

N300 WiFi Gigabit Router



NF12 USER GUIDE

Copyright

Copyright© 2015 NetComm Wireless Limited. All rights reserved.

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



Note: This document is subject to change without notice.

Save Our Environment

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

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

Please be responsible and protect our environment.

This manual covers the following products:

NF12 N300 WiFi Gigabit Router

DOCUMENT VERSION	DATE
1.0 – Initial document release	26 June 2015

Table of contents

Overview.....	5
Introduction.....	5
Target Users.....	5
Prerequisites.....	5
Notation.....	5
Product Introduction.....	6
Product Overview.....	6
Package Contents.....	6
Product Features.....	7
Physical Dimensions and Indicators.....	8
LED Indicators.....	8
Physical Dimensions.....	9
NF12 Default Settings.....	9
Interfaces.....	10
Safety and Product Care.....	11
Transport and Handling.....	11
Installation and Configuration.....	12
Placement of your NF12.....	12
Avoid obstacles and interference.....	12
Cordless Phones.....	12
Choose the “Quietest” Channel for your Wireless Network.....	12
Hardware installation.....	13
Connecting via a cable.....	13
Connecting wirelessly.....	13
Web Based Configuration Interface.....	14
First-time Setup Wizard.....	14
Device Info.....	15
Summary.....	15
WAN.....	16
Statistics.....	16
Route.....	17
ARP.....	17
DHCP.....	17
Advanced Setup.....	18
Layer2 Interface.....	18
WAN Service.....	18
LAN.....	24
NAT.....	26
Security.....	28
Parental Control.....	31
Quality of Service.....	32
Routing.....	34
DNS.....	36
UPnP.....	37
DNS Proxy.....	37
Interface Grouping.....	38
IP Tunnel.....	39
Certificate.....	40
Multicast (IGMP Configuration).....	41
Wireless.....	42
Basic.....	42
Security.....	43
MAC Filter.....	43
Wireless Bridge.....	44
Advanced.....	45
Station Info.....	46
Diagnostics.....	47
Diagnostics.....	47
Management.....	48
Settings.....	48
System Log.....	48

SNMP Agent	49
TR-069 Client	49
Internet Time	50
Access Control	51
Update Firmware	52
Save/Reboot	52
Additional Product Information	53
Establishing a wireless connection	53
Windows XP (Service Pack 3).....	53
Windows Vista.....	53
Windows 7	53
Mac OSX 10.6.....	53
Troubleshooting.....	54
Using the indicator lights (LEDs) to Diagnose Problems.....	54
Legal & Regulatory Information.....	55
Intellectual Property Rights.....	55
Customer Information	55
Consumer Protection Laws.....	55
Product Warranty	56
Limitation of Liability.....	56
Contact.....	57

Overview

Introduction






This guide provides information related to the installation, operation, and use of the NF12.

Target Users

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

Prerequisites

Before continuing with the installation of your NF12, please confirm that your equipment meets the minimum requirements below.

-  A configured WAN connection.
-  A computer with Windows®, Mac OS®, 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®, Safari®, etc.
-  Wireless computer system requirements:
 -  Computer with a working 802.11 b/g/n/ac wireless adapter.

Notation

The following symbols are used in this guide:



Indicates a note requiring attention.



Indicates a note providing a warning.



Indicates a note providing useful information.

Product Introduction

Product Overview

- 1 x 10/100/1000 Gigabit Ethernet WAN port for connection to fibre services
- 4 x 10/100/1000 Gigabit Ethernet LAN port for wired connections
- Wireless N300 Single Band Access point for multiple high speed WiFi Connections
- WPS button for simple setup of your wireless network
- NBN ready: carefully developed hardware and software features to ensure this device is optimised for use on the National Broadband Network
 - Wireline Routing Speeds
 - IGMP Snooping
 - IPTV IGMP v1 v2 Pass through
 - QoS
- IPv6 ready for the next generation IP addressing

Package Contents

The NF12 package consists of:

- 1 x N300 WiFi Gigabit Router
- 1 x Power Supply Unit (12V/1Amp)
- 1 x Ethernet Cable (RJ45)
- 1 x Wireless Security Card
- 1 x 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

