NetCommWireless

N300 WiFi Gigabit Router with Voice

NF5

USER GUIDE

Note: This document is subject to change without notice.

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

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

Please be responsible and protect our environment.

This manual covers the following products:
NetComm Wireless NF5 N300 WiFi Gigabit Router with Voice

DOCUMENT VERSION	DATE
1.0 – Initial document release	May 2013
1.1 – Revised QoS section	October 2013
1.2 – Minor corrections	November 2013
1.3 – Added Wireless Distribution System (WDS) description	May 2014
1.4 – Minor corrections	November 2014

NetCommWireless

Table of Contents

Overview

Introduction

This manual provides information related to the installation, operation, and use of the NF5.

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 NF5, please confirm that you comply with the minimum system requirements below.

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

Notation

The following symbols are used in this manual:

Indicates a note requiring attention.

Indicates a note providing a warning.

Indicates a note providing useful information.

Product Introduction

Product Overview

- Gigabit WAN port for a fixed line connection. Perfect for a future NBN/Fibre connection
- Establish up to 4 high speed wired connections with the Gigabit LAN ports
- Create a WiFi network to share your connection with multiple WiFi devices at speeds of up to 300Mbps
- One USB 2.0 port that can support 3G/4G USB modems or external hard drives. Insert your compatible 3G/4G USB modem for an alternate Internet connection. Plug in your external hard drive and share all of the stored files with connected users (optional configuration)
- One VoIP phone port to make calls over the Internet
- Supports IPv6 for next generation IP addressing

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

Package Contents

The NF5 package consists of:

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

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

Product Features

The NetComm Wireless NF5 is a future ready WiFi router that connects the home or office to super-fast broadband. Simply connect your fixed line modem to the Gigabit WAN port for instant Internet access - perfect for NBN/Fibre connections

The advanced network sharing function gives multiple users the freedom to watch movies, download music, play online games and enjoy other bandwidth intensive activities such as IPTV streaming on a single broadband account.

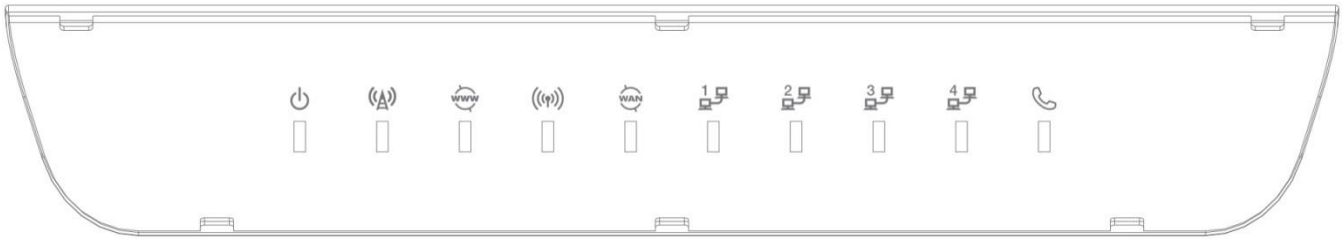
Enjoy extended WiFi coverage with high-speed WiFi N, or connect up to four wired devices via the Gigabit Ethernet ports. The device also features a USB 2.0 port for external hard drive storage or an alternate Internet source with a compatible 3G/4G USB modem. The VoIP phone port allows users to make phone calls over the Internet, making a phone line completely redundant and cutting phone costs.

The NF5 is also kind to the environment with innovative green features for power conservation. With support for IPV6, users are ensured that their router will be able to continue to access websites when new web addressing starts becoming a commonplace.

Physical Dimensions and Indicators

LED Indicators

The NF5 has been designed to be placed on a desktop. All of the cables exit from the rear for easy organization. The display is visible on the front of the NF5 to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.



LED INDICATOR	ICON	STATUS	DEFINITION
Power		Off	The NF5 is powered off.
		On	The NF5 is powered on and operating normally.
		Flashing	The NF5 is starting up.
3G/4G		Off	3G/4G not configured (no dongle connected).
		On	Connected to 3G/4G network.
		Flashing	Connecting.
WWW		Off	Internet connection not configured.
		On	Internet connected.
		Flashing	Internet traffic is being sent and received.
LAN 1-4		Off	No device is connected to the Ethernet LAN port.
		On	A device is connected to the Ethernet LAN port.
		Flashing	Data is being sent or received via the Ethernet LAN port.
WAN		Off	No device is connected to the Ethernet WAN port.
		On	A device is connected to the Ethernet WAN port.
WiFi		Off	WiFi is disabled on the NF5.
		On	WiFi is enabled on the NF5.
		Flashing	The NF5 is waiting for a WPS PBC connection.
VoIP		Off	No VoIP service is configured.
		On	The NF5 is registered with the configured VoIP service.
		Flashing	The NF5 is attempting to connect to the configured VoIP service.

Physical Dimensions

The following table lists the physical dimensions and weight of the NF5.

NF5 DIMENSIONS	
Length	119mm
Width	168mm
Height	27mm
Weight	226g

NF5 Default Settings

The following tables list the default settings for the NF5.

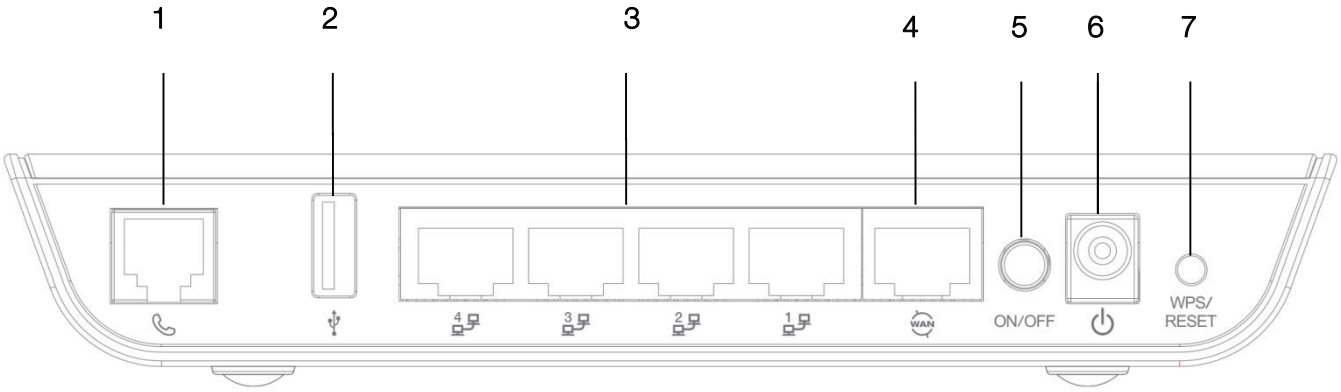
LAN (MANAGEMENT)	
Static IP Address	192.168.20.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1

WIRELESS (WIFI)	
SSID	(Refer to the included Wireless Security Card)
Security	WPA-SPK/WPA2-PSK (mixed mode)
Security Key	(Refer to the included Wireless Security Card)

NF5 WEB INTERFACE ACCESS	
Username	admin
Password	admin

Interfaces

The following interfaces are available on the NF5:



NUMBER	INTERFACE	DESCRIPTION
1	Telephone	Phone port for a standard PSTN analogue telephone handset. Connect a phone to this port to make use of a VoIP service.
2	USB 2.0	USB port for connection of a 3G/4G USB modem our USB external hard drive.
3	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
4	WAN	Gigabit WAN port for connection to a WAN network.
5	Power button	Turns the NF5 on or off.
6	Power jack	Connection point for the included power adapter. Connect the power supply here.
7	WPS button	Activate the WiFi WPS function by press/hold the WPS/RESET button for 1-3 seconds Activate the RESET function by press/hold the WPS/RESET button for 10 seconds To unmount the storage device safely, press/hold the WPS/RESET button for 4-6 seconds

Safety and Product Care

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

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

WARNING
Disconnect the power line from the device before servicing.

Transport and Handling

When transporting the NF5, 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 NF5

Placement of your NF5

The wireless connection between your NF5 and your WiFi devices will be stronger the closer your connected devices are to your NF5. Your wireless connection and performance will degrade as the distance between your NF5 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 NF5 in order to see if distance is the problem.

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

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF5, please try the following steps:

- In multi-storey homes, place the NF5 on a floor that is as close to the centre of the home as possible. This may mean placing the NF5 on an upper floor.
- Try not to place the NF5 near a cordless telephone that operates at the same radio frequency as the NF5 (2.4GHz).

Avoid obstacles and interference

Avoid placing your NF5 near devices that may emit radio "noise," such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows
- If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your devices and the NF5).

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 NF5 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 NF5.
- 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 NF5 to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

Choose the "Quietest" Channel for your Wireless Network

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

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

Hardware installation

1. Connect the power adapter to the Power socket on the back of the NF5.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF5 to power up.

Connecting via a cable

1. Connect the yellow Ethernet cable provided to one of the ports marked 'LAN' at the back of the NF5.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, and enter http://192.168.20.1 into the address bar and press enter.
5. Follow the steps to set up your NF5.

Connecting wirelessly

1. Ensure WiFi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the NF5.

Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF5

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF5.
4. Wait approximately 30 seconds for the connection to establish.
5. Open your Web browser, and enter http://192.168.20.1 into the address bar and press Enter.
6. Follow the steps to set up your NF5.

Web Based Configuration Interface

First-time Setup Wizard

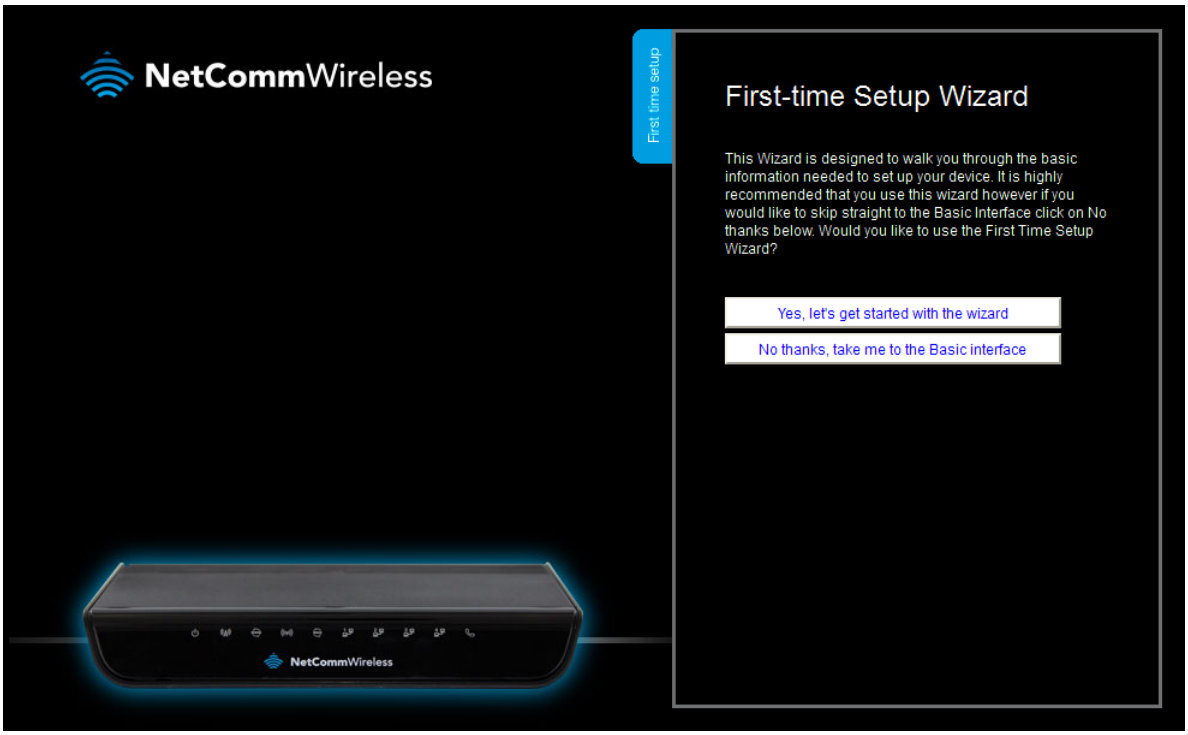
Please follow the steps below to configure your NF5 Wireless router via the web based configuration wizard.

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

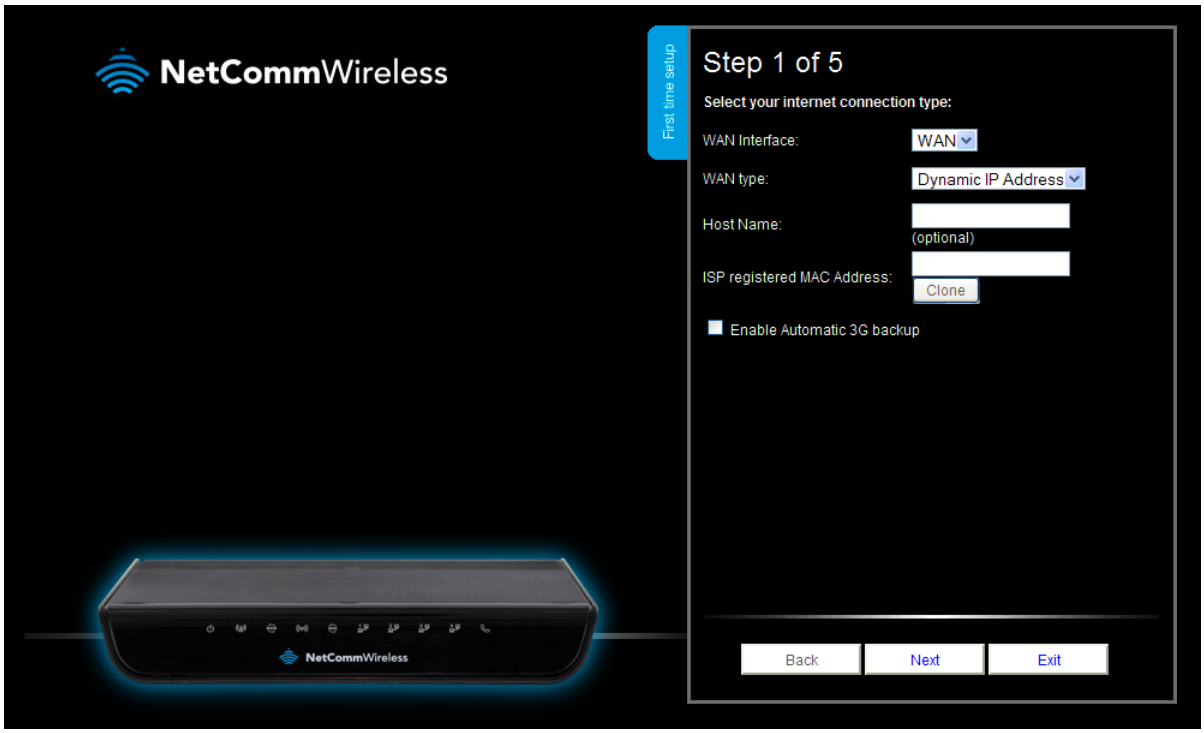
At the login screen, type **admin** in the username and password field, then click the **Login** button.

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

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

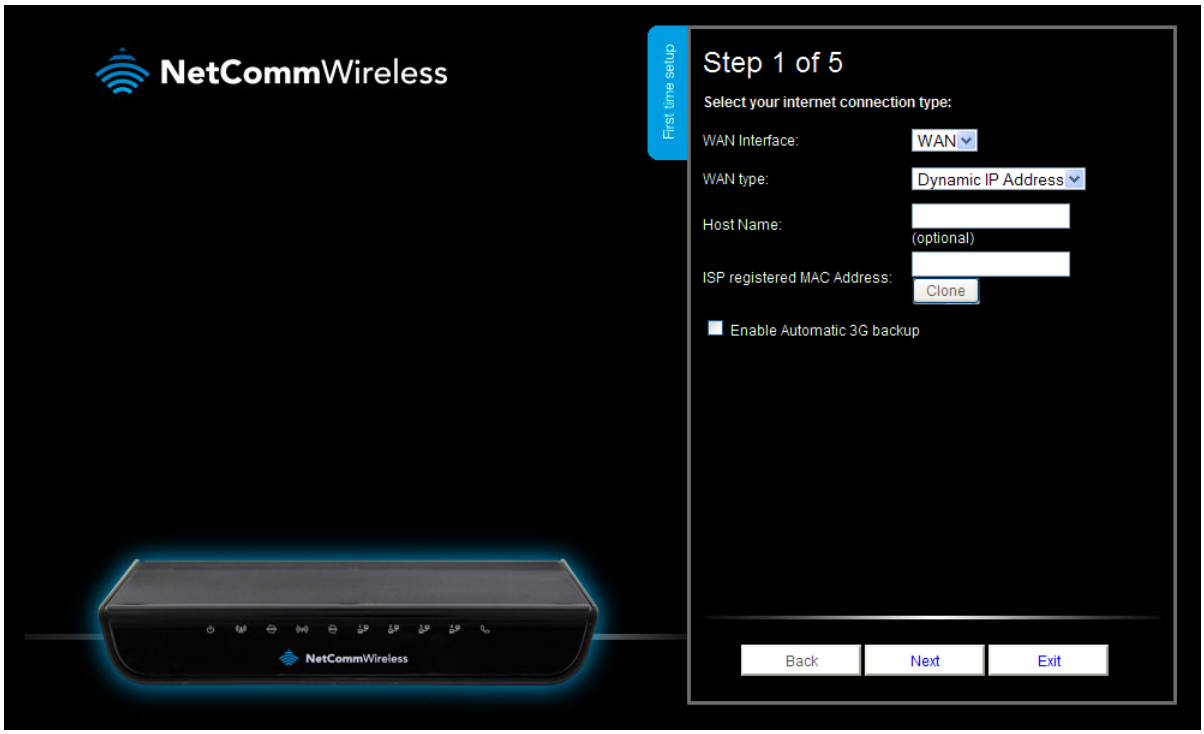


The wizard assists you in configuring the router and entering the information required to setup your Internet connection.



2. From the **WAN Interface** pull down menu, select the type of Internet connection you would like to use. You can select from:
   - 3G
   - WAN

WAN



Select the type of WAN connection:

Dynamic IP Address

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

Static IP Address

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

PPP over Ethernet (or PPPoE)

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

PPTP

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

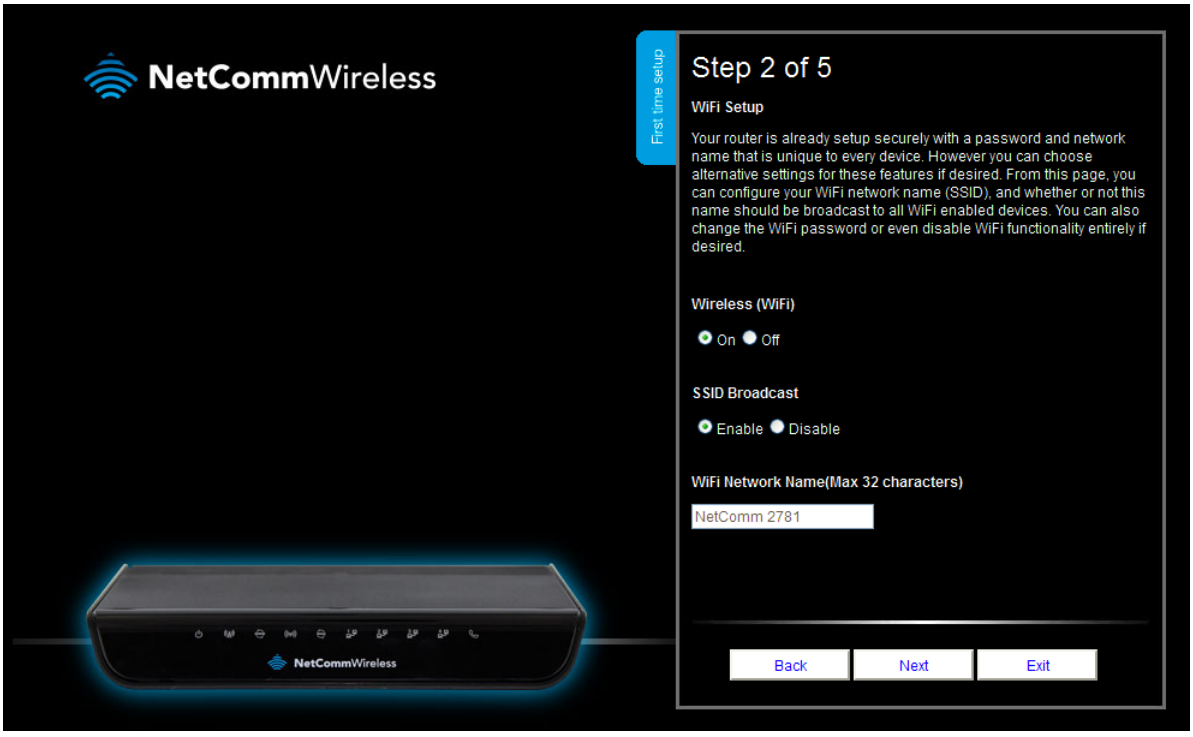
L2TP

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

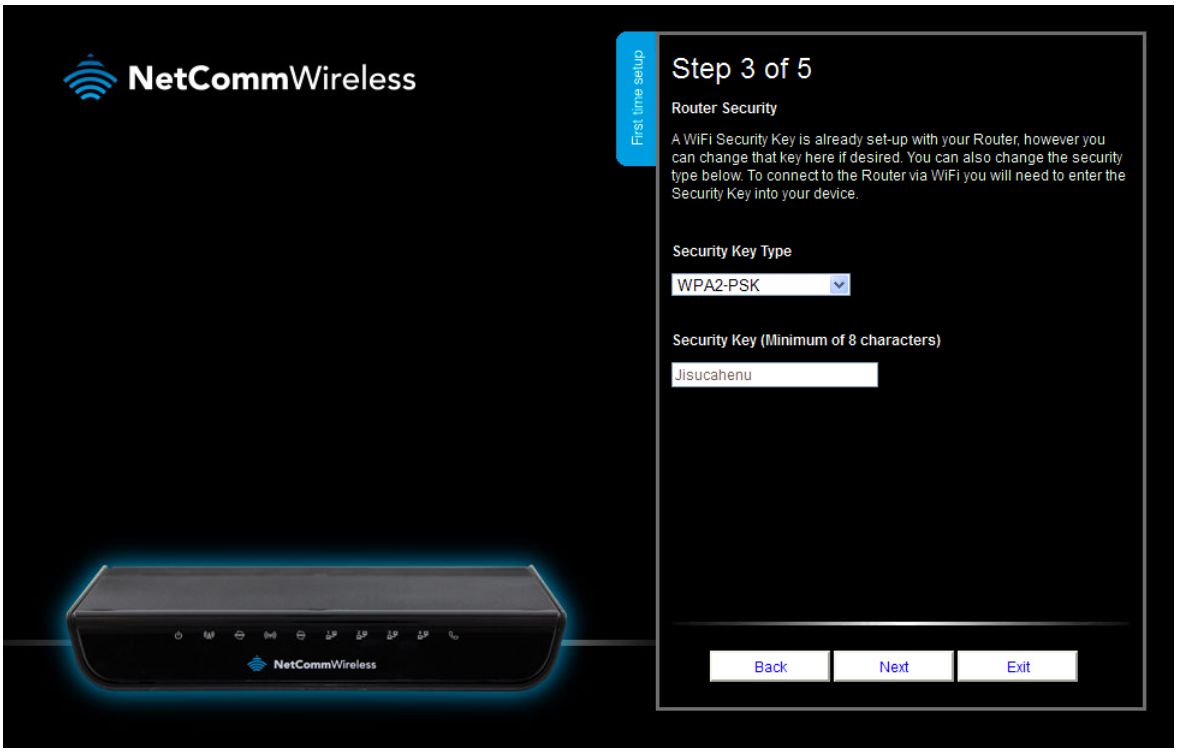
Click **Next** when you have entered the required details.

