiFi.

SSID Broadcast:

Select ‘Disable’ to hide the SSID of the NF2. If disabled, other people will not be able scan and detect your NF2’s SSID.

SSID Broadcast Name (Max 32 Characters):

The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless network so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.

Click “Next” to continue.

Figure 5: Setup Wizard Step 5 - 5.0 GHz Wireless Security Setup

This page allows you to configure the 5.0 GHz WiFi security settings for the NF2. Setting a strong wireless security level (such as WPA-PSK - AES) can prevent unauthorized access to your wireless network. Please enter the Security Key that you wish to use, or leave this field unchanged to use the default Security Key. Click “Next” to continue.

Figure 6: Setup Wizard Step 6 - Router Security Settings

In Step 6 of the NF2 Setup Wizard the administration password for the router can be set to prevent unauthorised access to the router management page. Enter the Desired Username and Desired Password, retyping the desired Password in the Retype Password field to confirm the new password. Click Next to continue the setup wizard.

Figure 7: Setup Wizard Step 7 - Summary

Review your settings then click “Finish” to save configuration. Click “Back” if you want to make any changes.

After clicking Finish, the NF2 will save your configuration and reboot itself. Please wait as this process takes about 2 minutes. You will be guided back to the management console once the process is complete.

Management Console Login Procedure

After first time setup, the management console will be password protected to prevent unauthorized access to the configuration settings of your NetComm NF2.

To log in to the management console, view the status and make changes to your NF2, please follow the steps below:

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to http://192.168.20.1
2. Enter the username and password configured during the first time setup and click the Submit button. Use the default username and password “admin” if these details have not been customized. Click “Login” to continue.

Please note: If you forget the username and password you selected during the NF2 set-up process, holding the reset button for over 10 seconds will restart the unit with the original settings (username: admin / password: admin).

Please note: In the event that your Internet connection becomes unavailable and no fail over service has been configured, the NetComm NF2 Management console page will display when attempting to browse to an Internet site.

Figure 8: Management Console Login

Management Console

Basic Status Overview

The basic status page provides basic system related information. It can be accessed by clicking on the “Switch to Basic view” button from the top of the status page.

Figure 9: Basic View – Status

The status page shows the current primary Internet connection, WAN/LAN status, MBB connection status, current Signal Strength (dBm) and the SIM Status.

ITEM	DEFINITION
WAN Type	The current WAN type set on the NF2.
IP Address	The current WAN IP Address is listed here.
Subnet Mask	The current subnet mask of the NF2 is listed here.
Gateway	The current gateway of the NF2 is listed here
3G Status	The current status of the 3G connectivity is listed here.
3G Signal Strength	The current signal strength of the MBB (Mobile Broadband) service connection.
Number of Clients connected on Wireless 2.4GHz	The current numbers of clients connected on the NF2 via 2.4GHz
Number of clients connected on Wireless 5GHz	The current numbers of clients connected on the NF2 via 5GHz

Table 7: Basic View - Status

2.4 GHz Wireless

Figure 11: Basic View – 2.4 GHz Wireless

This page allows you to configure basic 2.4 GHz WiFi settings for this device such as enabling/disabling the 2.4 GHz WiFi functionality, changing the 2.4 GHz Wireless Network Name (SSID) or the 2.4 GHz Wireless Security key. If you make any changes to the settings, click the "Save and apply changes" button to make these changes active.

OPTION	DEFINITION
Wireless (WiFi) ON/ OFF:	Changing this option to Off will turn off the WiFi feature on the NF2 and you will not be able to connect to your NF2 wirelessly.
SSID Broadcast	Select whether the NF2 will broadcast the SSID (Network Name) for any wireless device in range to detect
SSID Broadcast Name (SSID):	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters long.
Security key:	Enter your chosen Wireless Security key here. The default WPA-PSK key is printed on the wireless security card and on the Product ID on the bottom of the NF2. Please note that whilst the key can be customized on this page, the key will revert to the default if the NF2 is reset to factory default settings.

Table 8: Basic View - 2.4 GHz Wireless Settings

5.0 GHz Wireless

Figure 10: Basic - 5.0 GHz Wireless

This page allows you to configure basic 5.0 GHz WiFi settings for this device such as enabling/disabling the 5.0 GHz WiFi functionality, changing the 5.0 GHz Wireless Network Name (SSID) or the 5.0 GHz Wireless Security key. If you make any changes to the settings, click the "Save and apply changes" button to make these changes active.

OPTION	DEFINITION
Wireless (WiFi) ON/ OFF:	Changing this option to Off will turn off the WiFi feature on the NF2 and you will not be able to connect to your NF2 wirelessly.
SSID Broadcast	Select whether the NF2 will broadcast the SSID (Network Name) for any wireless device in range to detect.
WiFi Network Name (SSID):	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters long.
Security key:	Enter your chosen Wireless Security key here. The default WPA-PSK key is printed on the wireless security card and on the Product ID on the bottom of the NF2. Please note that whilst the key can be customized on this page, the key will revert to the default if the NF2 is reset to factory default settings.

Table 9: Basic View - 5.0 GHZ Wireless Settings

Mobile Broadband

Figure 11: Basic View - Mobile Broadband

This page allows you to configure the MBB (Mobile Broadband) WAN connection settings for the NF2.

OPTION	DEFINITION
Country	Select the country that your MBB (Mobile Broadband) provider is situated in.
Service Provider	Select the MBB provider for your 3G/4G dongle and/or SIM card.
Network Name (APN)	Enter the Access Point Name (APN) of your MBB provider.
SIM Status	This field indicates whether the SIM card has been detected and is functioning correctly.
PIN	If the SIM card requires a PIN to operate enter the PIN into this field.
Confirm PIN	If the SIM card requires a PIN to operate enter the PIN into this field also.

Table 10: Basic View - Mobile Broadband Settings

WAN

Figure 12: Basic View – WAN

This page gives the user the option of selecting the WAN interface type. Options include Dynamic IP address (the default option), Static IP Address, PPPoE, PPTP, or L2TP. There is also an option to enter a Host Name with which to access the router instead of having to enter an IP address into a browser, which may be difficult to remember. You can also press the clone button to automatically detect the WAN connection's MAC address.

OPTION	DEFINITION
WAN type	The current Wide Area Network (WAN) interface type can be selected here.
Host Name	The option to set a label to the router's IP address so that it can be accessed using the host name instead of via an IP address.
ISP Registered MAC address	The WAN connection's MAC address is the MAC address that the ISP will be detecting.
Enable 3G backup	Select this option if you require a Mobile Broadband WAN connection to act as a failover for the Ethernet WAN connection. Please see the Mobile Broadband page for a description of the 3G/4G settings.

Figure 13: Basic View - WAN Settings

Advanced Features

The basic configuration interface is intended to provide access to all the settings that most people will want to use on their NetComm NF2. There are advanced settings available if desired which are accessible by viewing the advanced settings pages. Click on the "Switch to Advanced View" option to configure the advanced features of your NF2.

Status

The status page provides system related information and is displayed when you login to the NetComm NF2 management console and switch to the Advanced View. By default, the status page will show IPv4 System Status, IPv6 System Status, Wireless 2.4 GHz Status, Wireless 5.0 GHz Status and Statistics

In addition there are button to Renew DHCP Leases, View System Logs, Clients List, NAT Status and to Refresh the status page.

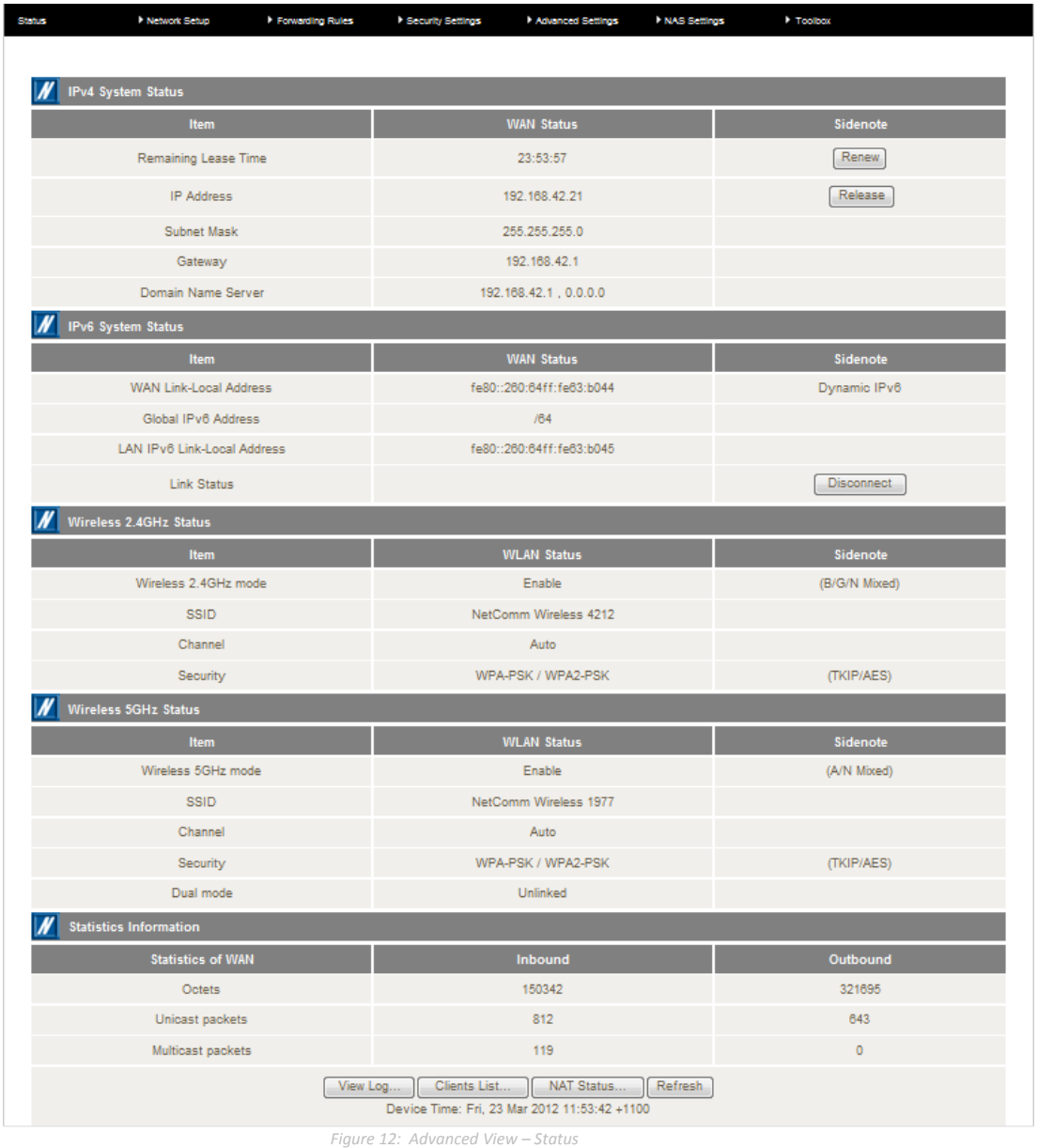


Figure 12: Advanced View – Status

Network Setup

Network Setup

Ethernet WAN

This page allows you to setup the Ethernet WAN (Wide Area Network) interface of the NF2 router. This is for an internet connection through the WAN port of the router instead of using a Mobile Broadband (MBB) WWAN connection.

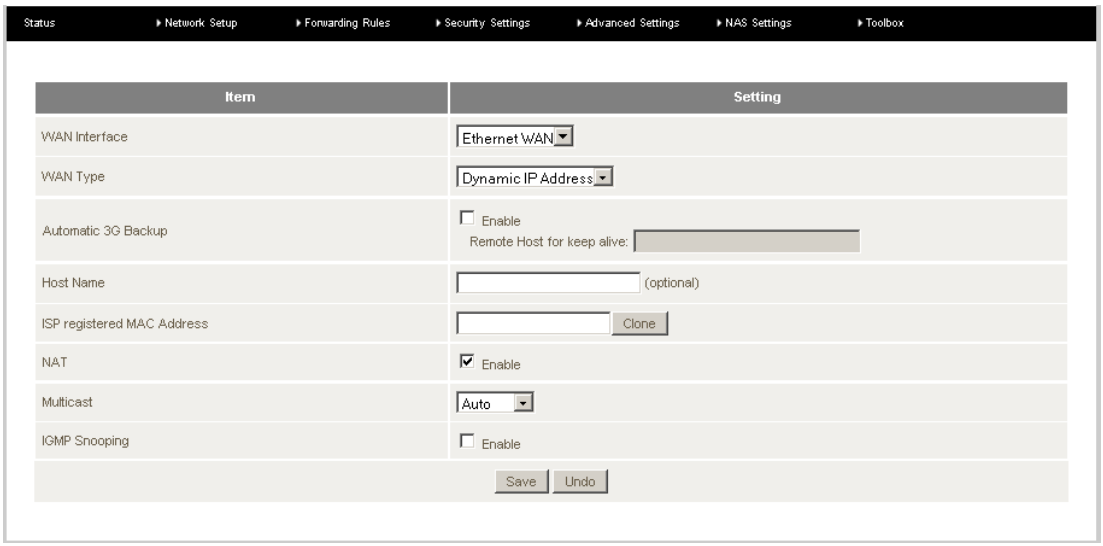


Figure 14: Advanced View – Ethernet WAN Settings

OPTION	DEFINITION
WAN Interface	Enter the WAN interface required. Options are Ethernet WAN or Wireless WAN (3G/4G Mobile Broadband).
WAN Type	Enter the WAN type of the WAN interface; Options include Dynamic IP Address (default), Static IP address, PPP over Ethernet (PPPoE), PPTP and L2TP.
Automatic 3G Backup	Select the Enable checkbox to enable automatic MBB backup of the Ethernet WAN interface. Enter an IP address or domain name into the Remote Host for Keep Alive field for the router to periodically check the status of the connection.
Host Name	This optional field can be used to create a domain name instead of using the IP address of the router to access the management console locally.
ISP Registered MAC Address	Press the clone button for the router to automatically detect the MAC address of the WAN interface.
NAT	Select this option if NAT (Network Address Translation) is required. In most cases NAT will be required. Therefore NAT is enabled by default.
Multicast	Select whether which version IGMP (Internet Group management Protocol) is required for your WAN connection. In most cases the Auto connection will suffice.
IGMP Snooping	Select whether you wish IGMP enabled on the WAN connection. IGMP snooping is the process of listening to (IGMP) network traffic. IGMP snooping, as implied by the name, allows the router to listen in on the IGMP conversation between computers and the routers. By listening to these conversations the router maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Table 11 - Advanced View – Ethernet WAN Settings

Wireless WAN

This page allows you to configure the Mobile Broadband (MBB) settings for use as the WAN interface of the router.

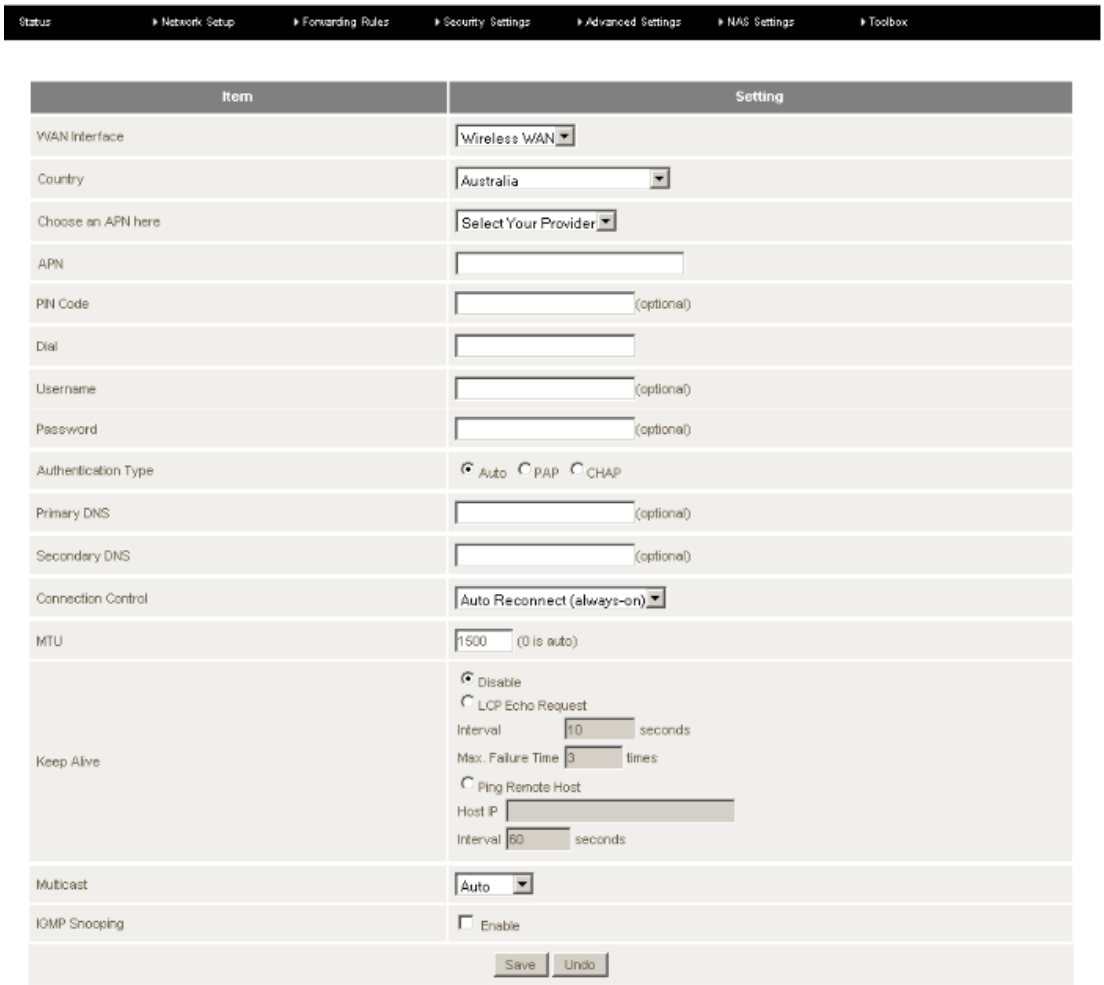


Figure 15: Advanced - Network Setup - Wireless WAN Setup

OPTION	DEFINITION
WAN Interface	Enter the WAN interface required. Options are Ethernet WAN or Wireless WAN (3G/4G Mobile Broadband).
Country	Enter the Country where the 3G/4G Internet Provider is operating. This field affected such settings as dial and ring tones, and the prefixes that need to be entered before making a call.
Choose an APN here	Enter your MBB (Mobile Broadband) provider here. Enter the Access Point Name that your MBB (Mobile Broadband) provider has recommended you use.
APN	Enter the Access Point Name that your MBB (Mobile Broadband) provider has recommended you use.
PIN Code	If your SIM card requires a PIN code, enter it in here.
Dial	The string value that needs to be dialled to make a 3G/4G connection. *99#
Authentication Type	Select the authentication type used by the MBB connection. If you are unsure what this is select the Auto option.
Primary DNS	Enter the Primary Domain Name Server address used by the MBB connection.
Secondary DNS	Enter the Secondary Domain Name Server address used by the MBB connection.
Connection Control	Select from the connection control options: Connect on Demand – Connect when a MBB WAN interface is attempting to make a connection. Auto Reconnect (always on) – Assume the MBB connection is always on and try to connect if the MBB connection is dropped. Manually – Connect the Wireless WAN interface only when a manual attempt is made.
MTU	Enter the Maximum Transmission Unit, the size of the largest packet that a network protocol can transmit.
Keep Alive	A mechanism for testing whether the MBB connection is active or not by periodically pinging a remote host.
Multicast	Select whether which version IGMP (Internet Group management Protocol) is required for your WAN connection. In most cases the Auto connection will suffice.
IGMP Snooping	Select whether you wish IGMP enabled on the WAN connection. IGMP snooping is the process of listening to (IGMP) network traffic. IGMP snooping, as implied by the name, allows the router to listen in on the IGMP conversation between computers and the routers. By listening to these conversations the router maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Table 12: Advanced - Network Setup - Wireless WAN

DHCP

DHCP is the means used so that all computers connected to the router can be assigned an IP address. This is essential before communications can start over the internet. Generally it is recommended to leave DHCP as default (enabled) unless instructed otherwise by your Internet Service Provider.