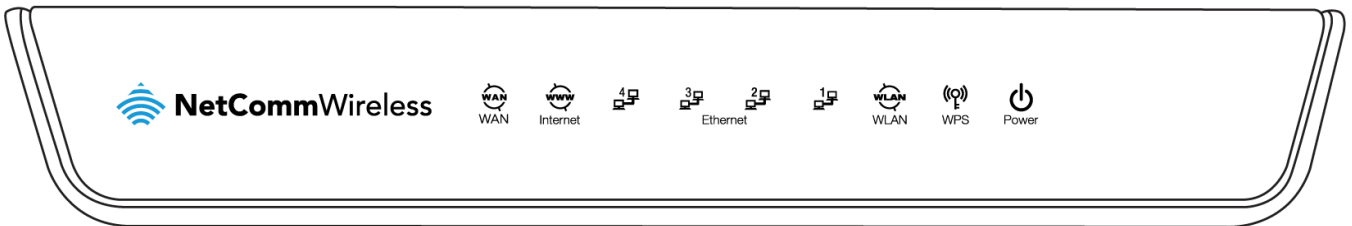
The NetComm Wireless NF12 is a future-ready WiFi router that connects home or office to super fast broadband. Simply connect your NBN/fibre connection to the Gigabit WAN port for an instant internet connection. The NF12 allow users to create a fast and powerful WiFi network with Wireless N speeds of up to 300Mbps¹, allowing WiFi enabled devices to connect to the router and share the internet connection. Up to four wired devices can also access the internet via the Gigabit LAN Ethernet ports. The device features Internet Protocol version 6 (IPv6) to prepare you for emerging technologies or applications associated with the next generation of internet.



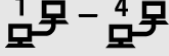



¹ Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

Physical Dimensions and Indicators

LED Indicators

The NF12 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 NF12 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
WAN		Off	No device is connected to the Ethernet WAN port.
		On	A device is connected to the Ethernet WAN port.
Internet		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.
WLAN		Off	The wireless radio is turned off.
		On	The wireless radio is turned on.
		Flashing	Data is being sent or received via the wireless radio.
WPS		Off	WPS is not active.
		Flashing	The NF-12 is waiting for a WPS PBC connection.
Power		Off	The NF-12 is powered off.
		On	The NF-12 is powered on and operating normally.
		Flashing	The NF-12 is starting up.

Physical Dimensions

The following table lists the physical dimensions and weight of the NF12.

NF12 DIMENSIONS	
Length (incl. antennas at 90 degrees)	150mm
Width	196mm
Height (not incl. antennas)	34mm
Weight	313g

NF12 Default Settings

The following tables list the default settings for the NF12.

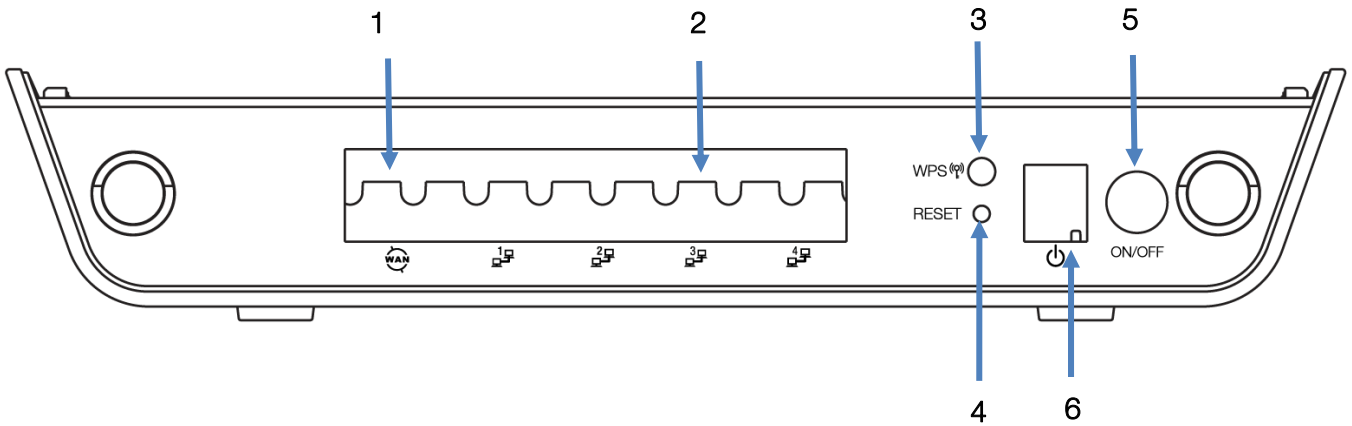
LAN (MANAGEMENT)	
Static IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