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

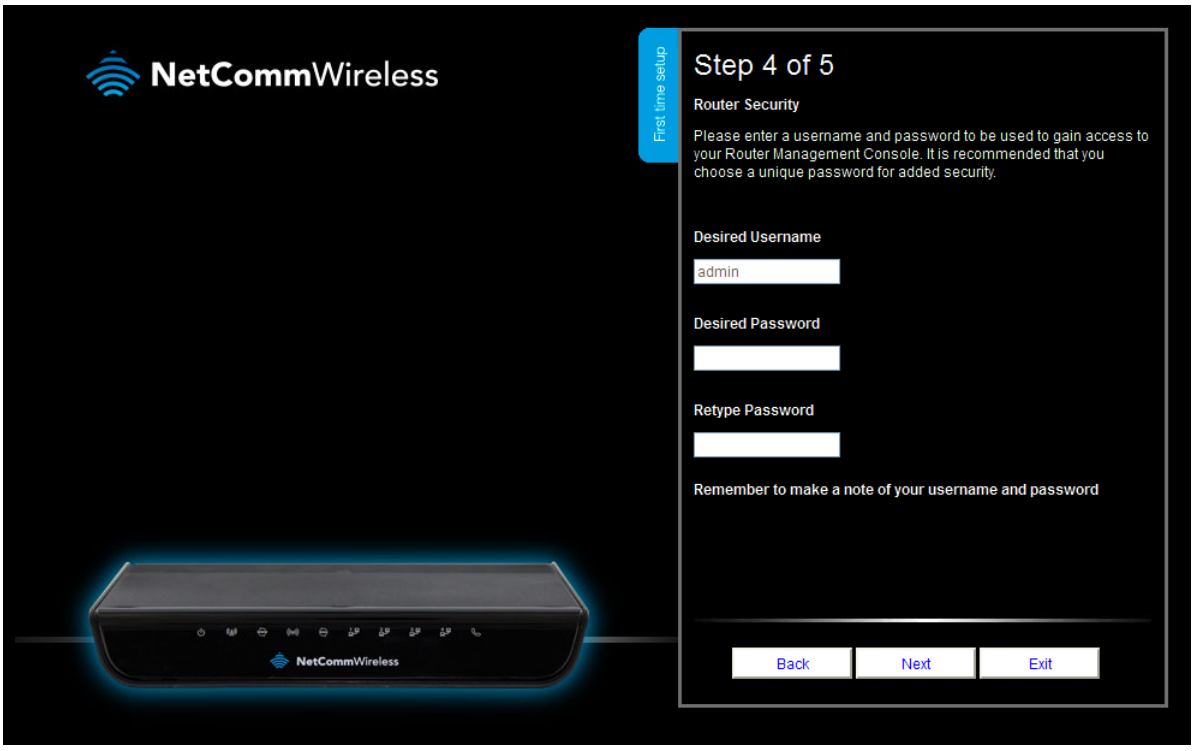
   (If you wish to use the default settings, click **Next**)



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



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



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

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

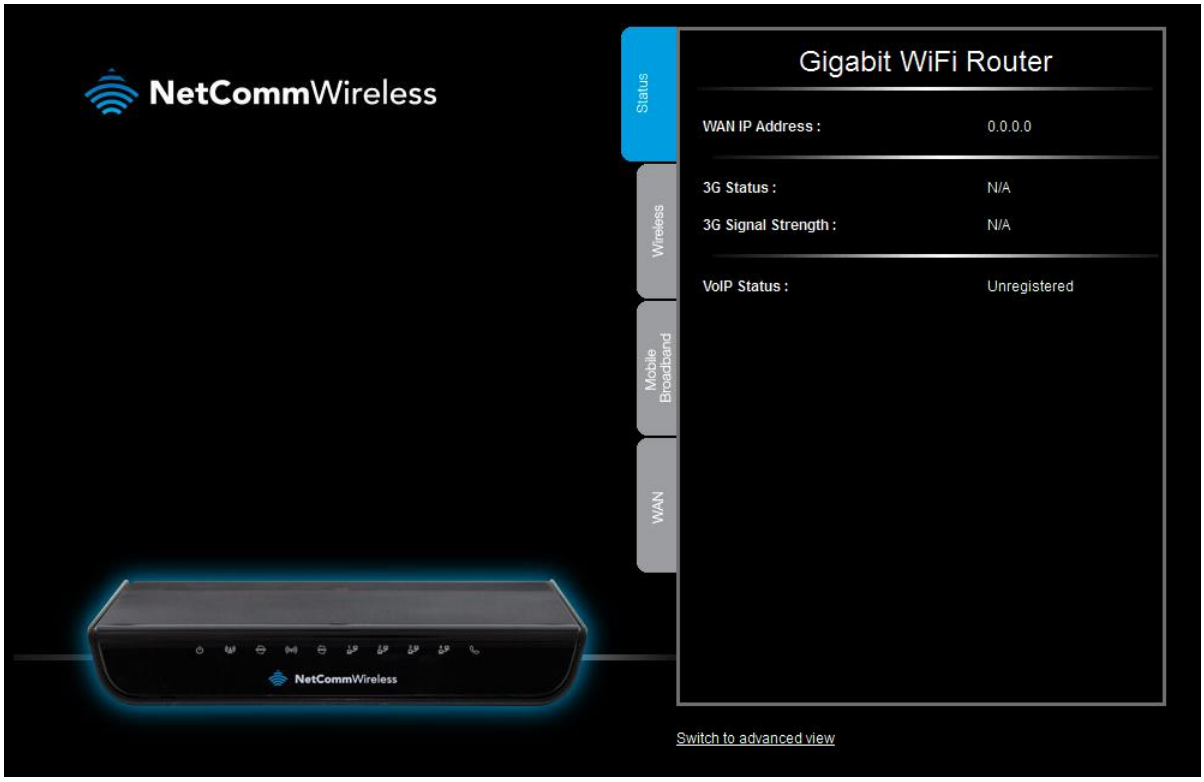
Basic View

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

Status

The Status tab displays the following information:

- The current WAN IP Address
- 3G Status
- 3G Signal Strength
- VoIP Status



Wireless

The wireless tab displays the following options:

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

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

Mobile Broadband

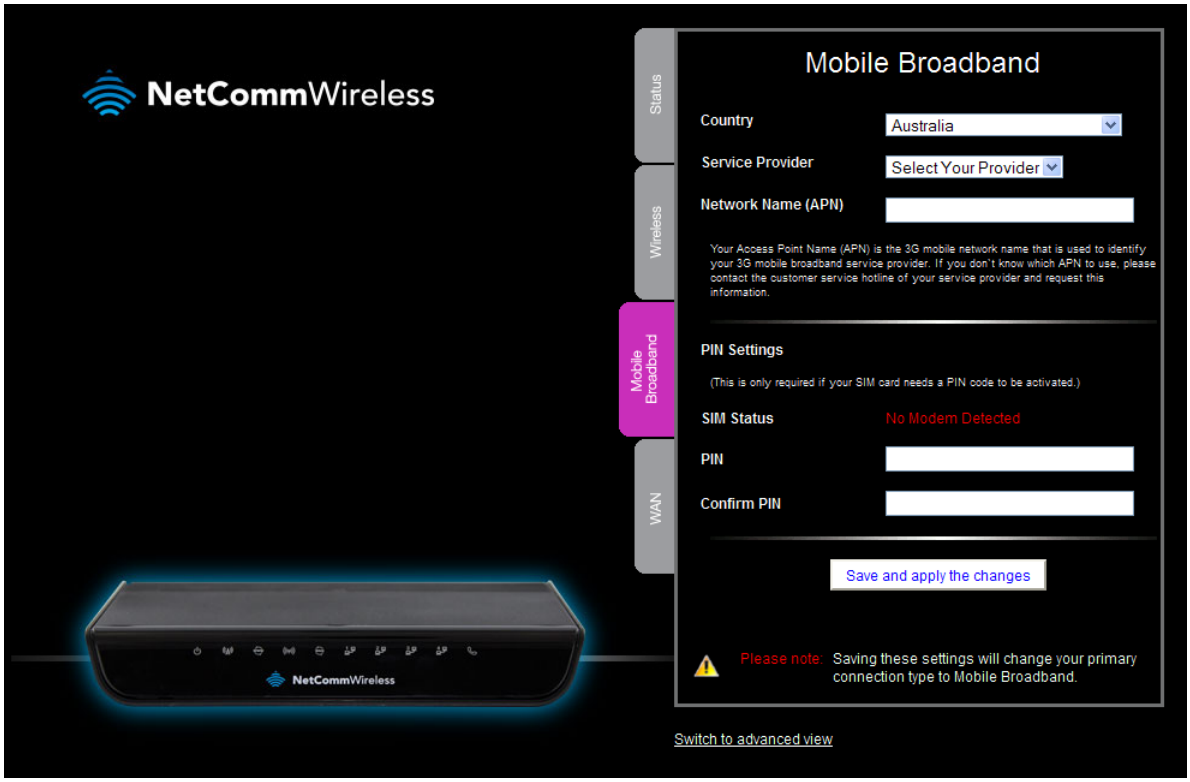
The following configuration options are available on the Mobile Broadband tab:

- Country
- Service Provider
- Network Name (APN)
- SIM Status
- PIN
- Confirm PIN

To configure your 3G/4G (Mobile Broadband) connection, select the applicable Country and Service Provider. The Network Name (APN) should be automatically filled with the correct APN. Please verify this with the information supplied by your 3G/4G provider.

The SIM Status will show if a PIN is required to use your SIM. If it is, enter the SIM PIN into the **PIN** and **Confirm PIN** fields.

If you make any changes to the 3G configuration, click the **Save and apply the changes** button to make these changes active.



Note: Saving any configuration changes on this page will make the Mobile Broadband connection the primary method of connecting to the Internet and disable other connection types.

WAN

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

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

The NF5 includes a failover feature whereby the router will automatically switch to the 3G/4G connection if the WAN connection should fail. To use this feature, select the **Enable Automatic 3G backup** option.

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

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

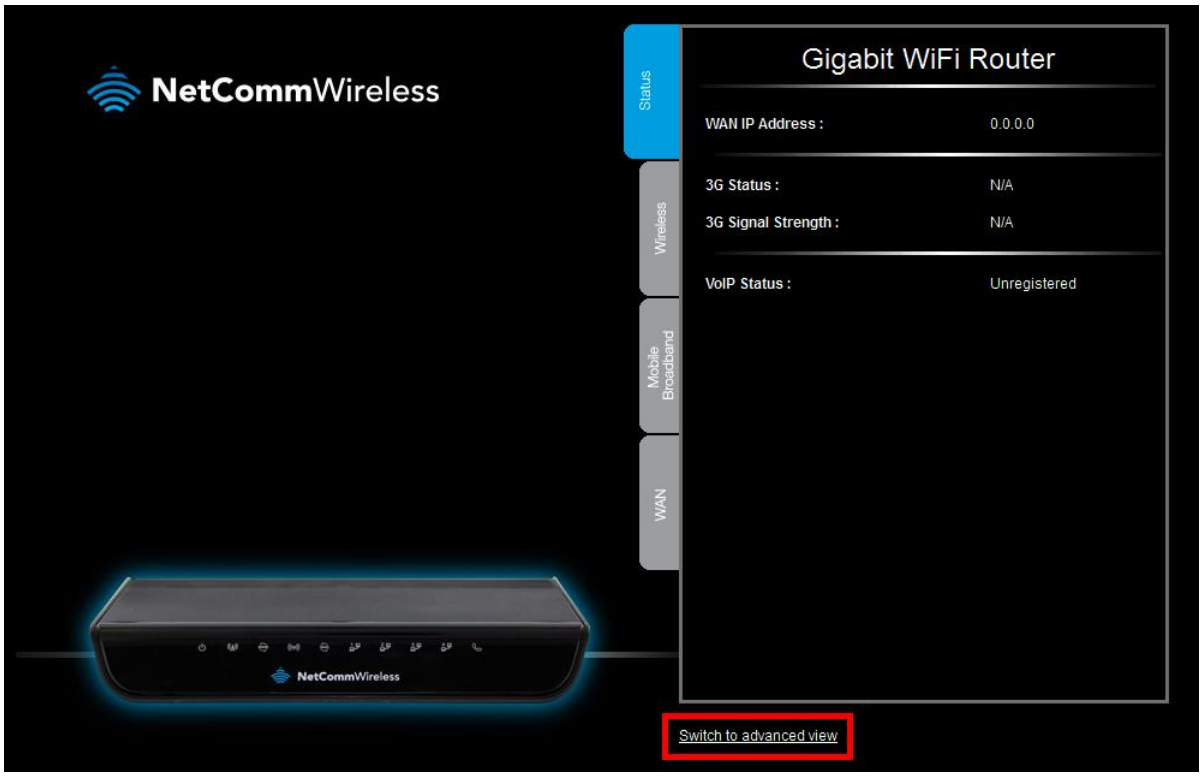
Advanced Configuration

To access the advanced configuration options of your NF5, you need to log in to the web configuration and change to Advanced view.

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

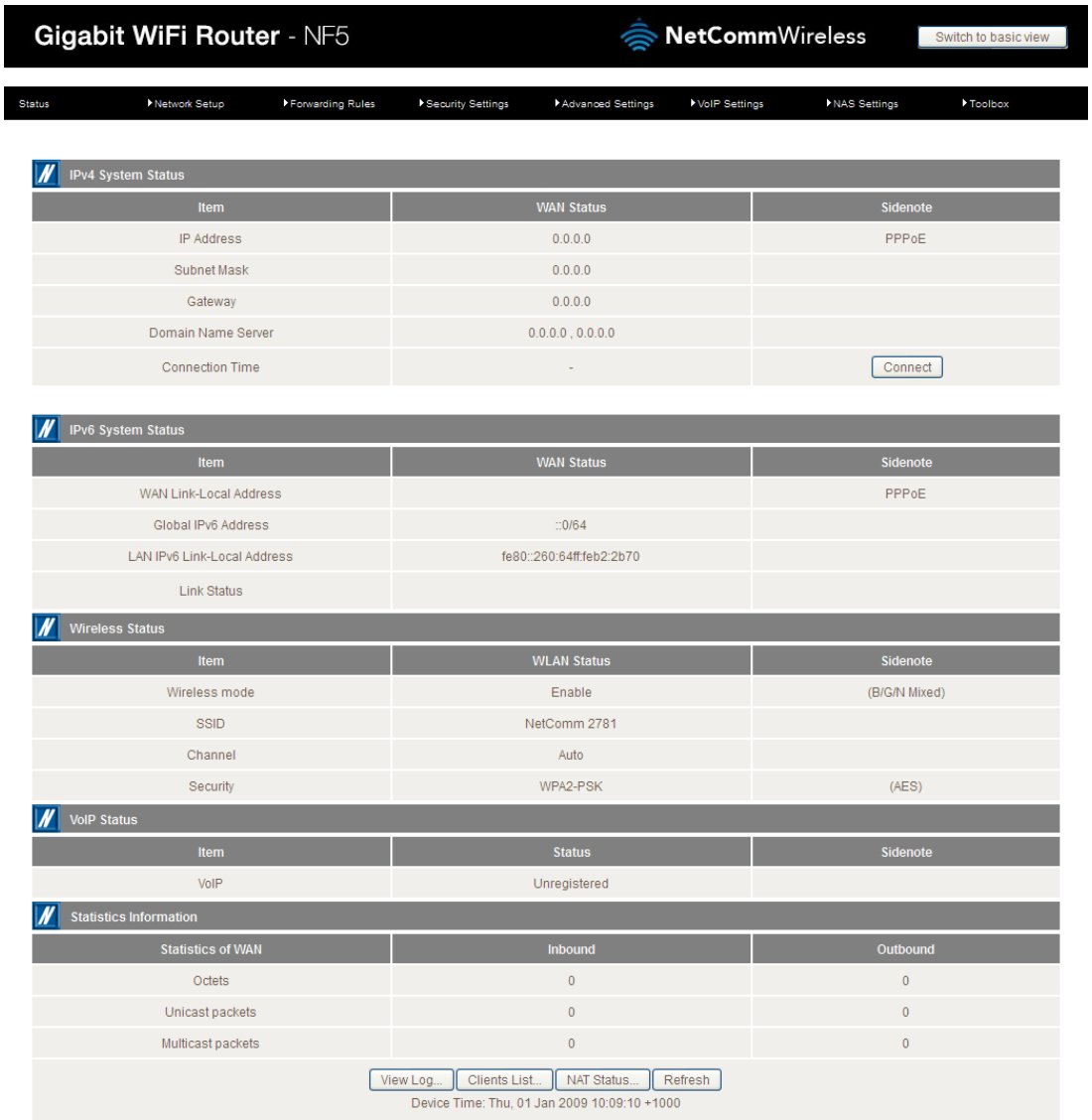
At the login screen, type **admin** in the Username and Password field and click the Login button.

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



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

Status



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

Network Setup

Network Setup

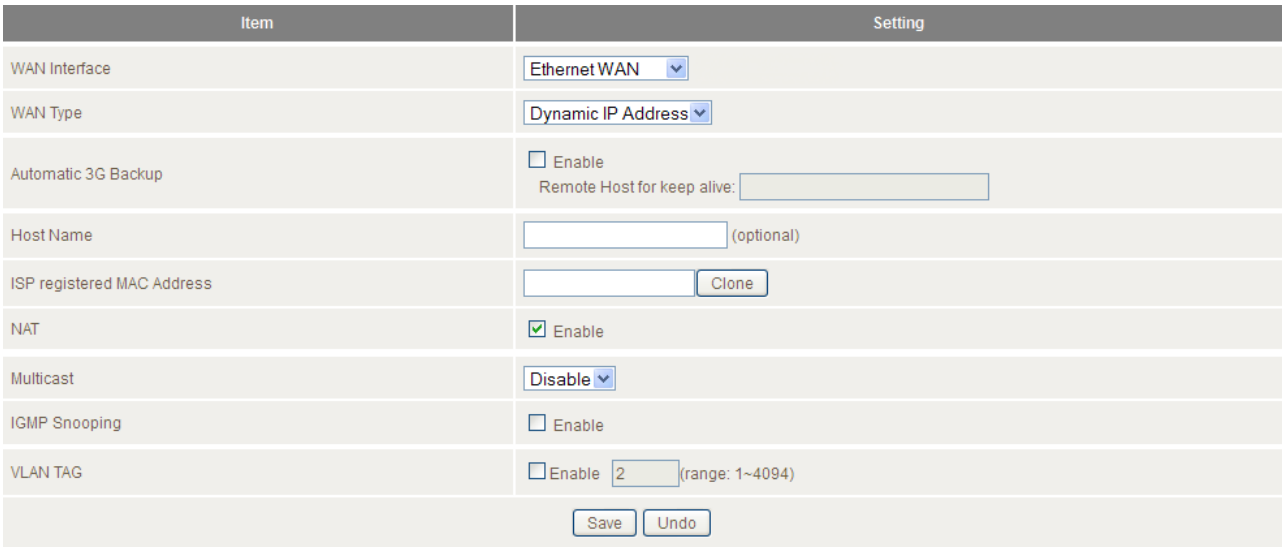
This page allows you to configure the Ethernet WAN (Wide Area Network) connection settings on the NF5.

Ethernet WAN

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

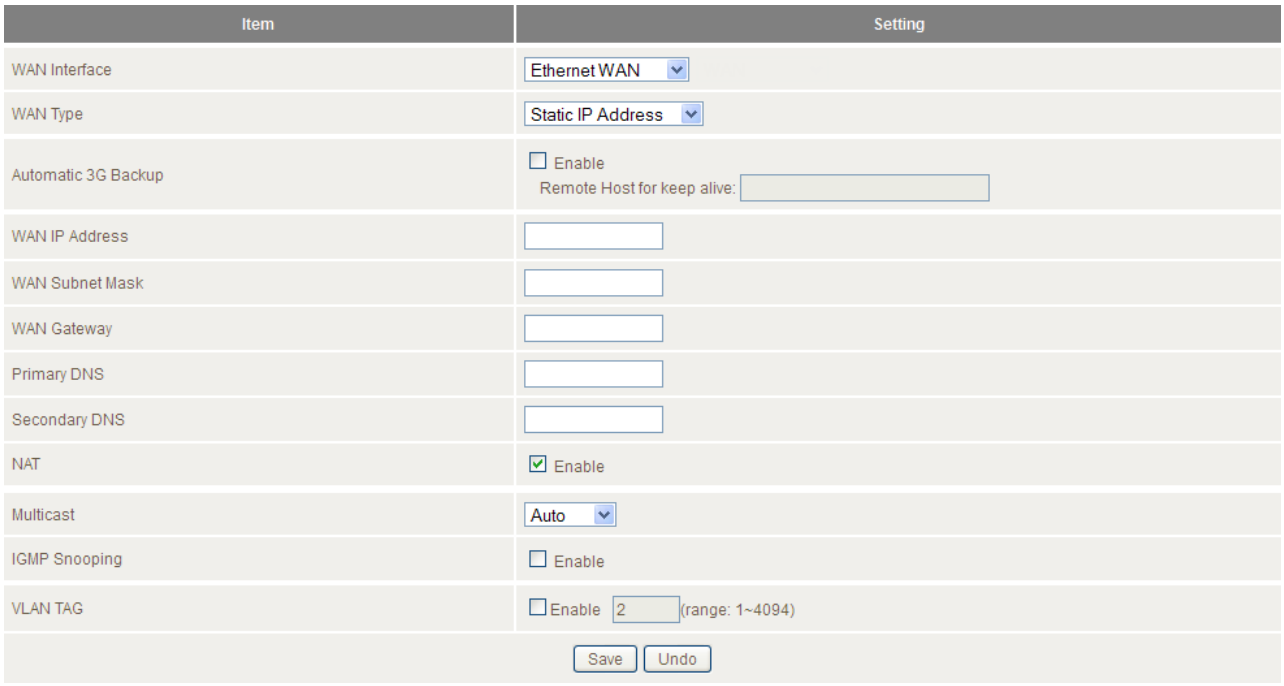
- Dynamic IP
- Static IP
- PPP over Ethernet
- PPTP
- L2TP