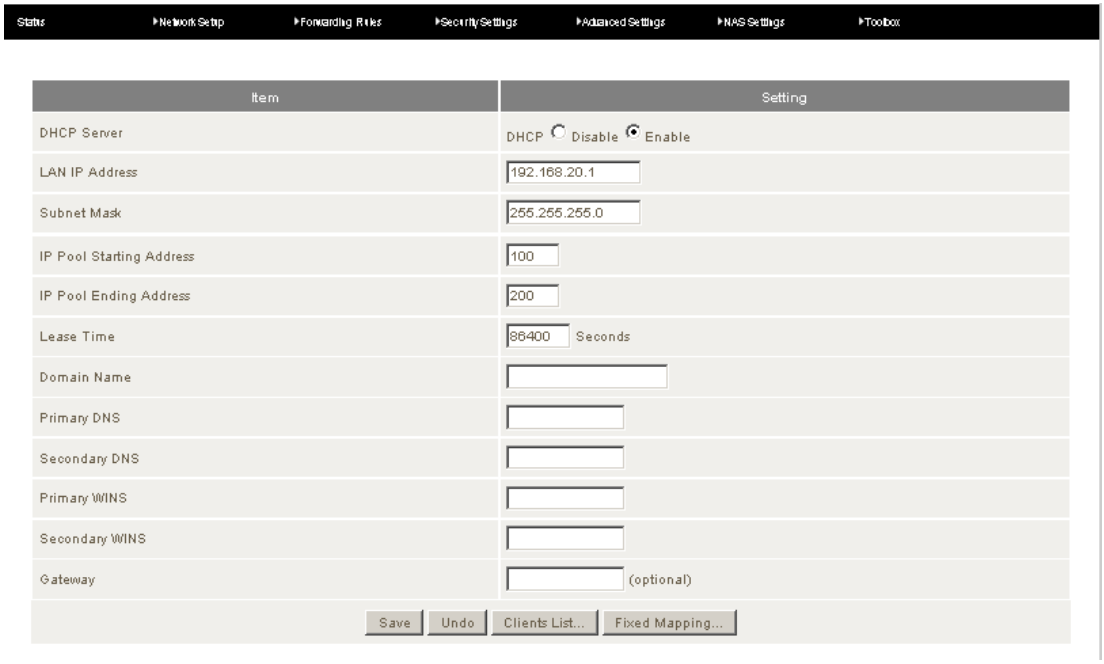


Figure 16: Advanced – DHCP

OPTION	DEFINITION
DHCP Server	The option to disable or enable the DHCP function.
LAN IP Address	The LAN IP address of the DHCP server/router.
Subnet Mask	The subnet mask used by the DHCP server.
IP Pool Starting Address	The stating IP address for the DHCP pool, in the above example is 192.168.20.100
IP Pool Ending Address	The ending IP address for the DHCP pool, in the above example is 192.168.20.200
Lease Time	The time in seconds that an IP address is leased for
Domain Name	The domain of the DHCP server.
Primary DNS	Enter the Primary Domain Name Server address used by the DHCP server.
Secondary DNS	Enter the Secondary Domain Name Server address used by the DHCP server.
Primary WINS	Enter the Primary WINS (Windows Internet Name Server) address used by the DHCP server.
Secondary WINS	Enter the Secondary WINS (Windows Internet Name Server) address used by the DHCP server.

Table 13: Advanced - DHCP Settings

Wireless 2.4 GHz

This page allows the user to configure the 2.4 GHz wireless settings on the NetComm NF2 including the wireless security types, wireless encryption, WDS (Wireless Distributed System) settings and WPS (Wireless Protected Setup) setup.

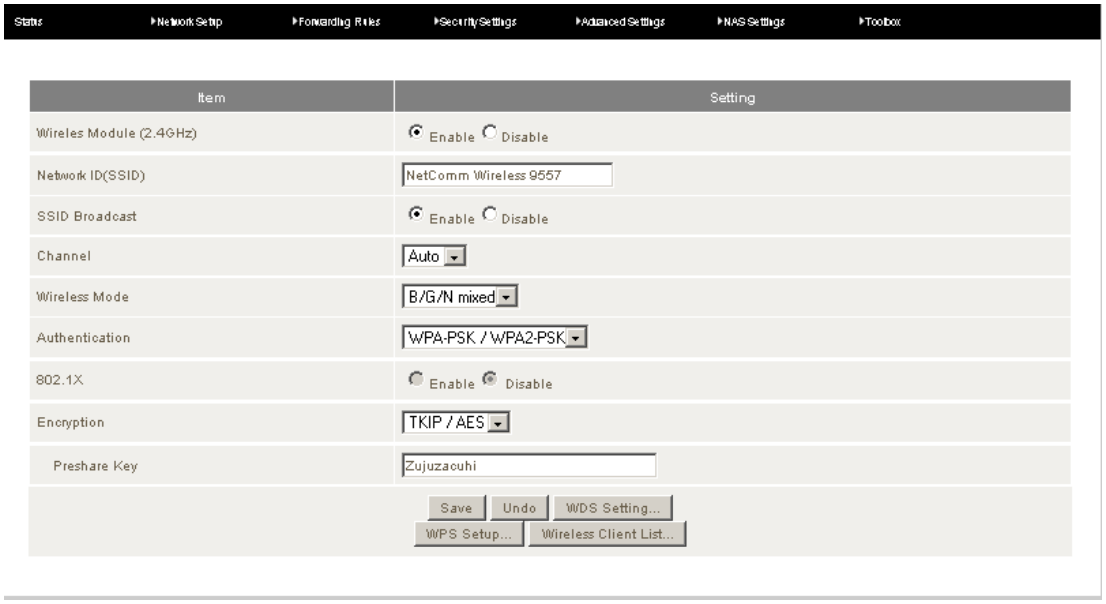


Figure 17: Advanced - Wireless 2.4 GHz

OPTION	DEFINITION
Wireless Module (2.4GHz)	The option to disable or enable the wireless 2.4 GHz function.
Network ID (SSID)	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters in length. It is recommended that the default SSID be changed for added security.
SSID Broadcast	Enabled by default, this field enables or disables the SSID broadcast, deciding whether the SSID will be hidden to all wireless clients, requiring a manual configuration to connect to the network or whether the SSID can be detected by wireless clients.
Channel	The wireless frequency used by the 2.4 GHz connection. Recommended channels to use include 1, 6 and 11.
Wireless Mode: There are 6 modes to select from:	
802.11b/g mixed mode:	Both 802.11b and 802.11g wireless devices can connect to the NetComm NF2.
802.11b only:	Select this if all of your wireless clients use 802.11b wireless protocol.
802.11g only:	Select this if all of your wireless clients are 802.11g wireless protocol.
802.11n only:	Select this if all of your wireless clients are 802.11n wireless protocol.
802.11g/n Mixed mode:	Select this if 802.11g and 802.11n wireless devices access your network.
802.11/b/g/n Mixed mode:	Select this if 802.11b and 802.11g and 802.11n wireless devices access your network.
Authentication	This field allows you to select the authentication type of the wireless security for the 2.4 GHz wireless network connection.
802.1x	This field gives the option to enable or disable the 802.1x authentication protocol.
Encryption	With this field the encryption that the wireless security will use on the 2.4 GHz wireless network can be selected.
Preshare Key	The wireless security password for the 2.4 GHz wireless network connection.

Table 14: Advanced Wireless 2.4 GHz Settings

WDS Settings

WDS (Wireless Distribution System) is a system that enables the wireless interconnection of access points, and allows a wireless network to be expanded using multiple access points without using a wired backbone to link them. To successfully link each WDS Access Point needs to be set with the same channel, SSID, encryption type and encryption key.

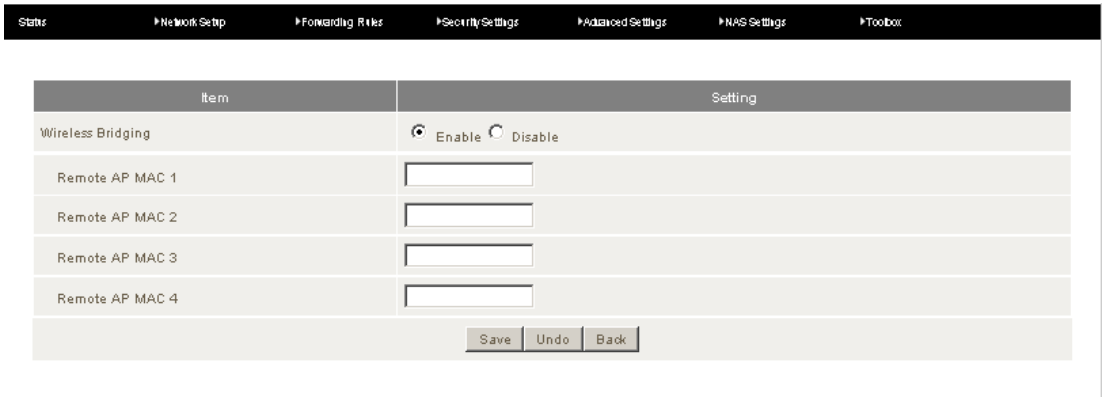


Figure 18: Advanced –WDS

Enter the MAC address of each Remote Access Point and press the Save button.

WPS Setup

WiFi Protected Setup is a computer standard that offers a quick and easy alternative to setting up a wireless network. WPS can be configured using a push button method or by using a PIN code.

Figure 19: Advanced - WPS Setup

OPTION	DEFINITION
WPS	Enable or disable WPS with this field.
AP PIN	Set the Access Point PIN by pressing the Generate New PIN button.
Config Mode	Select from being an enrolee or registrar. In most cases the router will be the registrar.
Config Status	This field gives the current WPS status. Press either the Release button to release a configured WPS setting or the Set button to configure the current WPS settings
Config Method	Select whether WPS should use Push button or PIN Code mode for its configuration.
WPS Status	This field advises the current WPS status.

Table 15: Advanced - WPS Setup settings

Wireless 5.0 GHz

This page allows the user to configure the 5.0 GHz wireless settings on the NetComm NF2 including the wireless security types, wireless encryption, WDS (Wireless Distributed System) settings and WPS (Wireless Protected Setup) setup.

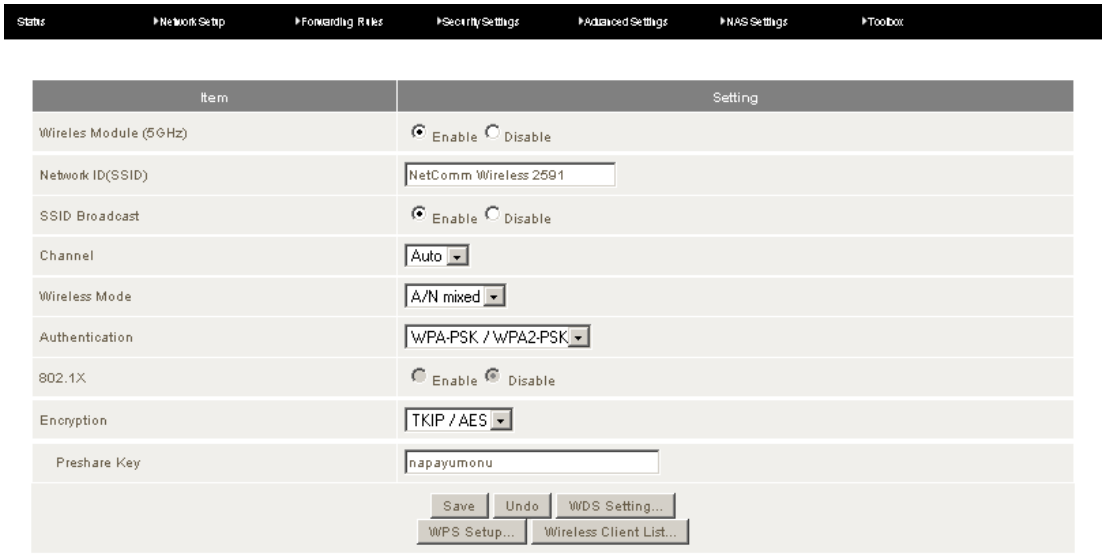


Figure 20: Advanced - 5.0 GHz Wireless

OPTION	DEFINITION
Wireless Module (5.0GHz)	The option to disable or enable the wireless 5.0 GHz function.
Network ID (SSID)	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters in length. It is recommended that the default SSID be changed for added security.
SSID Broadcast	Enabled by default, this field enables or disables the SSID broadcast, deciding whether the SSID will be hidden to all wireless clients, requiring a manual configuration to connect to the network or whether the SSID can be detected by wireless clients.
Channel	The wireless frequency used by the 5.0 GHz connection. Recommended channels to use include 1, 6 and 11.
Wireless Mode: There are 6 modes to select from:	
802.11b/g mixed mode:	Both 802.11b and 802.11g wireless devices can connect to the NetComm NF2.
802.11b only:	Select this if all of your wireless clients use 802.11b wireless protocol.
802.11g only:	Select this if all of your wireless clients are 802.11g wireless protocol.
802.11n only:	Select this if all of your wireless clients are 802.11n wireless protocol.
802.11g/n Mixed mode:	Select this if 802.11g and 802.11n wireless devices access your network.
802.11/b/g/n Mixed mode:	Select this if 802.11b and 802.11g and 802.11n wireless devices access your network.
Authentication	This field allows you to select the authentication type of the wireless security for the 5.0 GHz wireless network connection.
802.1x	This field gives the option to enable or disable the 802.1x authentication protocol.
Encryption	With this field the encryption that the wireless security will use on the 5.0 GHz wireless network can be selected.
Preshare Key	The wireless security password for the 5.0 GHz wireless network connection.

Table 16: Advanced - Network Setup - 5.0 GHz Wireless Settings

VPN – IPSec

This page allows the NetComm NF2 to act as a VPN IPSec endpoint. Internet Protocol Security (IPsec) is used to secure IP (Internet Protocol) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

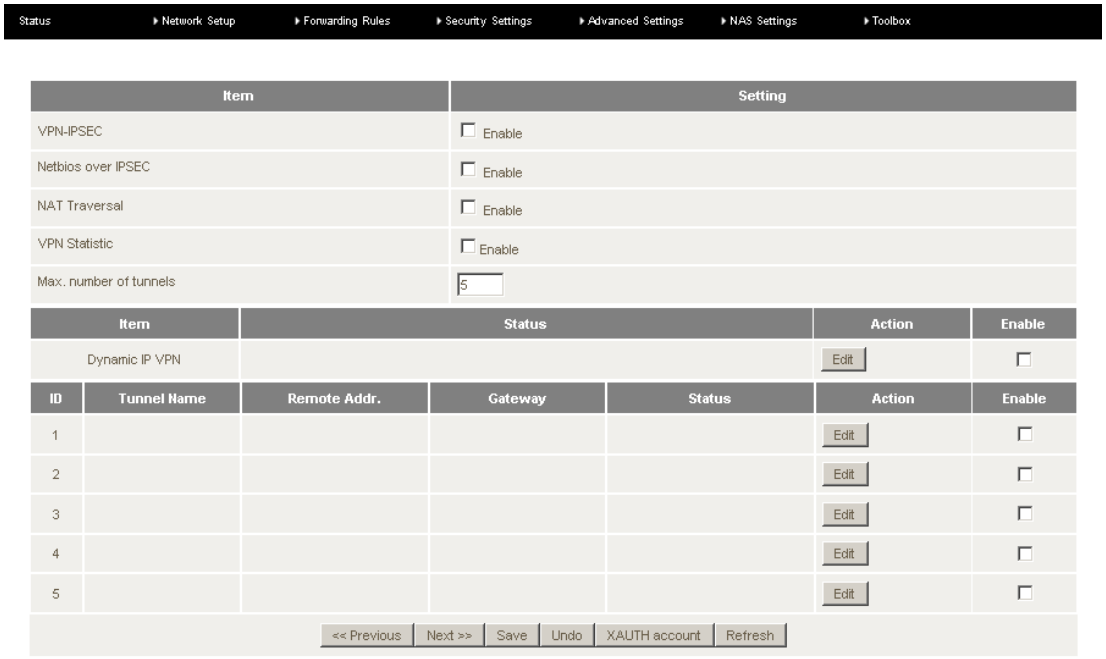


Figure 21: Advanced - Network Setup - IPSec

OPTION	DEFINITION
VPN-IPSEC	Select this checkbox to enable the router as a VPN-IPSec endpoint.
Netbios over IPSEC	Select this checkbox to enable Netbios over IPSEC.
NAT Traversal	Select this option to enable NAT Traversal of the IPSec connection.
VPN Statistic	Select this field to enable VPN statistics – including the VPN tunnel name, elapsed time of the VPN tunnel, incoming and outgoing packets.
Max. Number of Tunnels	Enter the maximum number of VPN tunnels that can be created at any one time.
Dynamic VPN	This field will create a VPN tunnel using dynamic IP addresses.

Table 17: Advanced - Network Setup -VPN-IPSec

VPN – IPSec Tunnel Setup

This page allows you to configure a VPN endpoint IPSec.