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

NF12 WEB INTERFACE ACCESS	
Username	admin
Password	admin

Interfaces




The following interfaces are available on the NF12:



NUMBER	INTERFACE	DESCRIPTION
1	WAN	Gigabit WAN port for connection to a WAN network.
2	LAN 1-4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
3	WPS button	Activate the WiFi WPS function by press/hold the WPS/RESET button for 1-3 seconds
4	Reset button	To reset the NF12 to the factory default settings, use a paper clip to hold down the reset button for 3 seconds, and then release it.
5	Power jack	Connection point for the included power adapter. Connect the power supply here.
6	Power button	Turns the NF12 on or off.

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 prevent the equipment from 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 NF12, we recommend that you return the product in the original packaging. This ensures the product will not be damaged.



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

Installation and Configuration

Placement of your NF12



The wireless connection between your NF12 and your WiFi devices will be stronger the closer your connected devices are to your NF12. Your wireless connection and performance will degrade as the distance between your NF12 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 NF12 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 NF12, please try the following steps:

-  In multi-storey homes, place the NF12 on a floor that is as close to the centre of the home as possible. This may mean placing the NF12 on an upper floor.
-  Try not to place the NF12 near a cordless telephone that operates at the same radio frequency as the NF12 (2.4GHz).





Avoid obstacles and interference

Avoid placing your NF12 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 NF12).

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 NF12 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 NF12.
-  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 NF12 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 NF12.
2. Plug the power adapter into the wall socket and switch on the power.
3. Wait approximately 60 seconds for the NF12 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 NF12.
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://192.168.1.1> into the address bar and press enter.
5. Follow the steps to set up your NF12.

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 NF12.



Note: Refer to the included Wireless Security Card for the default SSID and wireless security key of your NF12

3. When prompted for your wireless security settings, enter the Wireless security key configured on the NF12.
4. Wait approximately 30 seconds for the connection to establish.
5. Open your Web browser, and enter <http://192.168.1.1> into the address bar and press Enter.
6. Follow the steps to set up your NF12.

Web Based Configuration Interface

First-time Setup Wizard

Please follow the steps below to configure your NF12 Wireless router via the web based configuration wizard.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type <http://192.168.1.1/> into the address bar at the top of the window.

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



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

1. Click on **Basic Setup** on the left side of the screen. The wizard assists you in configuring the router and entering the information required to setup your Internet connection.

Basic > Quick Setup > Ethernet > PPPoE Information

Enter the User ID and Password assigned to you by your Internet Service Provider (ISP).

Protocol: PPPoE
User ID: tpg_acs@tpg_acs
Password:

Next

2. The Enable Wireless option is selected by default. If you wish to disable the wireless radio, remove the check from the Enable Wireless option. If you are using the wireless radio, enter your desired SSID (network name), then select an authentication type.

WPA2-PSK

This is the default authentication type.

Basic > Quick Setup > Wireless

Your router is already setup securely with a password and network name that is unique to every device. However you can choose alternative settings for these features if desired. From this page, you can configure your WiFi Network Name (SSID) and the WiFi security settings.

Enable Wireless

SSID: TPG BCED

Network Authentication: WPA2-PSK

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval: 0

WPA/WAPI Encryption: AES

Back Next

Device Info

Summary

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

Device Info

Manufacturer:	NetComm Wireless
Model:	NF12
Build Timestamp:	150515_1500
Serial Number:	64d95410bced
Firmware Version:	GRNV5.TT101B-B-NC-R4B019.EN
Bootloader (CFE) Version:	5.60.120-0.0
Wireless Driver Version:	5.100.138.23
Uptime:	0D 0H 8M 28S

This information reflects the current status of your WAN connection.