Dynamic IP Address



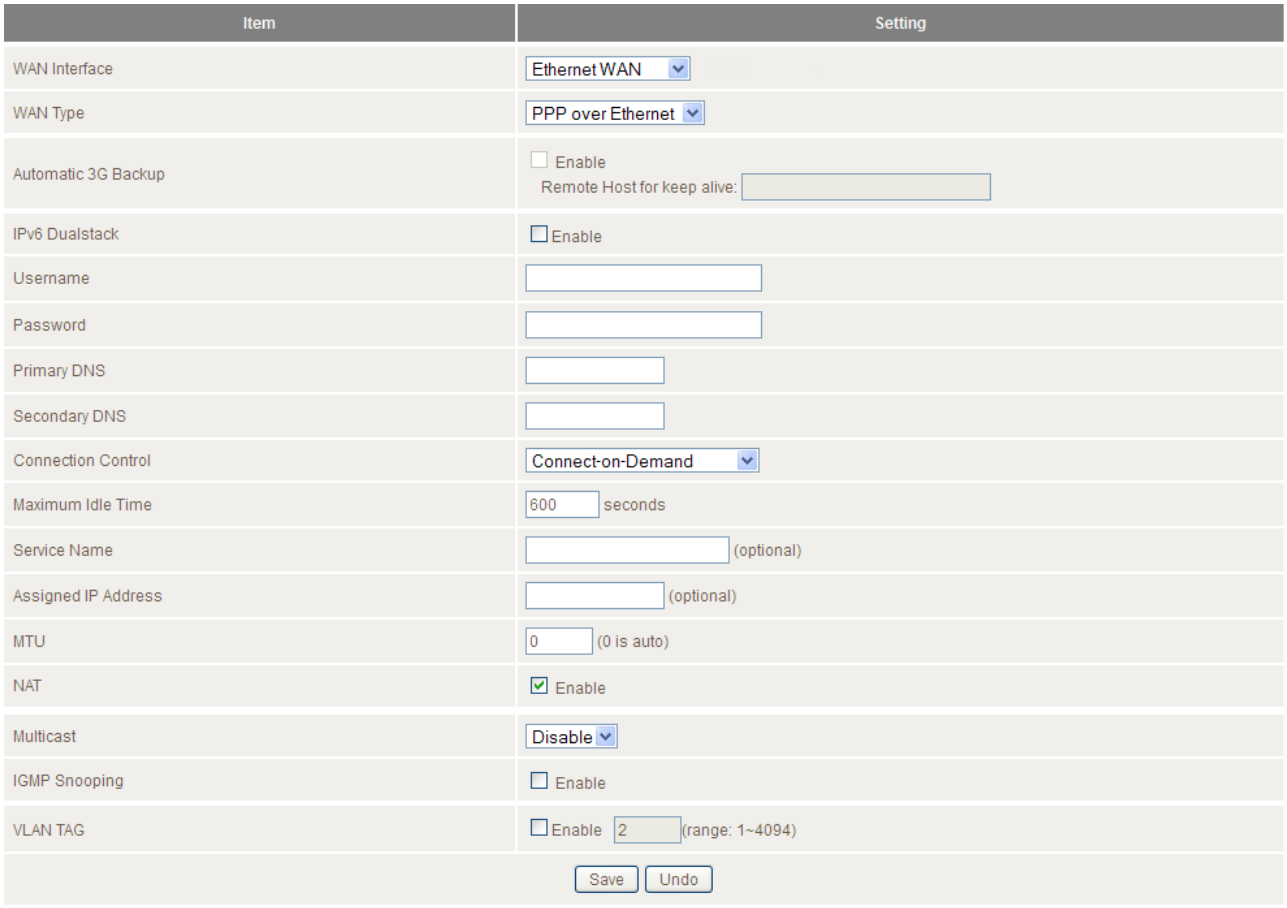
OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Automatic 3G Backup	Select this option to use the 3G/4G connection as a backup to the WAN connection. When you select this option, you must specify a domain name or IP address which the router will ping in order to check the status of the WAN connection. When this ping test fails, the router will switch to the 3G connection to ensure an internet connection is always available.
Host Name	Set the hostname for your connection *(Optional - Refer to your ISP for more information).*
ISP Registered MAC Address	You can change the WAN port MAC address if needed to clone your 3G modem *(Optional - Refer to your ISP for more information).*
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

Static IP Address



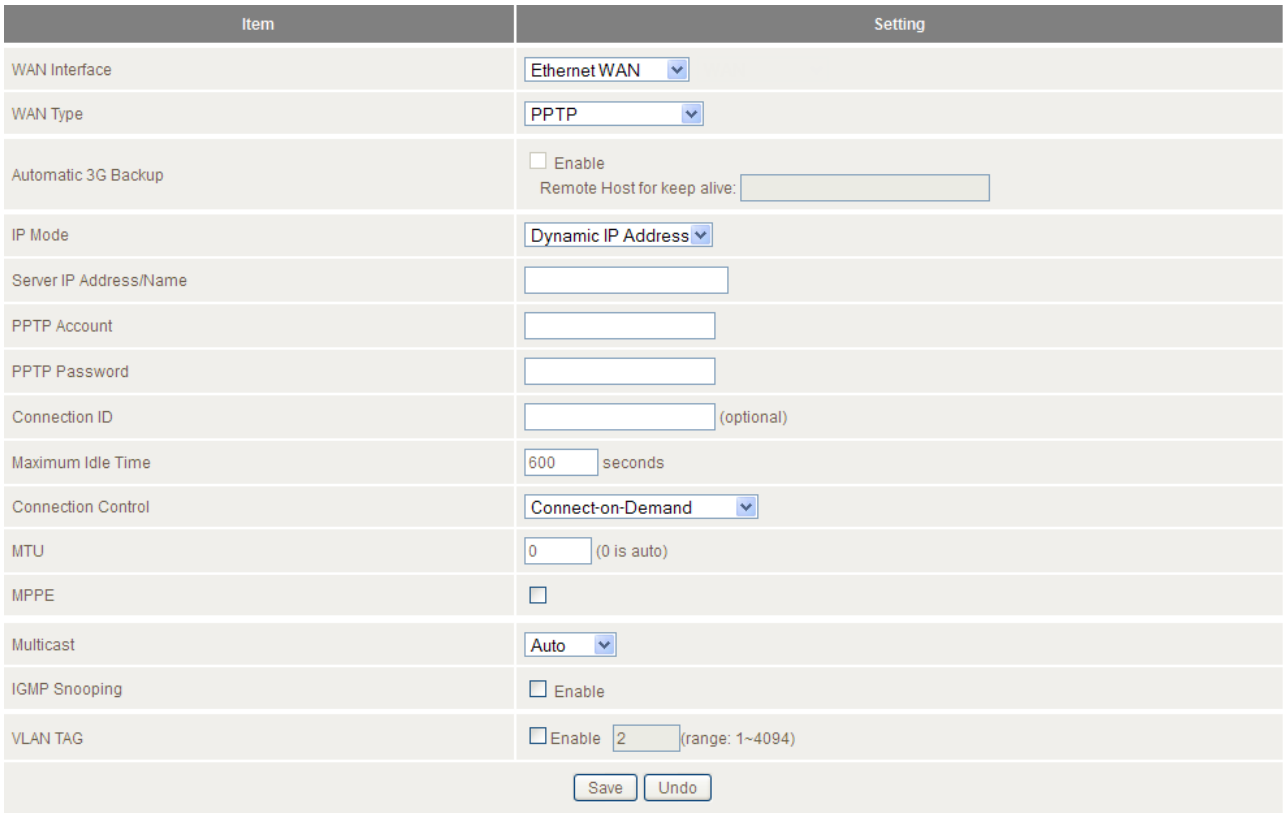
OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Automatic 3G Backup	Select this option to use the 3G/4G connection as a backup to the WAN connection. When you select this option, you must specify a domain name or IP address which the router will ping in order to check the status of the WAN connection. When this ping test fails, the router will switch to the 3G connection to ensure an internet connection is always available.
WAN IP Address	The static IP address assigned to you by your internet service provider.
WAN Subnet Mask	The subnet mask of the IP address assigned to you by your internet service provider.
WAN Gateway	The WAN Gateway provided to you by your internet service provider.
Primary DNS	This feature allows you to manually assign a Primary DNS Server *(Optional - Refer to your ISP for more information).*
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(Optional - Refer to your ISP for more information).*
NAT	This option enables or disables "Network Address Translation" for this connection type.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

PPP over Ethernet



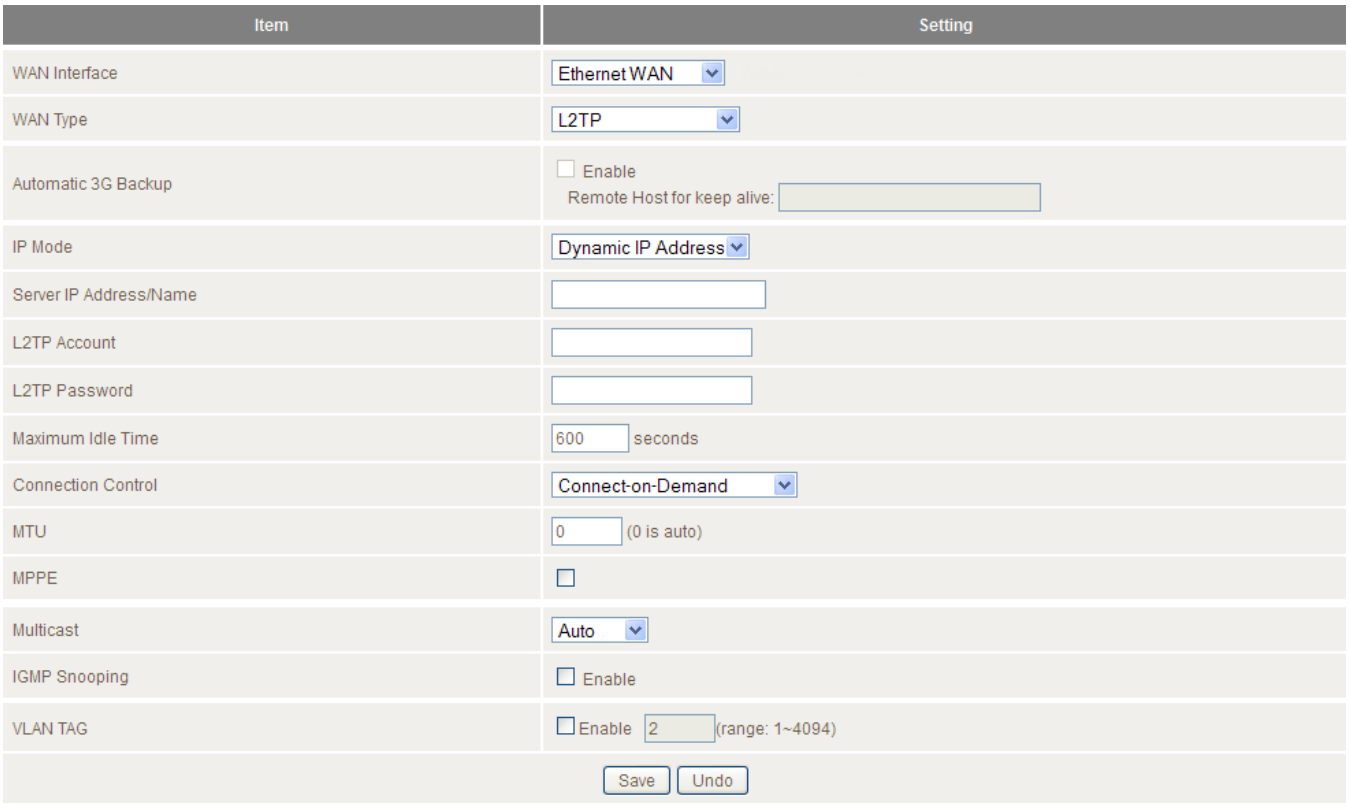
OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Automatic 3G Backup	Select this option to use the 3G/4G connection as a backup to the WAN connection. When you select this option, you must specify a domain name or IP address which the router will ping in order to check the status of the WAN connection. When this ping test fails, the router will switch to the 3G connection to ensure an internet connection is always available.
Username	The account name given to you by your ISP.
Password	The password given to you by your ISP.
Primary DNS	This feature allows you to manually assign a Primary DNS Server *(Optional - Refer to your ISP for more information).*
Secondary DNS	This feature allows you to manually assign a Secondary DNS Server *(Optional - Refer to your ISP for more information).*
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: **Connect-on-demand:** detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. **Auto-reconnect (always-on):** automatically reconnects the connection when it drops so that the internet connection is always on. **Manually**: Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Service Name	Enter the service name if your ISP requires it *(Optional - Refer to your ISP for more information).*
Assigned IP Address	Enter the IP address assigned to your service. This is usually left blank.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
NAT	This option enables or disables "Network Address Translation" for this connection type
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

PPTP



OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Automatic 3G Backup	Select this option to use the 3G/4G connection as a backup to the WAN connection. When you select this option, you must specify a domain name or IP address which the router will ping in order to check the status of the WAN connection. When this ping test fails, the router will switch to the 3G connection to ensure an internet connection is always available.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the PPTP IP Address, PPTP Subnet Mask and PPTP Default gateway in use for the connection *(Refer to your PPTP administrator for more information).*
Server IP Address/Name	Enter the PPTP server name or IP Address.
PPTP Account	Enter the PPTP username supplied by your PPTP administrator.
PPTP Password	Enter the PPTP password supplied by your PPTP administrator.
Connection ID	Enter an Optional name to identify the PPTP connection.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: **Connect-on-demand:** detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. **Auto-reconnect (always-on):** automatically reconnects the connection when it drops so that the internet connection is always on. **Manually**: Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the PPTP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

L2TP



Item	Setting
WAN Interface	Ethernet WAN
WAN Type	L2TP
Automatic 3G Backup	Enable Remote Host for keep alive:
IP Mode	Dynamic IP Address
Server IP Address/Name	
L2TP Account	
L2TP Password	
Maximum Idle Time	600 seconds
Connection Control	Connect-on-Demand
MTU	0 (0 is auto)
MPPE	
Multicast	Auto
IGMP Snooping	Enable
VLAN TAG	Enable 2 (range: 1~4094)
	Save Undo

OPTION	DEFINITION
WAN Interface	The interface to configure. When Mobile Broadband is selected, you may also configure whether the connection is active or inactive.
WAN Type	Use the drop down list to select the type of WAN connection you want to use.
Automatic 3G Backup	Select this option to use the 3G/4G connection as a backup to the WAN connection. When you select this option, you must specify a domain name or IP address which the router will ping in order to check the status of the WAN connection. When this ping test fails, the router will switch to the 3G connection to ensure an internet connection is always available.
IP Mode	Select to use either a static or dynamically assigned IP address for your connection. When selecting to utilise a static IP address, you will also need to enter the L2TP IP Address, L2TP Subnet Mask and L2TP Default gateway in use for the connection *(Refer to your PPTP administrator for more information).*
Server IP Address/Name	Enter the L2TP server name or IP Address.
L2TP Account	Enter the L2TP username supplied by your L2TP administrator.
L2TP Password	Enter the L2TP password supplied by your L2TP administrator.
Maximum Idle Time	When Connection Control is set to Connect-on-demand or Manually, the Maximum Idle Time field becomes available to allow you to specify how long the connection should be idle before it is disconnected. Enter an idle time in seconds.
Connection Control	This option allows you to select how the router should handle the Ethernet WAN connection. There are 3 options: **Connect-on-demand:** detects when a request from a machine on the local network makes a request to a remote network and establishes a connection upon receiving the request. **Auto-reconnect (always-on):** automatically reconnects the connection when it drops so that the internet connection is always on. **Manually**: Requires that you manually press the Connect button on the Status page in order to establish a broadband connection.
MTU	The default MTU value is 0 (auto). It is set automatically when you connect.
MPPE	Select to enable or disable the MPPE security extensions for the L2TP connection.
Multicast	Allows you to select the method of multicast or disable it.
IGMP Snooping	Allows you to enable or disable IGMP Snooping. IGMP Snooping configures the router to listen to IGMP conversations between hosts and routers and maintain a map of the links that need IP multicast streams.
VLAN TAG	VLAN tagging is primarily used in virtual networks which span over multiple switches. VLAN tagging involves the router inserting a VLAN ID into a packet header in order to identify which CLAN the packet belongs to. You may enable VLAN tagging and specify the ID with a value between 1 and 4094.

DHCP Server

This page allows you to change the Dynamic Host Configuration Protocol (DHCP) server settings on the NF5. The DHCP Server enables computers or devices connecting to the NF5 to automatically obtain their network configuration settings. By default, the DHCP server is enabled.

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

Item	Setting
DHCP Server	DHCP ○ Disable ◉ Enable
LAN IP Address	192.168.20.1
Subnet Mask	255.255.255.0
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	
Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
Gateway	(optional)
Save Undo Clients List... Fixed Mapping...	

OPTION	DEFINITION
DHCP Server	Enable or disable the DHCP server.
LAN IP Address	The local IP address of the NF5. *(The computers on your network must use this IP address as their Default Gateway. You can change it if necessary.)*
Subnet Mask	Enter the subnet mask for use on the local network. This would usually be set to 255.255.255.0.
IP Pool Starting/Ending Address	Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool
Lease Time	Length of the DHCP lease time
Domain Name	Optional, this information will be passed to the client
Primary DNS	Optional, this information will be passed to the client
Secondary DNS	Optional, this information will be passed to the client
Primary WINS	Optional, this information will be passed to the client
Secondary WINS	Optional, this information will be passed to the client
Gateway	Optional, this information will be passed to the client

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

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

DHCP Client LIst

This is the list of currently connected devices using DHCP.

IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.20.100	computer_name	00-40-F4-CE-FA-1E	Wired	23:34:40	☐

Delete | Back | Refresh | Fixed Mapping

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

DHCP Fixed Mapping

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

DHCP clients -- select one -- | Copy to | ID --

ID	MAC Address	IP Address	Enable
1	00:40:F4:CE:FA:1E	192.168.20.100	☑
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐

<< Previous | Next >> | Save | Undo | Back

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

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

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

Wireless

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

Item	Setting
Wireless Module	Enable Disable
Network ID(SSID)	NetComm 2781
SSID Broadcast	Enable Disable
Channel	Auto
Wireless Mode	B/G/N mixed
Authentication	Open
802.1X	Enable Disable
Encryption	None
	Save Undo WDS Setting... WPS Setup... Wireless Client List...

OPTION	DEFINITION
Wireless Module	Select to enable or disable the 2.4GHz Wireless network function of the NF5.
Network ID (SSID)	Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this product and other Access Points that have the same Network ID. *(Please refer to the included Wireless Security Card insert for your default SSID)*
SSID Broadcast	The router will broadcast the SSID so that wireless clients can find the wireless network.
Channel	The wireless radio channel in use by your network.
Wireless Mode	Choose B/G Mixed, B only, G only, and N only, G/N Mixed or B/G/N mixed. *(The factory default setting is B/G/N mixed)*
Authentication	You may select from the following authentication types to secure your wireless network: ▪ Open ▪ Shared ▪ Auto ▪ WPA ▪ WPA-PSK ▪ WPA2 ▪ WPA2-PSK ▪ WPA/WPA2 ▪ WPA-PSK/WPA2-PSK. WPA-PSK/WPA2-PSK is a newer type of security. This type of security gives a more secure network compared to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK. Please enter the key in the "Preshare Key". The key needs to be more than 8 characters and less than 63 characters. It can be any combination of letters and numbers. (Please refer to the included Wireless Security Card insert for your default WPA-PSK2 key)
802.1X	When Authentication is set to **Open**, you can enable 802.1X which enables Extensible Authentication Protocol (EAP) over wired or wireless networks.
Encryption	Select the type of encryption for your network. These options vary depending on the type of Authentication selected.

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

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

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

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

WDS Mode

The NF5 supports the configuration of a Wireless Distribution System (WDS). WDS allows you to expand your wireless network with multiple access points. The WDS feature on the NF5 creates a wireless connection between the NF5 and other NetComm Wireless routers supporting WDS to expand the range of your network. It creates a wireless connection between itself and up to 4 other routers while also allowing wireless clients to connect to it for internet access.

To configure WDS:

1. Set the Wireless security settings as desired on router 1 and router 2. The previous page describes the various fields and options.

Note: All Wireless setting must be identical between the two routers except for the Network ID (SSID)

2. Click the **WDS Settings** button on the **Wireless** page of each router.
3. Set the **WDS** option to **Enable** for each router.
4. On router 1, enter the MAC address of the other routers to be part of the WDS network in the **Remote AP MAC** fields.

Item	Setting
WDS	Enable Disable
Remote AP MAC 1	00:60:64:65:8E:FF
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	
	Save Undo Back

5. On router 2, enter the MAC address of the other routers to be part of the WDS network in the **Remote AP MAC** fields.

Item	Setting
WDS	Enable Disable
Remote AP MAC 1	00:60:64:63:ED:1E
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	
	Save Undo Back

6. Click the **Save** button.

Forwarding Rules

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

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

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

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

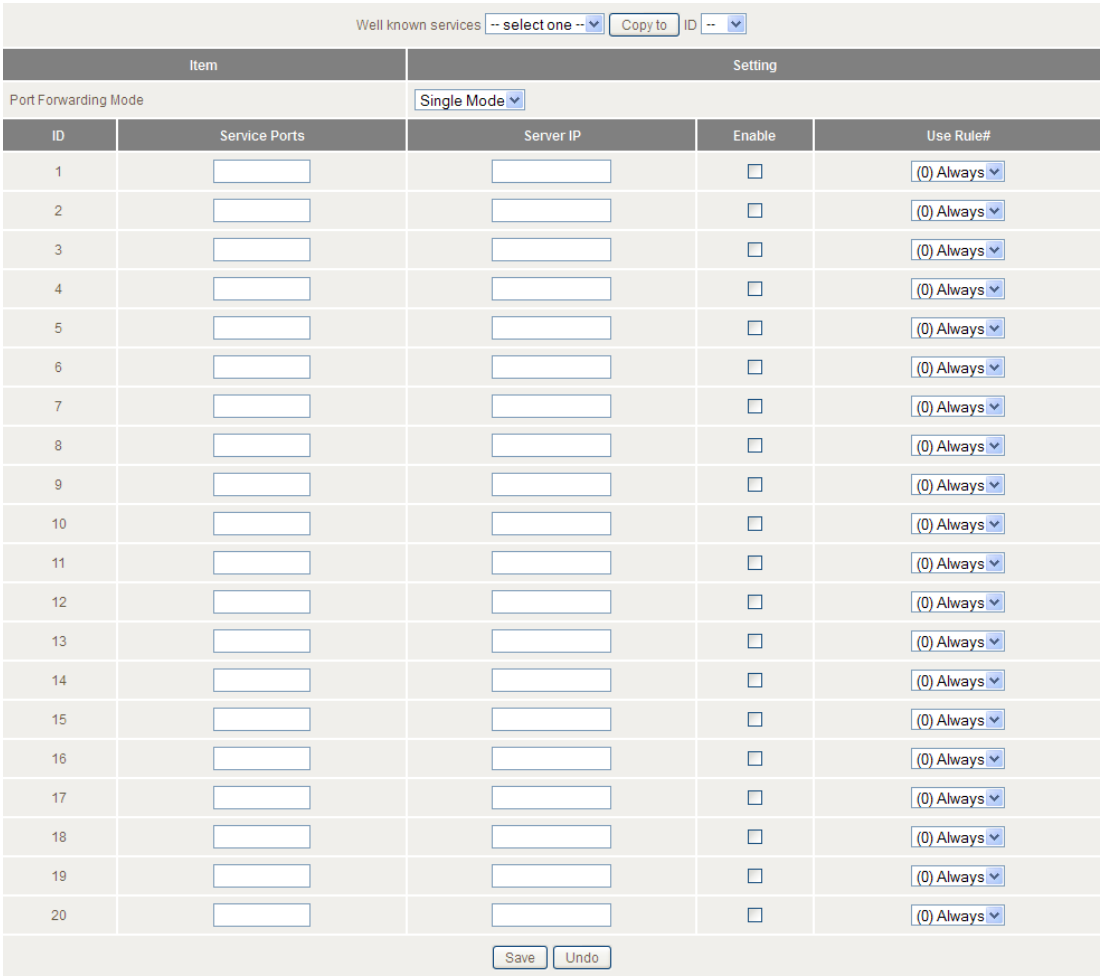
- Port Forwarding
- Port Triggering
- DMZ Host

Port Forwarding

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

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

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



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

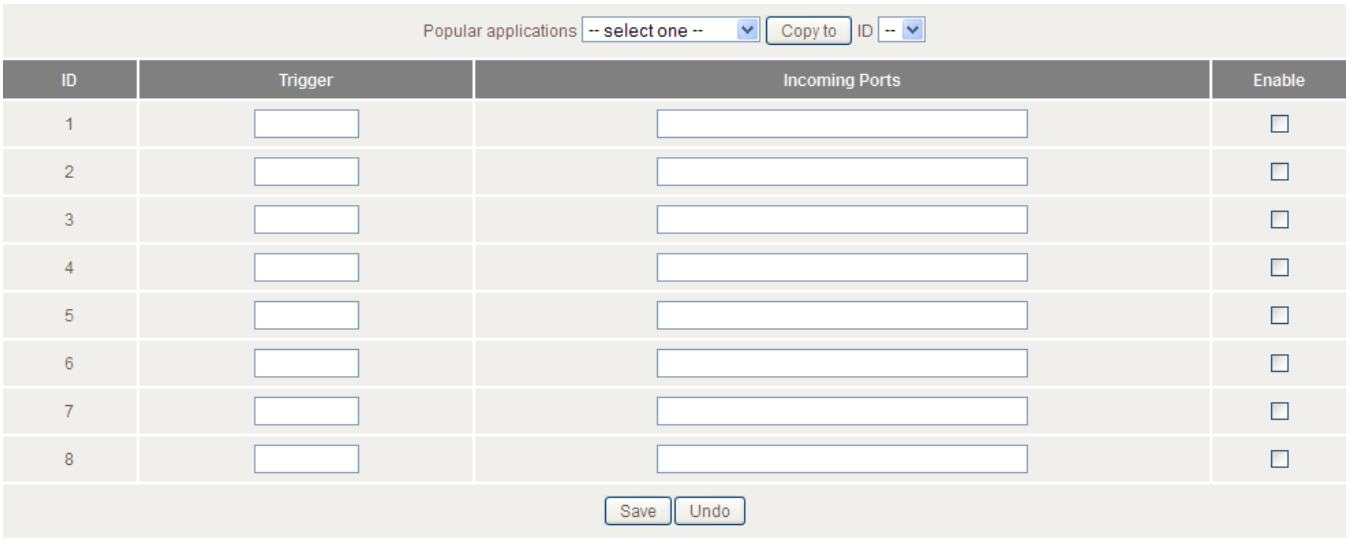
Note: At any given time, only one IP address can be bound to a particular Service Port.