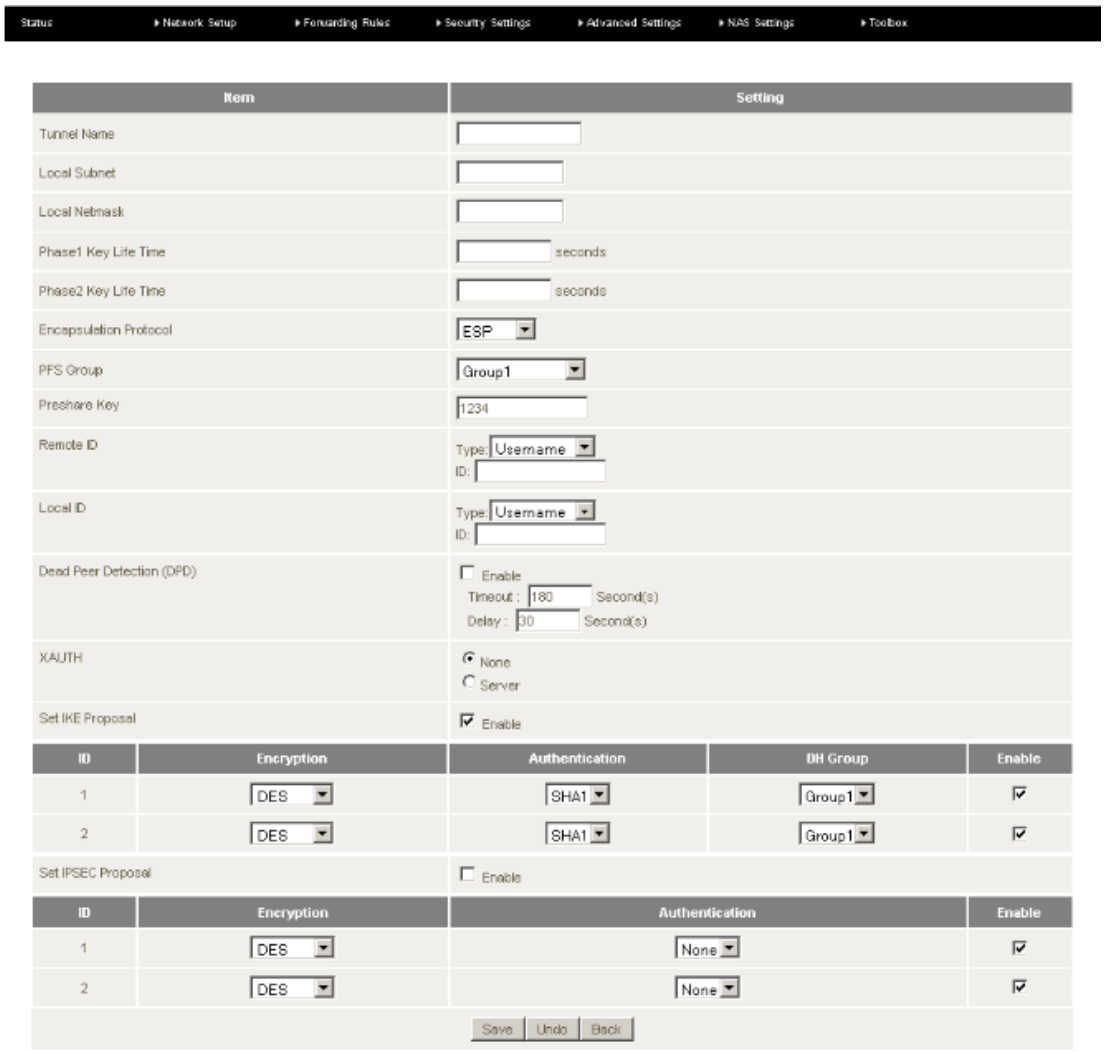


Figure 22: Advanced - Network Setup - Dynamic IPSec

OPTION	DEFINITION
Tunnel Name	Enter the VPN tunnel name.
Local Subnet	Enter the Local Subnet address.
Local Network	Enter the Local Network address.
Phase 1 Key Life Time	Enter the Phase 1 Key Life Time in seconds.
Phase 2 Key Life Time	Enter the time in seconds for the Phase 2 Key Life Time.
Encapsulation Protocol	Enter the encapsulation protocol for the VPN tunnel. Options are ESP (Encapsulated Security Payload), AH (Authentication Header) or ESP + AH.
PFS Group	Select the PFS (Perfect Forward secrecy) Group to be used.
Remote ID	Enter the remote ID and select the Remote ID type. Options include Username, FQDN (Fully Qualified Domain Name), User@FQDN or Key ID.
Local ID	Enter the local ID and select the local ID type. Options include Username, FQDN (Fully Qualified Domain Name), User@FQDN or Key ID
Dead Peer Detection (DPD)	Select to enable Dead Peer Detection, a means of detecting a dead IKE (Internet Key Exchange) peer. Set the timeout and delay in seconds.
Set IKE Proposal	Select to Enable IKE (Internet Key Exchange) Proposals.

Table 18: Advanced - Network Setup - VPN IPSec - Dynamic IPSec

VPN-L2TP

This page allows you to configure a Layer 2 Tunnelling protocol. It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide privacy.

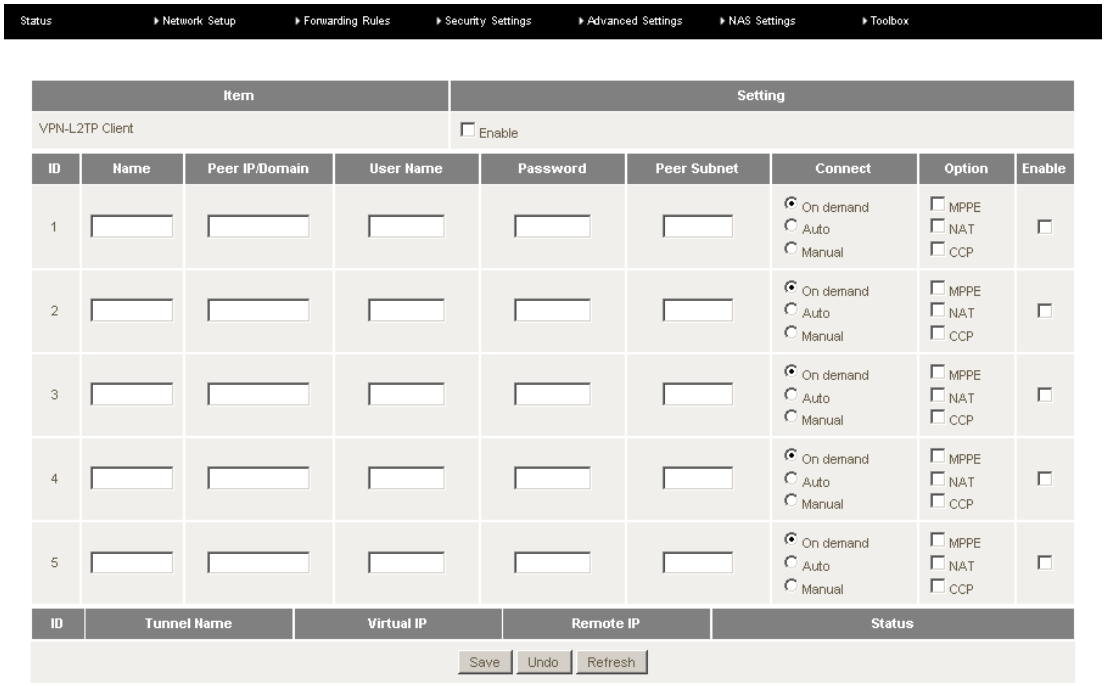


Figure 23: Advanced - Network Setup - L2TP

VPN-PPTP Client

The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

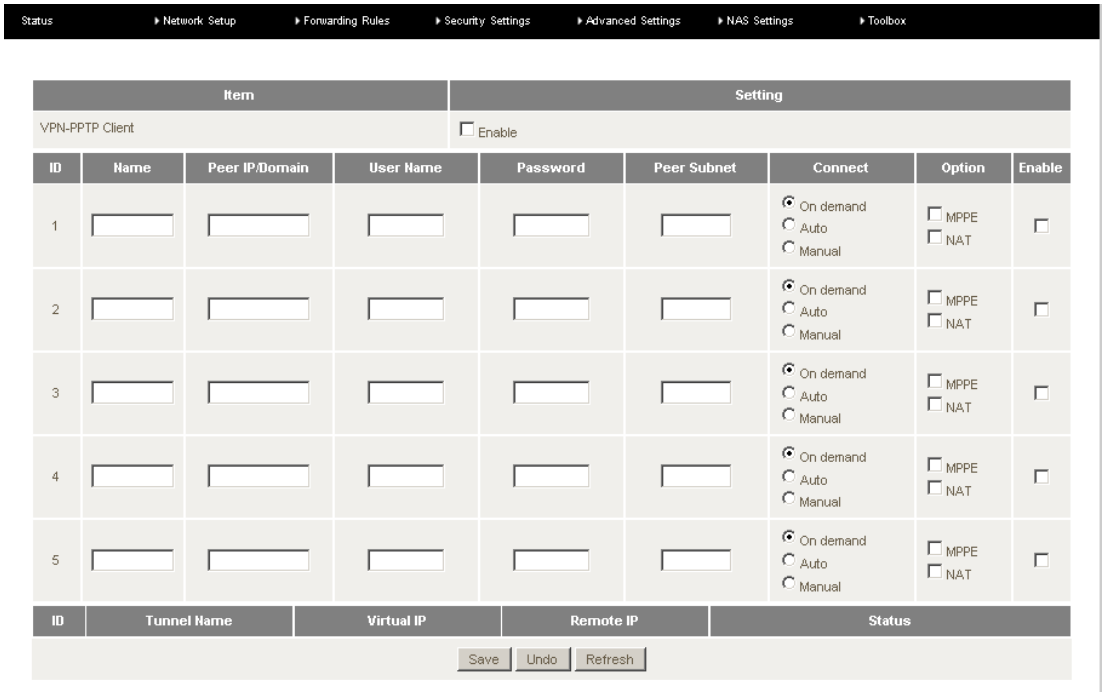


Figure 24: Advanced - Network Setup - PPTP Client

VPN – PPTP Server

This page allows the NetComm NF2 to become a PPTP VPN endpoint.

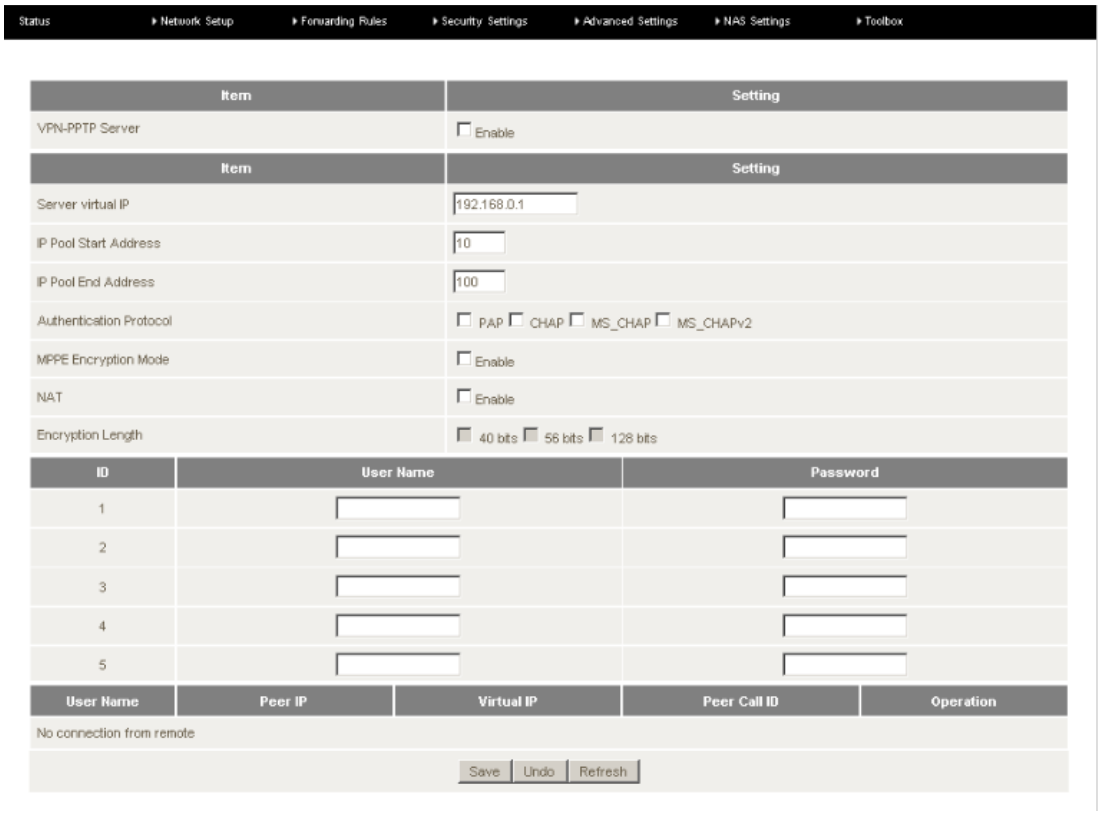


Figure 25: Advanced - Network Setup - VPN - PPTP Server

OPTION	DEFINITION
VPN-PPTP Server	Select this option to enable the VPN-PPTP Server function.
Server Virtual IP	Enter the IP address of the PPTP server.
IP Pool Start Address	The starting IP address for the DHCP pool, in the above example is 192.168.0.10.
IP Pool End Address	The ending IP address for the DHCP pool, in the above example is 192.168.0.100
Authentication Protocol	Select the authentication protocol you wish to use.
MPPE Encryption Mode	Select to enable MPPE Encryption Mode (Microsoft Point-to-Point Encryption).
NAT	Select to enable NAT on the PPTP server.
Encryption length	Enter encryption length for the packets sent through the VPN tunnel.

Table 19: Advanced - Network Setup - VPN - PPTP Server Settings

Change Password

This page allows you to change the administrator username and password to secure the NetComm NF2 management console against unauthorised access.

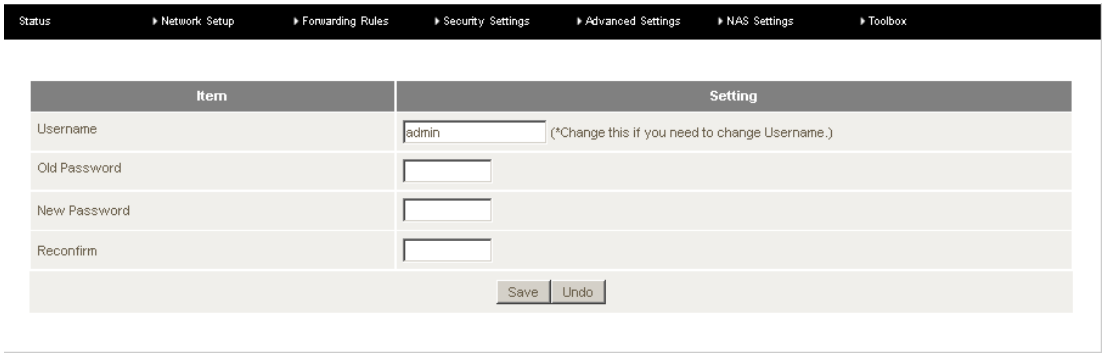


Figure 26: Advanced - Network Setup - Change Password

Forwarding Rules

The forwarding rules section deals with NAT traversal. Using the Virtual Server settings port forwarding can be configured. Special AP settings can be used to configure port triggering. In the Miscellaneous section a DMZ host can be configured and UPnP can be enabled or disabled.

Virtual Server

The Virtual Server page allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 20 entries can be configured. In addition a series of pre-configured commonly used ports can be selected for easy setup.

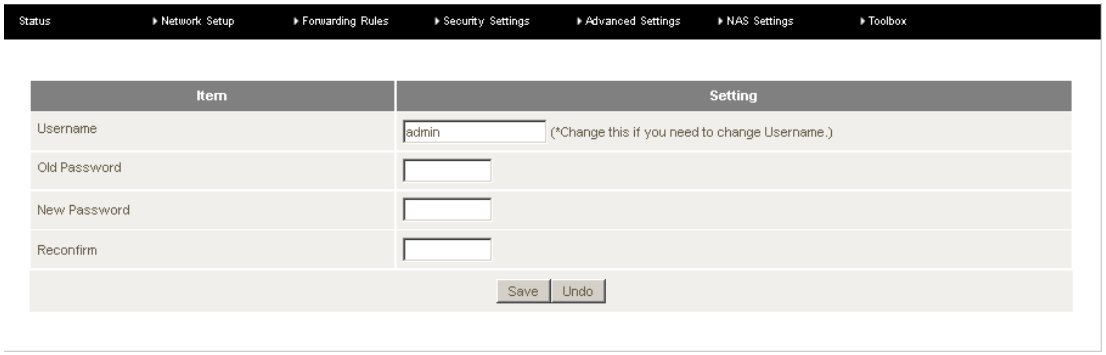


Figure 27: Advanced - Forwarding Rules - Virtual Server

OPTION	DEFINITION
Service Ports	Enter the port number or port range to be used with the Server IP address. For a port range entry use the format shown in the following example (81-90).
Server IP	Enter the local IP address of the device you wish to port forward to.
Enable	Select this option to enable the port forwarding rule.
Use Rule	Select when the port forwarding rule should be used. The default option is Always.

Table 20: Advanced - Forwarding Rules - Virtual Server Settings

Special AP

The Special AP page allows the router to be configured for port triggering. Port triggering allows a client device connected to the router to dynamically and automatically forward a specific port back to itself. Port triggering opens an incoming port when your computer is using a specified outgoing port for specific traffic. A selection of common port triggering settings come preconfigured on the NF2 for easy setup.

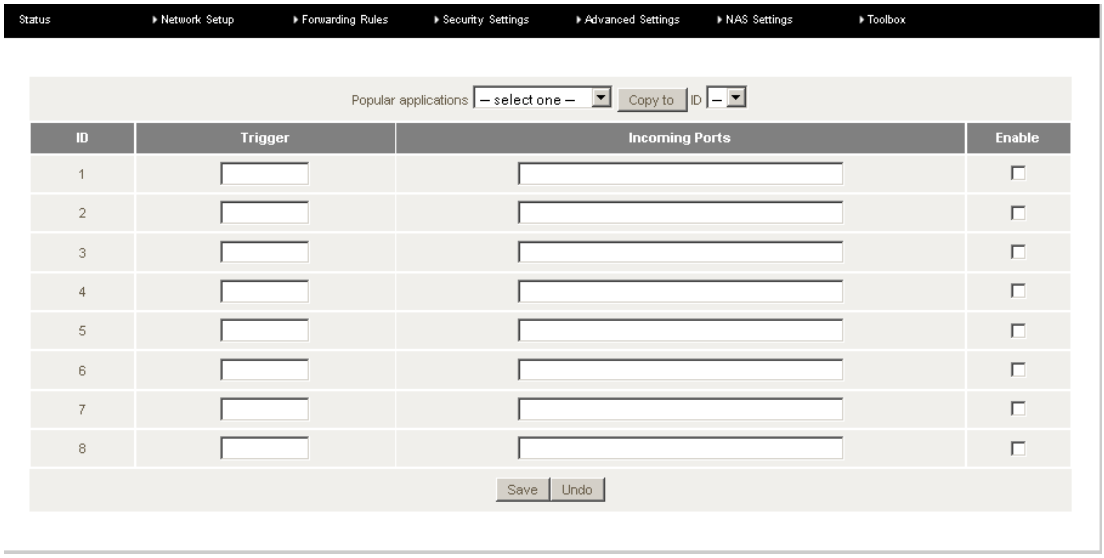


Figure 28: Advanced - Forwarding Rules - Port Triggering

OPTION	DEFINITION
Trigger	Enter the outgoing trigger port be opened by a device connected to the router.
Incoming Ports	Enter the incoming port number or port ranges. For a port range use a dash (-) between the lower and upper range numbers; e.g. 5000-6000. Use a comma between multiple numbers.
Enable	Select this option to enable or disable the port triggering rule.