LAN IPv4 Address:	192.168.1.1
Default Gateway:	
WAN IP Address:	
Primary DNS Server:	
Secondary DNS Server:	
LAN IPv6 Address:	fe80::1/64
Default IPv6 Gateway:	
Date/Time:	Sat Jan 1 00:08:29 2000

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

WAN

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

WAN Info

Interface	Description	Type	VLAN Mux ID	IGMP	NAT	Firewall	IPv4 Status	IPv6 Status	IPv4 Address	IPv6 Address
eth4.1	ipoe_eth4.10	IPoE	10	Disabled	Enabled	Enabled	Unconfigured	Unconfigured	0.0.0.0	

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

Statistics

LAN

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

Statistics -- LAN

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
eth0	0	11249	0	0	0	6497	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
wl0	0	0	0	0	0	0	0	0

[Reset Statistics](#)

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Statistics – WAN Service

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

Statistics -- WAN

Interface	Description	Received				Transmitted			
		Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
eth4.1	ipoe_eth4.10	0	0	0	0	0	0	0	0

[Reset Statistics](#)

INTERFACE	DESCRIPTION	
Received/Transmitted	Bytes	Rx/Tx (receive/transmit) packets in bytes.
	Packets	Rx/Tx (receive/transmit) packets.
	Errors	Rx/Tx (receive/transmit) packets with errors.
	Drops	Rx/Tx (receive/transmit) packets with drops.

Route

The Route page displays any routes that the router has detected.

Device Info -- Route

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate

D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

ARP

Click ARP to display the ARP information.

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

Device Info -- ARP

IP address	Flags	HW Address	Device
192.168.1.100	Complete	2C:44:FD:12:3C:6E	br0

DHCP

Click DHCP to display the DHCP information.

Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
NTCWKS0072	2c:44:fd:12:3c:6e	192.168.1.100	23 hours, 19 minutes, 45 seconds

You can use this to determine when a specific DHCP lease will expire, or to assist you with setting up Static DHCP addressing.

Advanced Setup

Layer2 Interface

ETH Interface

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

ETH WAN Interface Configuration

Choose Add, or Remove to configure ETH WAN interfaces.
Allow one ETH as layer 2 wan interface.

Interface/(Name)	Connection Mode	Remove
eth0/WAN	VlanMuxMode	<input type="checkbox"/>

Remove

WAN Service

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

Wide Area Network (WAN) Service Setup

Choose Add, Remove or Edit to configure a WAN service over a selected interface.

Interface	Description	Type	VLAN 802.1p	VLAN Mux ID	IGMP	NAT	Firewall	IPv4	IPv6	MLD	Remove	Edit
ppp0.1	pppoe_eth0	PPPoE	N/A	N/A	Disabled	Enabled	Enabled	Enabled	Disabled	Disabled	<input type="checkbox"/>	edit

Add Remove

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

WAN Service Interface Configuration

Select a layer 2 interface for this service

eth0/WAN ▾

Back Next

Select a WAN service type, enter a **Service Description**, enter the **802.1P Priority** and **802.1 VLAN ID** then click the **Next** button.

WAN Service Configuration

Select WAN service type:

- PPP over Ethernet (PPPoE)
- IP over Ethernet
- Bridging

Enter Service Description:

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.
For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

Enter 802.1P Priority [0-7]:

Enter 802.1Q VLAN ID [0-4094]:

Back Next

PPP over Ethernet

Enter the details as required by your Internet Service Provider and click the **Next** button.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method: **AUTO**

MTU[576-1492]:

- Enable IPv4 for this service
- Enable NAT
- Enable Fullcone NAT
- Enable Firewall
- Dial on demand (with idle timeout timer)
- PPP IP extension
- Use Static IPv4 Address
- Enable IPv6 for this service
- Enable PPP Debug Mode
- Bridge PPPoE Frames Between WAN and Local Ports

Multicast Proxy

- Enable IGMP Multicast Proxy

Select the Default Gateway for the WAN interface. Click the **Next** button.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0.1

Available Routed WAN Interfaces

ppp1.2

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

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

ppp0.1

->

<-

Available WAN Interfaces

ppp1.2

Back

Next

A summary of your settings is displayed. Click **Apply/Save** to finish.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back

Apply/Save

IP over Ethernet

Enter the details as required by your Internet Service Provider and click the **Next** button.