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

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

Port Triggering

Some applications like online games, video conferencing and Internet telephony require multiple connections to the internet. As such, these applications cannot work with a pure NAT router such as the NF5.



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

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

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

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

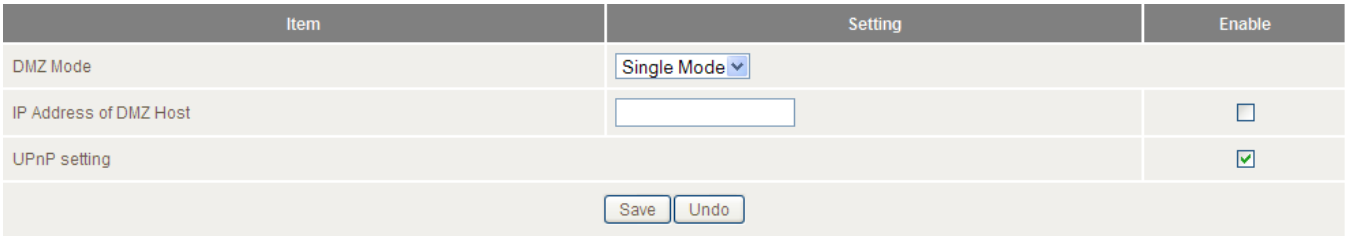
The NF5 also provides predefined settings for some popular applications.

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

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

Miscellaneous

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



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

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

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

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

Security Settings

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

Status

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

Item	Status		
Outbound Filter	Disable		
Local Client	Only Deny Remote Host	Service	Working Time

Item	Status		
Inbound Filter	Disable		
Remote Host	Deny Remote Host to access	Service	Working Time

Item	Status
Domain Filter	Disable
Domain	Access
All other Domains	Yes

Refresh

Packet Filters

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

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

Outbound Filter:

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

Item	Setting
Outbound Packet Filter	☐ Enable
◉ Allow all data through the router except data that matches the specified rules. ○ Deny all data through the router except data that matches the specified rules.	

ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	☐	(0) Always
2		:	☐	(0) Always
3		:	☐	(0) Always
4		:	☐	(0) Always
5		:	☐	(0) Always
6		:	☐	(0) Always
7		:	☐	(0) Always
8		:	☐	(0) Always

First page | Previous page | Next page | Last page | Save | Undo | Inbound Filter... | MAC Level...

There are two types of filtering policies:

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

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

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

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

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

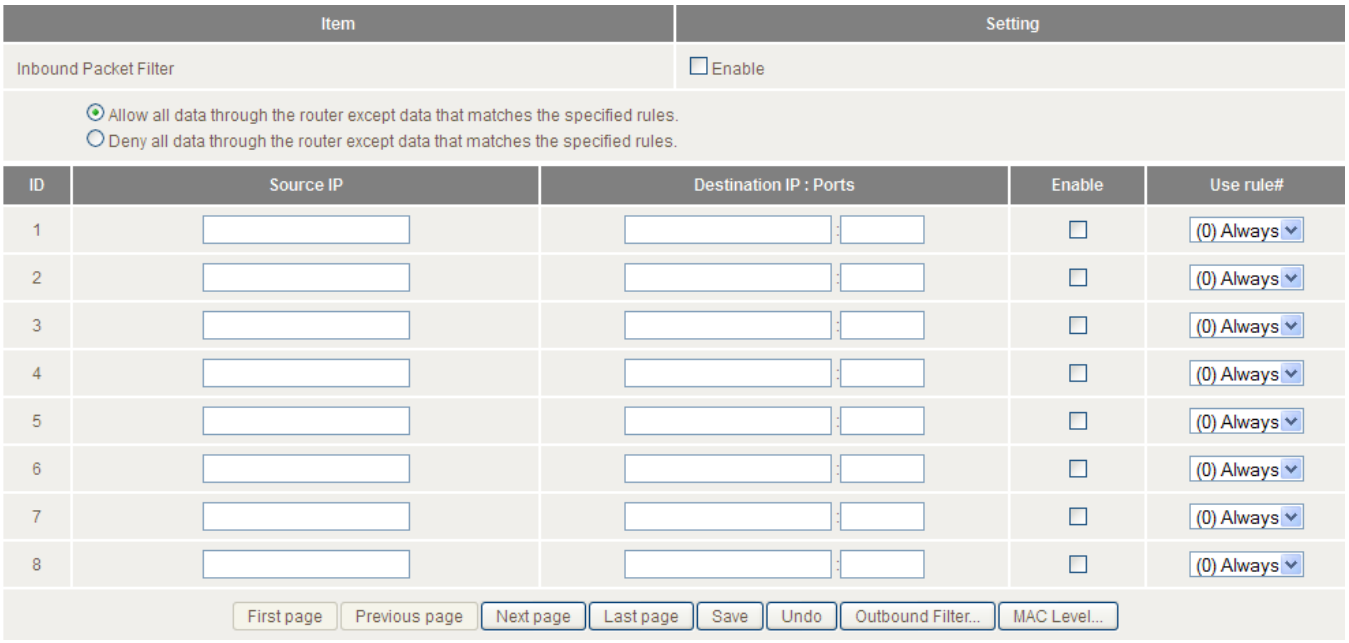
The Packet Filter also works with Scheduling Rules, and gives you more flexibility on Access control.

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

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

Inbound Filter

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

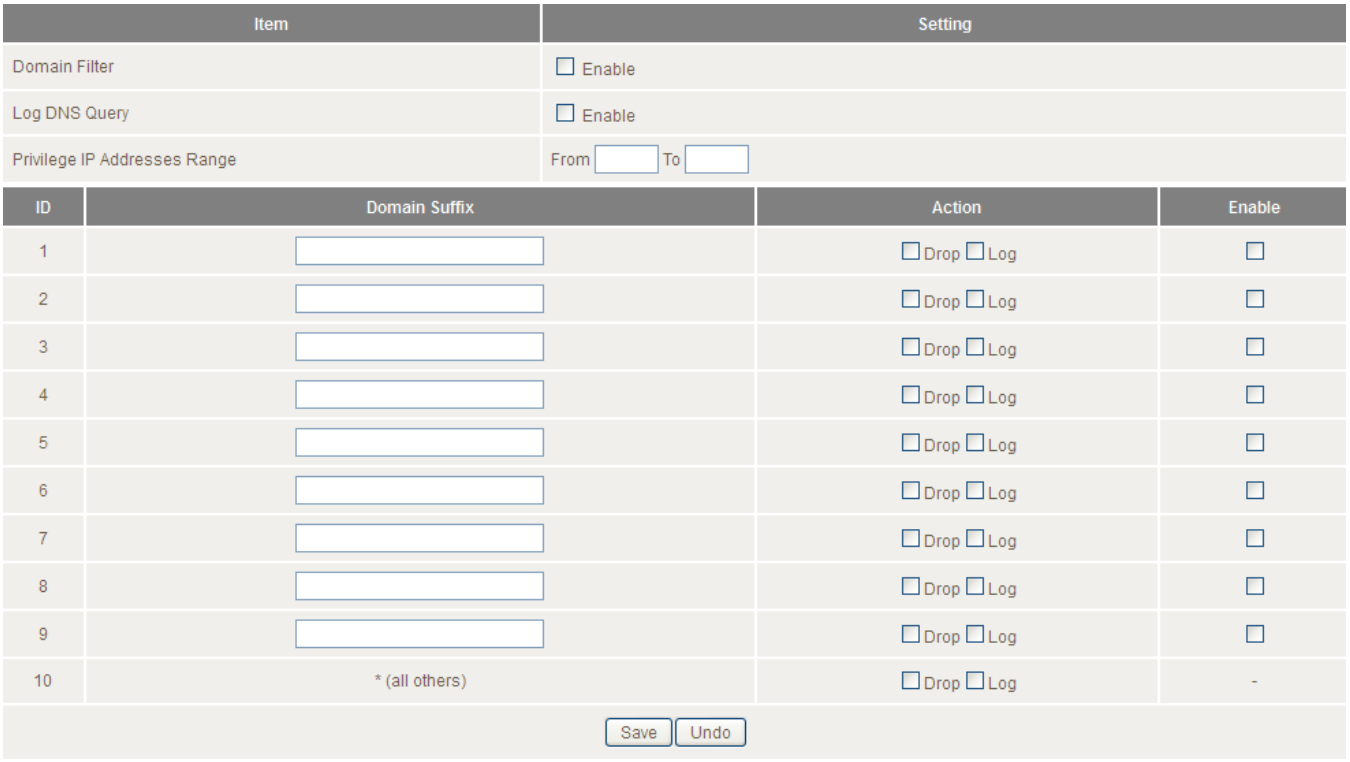


Click **Save** to save the settings or **Undo** to cancel.

Domain Filters

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

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



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

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

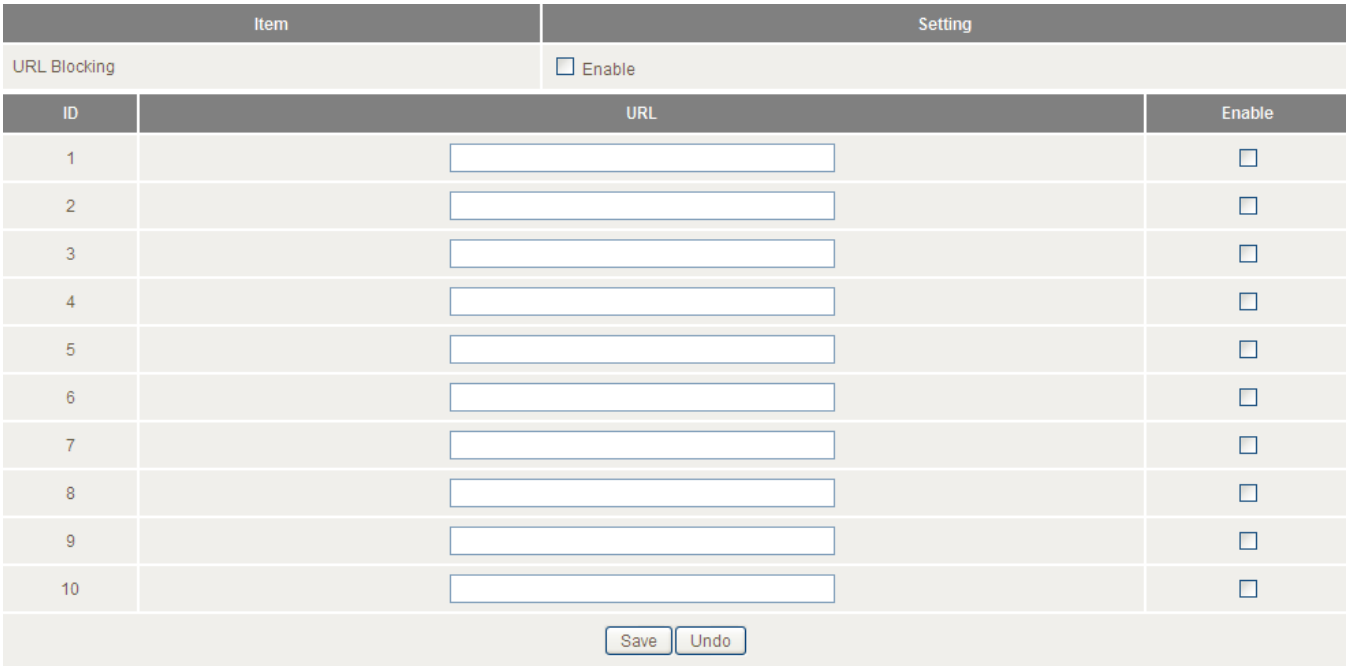
OPTION	DEFINITION
Domain Suffix	Please type the suffix of the URL that needs to be restricted. For example, ".com", "xxx. com".
Action	The router action that you want when someone is accessing a URL that matches the specified domain suffix. Select Drop to block the access and/or select Log to log this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

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

URL Blocking

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

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



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

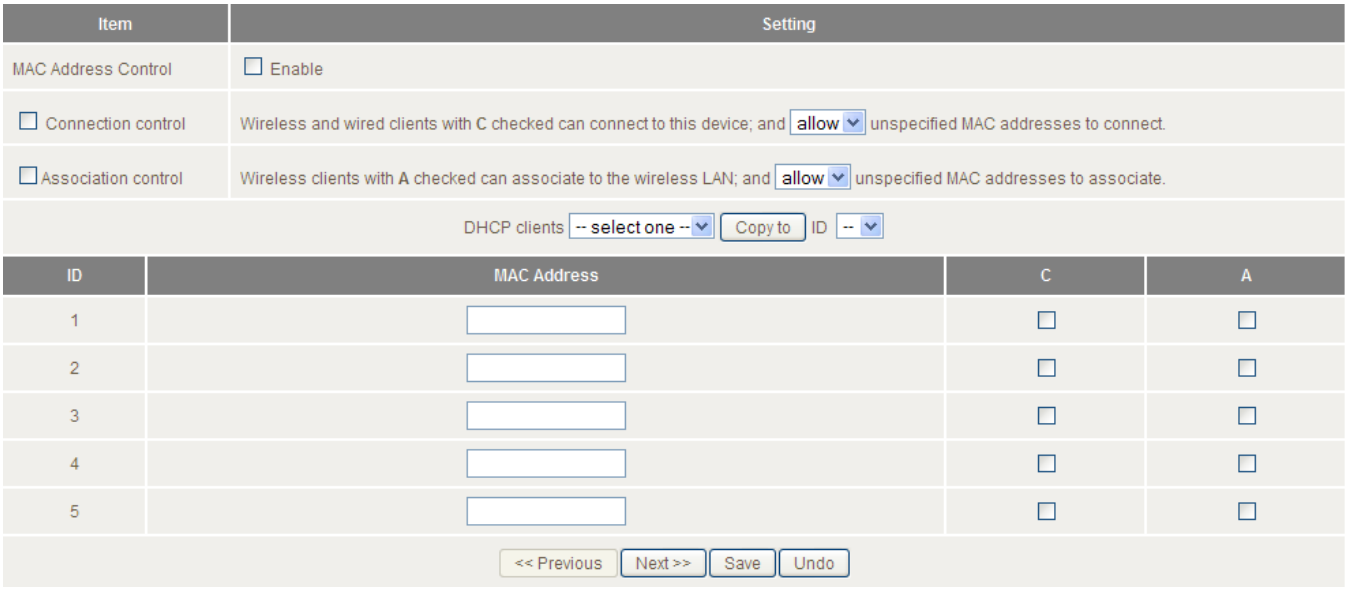
OPTION	DEFINITION
URL	If any part of the Website's URL matches the pre-defined word then the connection will be blocked. For example, you can use pre-defined word "sex" to block all websites if their URLs contain the pre-defined word "sex".
Enable	Tick to enable the rule.

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

MAC Control

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

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



Two types of MAC Control are available:

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

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

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

Miscellaneous

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

Item	Setting	Enable
Administrator Time-out	300 seconds (0 to disable)	
Remote Administration	/ :	☐
Discard PING from WAN side		☑
DoS Attack Detection		☑
Keep WAN in stealth mode		☐
	Save Undo	

OPTION	DEFINITION
Administrator Time-out	The period of time with no activity in the web configuration page to logout automatically, set this to zero to disable this feature.
Remote Administrator Host/Port	Normally only Intranet users can browse the built-in web pages to perform administration tasks. This feature enables you to perform administration tasks from a remote host. If this feature is enabled, only the specified IP address can perform remote administration.
Discard PING from WAN side	When this feature is enabled, your router will not respond to ping requests from remote hosts.
DoS Attack Detection	When this feature is enabled, the router will detect and log where the DoS attack comes from on the Internet.

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

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

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

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

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

Advanced Settings

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

Status

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

Item	Status
System Time	Thu, 01 Jan 2009 14:05:16 +1000

Item	Status
DDNS	Disable
Provider	-

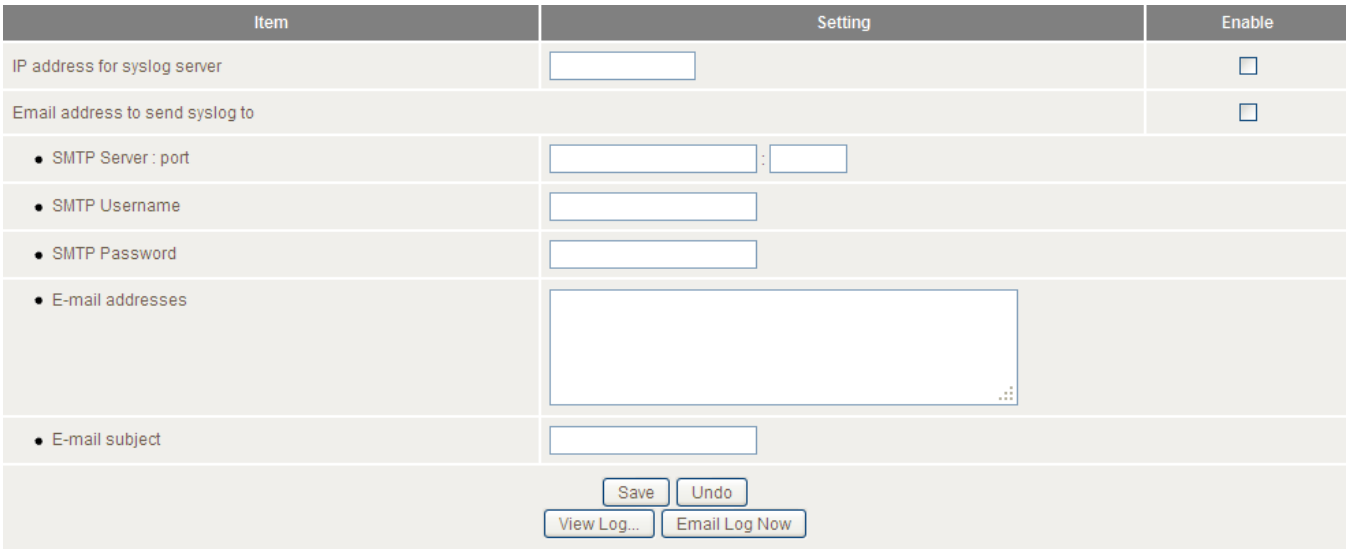
Item	Status		
Dynamic Routing	Disable		
Static Routing	Disable		
Destination	Subnet Mask	Gateway	Hop

Item	Status			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time

Refresh

System Log

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



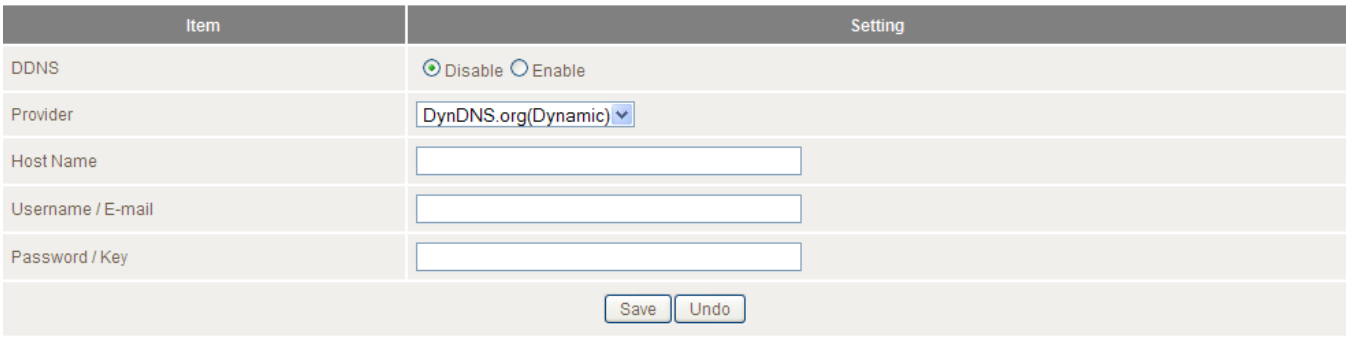
OPTION	DEFINITION
IP Address for remote System Logs (syslog)	The IP address of the syslog server where the system log data will be sent. Click the "Enable" checkbox to enable this function.
Email address to send syslog to	Click the “Enable” checkbox to enable this function.
SMTP Server : port	Enter the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

Dynamic DNS

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

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

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



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

- Host Name
- Username/Email
- Password/Key

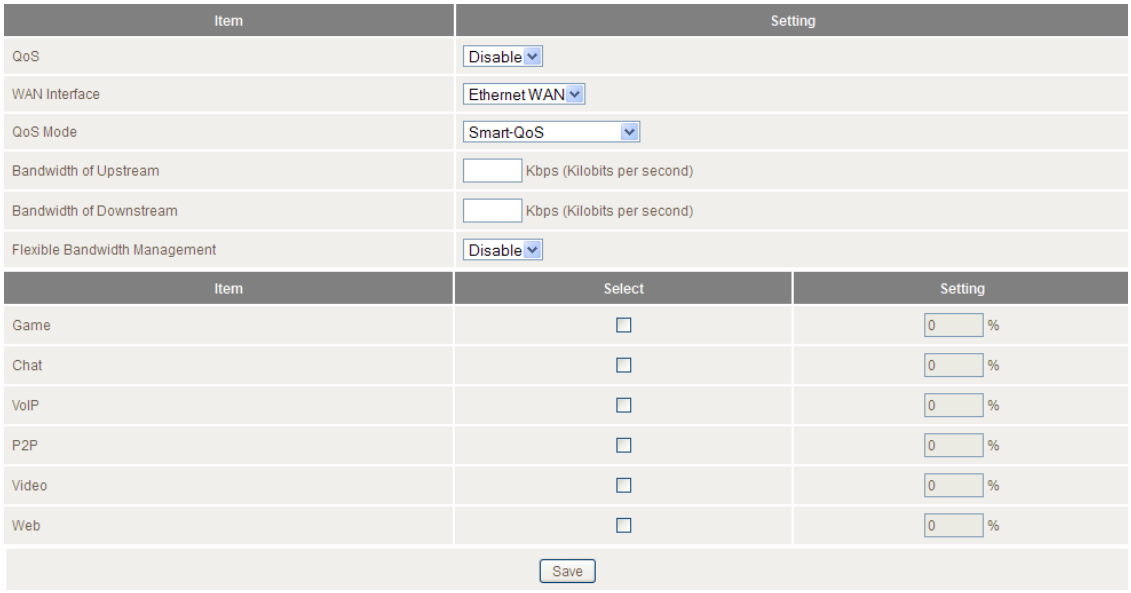
To enable the Dynamic DNS feature on the unit, select the **Enable** option, choose the appropriate Dynamic DNS Provider and enter the details supplied by your Dynamic DNS provider.