Table 21: Advanced - Forwarding Rules - Port Triggering Settings

Miscellaneous

The miscellaneous page gives the user the option of enabling or disabling UPnP protocol or the option to assign a device connected to the router as a DMZ host. A DMZ host is a host on the internal network that has all ports exposed to a WAN connection, except those ports otherwise forwarded.

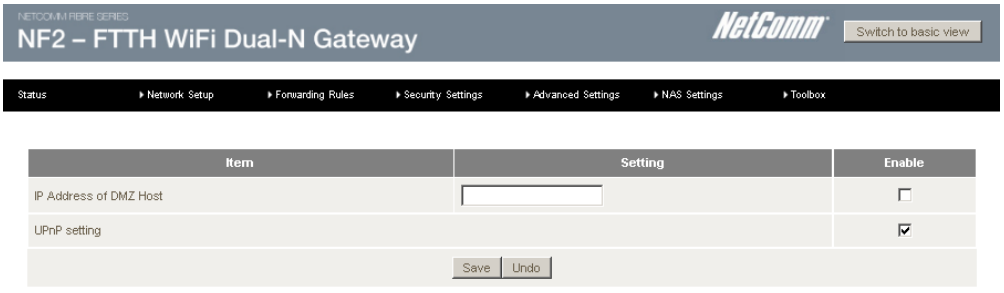


Figure 29: Advanced - Forwarding Rules - Miscellaneous

Security Settings

The security settings menu has such configuration options for the NetComm NF2 as Packet Filtering, MAC Filtering, Domain Filtering, URL Blocking, MAC Control and Remote Administration settings.

Status

The Security Settings Status page provides an overview of the current IP filter, MAC filter and domain filter rules in place on the NF2.

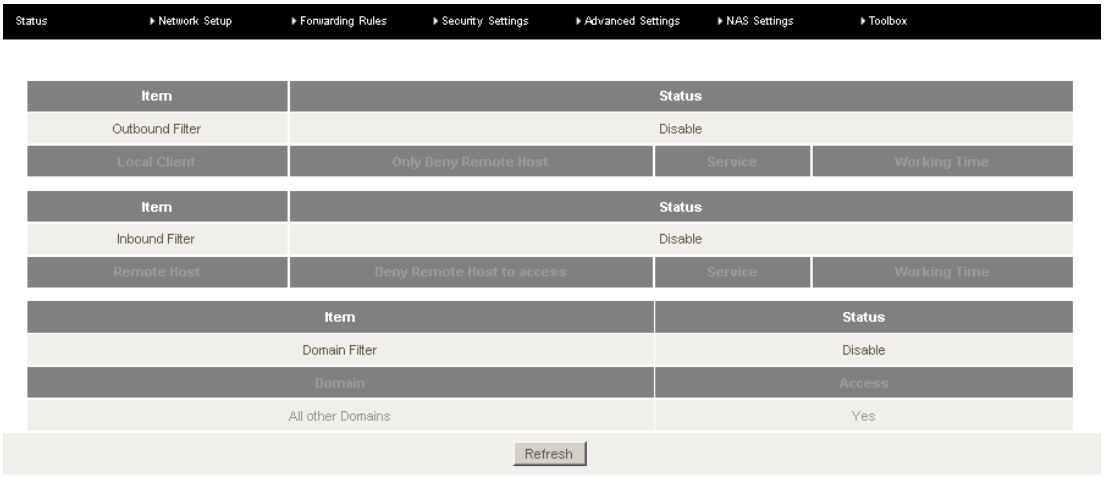


Figure 30: Advanced - Security Settings – Status

Packet Filtering

The inbound and outbound packet filtering function gives the network administrator the option of denying or allowing data packets to be transmitted through to the WAN interface when any of the specified rules are met. Conversely any other data packets not matching these rules will be denied or allowed access through the network as specified by the network administrator.

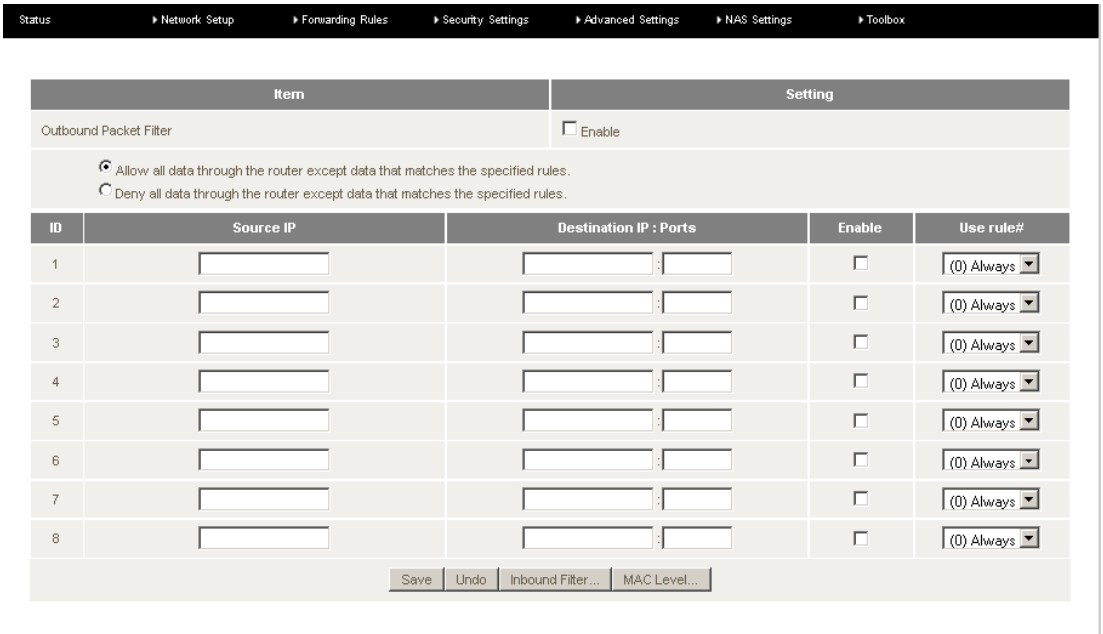


Figure 31: Advanced - Security Settings - Packet Filtering

OPTION	DEFINITION
Source IP	Enter the local source IP address where the packet originates from for an outgoing packet filter rule or is being sent to for an incoming packet filter rule.
Destination IP: Ports	Enter the WAN IP address and port number or range where the packet is directed to or from..
Enable	Select this option to make the packet filter rule active.
Use Rule#	Select when the rule is to be used. The default value is Always.

Table 22: Advanced - Security Settings - Packet Filtering Settings

MAC Control

The MAC filter function can be used to restrict access to the NF2 for both wired and wireless clients. Using Connection Control wired and wireless clients can connect to the router and either allow or deny any unspecified MAC addresses connection access. Using association control wireless clients can associate to the wireless LAN. All other unspecified wireless clients can be allowed or denied association rights.

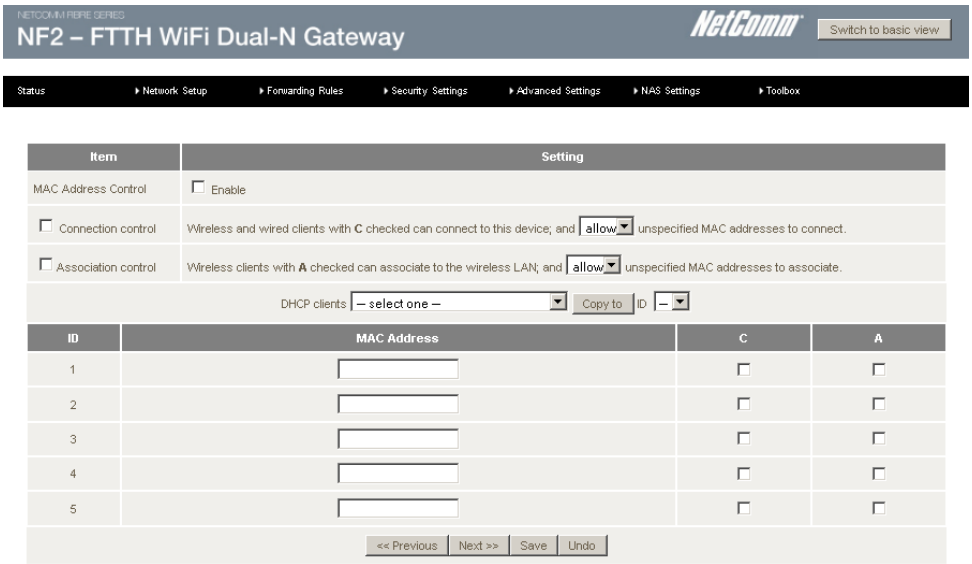


Figure 32: Advanced - Security Settings - MAC Filtering

Domain Filter

Domain Filtering can be used to monitor and or deny access to specified domain names.

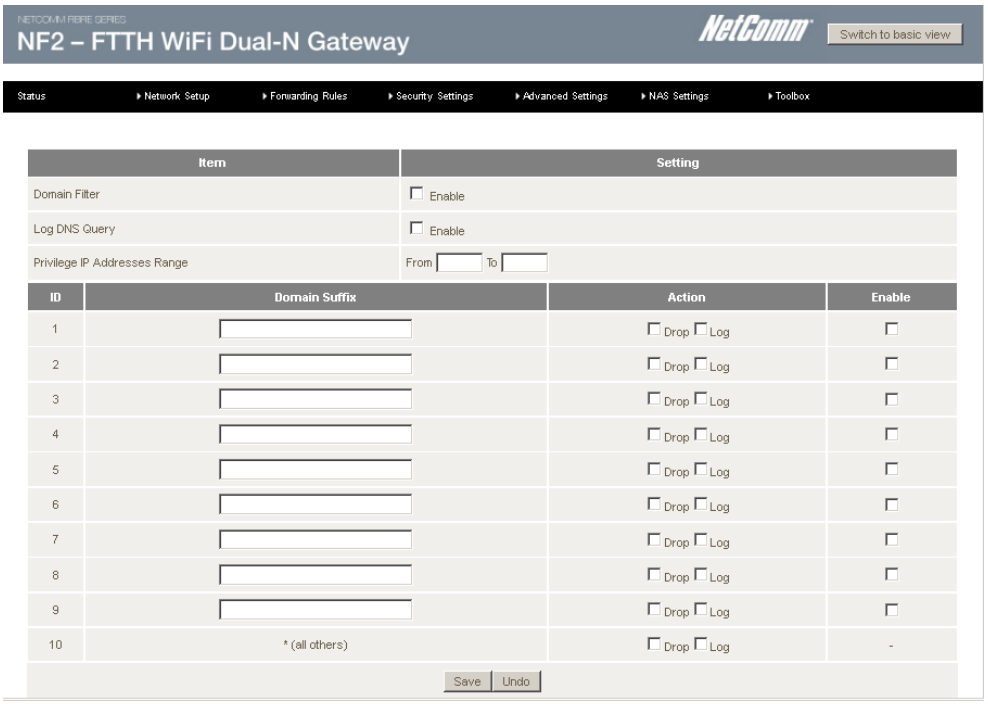


Figure 33: Advanced - Security Settings - Domain Filter

OPTION	DEFINITION
Domain Filter	Select this option to enable Domain Filtering
Log DNS Query	Select this option to log DNS Queries for all specified domain names.
Privilege IP Addresses Range	Enter the range of IP addresses that will not be filtered.
Domain Suffix	Enter the domain name you wish to deny or have log.
Drop	Select drop if you wish to deny access to the specified domain name
Log	Select Log if you wish to log any attempts to access the specified domain name.
Enable	Select this option to enable the domain filter rule.

Table 23: Advanced - Security Settings - Domain Filtering Settings:

URL Blocking

The URL blocking function can deny access to specified URL addresses.

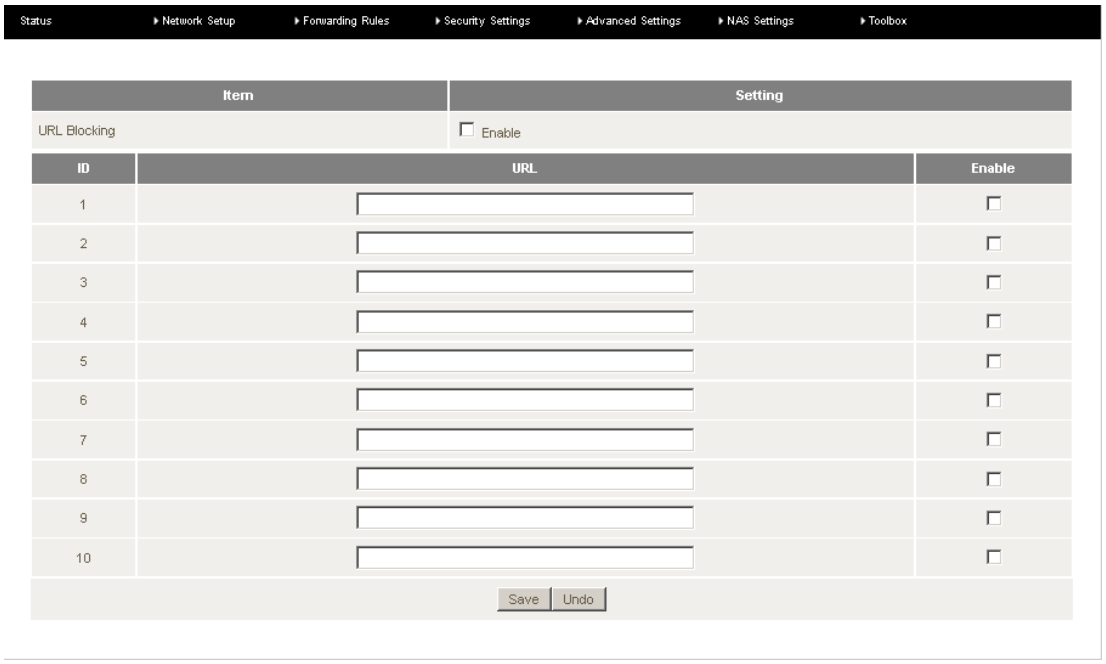


Figure 34: Advanced - Security Settings - URL Blocking

Miscellaneous

The Security Settings Miscellaneous section provides access to remote administration settings, administrator time out and DoS (Denial of Service) Attack Detection amongst other things.

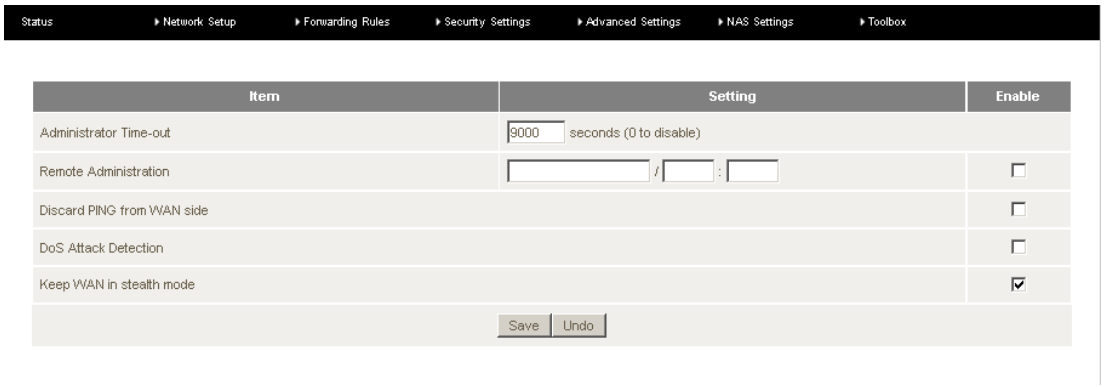


Figure 35: Advanced - Security Settings - Miscellaneous

Advanced Settings

The Advanced Settings menu has System log, Dynamic DNS, QoS (Quality of Service), SNMP (Simple Network Management Protocol), Routing, System Time, Scheduling, IPv6, TR-069 and VLAN options.

Status

The status page shows the current status of the Advanced Settings on the NF2.

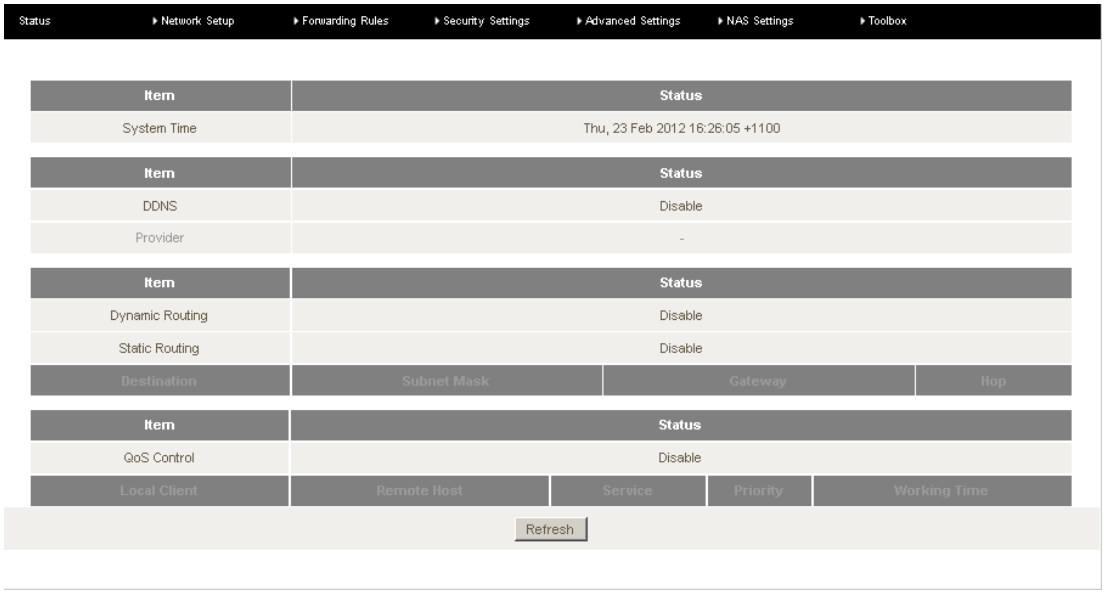


Figure 36: Advanced - Advanced Settings – Status

System Log

As well as viewing the system log entries locally the System Log page allows a network administrator to configure the router's system log to be sent to a remote system log server or to be emailed to nominated email addresses of the administrator's choice.

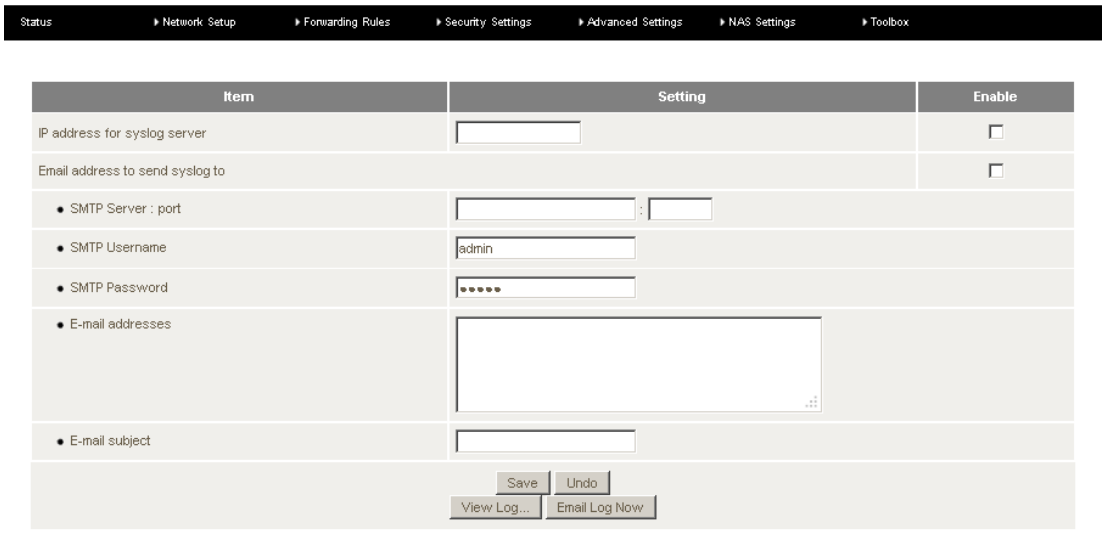


Figure 37: Advanced - Advanced Settings - System Log

OPTION	DEFINITION
IP Address for Syslog Server	For sending the system log information to a remote server, enter the IP address of your System Log server.
Email Address to Send Syslog to	If you would like to send the system log details via email select this option and enter the appropriate details.
SMTP Server: port	Enter the name of the outgoing mail server to use in sending out the system log server.
SMTP Username	If a username is required for the outgoing mail server, enter it into this field.
SMTP Password	If a password is required for the outgoing mail server, enter it into this field.
Email Addressees	Enter the email addresses of where you wish the system log details to be sent to.
Email Subject	Enter a Subject for the System Log Email.
View Log	View the System Log entries locally.
Email Log Now	If the email settings are correct the emails containing the system log will be sent on pressing this button.

Table 24: Advanced - Advanced Settings - System Log Settings

Dynamic DNS

Dynamic DNS or DDNS is used for the updating in real time of Domain Name System (DNS) name servers to keep the active DNS configuration of their hostnames, addresses and other information up to date. To use these settings you will need a dynamic DNS account with Dyndns.org, No-IP.com, TZO.com or dhs.org.

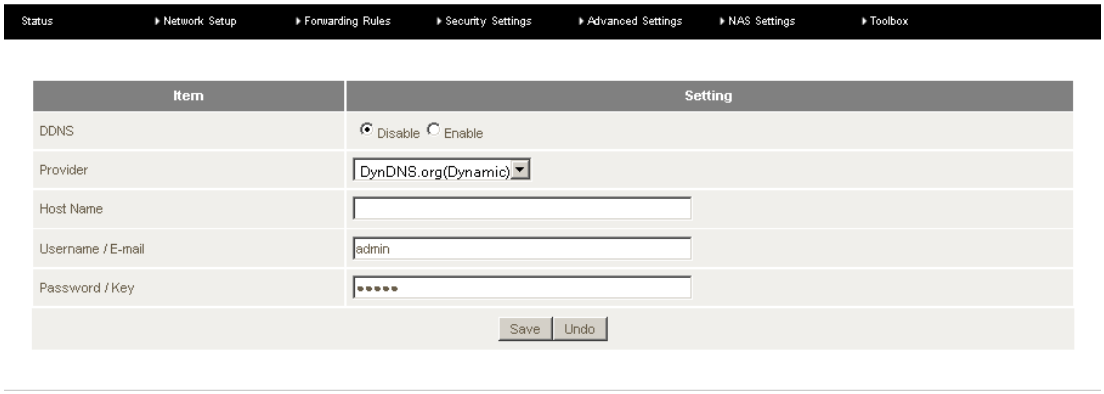


Figure 38: Advanced - Advanced Settings - Dynamic DNS

OPTION	DEFINITION
DDNS	The option to disable or enable the DHCP function.
Provider	Select your dynamic DNS provider.
Host Name	Enter the hostname / host domain name / host address.
Username / Email	Enter the dynamic DNS account username.
Password / Key	Enter the dynamic DNS account password.

Table 25: Advanced - Advanced Settings - Dynamic DNS Settings

QoS (Quality of Service)

Quality of Service (QoS) refers to resource reservation control mechanisms with the ability to provide a different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required packet transfer rate or delay may be guaranteed.

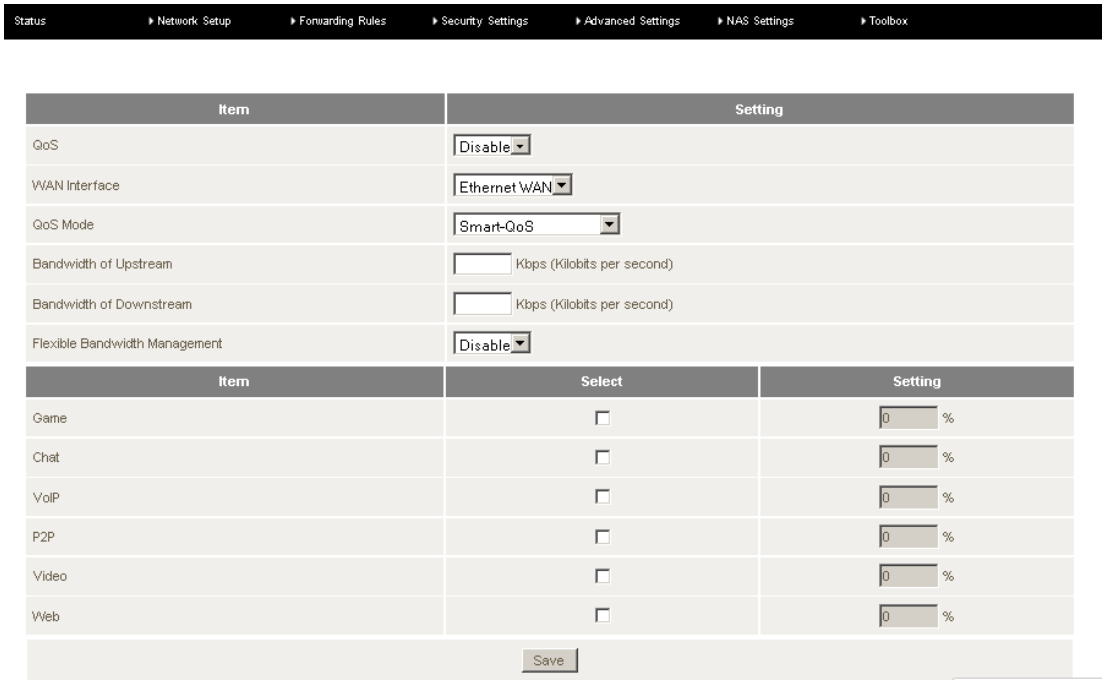


Figure 39: Advanced - Advanced Settings - QoS

OPTION	DEFINITION
QoS	Select the Enable option to enable Quality of Service (QoS).
WAN Interface	Select the WAN interface you wish to configure QoS for.
QoS Mode	Select the QoS Mode to use.
Bandwidth of Upstream	Set the Upstream limit in Kilobits per second (Kbps).
Bandwidth of Downstream	Set the Downstream limit in Kilobits per second (Kbps).
Flexible Bandwidth Management	Select this option to Enable to allow the router to assign the QoS percentage rates or set this option to disable and manually enter the QoS percentage rates for the Item fields.

Table 26: Advanced - Advanced Settings - QoS Settings

SNMP

SNMP, short for Simple Network Management Protocol is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

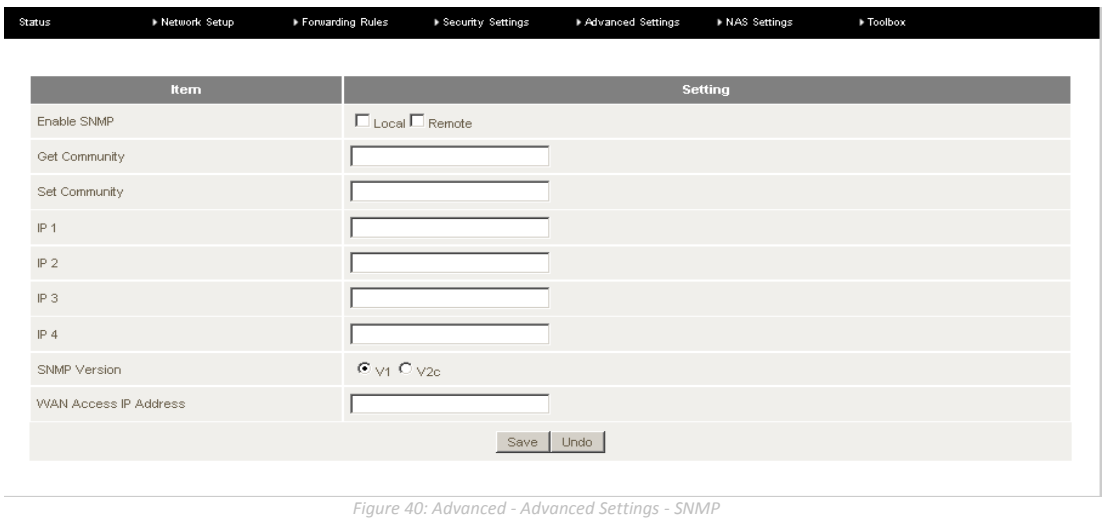


Figure 40: Advanced - Advanced Settings - SNMP

OPTION	DEFINITION
Enable SNMP	The option to disable or enable the SNMP function.
Get Community	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The Get Community field gets the current community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are: Write – private; Read – public.
Set Community	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The Set Community field sets the new community name used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are: Write – private; Read – public.
IP 1	Enter the IP address for one of the local clients connected to router. SNMP will then gather and transmit the network information that you specified.
IP 2	Enter the IP address for the second of the local clients connected to router. SNMP will then gather and transmit the network information specified.
IP 3	Enter the IP address for the third of the local clients connected to router. SNMP will then gather and transmit the network information specified.
IP 4	Enter the IP address for the fourth of the local clients connected to router. SNMP will then gather and transmit the network information specified.
SNMP Version	Select the version SNMP you wish to use with the NF2.
WAN Access IP Address	Enter the WAN Access IP Address used to provide (WAN) Wide Area Network connectivity to the internet.

Table 27: Advanced - Advanced Settings - SNMP Settings

Routing

The Routing page in the Advanced Settings section of the NF2 provides a network administrator with the means to configure the routing method that the NF2 will use, either dynamic routing or static routing. Routes are called static if they do not change over time. Thus a static routing table is loaded with values when the system starts and the routes do not change unless an error is detected. Conversely, dynamic routing refers to a system that can change its routing table information over time. With dynamic routing, software known as RIP (Routing Information Protocol) interacts with network devices and learns the optimal route to each location. Then RIP updates the local routing table to ensure datagrams follow the optimal routes.

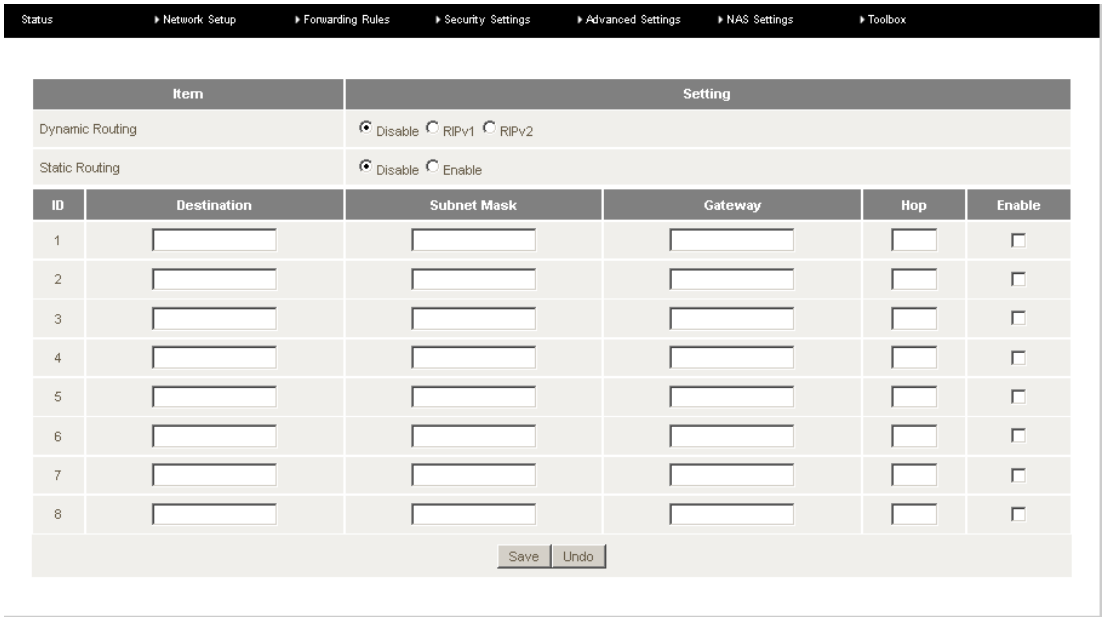


Figure 41: Advanced - Advanced - Settings - Routing

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

Please note: Only select RIPv2 if you have a different subnet in your network. Otherwise, please 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 clicking the Enable checkbox.

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

System Time

The NF2 router time can be synchronised either to a local PC or using NTP (Network Time Protocol) settings to a standard global internet time. These settings will affect functions such as System Log statistics, scheduling and Firewall settings

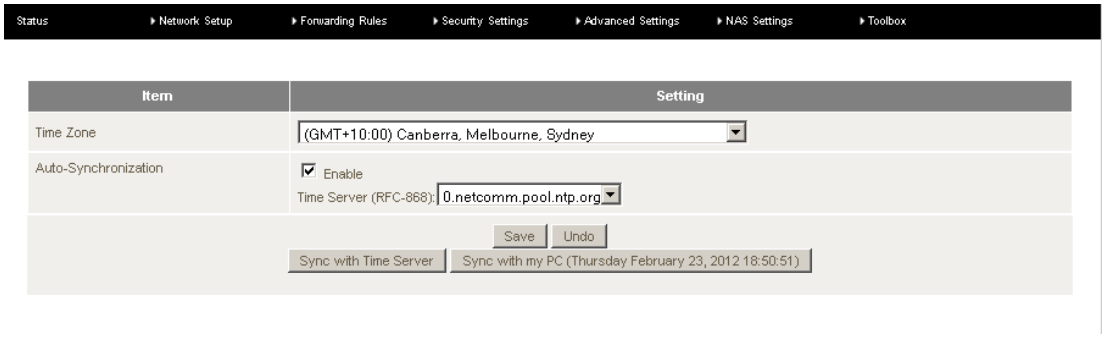


Figure 42: Advanced - Advanced Settings -System Time

OPTION	DEFINITION
Time Zone	Select the GMT offset for your location.
Auto-Synchronization	Select an NTP (Network Time Protocol) time server to synchronise to the global internet time with.
Sync with Time Server	Select this button to initiate the router time synchronisation to the specified network time server above.
Sync with my PC	Select this button to initiate the router time synchronization to the computer you are currently logged into the router with.

Table 28: Advanced - Advanced Settings - System Time

Scheduling

The NF2 has built in scheduling, allowing the router to be switched on or off. This offers a means of parental control. To create a schedule, ensure the enable Schedule option is selected and press the Add New button.