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

QoS

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

As part of a strategy to provide Quality of Service, the NF5 supports Type of Service (ToS), the Differentiated Services (DiffServ) architecture and IEEE P802.1p priority tags (specified in the IEEE 802.1Q standard). DiffServ is a mechanism for classifying and managing network traffic by marking each packet on the network with a Differentiated Services Code Point (DSCP) which is a field in an IP packet used for classification purposes and operates at the IP layer. The NF5 also supports 802.1p priority tags which operate at the media access control (MAC) level. ToS, like DSCP, is a field in the header of IP packets that marks packets with different types of service such as minimize delay, maximize throughput, maximize reliability, minimize cost or normal service.



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

Basic QoS configuration

To configure QoS:

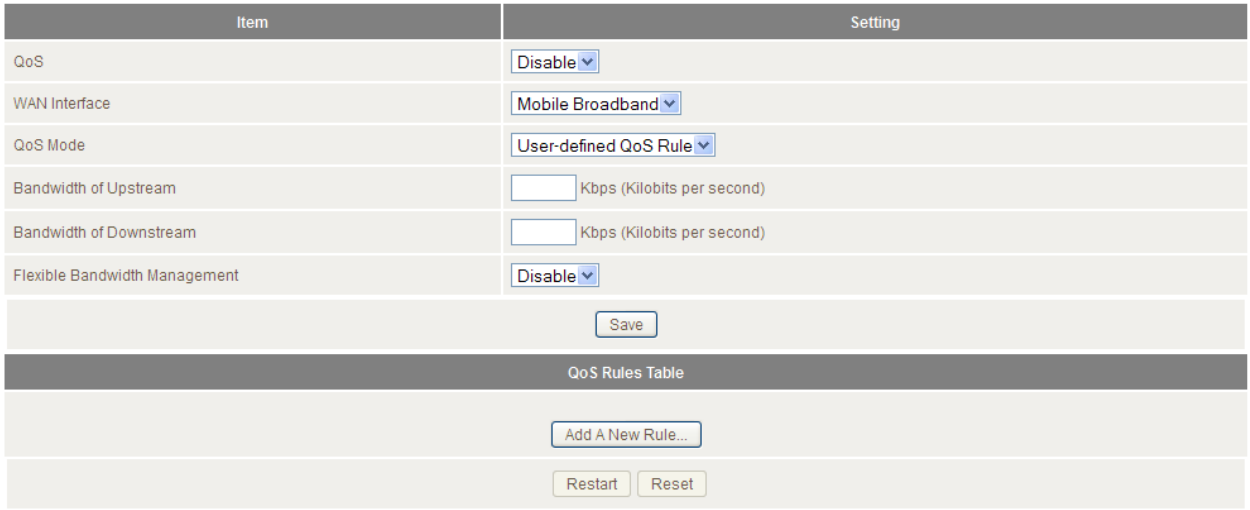
1. Set the **QoS** item to **Enable.**
2. The **WAN Interface** item displays the current WAN interface in use by the router and therefore to which interface the configuration applies.
3. Use the **QoS Mode** drop down list to set the QoS mode to **Smart-QoS.**
4. In the **Bandwidth of Upstream** field,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

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

Advanced QoS configuration

To configure QoS:

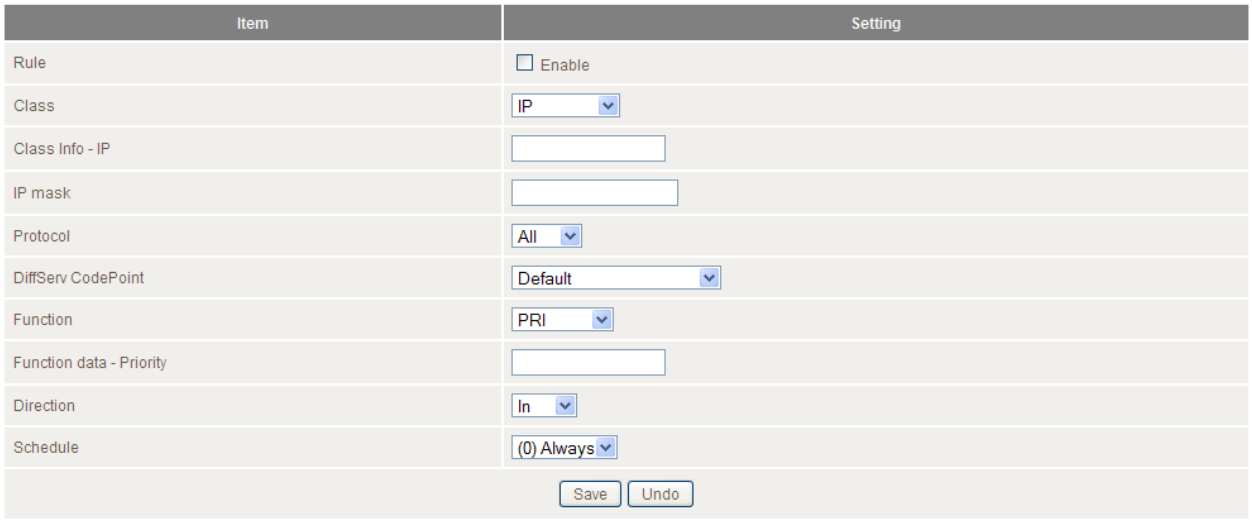
1. Set the **QoS** item to **Enable.**
2. The **WAN Interface** item displays the current WAN interface in use by the router and therefore to which interface the configuration applies.
3. Use the **QoS Mode** drop down list to select **User-defined QoS Rule** to display the QoS rules table.



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

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

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



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

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

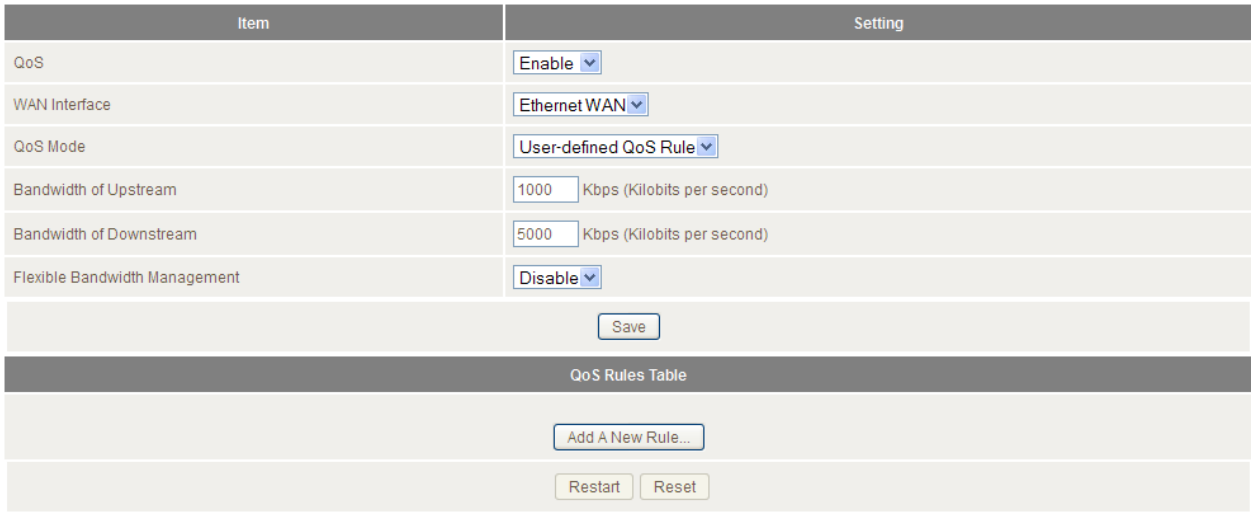
Note: For further instructions on scheduling rules, please refer to the "Scheduling" section later in this guide

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

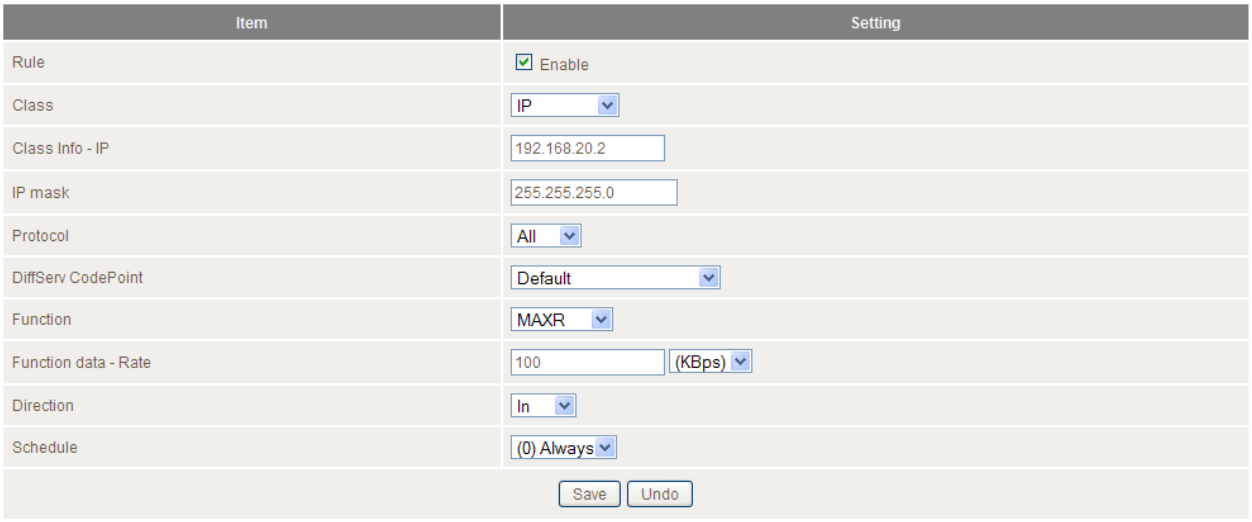
QoS configuration examples

Example 1.

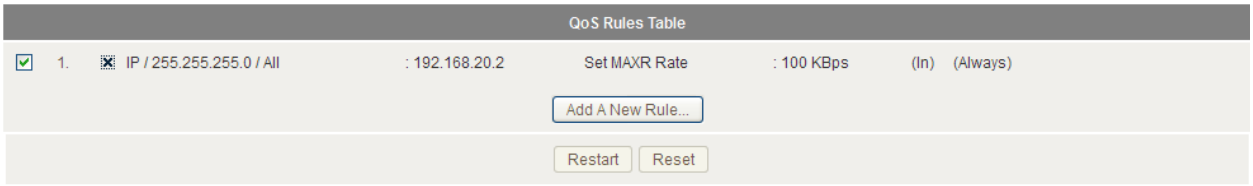
To limit downstream bandwidth on LAN port 1 (IP address 192.168.20.2) to 100 KBps:



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



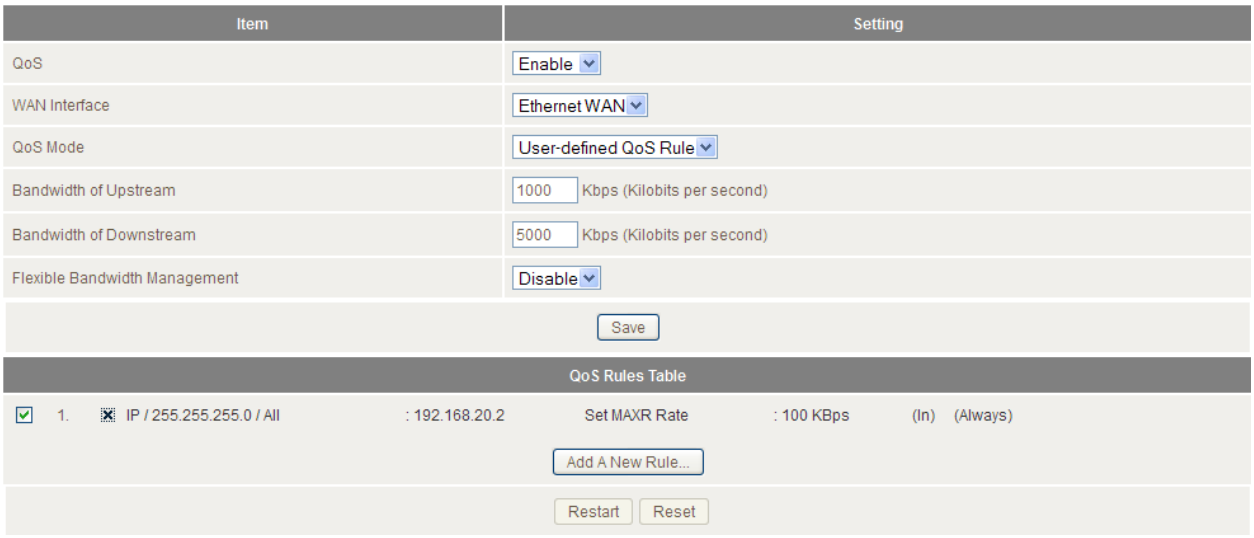
The QoS rule is displayed in the QoS Rules Table at the bottom of the screen. The machine on LAN port 1 is now always restricted to a maximum download speed of 100 KBps at all times.



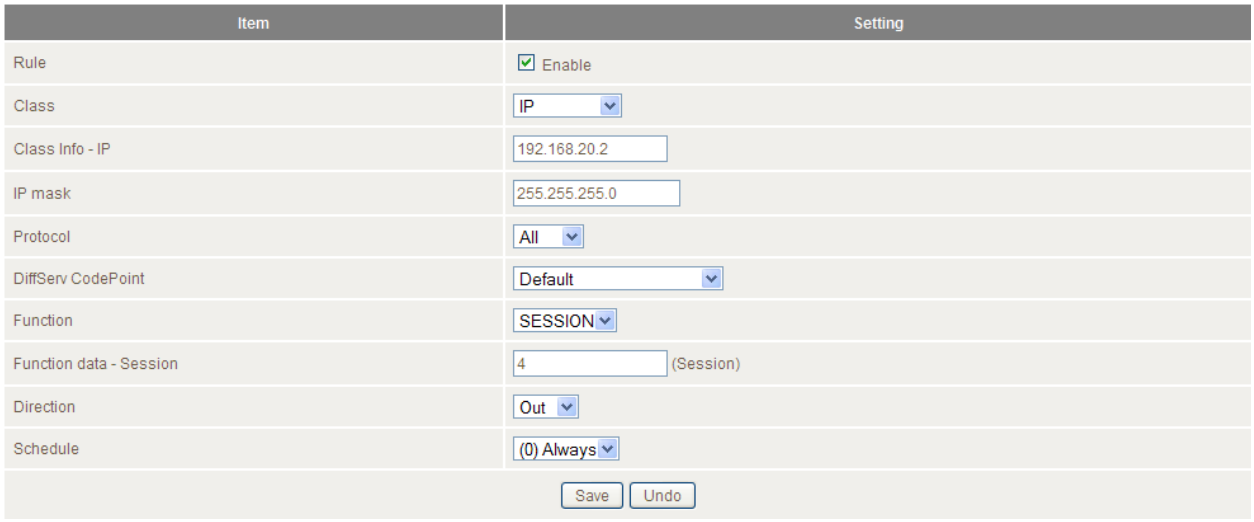
To disable the rule, remove the check from the checkbox on the left. To delete the rule, click the X in the box after the rule number.

Example 2

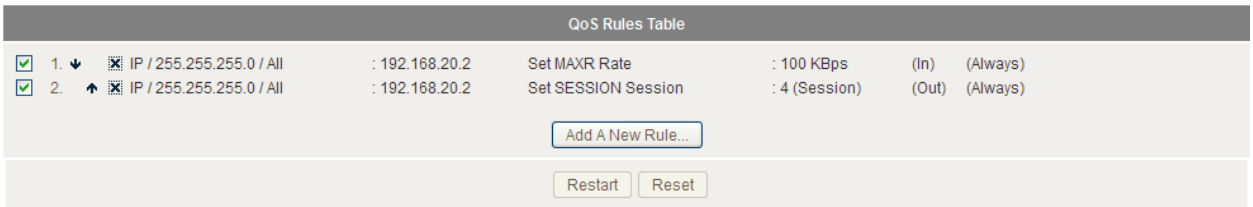
To limit the number of sessions (per port) that can be made in an outbound direction from the machine on LAN port 1 (192.168.20.2) to 4 sessions:



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



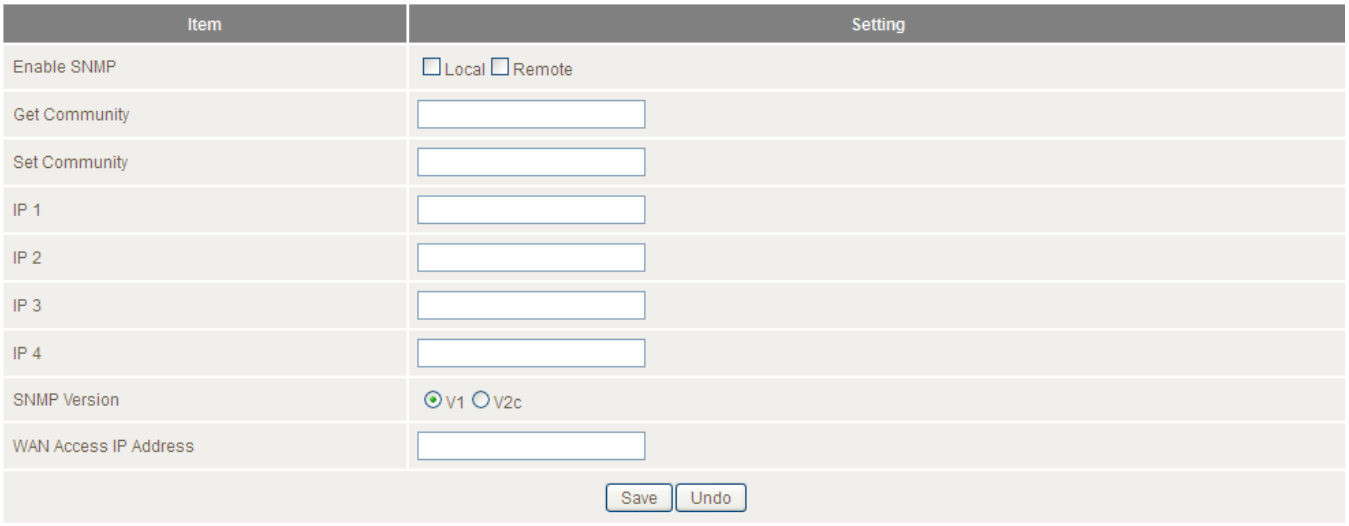
The QoS rule is displayed in the QoS Rules Table at the bottom of the screen. The machine on LAN port 1 will not be able to make more than 4 simultaneous outbound connections to a server.



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

SNMP

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



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

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

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

Routing

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

These settings are used to setup the static and dynamic routing features of the NF5.

Item	Setting
Dynamic Routing	◉ Disable ○ RIPv1 ○ RIPv2
Static Routing	◉ Disable ○ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐

Save Undo

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

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

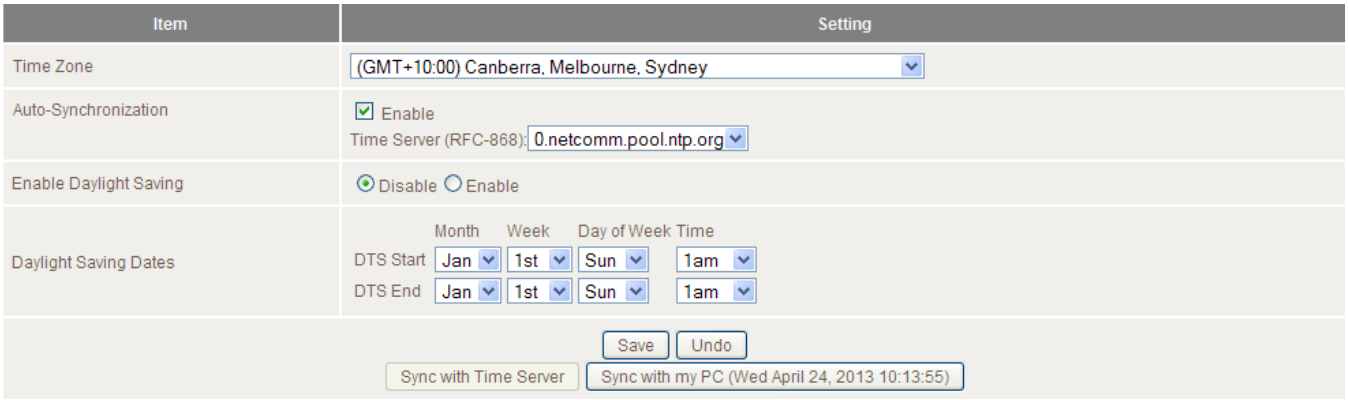
Static Routing:
For static routing, you can specify up to 8 routing rules.

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

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

System Time

This page allows you to change the System time setting on the NF5.