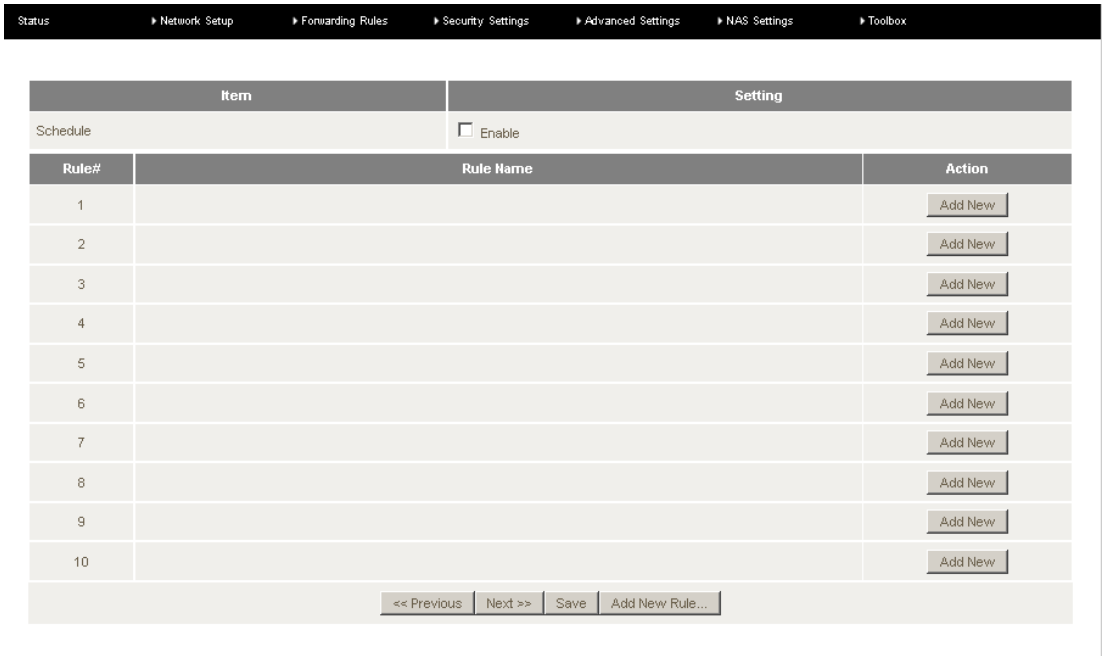


Figure 43: Advanced - Advanced Settings – Schedule

Adding a Schedule

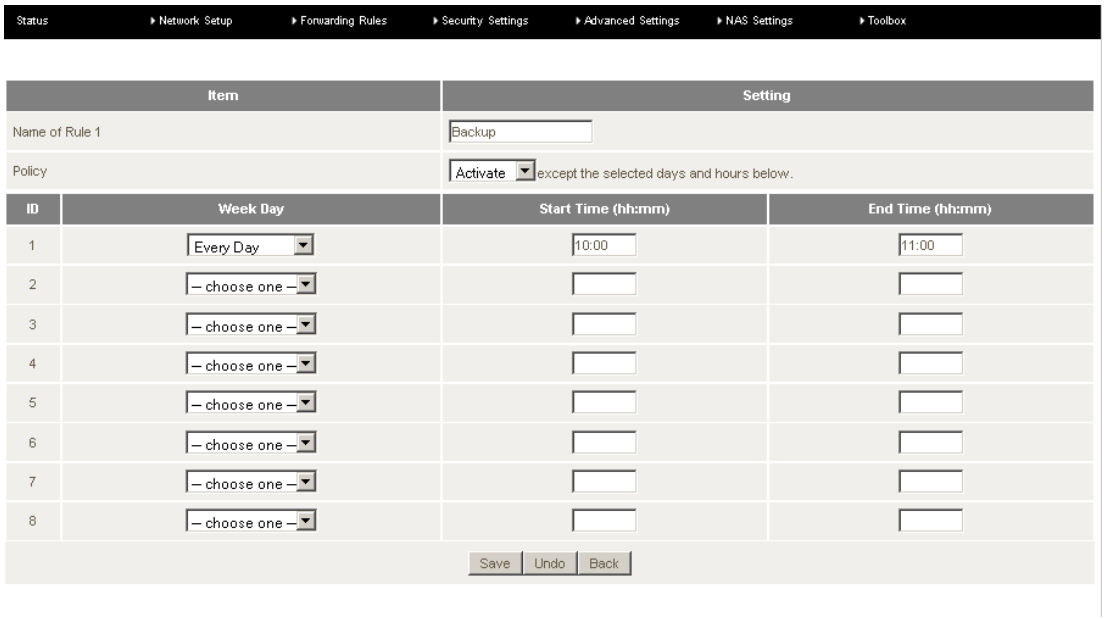


Figure 44: Advanced - Advanced Settings - Adding a Schedule

OPTION	DEFINITION
Name of Rule	Enter a name for the Schedule.
Policy	Use the Policy option to set each rule defined to Activate or Deactivate the router except the selected days and hours below.
Week Day	Select the day(s) of the week you wish the rule to be used on.
Start Time (hh:mm)	Enter the Start time for the rule to begin.
End Time (hh:mm)	Enter the End time for the rule to end.

Table 29: Advanced - Advanced settings - Adding a Schedule Settings

IPv6

The NF2 router can be configured to use IPV6 routing configuration.

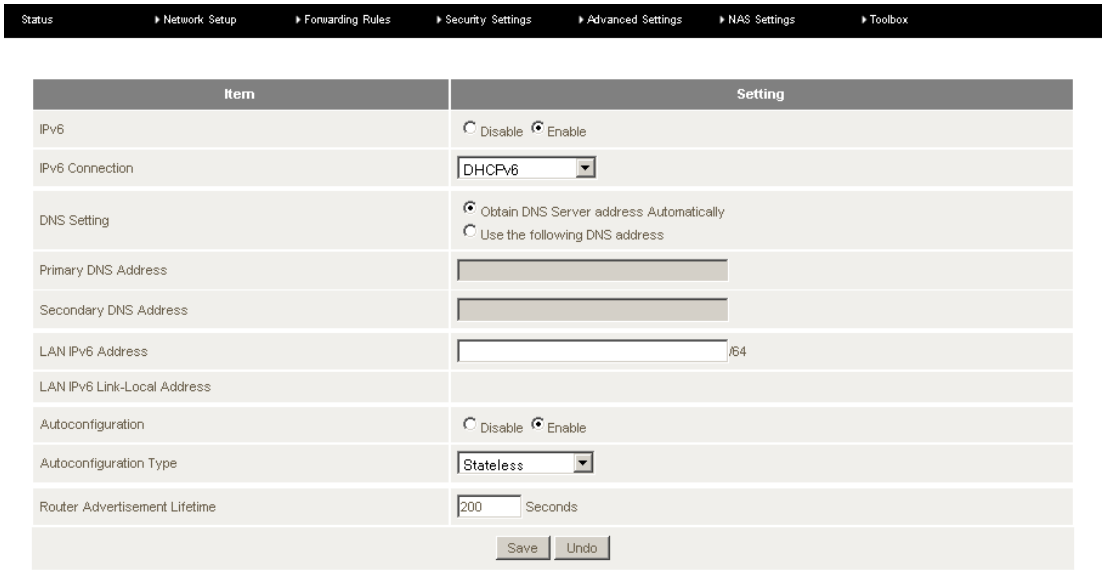


Figure 45: Advanced - Advanced Settings - IPV6

OPTION	DEFINITION
IPv6	The option to enable or disable IPv6.
IPv6 Connection	Select the type of IPv6 for the router to use. Options include : ▪ Dynamic DHCPv6 - an IPv6 address is assigned by the router automatically, ▪ Static IPv6 - a static IPv6 address assigned by an Internet Service Provider can be assigned to the router. ▪ PPPoE – for using an IPv6 address over PPPoE. ▪ 6 to 4 – This option converts an IPv6 address to an IP v4 address. ▪ IPv6 in IPv4 tunnel – This option uses an IPv6 address through an IPv4 tunnel.
DNS Setting	Select Obtain a DNS Server address automatically assigned by the router or assign your own static Primary and Secondary DNS addresses.
LAN IPv6 Address	Enter the local IPv6 address in this field.
Auto-configuration	Select to enable auto configuration of the IPv6 address.
Auto-configuration Type	Select either Stateless or Stateful IPv6 auto configuration. Stateless Address Auto configuration (or SLAAC) can be used by devices connecting to a routed network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. This is generally streamlined and simplified compared to Stateful Auto-configuration. Stateful IPv6 also known as DHCPv6 uses a dedicated configuration mechanism that is more comprehensive than Stateless Auto configuration catering to all the information needs in the form of required parameters to the network devices
Router Advertisement lifetime	When a computer host first connects to the NF2 router using IPv6 it sends a link-local router solicitation multicast request for its configuration parameters. If the NF2 router is configured correctly it will respond with a router advertisement packet that contains network-layer configuration parameters. The Router advertisement lifetime is the amount of time that the router advertisement is broadcast as a multicast after receiving the request.

Table 30: Advanced - Advanced Settings – IPv6 Settings

TR-069

The TR-069 (technical report 069) protocol uses a SOAP/HTTP protocol to provide communications between Customer-Premises Equipment (CPE) and an Auto-Configuration Server (ACS) for the purpose of automated configuration of the CPE devices.

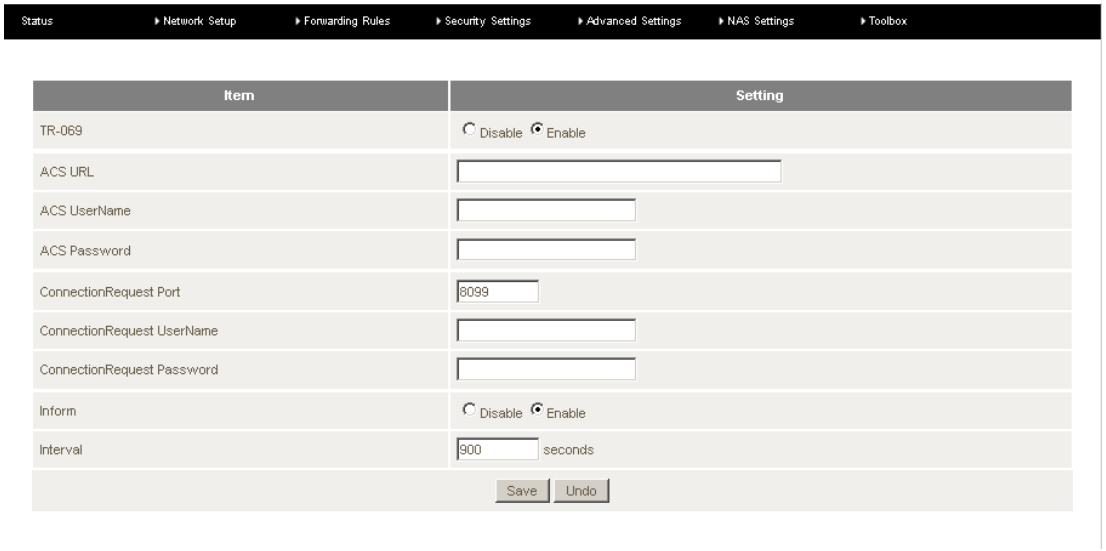


Figure 46: Advanced - Advanced Settings - TR-069

OPTION	DEFINITION
TR-069	Select the enable option to enable the TR-069 protocol on the NF2.
ACS URL	Enter the URL of the Auto-Configuration Server in this field.
ACS UserName	Enter the user name of the Auto-Configuration Server here.
ACS Password	Enter the password of the Auto-Configuration Server here.
Connection Request Port	Enter the port number to be used by a CPE in sending an Inform message to the ACS server to initialise a connection.
Connection Request UserName	Enter the Connection Request username to be used by each of the CPE devices to authenticate with the ACS server.
Connection Request Password	Enter the Connection Request password to be used by each of the CPE devices to authenticate with the ACS server.
Inform	Set the Inform to enable or disable to accept or deny an inform message from a CPE device to the ACS server.
Interval	Enter the interval in seconds between Inform messages being sent to the ACS server.

Table 31: Advanced - Advanced Settings - TR-069

VLAN

The VLAN section of the NF2 allows for the creation of a virtual LAN across one or more of the Ethernet and wireless interfaces

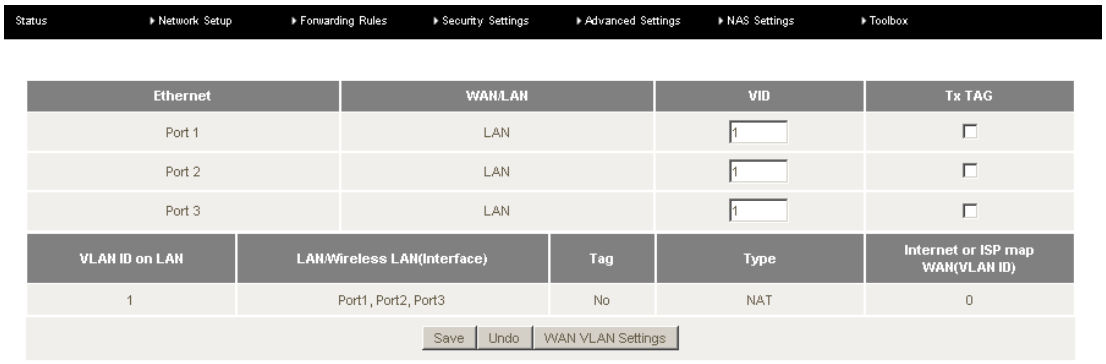


Figure 47: Advanced – Advanced Settings – VLAN

Enter the Virtual ID for each Ethernet port and tick whether the data transmitted needs to be tagged, a part of VLAN tagging. For WAN VLAN settings press the WAN VLAN Settings button.

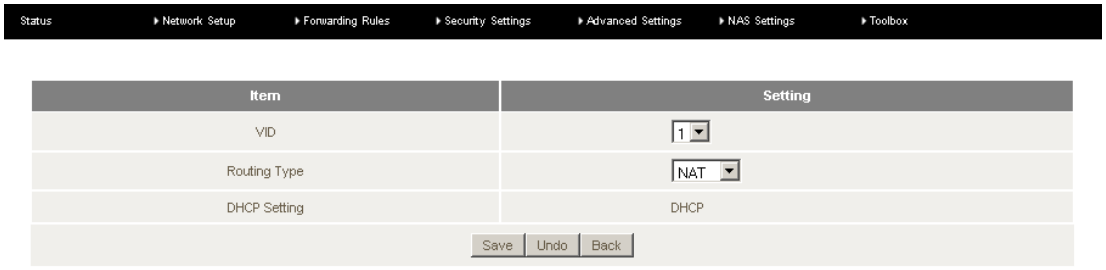


Figure 48: Advanced - Advanced Settings - VLAN - WAN VLAN

Select the appropriate VID (Virtual ID) and select the Routing Type, either NAT or Bridging. Press the Save button to save any changes to the settings.

NAS Settings

The NAS (Network Attached Storage) settings allow the NF2 to act as a file server. Options available include Disk Utility, File Sharing, Access Control, iTunes Server, Download Assistant, Download Status and Web HDD.

Disk Utility

Using the disk utility function a connected USB drive will be detected and displayed as the example in Figure 47 shows. The option to format the drive can also be found on this by pressing the Format button. The drive can be checked for integrity by pressing the Check button and Unmounted by pressing the Unmount button.

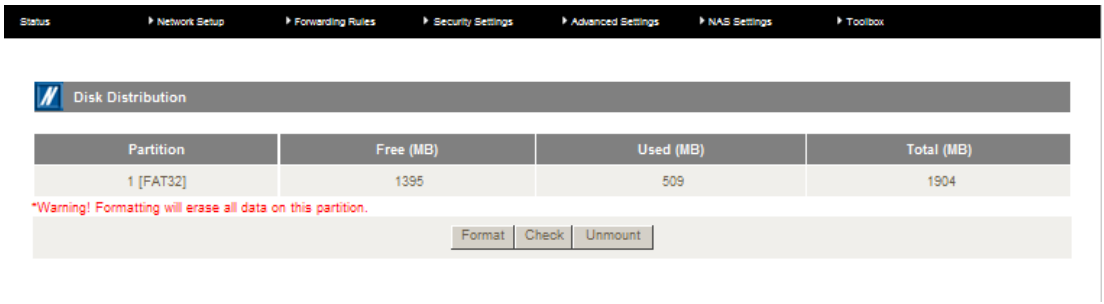


Figure 49: Advanced - Advanced Settings - Disk Utility

File Sharing

The file sharing option under NAS settings allows the router NAS (Network Attached Storage) to join an existing network Workgroup. An FTP connection to the NAS device can also be configured by pressing the FTP Service Configuration button.

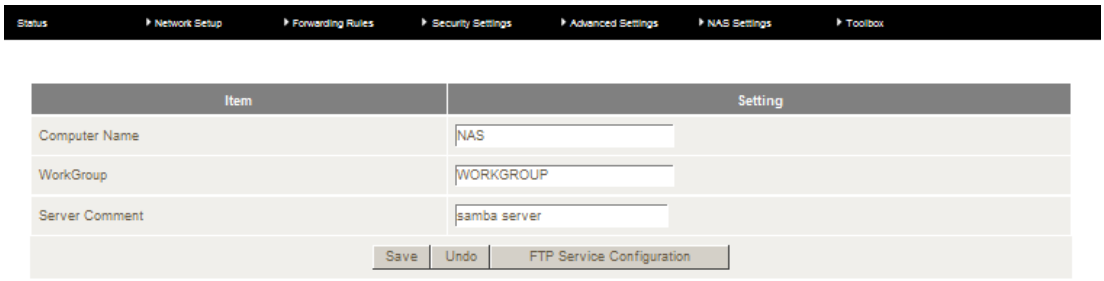


Figure 50: Advanced - NAS Settings - File Sharing

FTP Service Configuration

The FTP (File Transfer Protocol) Service Configuration allows the NAS storage files to be accessed and transmitted over a TCP based network.

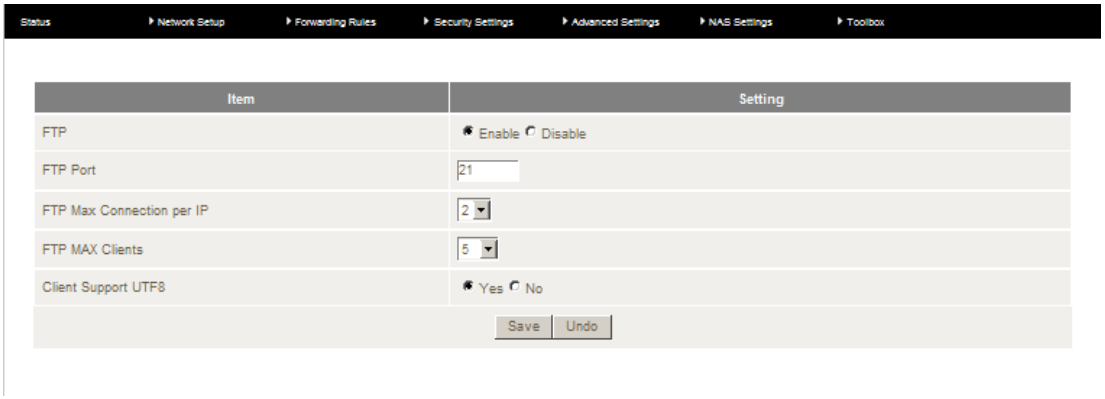


Figure 51: Advanced - NAS Settings - File Sharing -FTP Service Configuration

OPTION	DEFINITION
FTP	Select this option to enable or disable the FTP function.
FTP Port	Enter the port number to be used by the FTP protocol.
FTP Max Connection per IP.	Select the maximum number of FTP connections over any one IP address.
FTP Max Clients	Select the maximum number of clients that can connect via FTP at any one time.
Client Support UTF8	Select whether the router will support client connections with UTF-8, one of the most common Unicode standards. As the name implies UTF-8 uses one byte (8 bits) for any ASCII character and up to 4 bytes for other characters.

Table 32: Advanced - NAS Settings - File Sharing - FTP Service Configuration

Access Control

The Access Control section of the NF2 NAS Settings, allow a network administrator to set either a guest level security with no authentication required or to use authentication mode where a username and password is required to access the NAS server files.

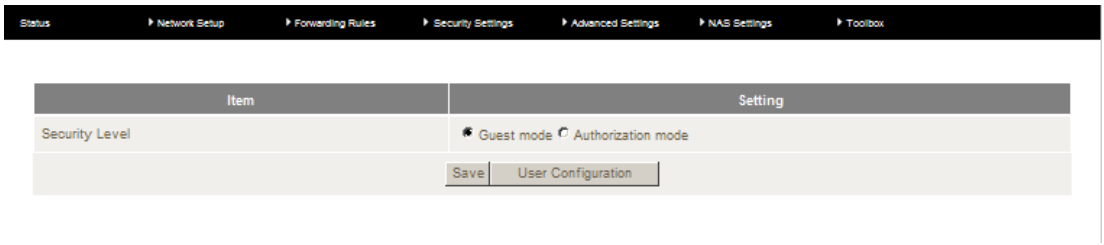


Figure 52: Advanced - NAS Settings -Access Control

To setup authentication for the NAS storage select Authorization Mode and press the User Configuration button.

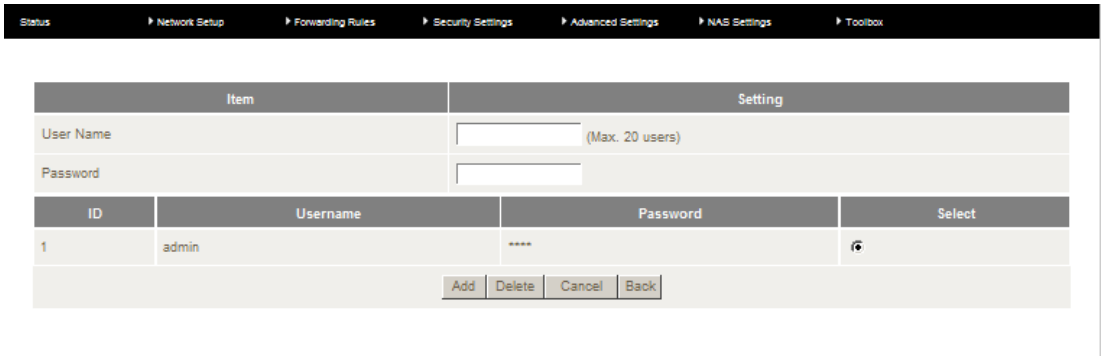


Figure 53: Advanced - NAS Settings - Access Control – Authentication Mode

Enter a user name and password and press the Add button to save the authentication details. Up to 20 usernames and passwords for NAS storage authentication can be stored on the router.

iTunes Server

The iTunes Server function enables any applicable media on any attached USB storage to be directly access from within iTunes. To enable this, click on the ‚Enable' radio button in the ‚Service' section. Click the ‚Save' button to save any configuration changes you have made

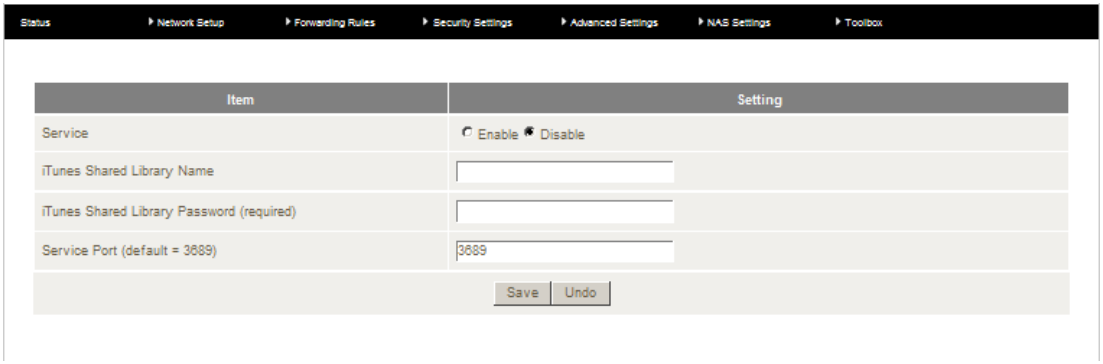


Figure 54: Advanced - NAS Settings - iTunes Server

NAME	DESCRIPTION
Service	Select this option to enable or disable the iTunes Server functionality.
iTunes Shared Library Name	Enter the name that will appear in your iTunes application as a library list.
iTunes Shared Library password (required)	Enter the password required to access your iTunes server content.
Service Port	Enter the port number that the iTunes Shared Library uses to connect with the internet. The default port number is 3369.

Table 33: Advanced - NAS Settings - iTunes Server

Download Assistant

The download assistant gives the user a means of automating the downloading of files from the internet at scheduled dates and times to a location of the user's choice. There are two methods available to complete the downloading, FTP and HTTP.

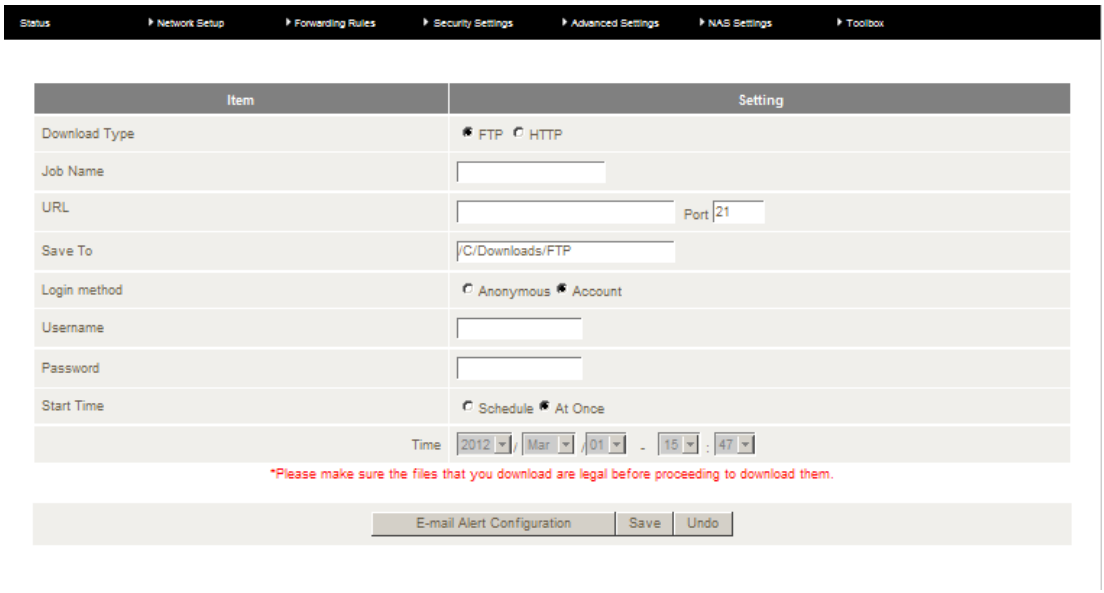


Figure 55: Advanced - NAS Settings - Download Assistant – FTP

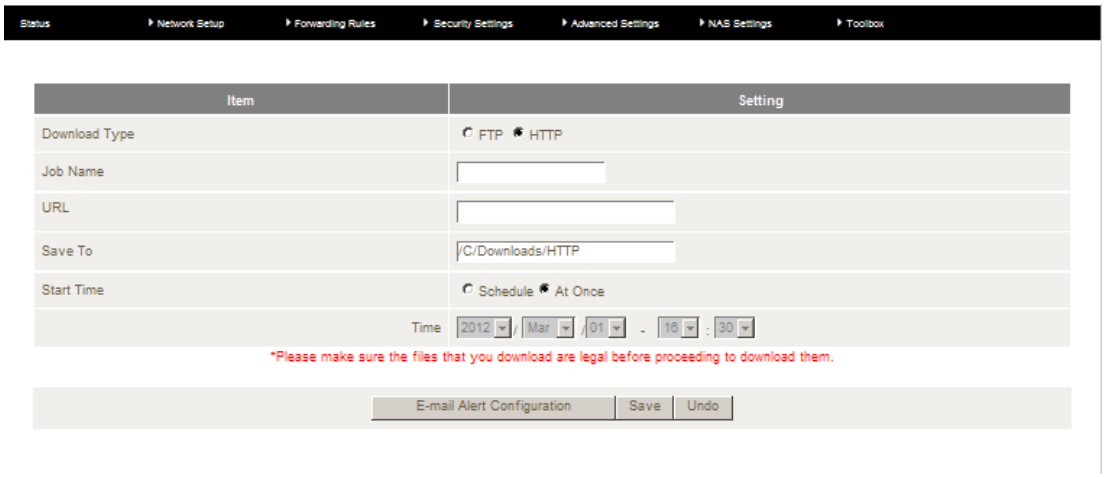


Figure 56: Advanced - NAS Settings - Download Assistant - HTTP

OPTION	DEFINITION
Download Type	Select the protocol to use to complete the download.
Job Name	Enter a name for the download job.
URL/Port	Enter the path and filename and port number to the document to be downloaded. The default port number for using FTP is port 21.
Save To	Enter the local location where the file will be saved to.
Login Method	Select the authentication required if any. For no authentication use anonymous. For use with an FTP account select Account.
Username	Enter the username for an FTP account.
Password	Enter the Password for an FTP account.
Start Time	Select the date/time for the download to commence.
Email Alert Configuration	Press this button to setup an email alert to advise a network administrator that the download has completed.

Table 34: Advanced - NAS Settings - Download Assistant Settings

Download Assistant – Email Alert

To set up an email to alert the network administrator that a download is complete select the Email Alert Configuration button. The following screen will appear.

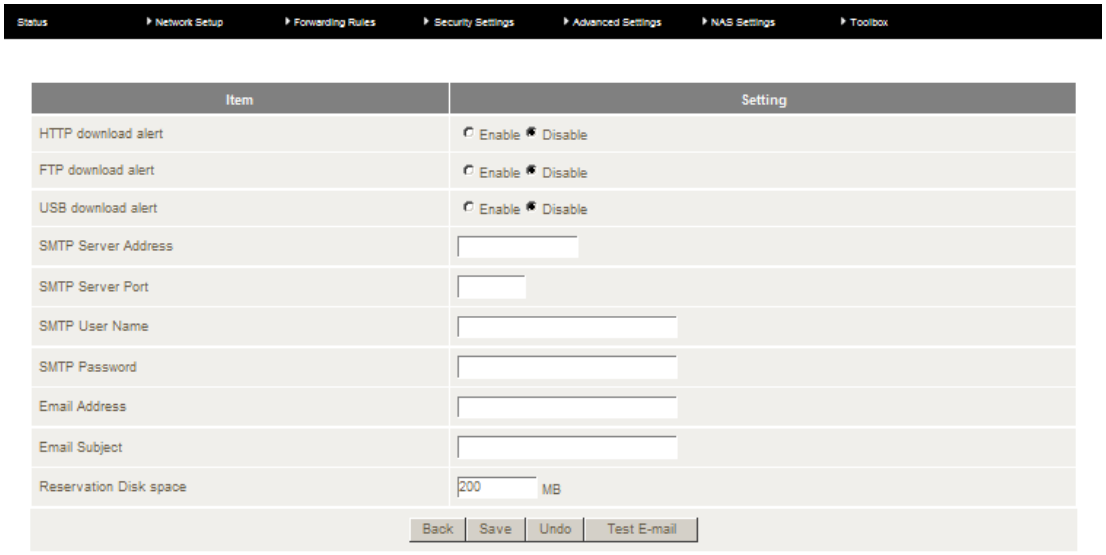


Figure 57: Advanced - NAS Settings - Download Assistant - Email Alert

OPTION	DEFINITION
HTTP Download Alert	Use this option to disable or enable the HTTP Download Alert function.
FTP Download Alert	Use this option to disable or enable the FTP Download Alert function.
USB Download Alert	Use this option to disable or enable the USB Download Alert function.
SMTP Server Address	Enter the SMTP outgoing email server address that will be used to send emails from the router.
SMTP Server Port	Enter the port number that the SMTP server uses.
SMTP User Name	If required by the SMTP server, enter the SMTP user name.
SMTP Password	If required by the SMTP server, enter the SMTP password.
Email Address	Enter the Email address to send the Download Alert Email to.
Email Subject	Enter the Email Subject that the Download Alert Email will have.
Reservation Disk Space	Enter the amount of disk space (in MB) that the Download Alert Emails will need.

Table 35: Advanced - NAS Settings - Download Assistant - Email Alert Settings

Download Status

The download status page lists all downloads that are running, waiting to run or are scheduled to run.

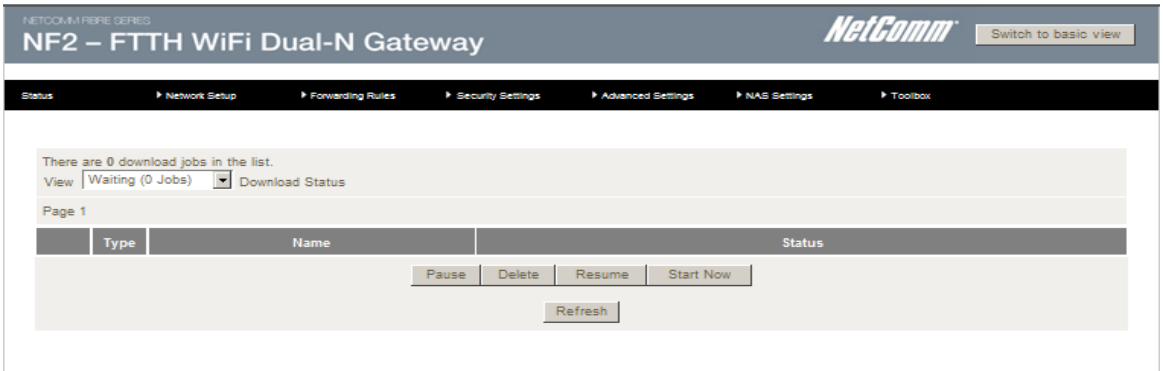


Figure 58: Advanced - NAS Settings - Download Status

Web HDD

The Web HDD function provides a web page based Windows Explorer type view of the content of any attached USB storage. Using this interface you are able to upload, download or delete files and folders as well as create directories. Click through the displayed folders to show any stored files.

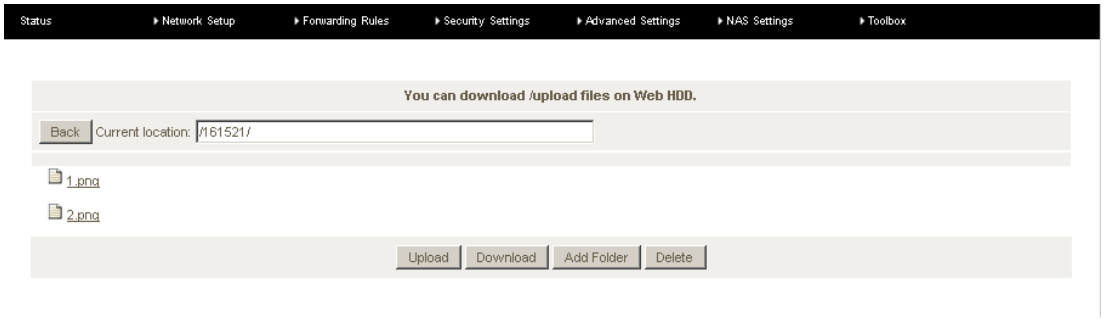


Figure 59: Advanced - NAS Settings - Web HDD

Single click on any items to select them and click the appropriate button or double click folders to view any content.

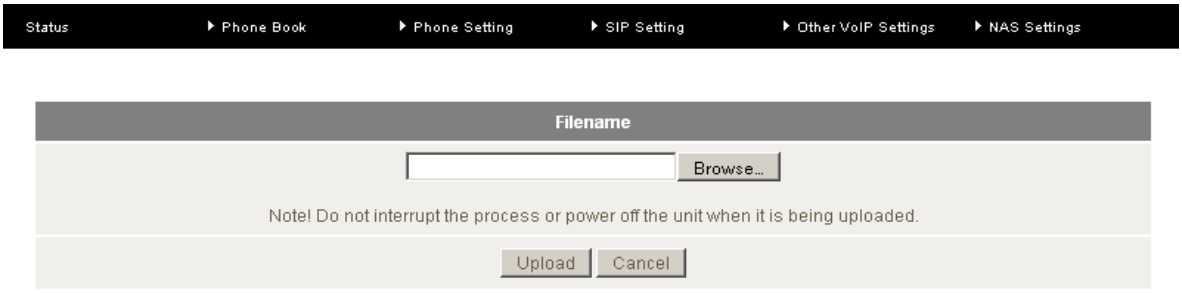


Figure 60: Advanced - NAS Settings - Web HDD - Upload File

You can then click the Browse' button and then navigate to the file you would like to upload. To upload files to your Web HDD click the Upload button. Once selected, this file will be copied to the Web HDD and become available to download by connected devices.

Toolbox

The Toolbox menu provides access to maintenance settings of the NF2. Menu options include System Info, Restore Settings, Firmware Upgrade, Backup Settings, Reset to Default, Reboot, Startup Wizard, Miscellaneous and Logout.

System Info

The System Info section provides access to the system log entries of the NF2. The system log entries can be saved to a file by pressing the Download button at the bottom of the page.

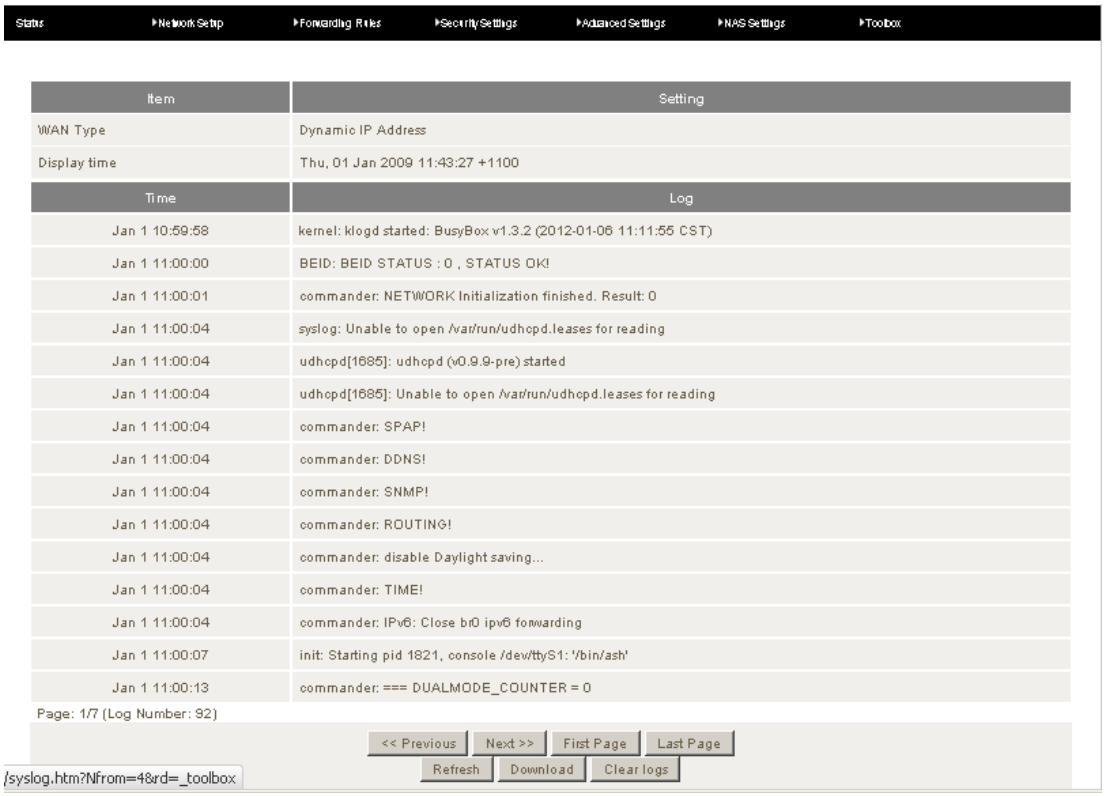


Figure 61: Advanced - Toolbox - System Info

Restore Settings

The restore settings page can be used to load a previously saved router configuration. It is recommended using an Ethernet cable connection to upload any configuration settings. Do not power off the router until the configuration settings are successfully updated and the router has automatically restarted.