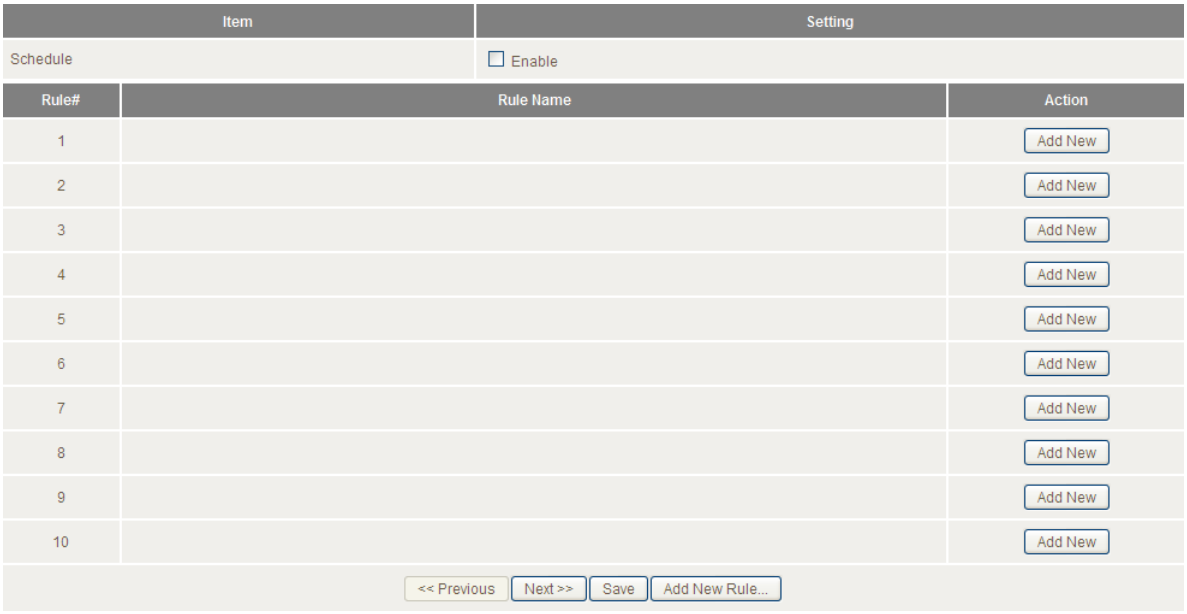


OPTION	DEFINITION
Time Zone	Select the time zone where this device is located.
Auto-Synchronization	Select the "Enable" checkbox to enable this function.
Enable Daylight Saving	Enables or disables the router's automatic daylight saving adjustment feature.
Daylight Savings Dates	Use the drop down lists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

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

Scheduling

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

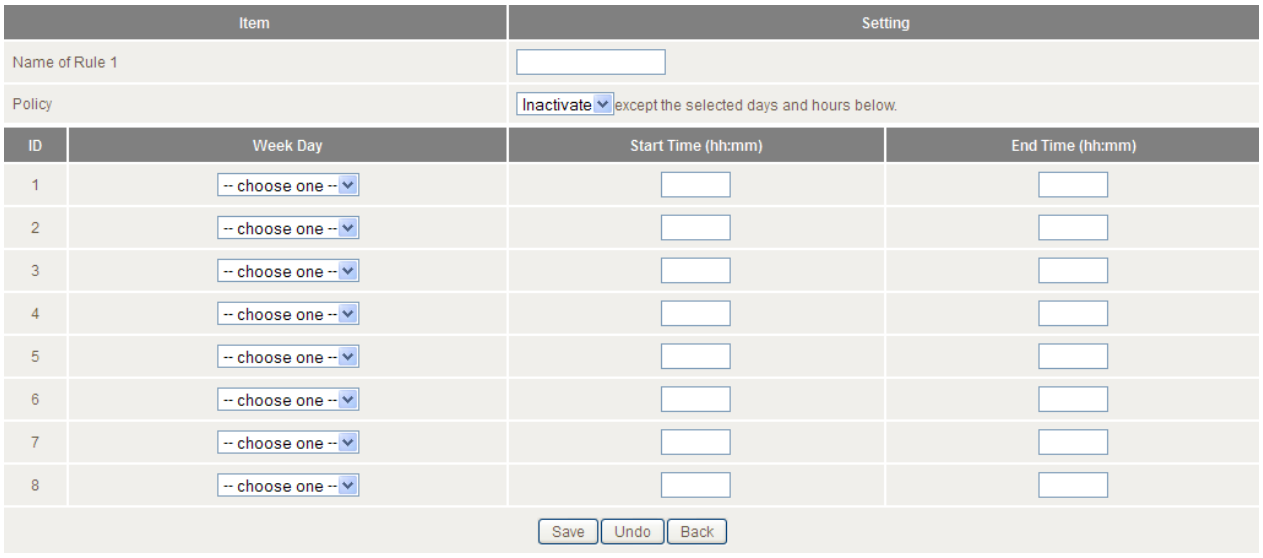


Item	Setting
Schedule	☐ Enable

Rule#	Rule Name	Action
1		Add New
2		Add New
3		Add New
4		Add New
5		Add New
6		Add New
7		Add New
8		Add New
9		Add New
10		Add New

<< Previous | Next >> | Save | Add New Rule...

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



Item	Setting
Name of Rule 1	
Policy	Inactivate except the selected days and hours below.

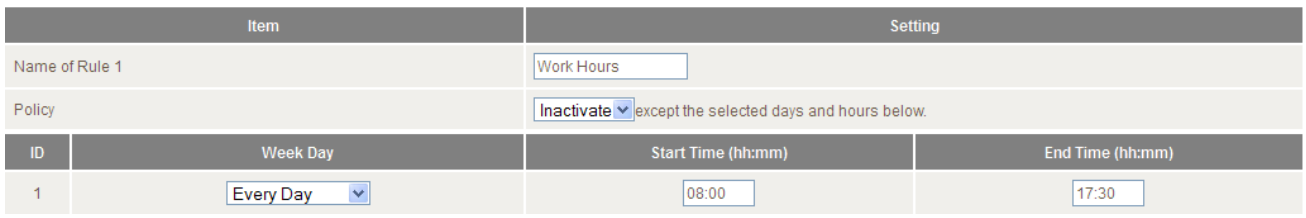
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one --		
2	-- choose one --		
3	-- choose one --		
4	-- choose one --		
5	-- choose one --		
6	-- choose one --		
7	-- choose one --		
8	-- choose one --		

Save | Undo | Back

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

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

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



Item	Setting
Name of Rule 1	Work Hours
Policy	Inactivate except the selected days and hours below.

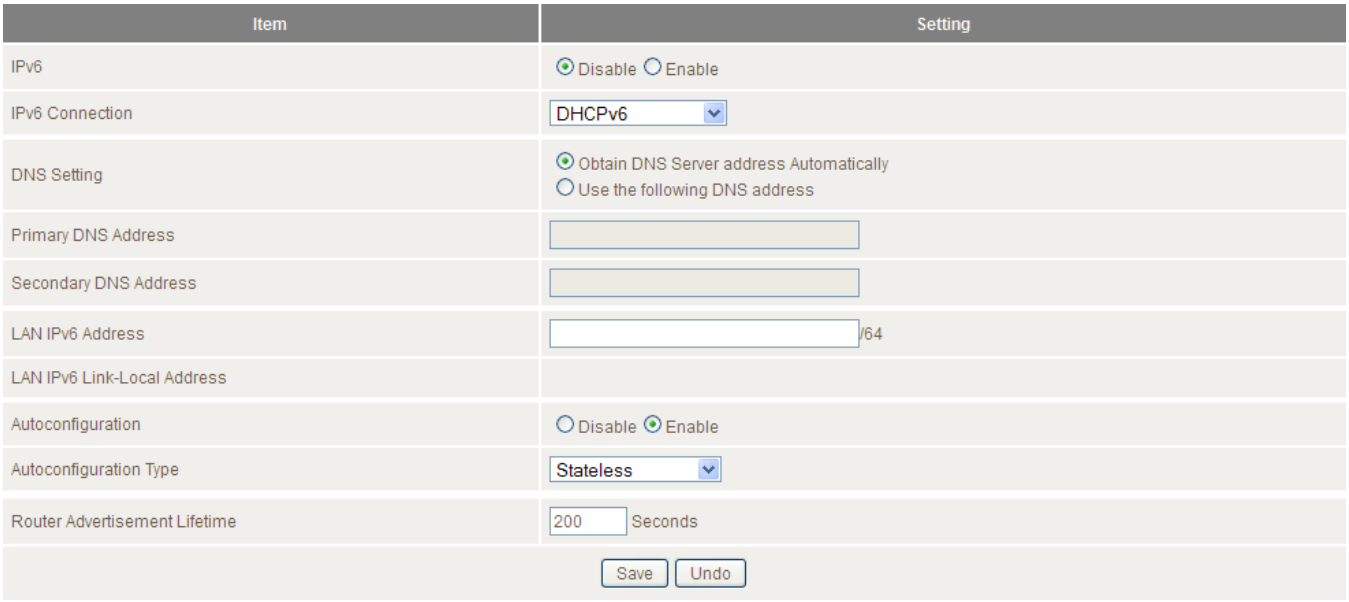
ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	Every Day	08:00	17:30

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

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

IPv6

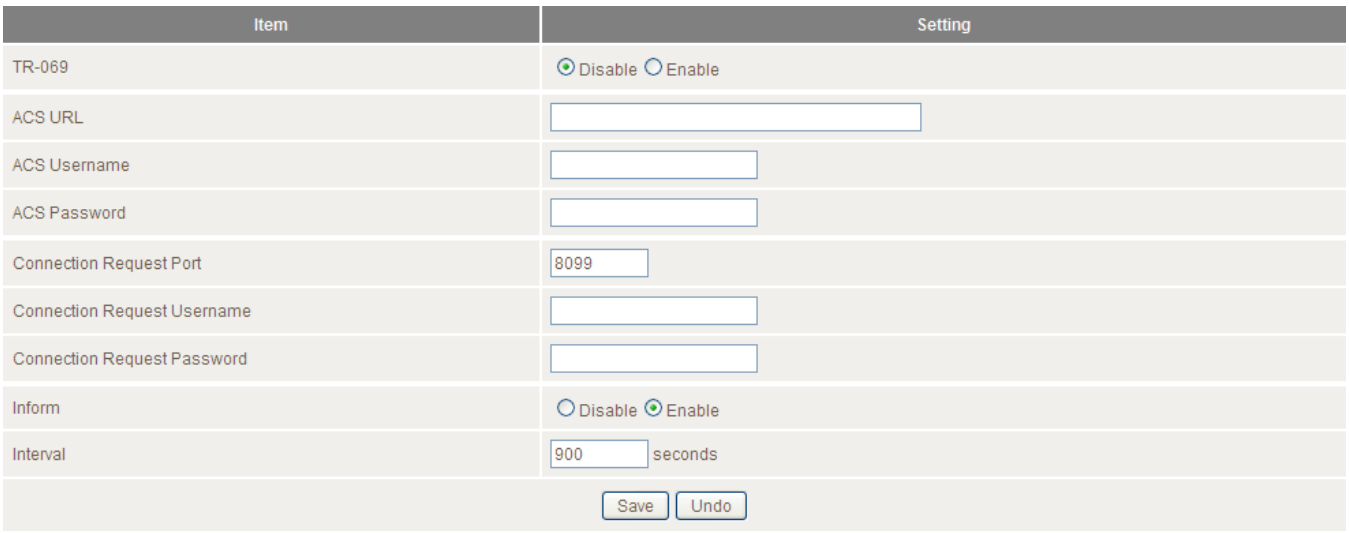
The IPv6 page enables you to configure the settings used for an IPv6 connection (if supported by your Internet Service Provider).



OPTION	DEFINITION
IPv6	Select to enable or disable IPv6 functionality.
IPv6 Connection	Select the type of IPv6 connection to utilise for your service. You can select from: ▪ Static IPv6 ▪ DHCPv6 ▪ PPPoE ▪ 6 to 4 ▪ IPv6 in IPv4 Tunnel ▪ PPPoA Select the type of connection as required by your Internet Service Provider for their IPv6 service.
DNS Setting	Select whether to automatically obtain DNS Server addresses or use the ones you manually specify.
Primary DNS Address	Enter the Primary DNS Address for the IPv6 connection.
Secondary DNS Address	Enter the Secondary DNS Address for the IPv6 connection.
LAN IPv6 Address	The IP Address to use for the IPv6 service connection.
LAN IPv6 Link-Local Address	The current local LAN IPv6 address of the NF5.
Autoconfiguration	Select to enable or disable IPv6 auto configuration (if supported by your Internet Service Provider).
Autoconfiguration Type	Select the appropriate type of auto configuration mode as required by your Internet Service Provider for their IPv6 service.
Router Advertisement Lifetime	Enter the length of time between the router advertising its availability on the IPv6 connection.

TR-069

The TR-069 client allows the NF5 to be automatically configured from a TR-069 server. Enter the applicable configuration options to enable the router to contact the TR-069 server and retrieve any configuration options.

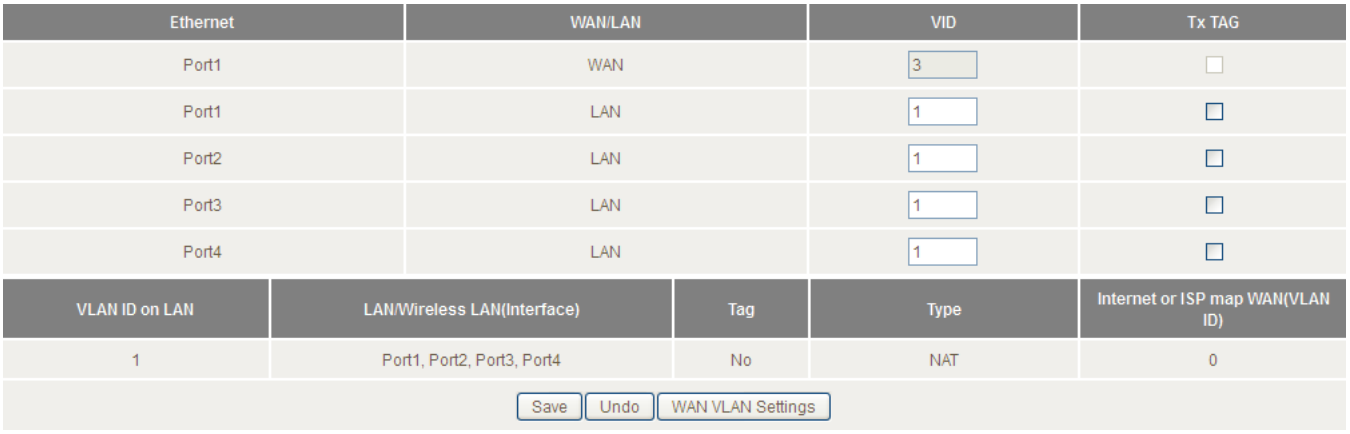


OPTION	DEFINITION
TR-069	Select to enable or disable the TR-069 automatic configuration function.
ACS URL	Enter the URL of the ACS server for automatic configuration.
ACS User Name	The username required to login to the ACS server.
ACS Password	The password required to login to the ACS server.
Connection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

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

VLAN

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



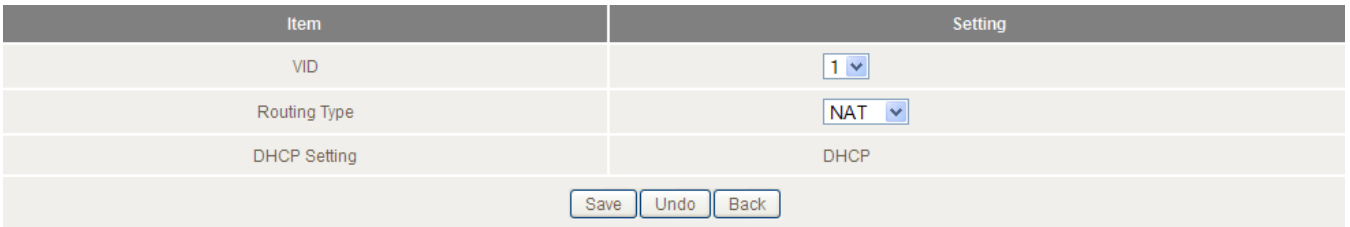
Ethernet	WAN/LAN	VID	Tx TAG
Port1	WAN	3	☐
Port1	LAN	1	☐
Port2	LAN	1	☐
Port3	LAN	1	☐
Port4	LAN	1	☐

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

Save Undo WAN VLAN Settings

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

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

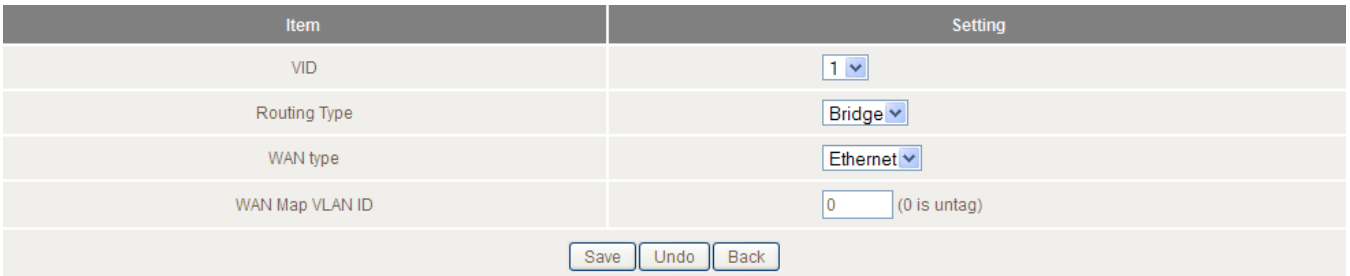


Item	Setting
VID	1
Routing Type	NAT
DHCP Setting	DHCP

Save Undo Back

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

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



Item	Setting
VID	1
Routing Type	Bridge
WAN type	Ethernet
WAN Map VLAN ID	0 (0 is untag)

Save Undo Back

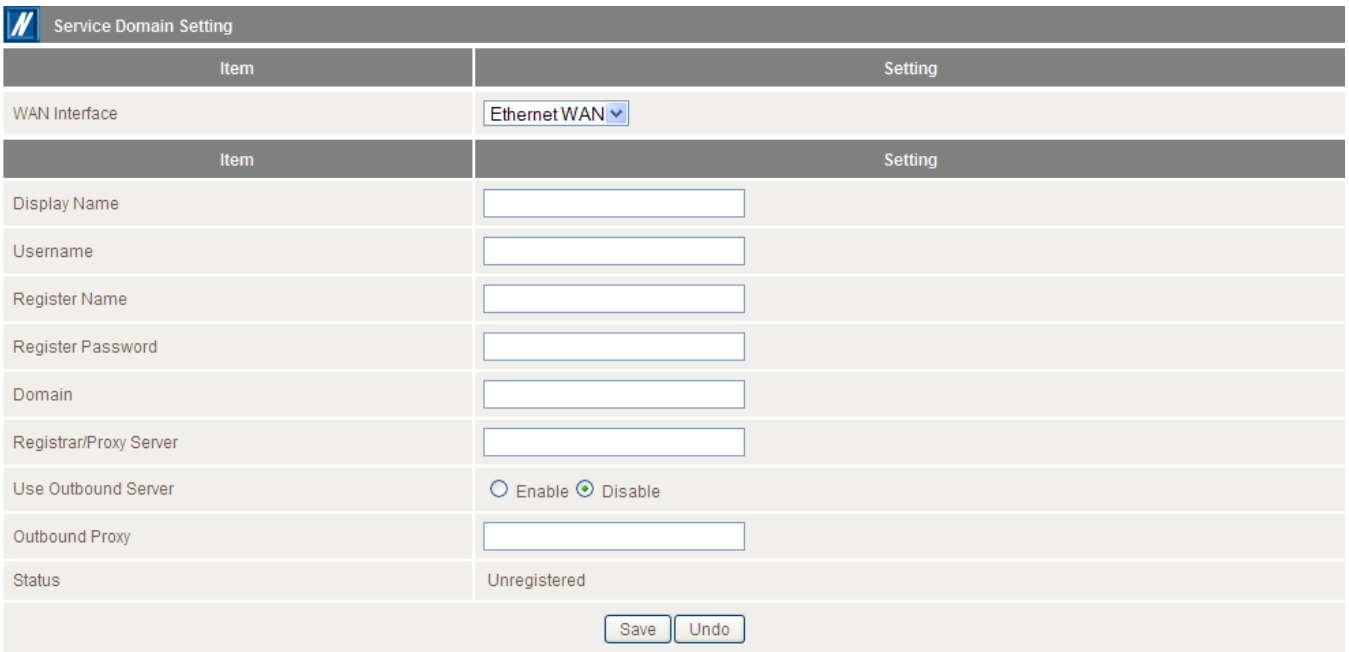
OPTION	DEFINITION
VID	Use the drop down list to select the VID you want to configure.
Routing Type	Use the drop down list to type of routing for the selected VID.
WAN type	Use the drop down list to select which WAN type the VLAN uses.
WAN Map VLAN ID	Enter the VLAN ID to tag packets on the WAN interface.

VoIP Settings

Configurations

Service Domain

The Service Domain page is where you enter your VoIP service settings as supplied by your VoIP service provider (VSP). If you are unsure about a specific setting or have not been supplied information for a particular field, please contact your VOIP service provider to verify if this setting is needed.

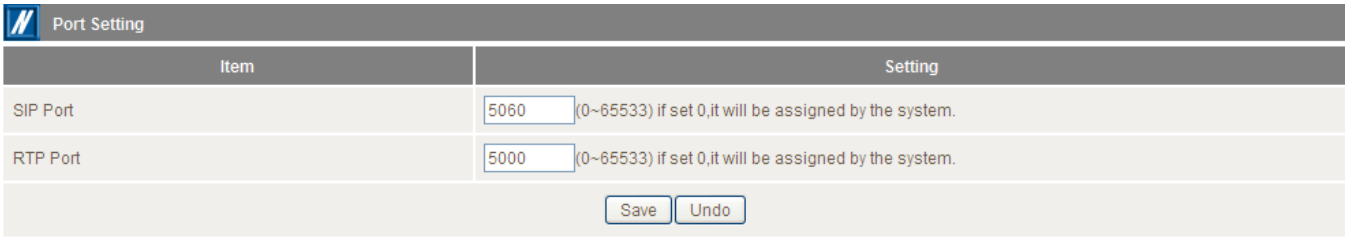


OPTION	DEFINITION
Display Name	Enter the display name for your VoIP service.
User Name	Enter the User Name for your VoIP service.
Register Name	Enter the Register Name (May be called the “Auth ID”) for your VoIP service.
Register Password	Enter the Register Password (May be called the “Auth Password”) for your VoIP service.
Domain	Enter the Domain for your VoIP service.
Registrar/Proxy Server	Enter the Registrar or Proxy Server for your VoIP service.
Use Outbound Server	Enable or Disable the use of an Outbound Proxy for VOIP calls.
Outbound Proxy	Enter the Outbound Proxy server address to use.
Status	The current status of your VOIP service.

Click **Save** to save your settings and connect to your VoIP service or **Undo** to discard the settings entered.

Port Setting

The Port Setting page enables you to specify a different SIP or RTP Port number to connect to your VoIP service on.



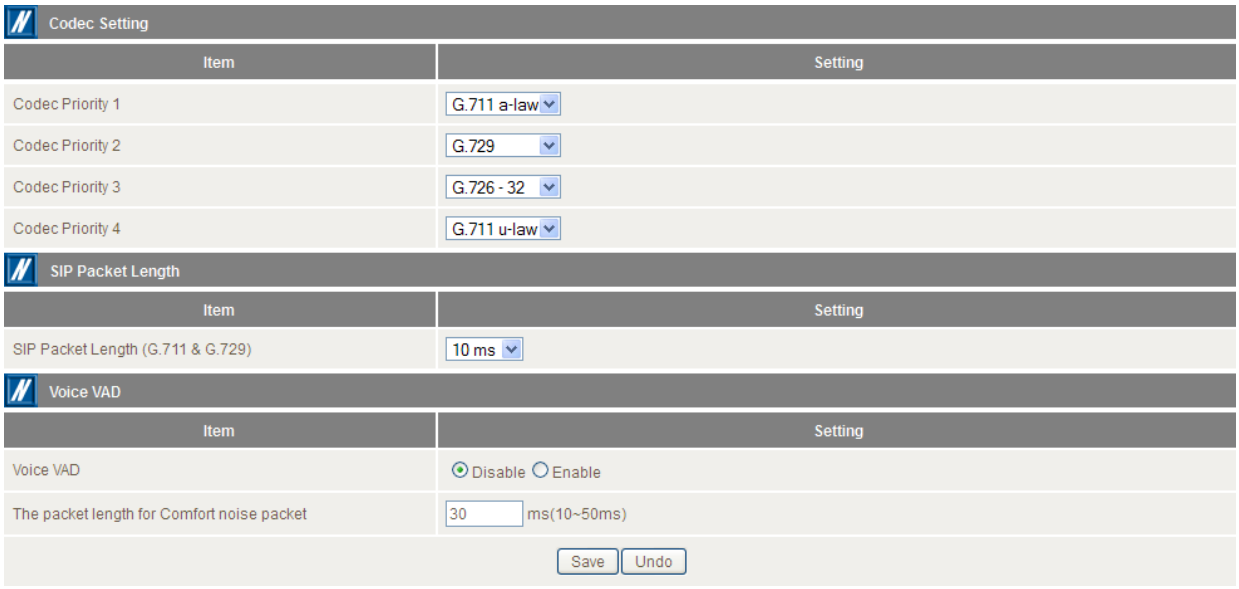
OPTION	DEFINITION
SIP Port	Select the port for SIP traffic to use.
RTP Port	Select the port for RTP traffic to use.

This setting should not need to be changed unless directed to do so.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Codec Setting

The Codec Setting page enables you to select which audio codec to use with your VoIP service. This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with VoIP call sound quality.



The following codec are available for use:

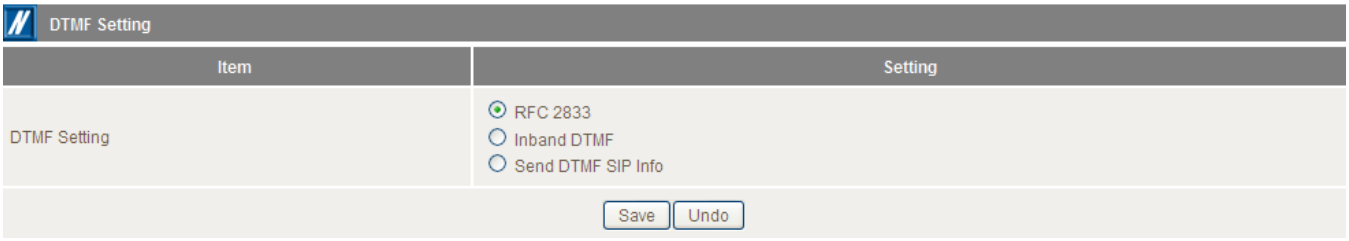
- G.729
- G.711 a-law
- G.711 u-law
- G.726 -32

OPTION	DEFINITION
Codec Priority 1	Set the codec you would like to try first with your VoIP service.
Codec Priority 2	Set the codec you would like to try second with your VoIP service.
Codec Priority 3	Set the codec you would like to try third with your VoIP service.
Codec Priority 4	Set the codec you would like to try fourth with your VoIP service.
G.711 & G.729 Packet Length	Adjust the packet length size. This can reduce or increase the bandwidth required for a VoIP call.
Voice VAD	Adjust the 'Voice Activity Detection' interval. This should not be adjusted unless the words in your conversation are being cut off. (This setting should not need to be changed.)
The packet length for Comfort noise packet	Set the time in milliseconds for which comfort noise is used to simulate background noise at your end of the connection.

Click **Save** to save your settings or **Undo** to discard the settings entered.

DTMF Setting

The DTMF Setting page enables you to specify which DTMF standard to use on your VoIP service.



The following DTMF standards are available for use:

- RFC 2833
- Inband DTMF
- Send DTMF SIP Info

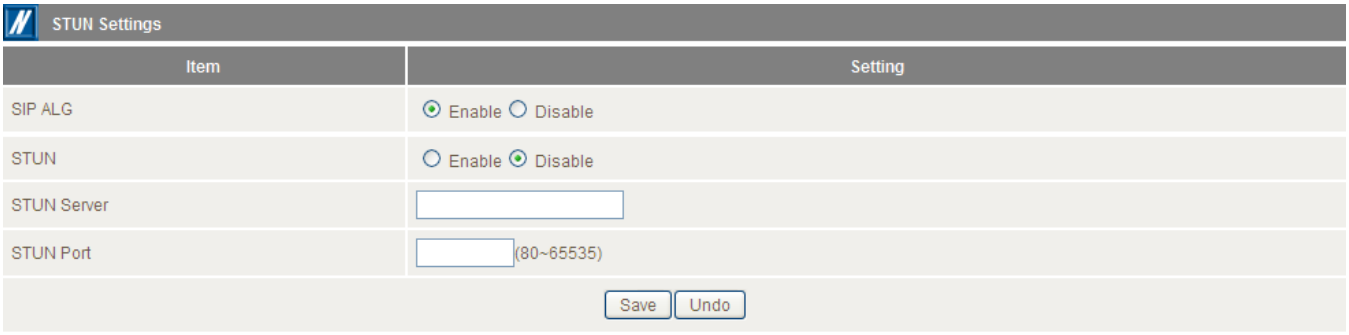
This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with DTMF based services
(Automated Telephone services, Answering machines, etc).

OPTION	DEFINITION
DTMF Setting	Select the which DTMF standard you would like to use.

Click **Save** to save your settings or **Undo** to discard the settings entered.

STUN Settings

The STUN Settings page enables you to configure settings related to using a STUN server with your VoIP service. A STUN (Session Traversal Utilities for NAT) server is used to permit NAT traversal for applications of real-time voice, video, messaging and other interactive IP communications. This information will usually be supplied by your VoIP service provider and should not be needed unless you are experiencing issues with VoIP calls or signing into your VoIP service.

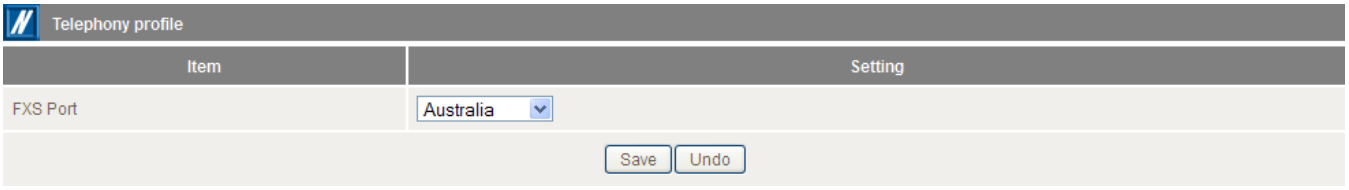


OPTION	DEFINITION
SIP ALG	A SIP Application Gateway provides functionality to allow VoIP traffic to pass both from the private the public and public to private side of the firewall when using network address translation (NAT).
STUN	Select to Enable or Disable the STUN server functionality of the NF5.
STUN Server	Enter the STUN Server address to use.
STUN Port	Enter the Port with which to connect to the STUN server on.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Telephony Profile

The Telephony Profile page enables you to configure the way the FXS phone port (RJ-11) operates.

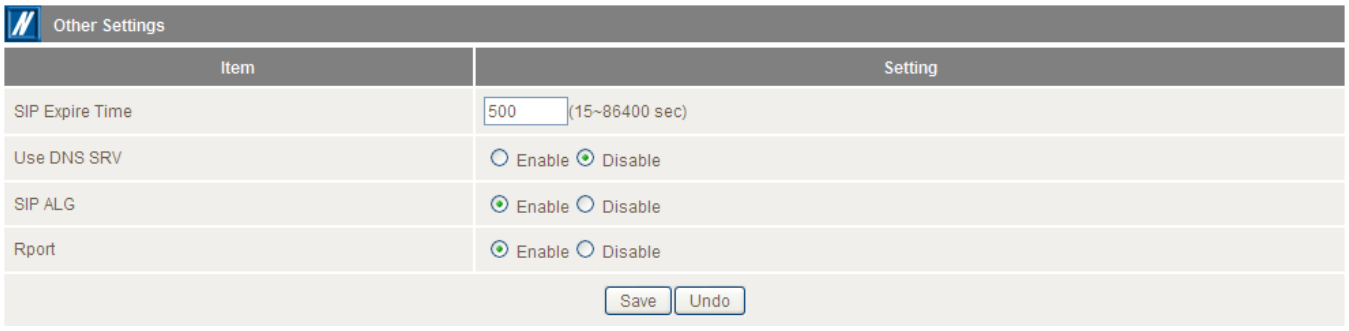


Use the drop down list to select the region closest to you to configure the FXS port operation.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Other Settings

The Other Settings page enables you to specify a different SIP expire time and select to enable the DNS SRV function. This information will usually be supplied by your VoIP service provider and should not need to be changed unless you are experiencing issues with VoIP calls or signing into your VoIP service.



OPTION	DEFINITION
SIP Expire Time	Set the length of time between the NF5 refreshing its connection to your VoIP service provider
Use DNS SRV	Enable or Disable the DNS SRV function on the NF5.
SIP ALG	A SIP Application Gateway provides functionality to allow VoIP traffic to pass both from the private the public and public to private side of the firewall when using network address translation (NAT).
Rport	Rport allows a client to request that the server send the response back to the source IP address and port from which the request originated.

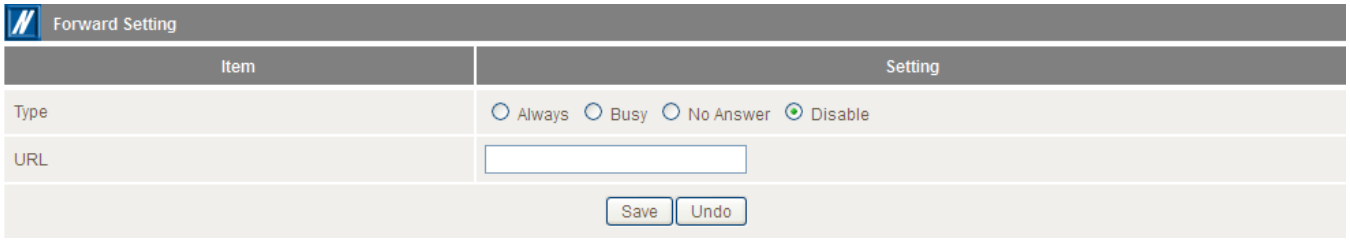
Click **Save** to save your settings or **Undo** to discard the settings entered.

Call Features

The Call Features pages enable you to configure settings for features such as call waiting, call forwarding and caller ID.

Call Forward

The Call Forward page enables you to configure the type of call forwarding you would like to use and the SIP address to which any such calls should be forwarded.



You can select from the following call forwarding conditions:

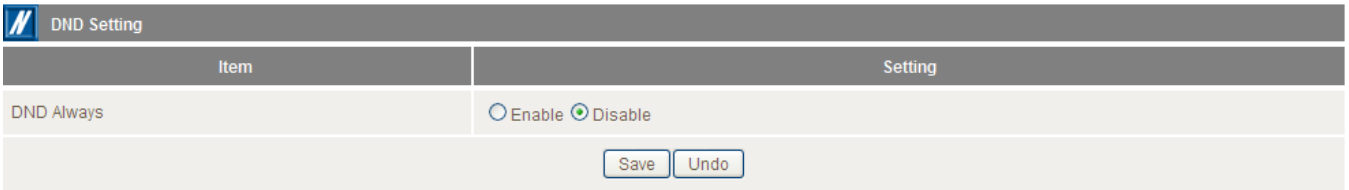
- Always
- Busy
- No Answer
- Disable

OPTION	DEFINITION
Type	Select the type of Call Forwarding you would like to use.
URL	Enter the address to forward VOIP calls to.

Click **Save** to save your settings or **Undo** to discard the settings entered.

DND Setting

The DND Setting page enables you to configure Do Not Disturb (DND) mode. This will prevent calls coming through to your phone.



OPTION	DEFINITION
DND Always	Enable or Disable the DND feature.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Caller ID

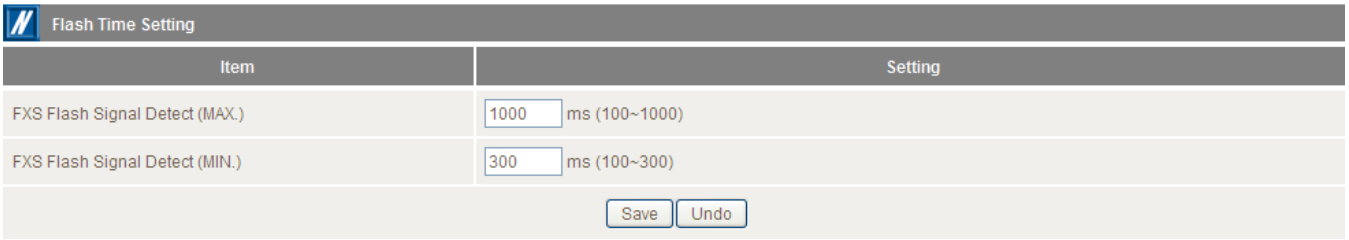
The Caller ID page enables you to configure whether your Caller ID is sent when receiving an inbound call.
(If supported by your VOIP service)

OPTION	DEFINITION
Caller ID	Select to use or Disable Caller ID.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Flash Time

The Flash Time page enables you to configure the minimum and maximum time a hook flash signal can occur for the NF5 to recognise it.



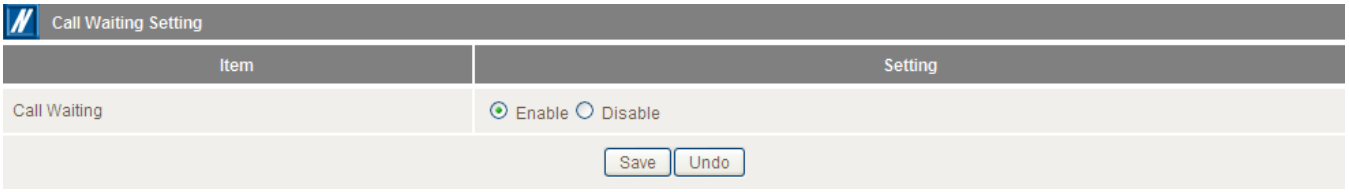
OPTION	DEFINITION
FXS Flash Signal Detect (MAX)	Enter the maximum time (in milliseconds) to detect a hook flash.
FXS Flash Signal Detect (MIN)	Enter the minimum time (in milliseconds) to detect a hook flash.

This setting should not need to be changed unless directed to do so.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Call Waiting

The Call Waiting page enables you to utilise call waiting with your VoIP service.
(If supported by your VoIP service)

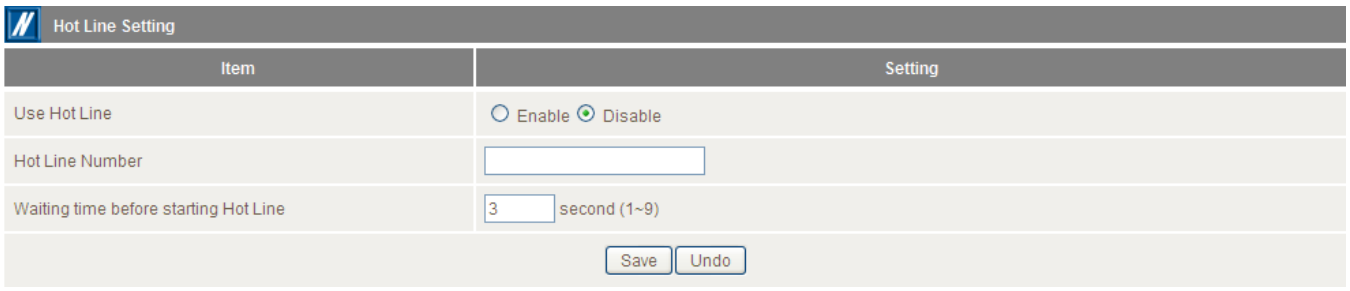


OPTION	DEFINITION
Call Waiting	Select to Enable or Disable the call waiting feature on the NF5.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Hot Line

The Hot Line page enables you to configure a telephone number which can be called without dialling any numbers at all (simply pick up the telephone handset) after the specified waiting time.

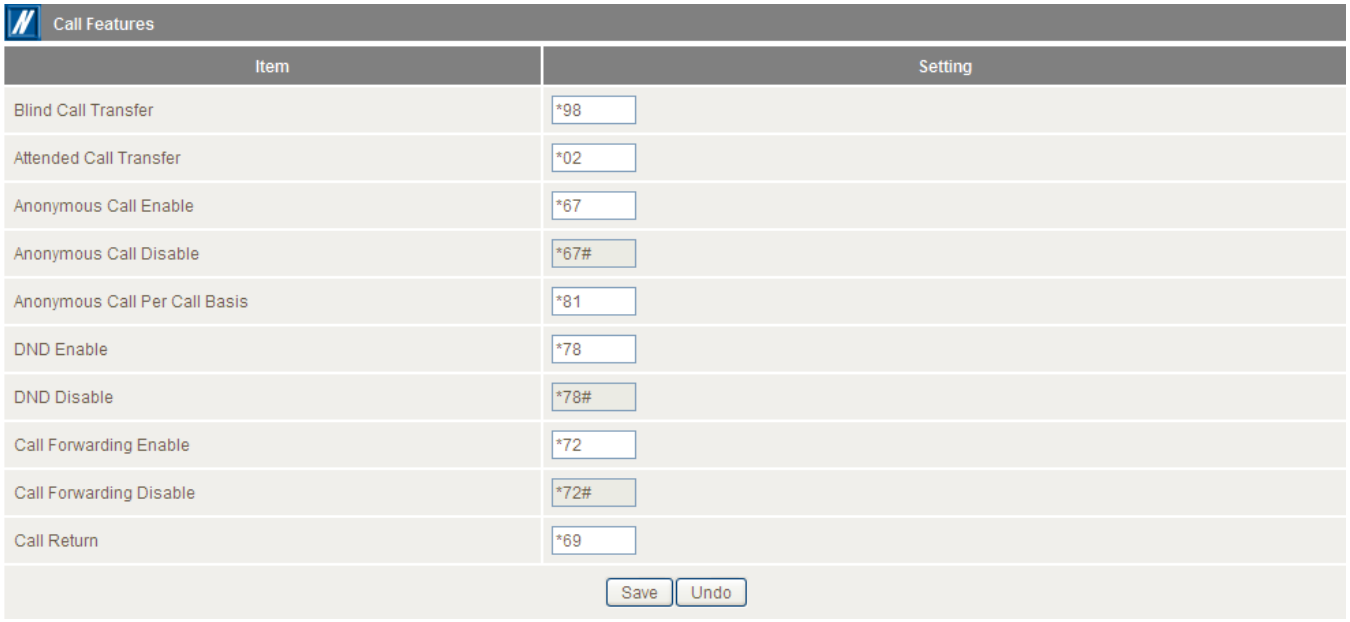


OPTION	DEFINITION
Use Hot Line	Select to Enable or Disable the Hot Line feature of the NF5.
Hot Line Number	Enter the number to forward Hot Line calls to.
Waiting time before starting Hot Line	Enter the amount of time to wait before forwarding a call to the Hot Line number.

Click **Save** to save your settings or **Undo** to discard the settings entered.

Call Features

The Call Features page enables you to configure the dialling codes used to activate or deactivate features on your VoIP service.
(If supported by your VoIP Provider)



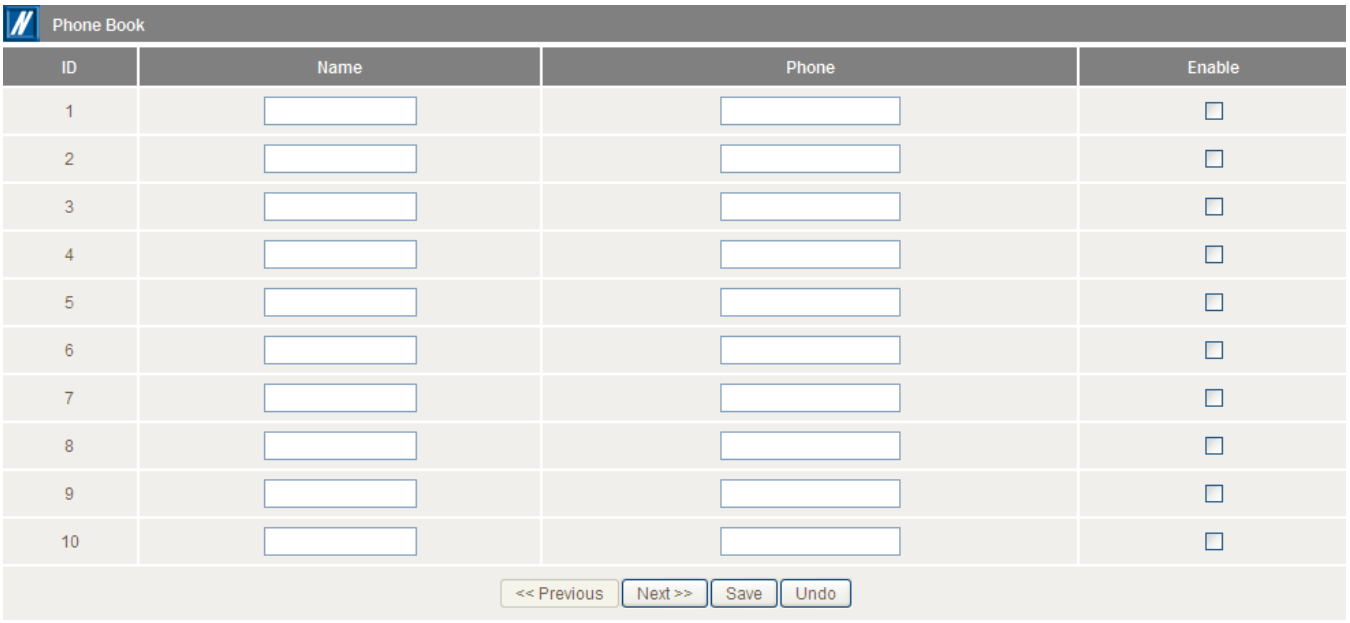
You can change the dial codes on the following VoIP service features:

- Blind Call Transfer
- Anonymous Call Enable
- Anonymous Call Disable
- Anonymous Call per Call Basis
- DND Enable
- DND Disable
- Call Forwarding Enable
- Call Forwarding Disable
- Call Return

Click **Save** to save your settings or **Undo** to discard the settings entered.

Phone Book

The Phone Book page lets you to enter phone numbers into a database for easy calling. Phone book numbers are stored on the NF5.



The Phone Book page enables you to enter phone book entries. You are able to enter up to 140 entries.

The corresponding name is displayed when a VoIP call is received from that number.
(If supported by your VOIP service and telephone handset)

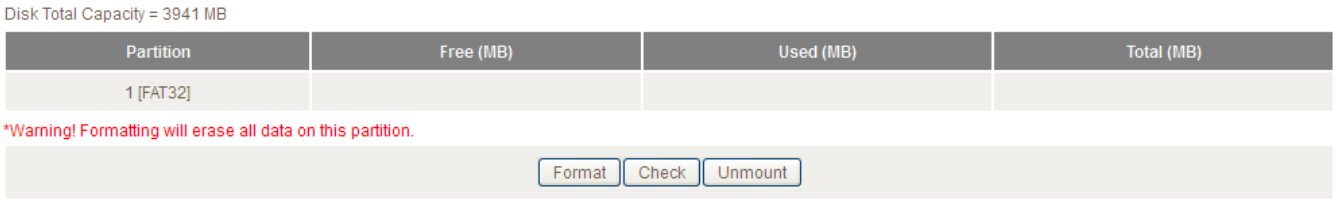
Click **Save** to save your settings or **Undo** to discard the settings entered.

NAS Settings

The NAS Settings page enables you to configure the network area storage (NAS) function of the NF5. This function can be used to remotely access files stored on an attached USB hard drive. Click on any of the menu items to access the respective configuration page.

Disk Utility

The Disk Utility function enables you to check any attached USB storage for errors. The NF5 will scan the attached storage and determine if there are any file system errors present. File System errors can prevent you being able to access stored content. You can also format (erase) any attached storage if needed. Simply click the appropriate button to perform either task.