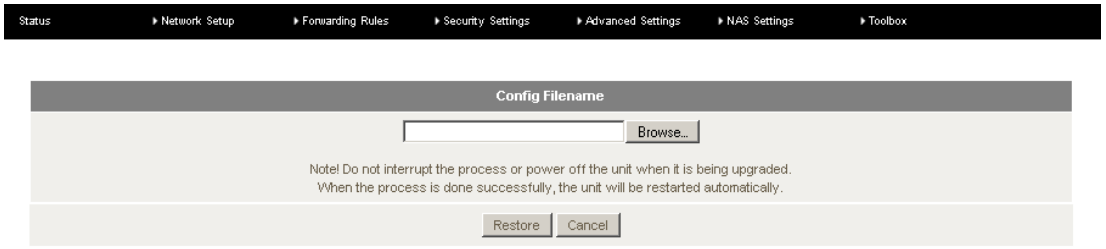


Figure 62: Advanced - Toolbox - Restore Settings

Firmware Upgrade

This page can be used to upload the latest firmware version for the NF2 as it becomes available.

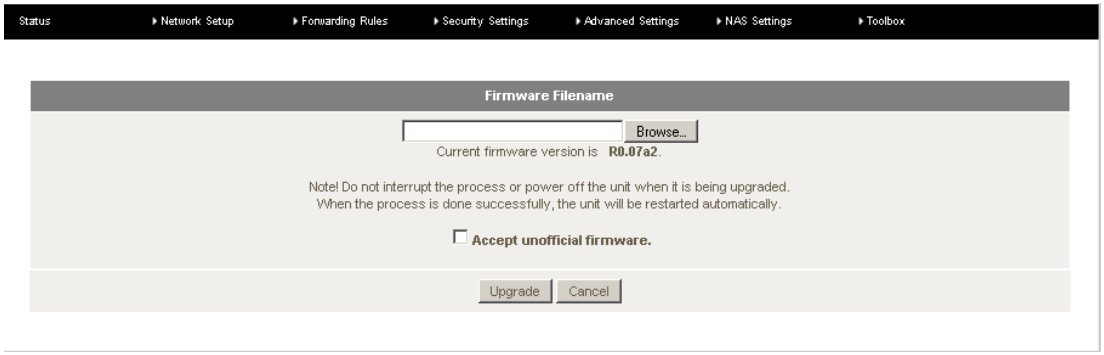


Figure 63: Advanced - Toolbox - Firmware Upgrade

Click the "Browse" button and navigate to the location where you have saved the firmware update file. You can then upgrade the firmware by clicking the "Upgrade" button. Do not power off the device until the firmware upgrade has completed and the router has automatically restarted.

Backup Settings

This option allows the network administrator to save the configuration settings of the NF2 to a file that can be uploaded to another NF2 or uploaded into the NF2 at a later date. The name of the file can be changed but it is recommended to leave the suffix as .bin.

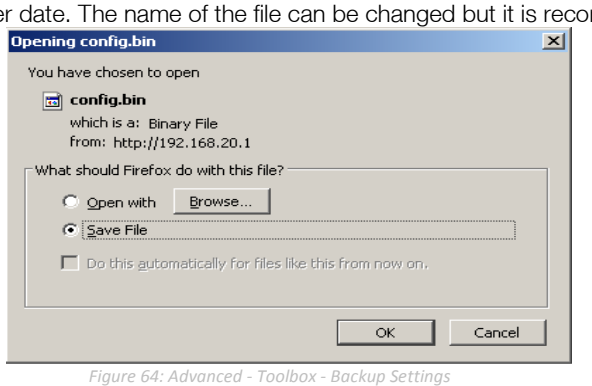


Figure 64: Advanced - Toolbox - Backup Settings

Reset to Default

This option can be used to reset all settings on the NF2 to factory default settings. It is recommended to reset the router to factory default settings after a firmware upgrade.

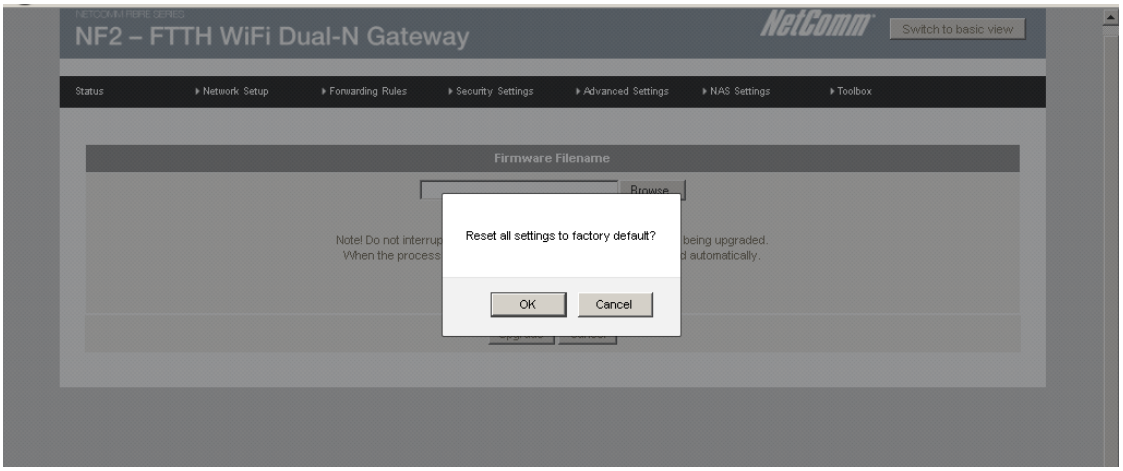
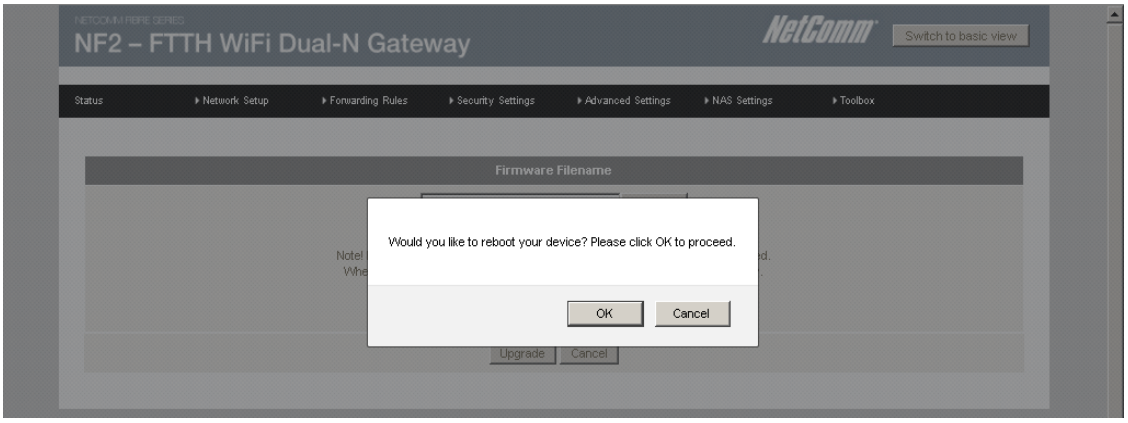


Figure 65: Advanced - Toolbox - Reset to Default

Reboot

Use this option to reboot the router after making any changes to the configuration settings.



Startup Wizard

The Startup Wizard option will return the user to the NF2 Startup wizard so that the router can be reconfigured.

Figure 66: Advanced - Toolbox - Startup Wizard

Miscellaneous

The Miscellaneous page provides settings for Wake on LAN, has provision for ping tests, and has the option to DIM the LEDs on the front of the unit. Wake-on-LAN enables the router to start-up a computer or device (if the computer supports it) when a WOL packet is detected on the network going to the client MAC you have entered.

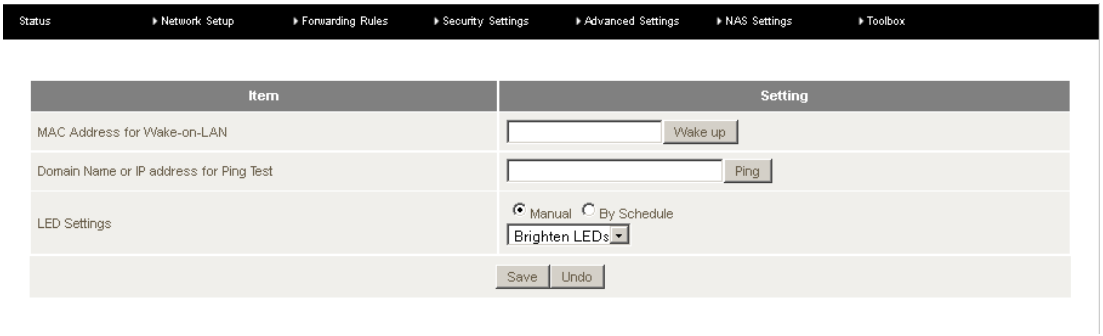


Figure 67: Advanced - Toolbox – Miscellaneous

OPTION	DEFINITION
MAC Address for Wake on LAN	Enter the MAC address of the computer you would like to wake up from stand-by mode.
Domain Name or IP Address for PING Test	Enter the domain name or IP address you wish to attempt to ping to.
LED Settings	Select the manually control the LED brightness.

Table 36: Advanced - Toolbox - Miscellaneous

Logout

The logout option gives the user the option to logout of the NF2 Graphical User Interface.

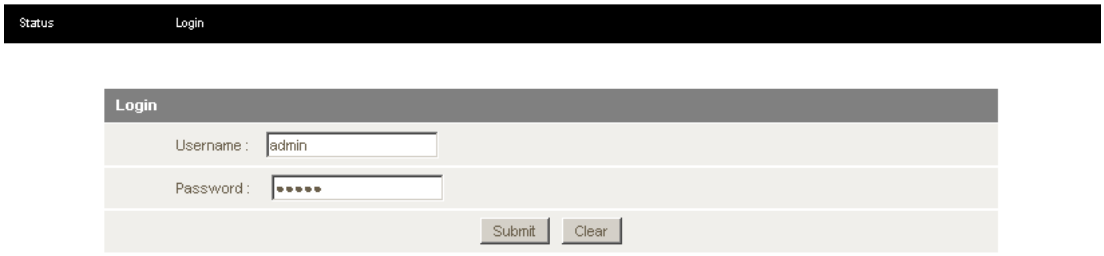


Figure 68: Advanced - Toolbox - Logout

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 2)

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 NB16WV 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.

Please note: For other operating system (Windows 98SE, Windows ME, Windows 2000 etc) or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adapter documentation for additional information.

Technical Data

The following table lists the hardware specifications of the NF2™ Hub.

MODEL	NF2™ HUB
Wireless WAN	1 x USB 2.0 port for external HSPA modem PPP (for WCDMA / HSPA)
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	USB 2.0 x 2, 10/100/1000 Ethernet LAN x 3,1 x 2.4GHz WLAN,1 x 5.0 GHZ WLAN
Antenna connector	SMA (female connector)
LED Indicators	Power, 3G, WWW, WiFi, WAN, WDS, LAN 1-3
Operating Temperature	0 ~ 50 degrees Celsius (operating temperature)
Power input	12VDC – 1.5A
Dimensions & Weight	133 mm (L) x 137 mm (H) x 34 mm (W) 250 grams
Regulatory Compliancy	C-Tick

Table 38 - Technical Specifications for the NetComm NF2

Electrical Specifications

A suitable power supply is available on request or via direct purchase from the NetComm Online shop. It is recommended that the NF2™ Hub be powered using the 12VDC/1.5A power supply which is included with the device.

Environmental Specifications / Tolerances

The NF2™ Hub is able to operate over a wide variety of temperatures from 0˚C ~ 50˚C (ambient).

FAQ

1. Does the Dual Band WiFi Gigabit Hub require any configuration out of the box?

   No, the NF2™ Hub is a plug and play device. Plug the device into an electrical outlet and once the status indicator lights are on, plug in your LAN cable for data connectivity. For WiFi connectivity the default SSID (Service Set Identifier) and network key (password) are located on the bottom of the device. If you would like to customize your settings you can enter 192.168.20.1 into your Web browser to access the Management Console and device settings.

2. I cannot seem to access the web page interface.

   The default IP address of the unit is 192.168.20.1, so first try to open a web browser to this address. Also check that your laptop/ PC is using the same subnet as the router's Ethernet port. I.e. An IP address has been assigned to your computer in the range of 192.168.20.x where x can equal 2 – 254.

3. The router has a connection but cannot access the internet

   Check that DNS Proxy is enabled by clicking on the Network Setup > DHCP Server page on the configuration interface. Make sure that the DHCP DNS server address 1 IP address is set to the same address as that of the Ethernet port.

4. Is the Dual Band WiFi Gigabit Hub secure; can other people access my wireless network?

   The Dual Band WiFi Gigabit Hub comes configured with WPA-PSK/WPA2-PSK WiFi security enabled. When you first access the Internet, type 192.168.20.1 into the address bar, the wizard will pop up to configure your computer to connect with the wireless security settings of your choice (please see the Quick Start Guide for more information on connecting your data devices to the Dual Band WiFi Gigabit Hub). Only people you allow access to, will be able to connect to the Dual Band WiFi Gigabit Hub ensuring your connection is secure and safe.

5. Can I change the name and password of my wireless network?

   Yes. You can change your Dual Band WiFi Gigabit Hub settings from the browser user interface by typing 192.168.20.1 into the address bar of your Web browser. You can change the WiFi network name or SSID (Service Set Identifier), WiFi security standard (WPA, WPA2, WEP) and your WiFi password.

6. How do I share my Internet connection, using the Dual Band WiFi Gigabit Hub, with other users?

   Provide the SSID (Service Set Identifier) and WiFi network password of your Dual Band WiFi Gigabit Hub for any users you want to share your WiFi Internet connection with. Each user will need to select the Dual Band WiFi Gigabit Hub SSID, on their WiFi enabled computer or device and enter the network password you provide.

7. What is the difference between upload and download speeds and why do they differ?

   Upload is when you send information (e.g. emails) from your computer and download is when you receive information via the Internet. The speeds at which upload and download operate depend on the way you use the Internet and the size of files you send and receive.

8. Do I need to attach an antenna on this device?

   Yes. Your Dual Band WiFi Gigabit Hub comes equipped with an antenna; you need to attach the WiFi antenna to send and receive wireless signals.

9. I have lost the security card that came with the setup instructions. What can I do?

   If you have lost your security card, and forgotten the wireless security details (SSID and WiFi network password), there is a label attached to the base of your Dual Band WiFi Gigabit Hub with all your original security details. If the label is unreadable or has been removed, the WiFi network password can be viewed or reset by logging in to the Management Console using an Ethernet Cable connected to the LAN port of the NF2™ Hub.

10. I forgot my Management Console password. What can I do?

    If you have forgotten your Management Console password and cannot access the Web user interface, you will need to reset your Dual Band WiFi Gigabit Hub back to factory default settings. To reset your device press and hold the reset button on the back of your Dual Band WiFi Gigabit Hub for 10-15 seconds until all the indicator lights on the unit flash to indicate the device is reset. After a reset, use the default WiFi settings (SSID and WPA key) which can be found on the base of your Dual Band WiFi Gigabit Hub. (Note - this will also reset any custom settings and passwords you may have already set up).

11. Can I use the Dual Band WiFi Gigabit Hub overseas?

    No. The Dual Band WiFi Gigabit Hub is not equipped for international roaming or data services.

Appendix A: Tables

Table 1 - Document Revision History 2
Table 2 - LED Indicators 7
Table 4: LAN Management Default Settings 9
Table 5: WAN Port Default Settings....9
Table 6: WiFi Default Settings....9
Table 7: Web Interface Default Settings....9
Table 8: Basic View - Status 19
Table 9: Basic View - 2.4 GHz Wireless Settings 20
Table 10: Basic View - 5.0 GHZ Wireless Settings....21
Table 11: Basic View - Mobile Broadband Settings 22
Table 12 - Advanced View – Ethernet WAN Settings 25
Table 13: Advanced - Network Setup - Wireless WAN....26
Table 14: Advanced - DHCP Settings 27
Table 15: Advanced Wireless 2.4 GHz Settings 28
Table 16: Advanced - WPS Setup settings 29
Table 17: Advanced - Network Setup - 5.0 GHz Wireless Settings....30
Table 18: Advanced - Network Setup -VPN-IPSec 31
Table 19: Advanced - Network Setup - VPN IPSec - Dynamic IPSec 32
Table 20: Advanced - Network Setup - VPN - PPTP Server Settings....34
Table 21: Advanced - Forwarding Rules - Virtual Server Settings 36
Table 22: Advanced - Forwarding Rules - Port Triggering Settings 37
Table 23: Advanced - Security Settings - Packet Filtering Settings....39
Table 24: Advanced - Security Settings - Domain Filtering Settings:....40
Table 25: Advanced - Advanced Settings - System Log Settings 43
Table 26: Advanced - Advanced Settings - Dynamic DNS Settings....43
Table 27: Advanced - Advanced Settings - QoS Settings 44
Table 28: Advanced - Advanced Settings - SNMP Settings....45
Table 29: Advanced - Advanced Settings - System Time....46
Table 30: Advanced - Advanced settings - Adding a Schedule Settings 47
Table 31: Advanced - Advanced Settings – IPv6 Settings 48
Table 32: Advanced - Advanced Settings - TR-069 49
Table 33: Advanced - NAS Settings - File Sharing - FTP Service Configuration....52
Table 34: Advanced - NAS Settings - iTunes Server....54
Table 35: Advanced - NAS Settings - Download Assistant Settings....55
Table 36: Advanced - NAS Settings - Download Assistant - Email Alert Settings 56
Table 37: Advanced - Toolbox - Miscellaneous 61

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 vested in NetComm Wireless Limited (ACN 002490486) (NetComm) (or its licensors). This Manual does not transfer any right, title or interest in NetComm's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm 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.

NetComm is 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 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:
    - Change the direction or relocate the receiving antenna.
    - Increase the separation between this equipment and the receiver.
    - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
    - Consult an experienced radio/TV technician for help.
3. 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. 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 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 within 30 days of the original purchase by registering online via the NetComm web site at www.NetComm.com.au. 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 Section 3 above). Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see Section 3 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 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 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;

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; 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 Section 3 above), NetComm accepts no liability or responsibility, for consequences arising from the use of this product. NetComm 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'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's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm 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 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 is unable to limit its liability as set out above, NetComm 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
P: +61(0)2 9424 2070 F: +61(0)2 9424 2010
E: sales@NetComm.com.au
W: www.NetCommlimited.com