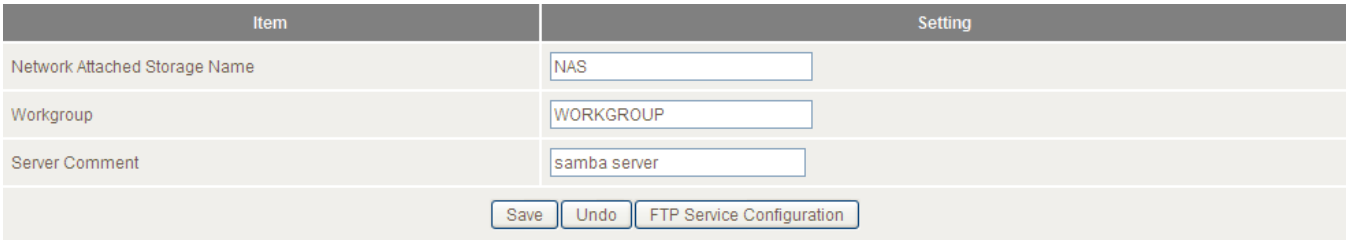


File Sharing

The File Sharing function enables the NF5 to take part in a Windows networking environment. Once configured, the attached USB Storage can be viewed from Windows by typing:

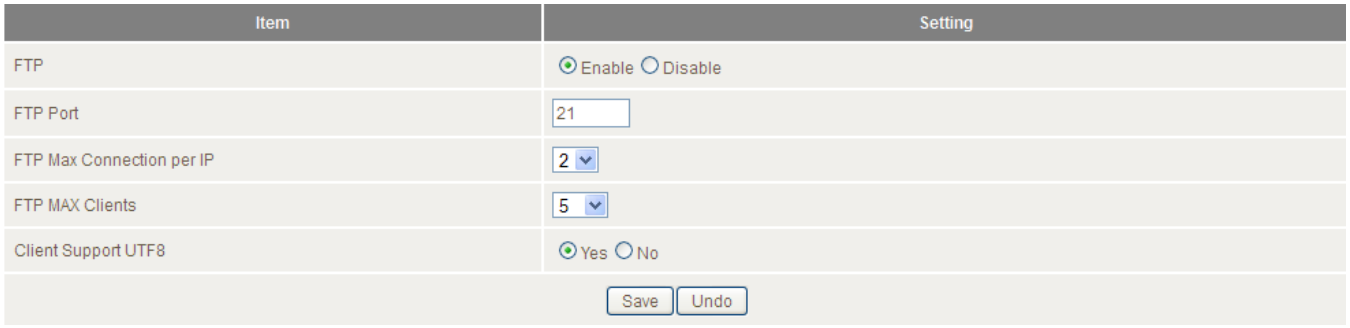
\\<Configured Name of the NF5>\Storage\

Files can then be dragged and dropped onto the attached USB storage.



OPTION	DEFINITION
Network Attached Storage Name	Enter the computer name the NF5 is to use on the network.
WorkGroup	Enter the network workgroup the NF5 is to be a member of.
Server Comment	Enter the comment to be displayed when a list of network hosts is shown.

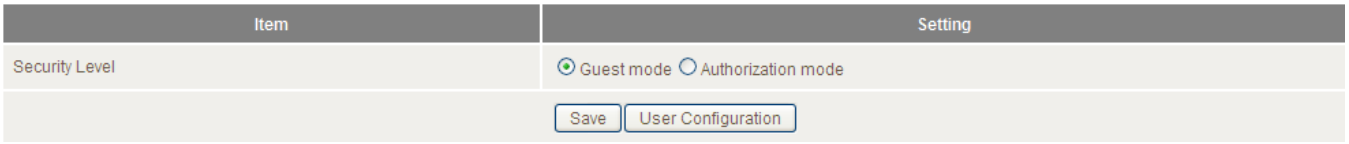
The File Sharing configuration also enables you to enable the built-in FTP server function and the associated settings:



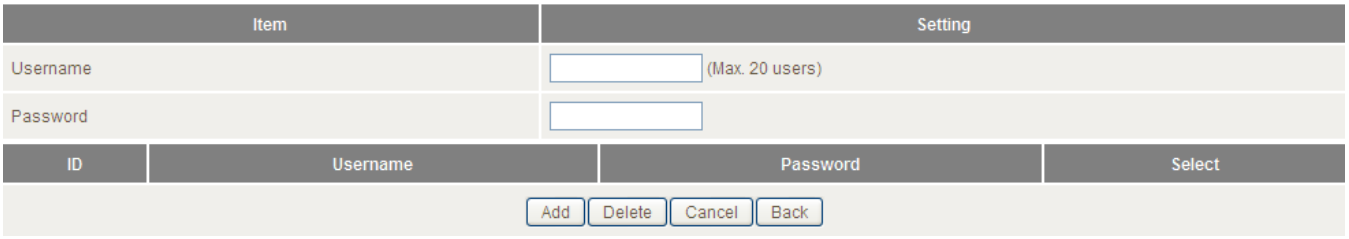
OPTION	DEFINITION
FTP	Select to enable or disable the FTP server function.
FTP Port	Enter the network port the FTP server should run on.
FTP Max Connections per IP	Enter the maximum number of concurrent connections which can be used by a particular IP address.
FTP Max Clients	Enter the maximum number of clients which can connect to the FTP concurrently.
Client Support UTF8	Enable Unicode support for connected clients.

Access Control

The Access Control function provides control over which users can access any attached USB Storage. By default, the NF5 is in "Guest Mode" which means anyone can access the attached hard drive.



Enabling "Authorization Mode" allows the creation of specific user accounts with a password to further control access permissions. To enable this, click on the **Authorization Mode** radio button and click **Save**. You can then click on the **User Configuration** button in order to create the required user accounts.



Add the user name and password and then click the **Add** button. Alternatively, to remove a user, click on the radio button to the right of the username and then select **Delete**.

Download Assistant

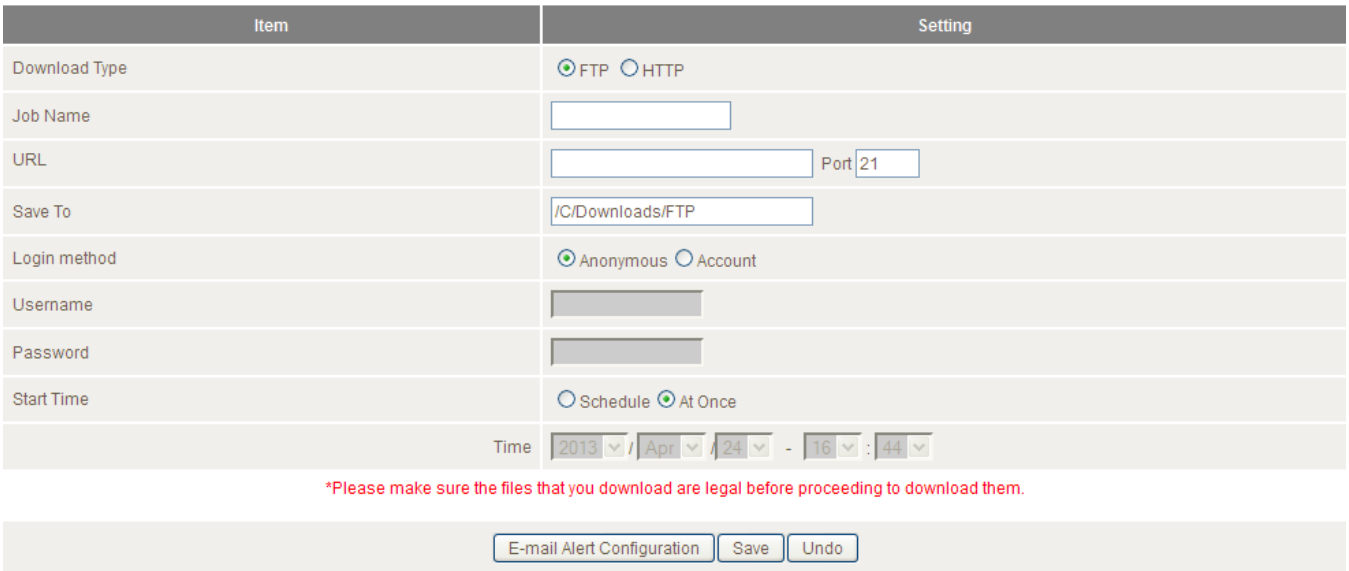
The Download Assistant enables you to schedule the NF5 to perform a download from an Internet host.

You are able to select from two download types:

- FTP
- HTTP

Each type of download job requires different configuration options.

FTP

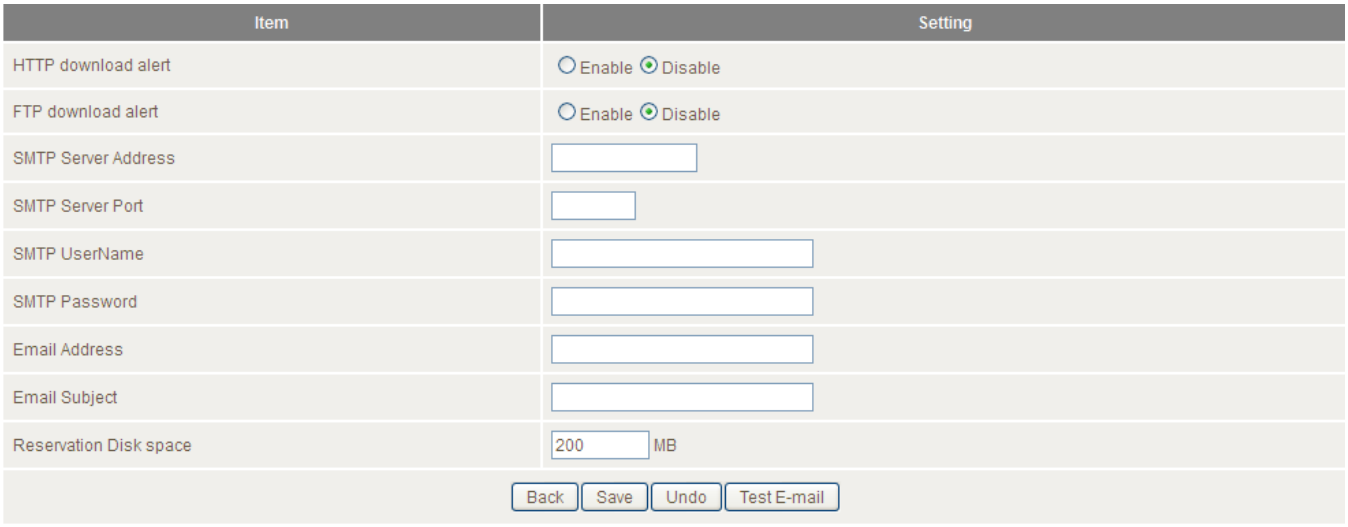


OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Port	The port required for the FTP server *(This would usually be left as 21).*
Save To	The location on the NF5 to save the downloaded file to.
Login Method	Select the type of authentication required by the FTP server *(Selecting anonymous means a username and password are not required).*
Username	The username required to access the FTP server.
Password	The password required to access the FTP server.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

HTTP

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download from.
Save To	The location on the NF5 to save the downloaded file to.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

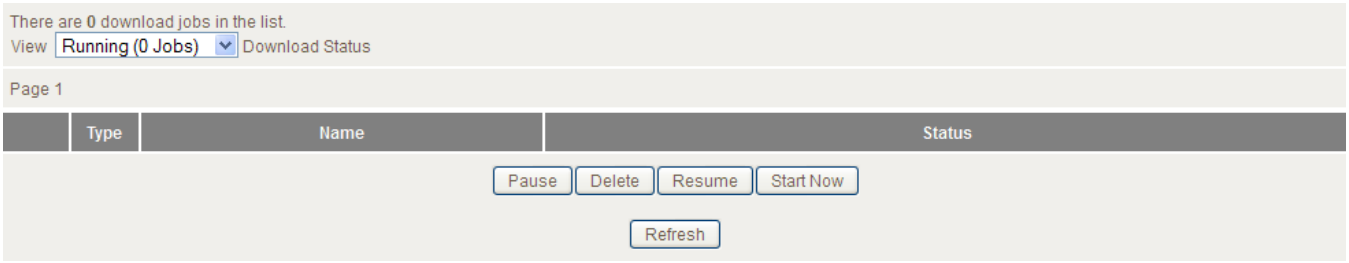
You can also configure the NF5 to send an e-mail on completion of the scheduled download. Click on the "E-mail Alert Configuration" button to setup this option.



OPTION	DEFINITION
HTTP Download Alert	Select to enable or disable an alert to be sent for a completed HTTP download.
FTP Download Alert	Select to enable or disable an alert to be sent for a completed FTP download.
USB Download Alert	Select to enable or disable an alert to be sent for a completed USB download.
SMTP Server Address	Enter the address of the email server to be used to send the alerts.
SMTP Server Port	Enter the port which the email server is running on.
SMTP User Name	Enter the username required to login to the email server.
SMTP Password	Enter the password required to login to the email server.
Email Address	Enter the email address any alerts are to be sent to.
Email Subject	Enter the subject to be used on any email alerts sent out.
Reservation Disk Space	Enter the amount of disk space to reserve on the NF5 for the specified download.

Download Status

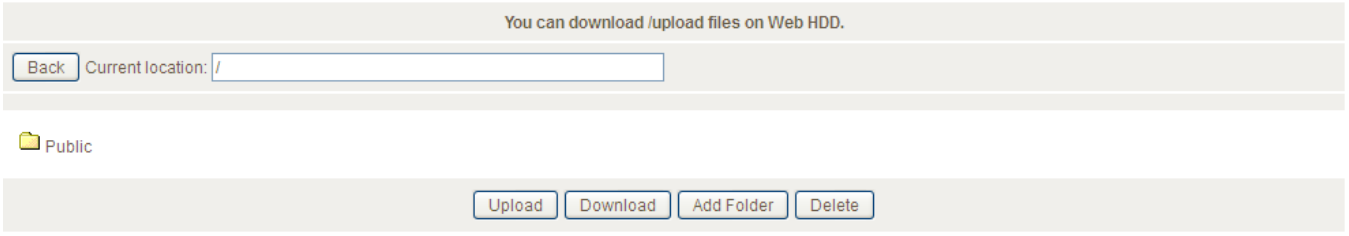
The Download Status page enables you to monitor previously scheduled Download Assistant jobs. From this page you are able to Start, Pause, Resume or Delete any Download Assistant jobs.



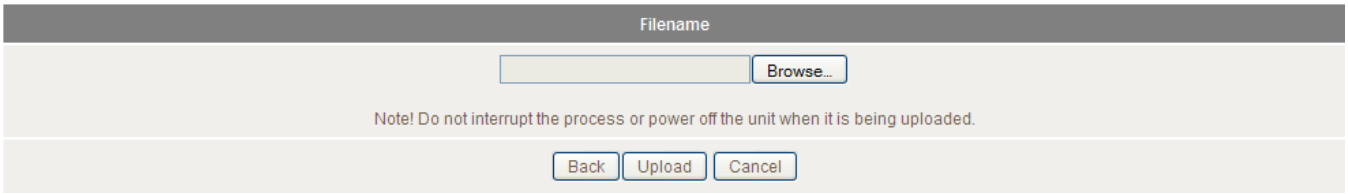
The View drop-down list enables you to select whether currently running jobs, waiting jobs or scheduled jobs are displayed. Once listed, click on the checkbox on the left hand side of the listed jobs and then click the appropriate function button.

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.



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



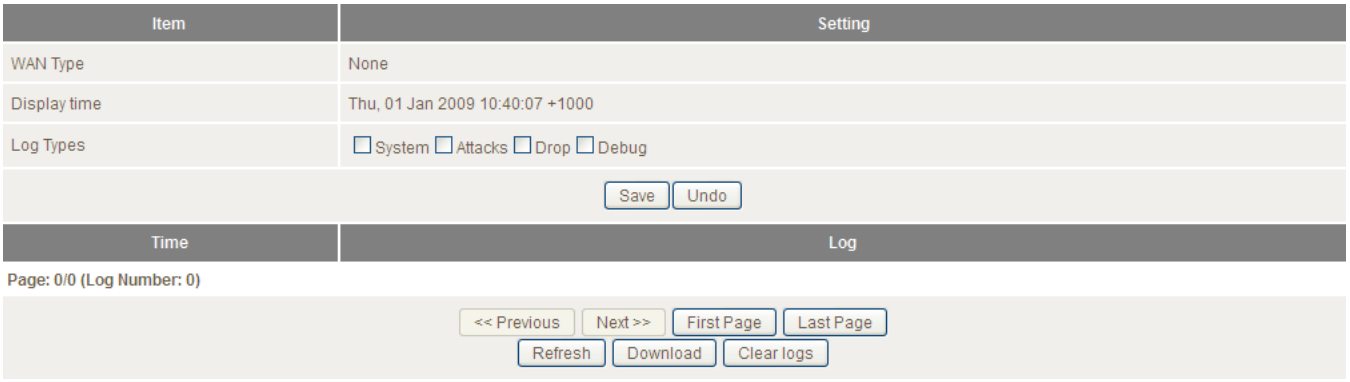
To upload files to your Web HDD, click the **Upload** button. You can then click the **Browse** button and then navigate to the file you would like to upload. Once selected, this file will be copied to the Web HDD and become available to download by connected devices.

Toolbox

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

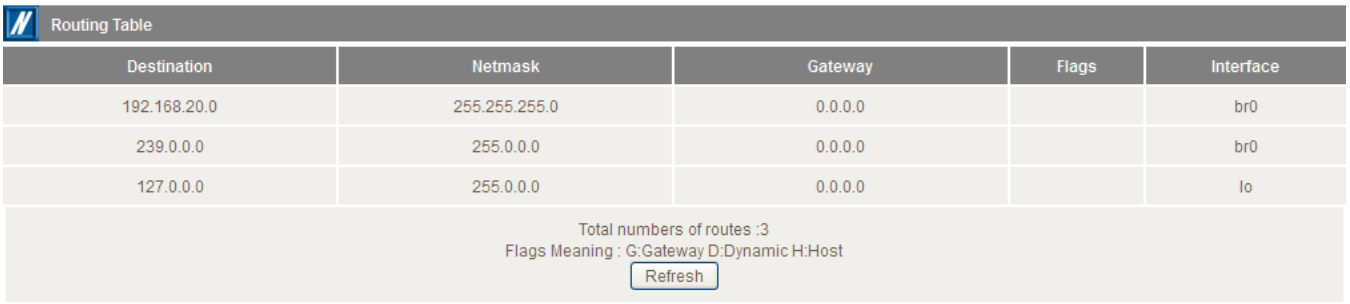
System Info

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



Routing Table

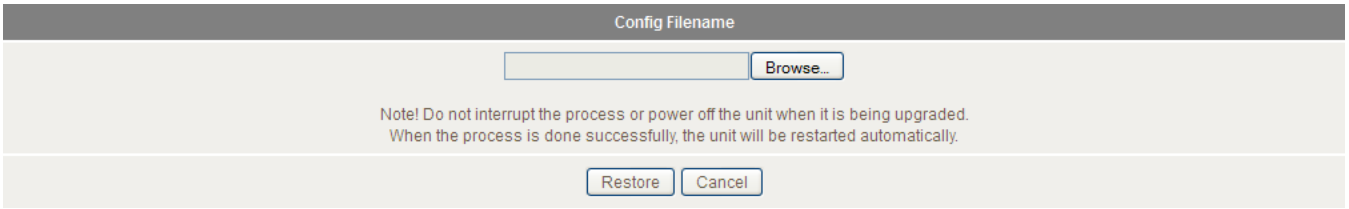
The Routing table displays the current routes in place on the router.



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

Restore Settings

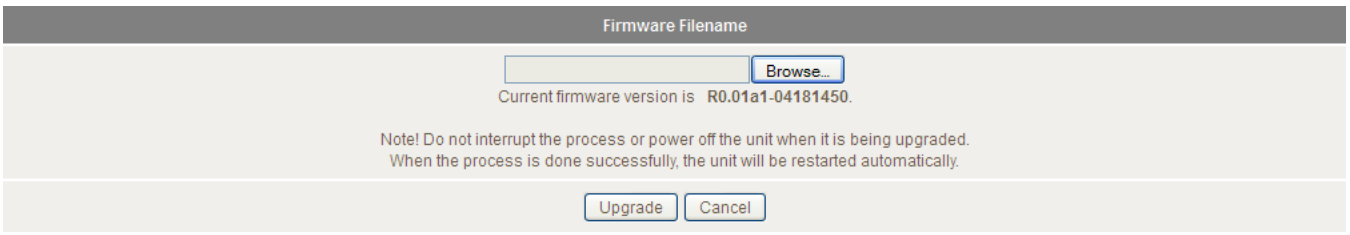
The Restore settings page allows you to restore a previously saved configuration of the router. This is handy for reverting to a working configuration when making changes to the router's settings.



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

Firmware Upgrade

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



Backup Settings

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

Reset to Default

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

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

Reboot

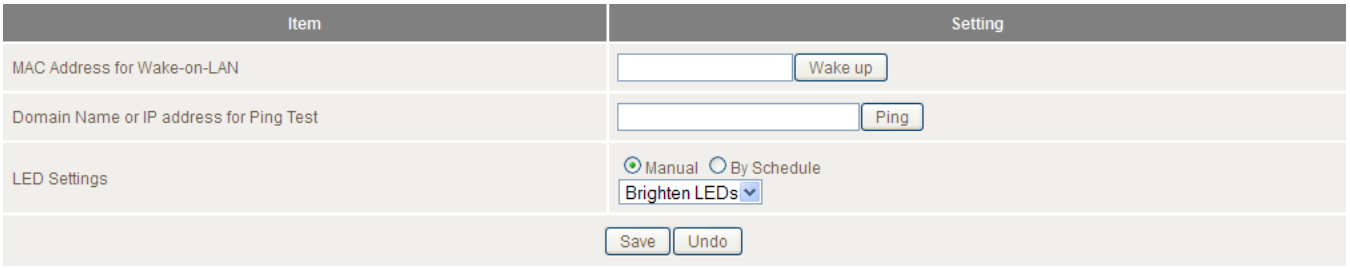
Click the **Reboot** menu item to restart the router.

Startup Wizard

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

Miscellaneous

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



Logout

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

Additional Product Information

Establishing a wireless connection

Windows XP (Service Pack 3)

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

Windows Vista

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

Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key *(*refer to the included wireless security card for *the default wireless network key)*.
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NF5 with "Connected" next to it.

Mac OSX 10.6

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

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

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NF5 power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NF5 and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF5 off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NF5. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NF5's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.
5	If you are still not able to access the web configuration pages, reset the router to the factory default settings by pressing the reset button for ten seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NF5 restarts. Navigate to 192.168.20.1 in your web browser and enter "admin" (without the quotes) as the username and password.

The web configuration does not display properly.

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

Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for ten seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF5 restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

WLAN Interface

I cannot access the NF5 from the WLAN or ping any computer on the WLAN.

STEP	CORRECTIVE ACTION
1	Check the Wi-Fi LED on the front of the unit and verify the WLAN is enabled as per the LED Indicator section.
2	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NF5 and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

Technical Data

The following table lists the hardware specifications of the NF5.

MODEL	NF5
Wireless WAN	PPP (for WCDMA / HSPA)
Ethernet WAN	1 x Gigabit WAN port (10/100/1000 Mbps)
Connectivity	1 x 10/100/1000 Mbps WAN, 4 x 10/100/1000 Mbps LAN, 1 x RJ-11 Telephone Handset, 1 x WLAN, 1 x USB 2.0
LED Indicators	Power, Mobile Broadband, WWW, WiFi, WAN, LAN 1-4, VoIP.
Operating Temperature	Operating temperature: 0˚C - 40˚C, Humidity: 10%-90% non-condensing Storage temperature: -10˚C - 70˚C, Humidity: 0%-95% non-condensing
Power Input	12V DC - 1.5A
Dimensions & Weight	168 mm (L) x 119 mm (W) x 27 mm (H) 226 grams
VoIP	PROTOCOL SIP 2.0 VOICE COMPRESSION G.711-Alaw voice compression G.711-Mulaw voice compression G.726-32 voice compression G.729AB voice compression G.168 116 ms tail line echo cancellation CALL FUNCTION Call forward Caller ID Dial plan Call waiting 3-way conference call Hot line
Regulatory Compliance	A-Tick

Electrical Specifications

It is recommended that the NF5 be powered by the supplied 12V DC, 1.5A power supply. A replacement power supply is available from the NetComm Wireless Online shop.

Environmental Specifications / Tolerances

The NF5 housing enables it to operate over a wide variety of temperatures from 0˚C - 40˚C (operating temperature).

Legal & Regulatory Information

Intellectual Property Rights

Customer Information

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

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

Consumer Protection Laws

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

Product Warranty

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

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

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

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

Limitation of Liability

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

Contact

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