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in IPoE mode.

If "Use the following Static IPv4/IPv6 address" is chosen, enter the WAN IPv4/IPv6 address, subnet mask/prefix Length and interface gateway.

Enable IPv4 for this service

Obtain an IP address automatically

Option 55 Request List : (e.g:1,3,6,12)

Option 58 Renewal Time: (hour)

Option 59 Rebinding Time: (hour)

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: Disable Enable

Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Primary DNS server:

Secondary DNS server:

Enable IPv6 for this service

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

Network Address Translation Settings

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

- Enable NAT
- Enable Fullcone NAT
- Enable Firewall

IGMP Multicast

- Enable IGMP Multicast

Select the Default Gateway for the WAN interface. Click the **Next** button.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

ppp0.1

->

<-

Available Routed WAN Interfaces

eth0.2

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

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces



Back Next

A summary of your settings is displayed. Click **Apply/Save** to finish.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

Bridging

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

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

Use the arrow buttons to move the interfaces required to the list on the left. Click **Next**.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces

eth4.1

->

<-

Available Routed WAN Interfaces

ppp0.2

Back Next

DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces

eth4.1

->

<-

Available WAN Interfaces

ppp0.2

Back Next

A summary of your settings is displayed. Click **Apply/Save** to commit your settings to the router.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

LAN

The LAN window allows you to modify the settings for your local area network (LAN).

IPv4 Autoconfig

Configure the Broadband Router IP Address and Subnet Mask for LAN interface. Group Name **Default** ▼

IP Address:

Subnet Mask:

Enable IGMP Snooping

Enable LAN side firewall

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time: week:

 day:

 hour:

 minute:

 second:

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address	IP Address	Remove
<input type="button" value="Add Entries"/> <input type="button" value="Remove Entries"/>		

Configure the second IP Address and Subnet Mask for LAN interface

The following options are available to configure:

PARAMETER	DEFINITION
IP Address	Enter the IP Address to use for the NF12
Subnet Mask	Enter the subnet mask
Enable IGMP Snooping	Enable IGMP Snooping and select the IGMP Snooping mode to use
Enable LAN side Firewall	Enable the LAN side firewall to restrict traffic between LAN hosts
Enable DHCP Server	Select to enable or disable the DHCP server and enter the start and end address for the DHCP IP Address pool.
Configure the second IP Address	This option enables you to set a secondary IP Address for the NF12

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

DHCP Static IP Lease

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

MAC Address:

IP Address:

To set a DHCP reservation, enter the MAC Address of the chosen host and IP to use and then click Apply/Save.

The NF12 enables you to set the DHCP options which are provided to hosts attempting to connect to the DHCP server.

These options should not normally need to be set or changed.

Click Apply/Save to save the new LAN configuration settings.

IPv6 Autoconfig

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

IPv6 LAN Auto Configuration

Note: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Interface ID does NOT support ZERO COMPRESSION "::". Please enter the complete information. For example, Please enter "0:0:0:2" instead of "::2".

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

Enable DHCPv6 Server and RADVD

Stateless

Stateful

Start interface ID:	<input type="text" value="0:0:0:2"/>
End interface ID:	<input type="text" value="0:0:0:254"/>
Leased Time: week:	<input type="text" value="0"/>
day:	<input type="text" value="1"/>
hour:	<input type="text" value="0"/>
minute:	<input type="text" value="0"/>
second:	<input type="text" value="0"/>

Site Prefix Configuration

Delegated Site Prefix from WAN

Static Site Prefix

Site Prefix:

Site Prefix Length:

Enable MLD Snooping

Save/Apply

OPTION	DEFINITION
Static LAN IPv6 Address Configuration	Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider.
Enable DHCPv6 Server and RADVD	The Router Advertisement Daemon (radvd) is an open-source software product that implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) as specified in RFC 2461. The Router Advertisement Daemon is used by system administrators in stateless auto-configuration methods of network hosts on Internet Protocol version 6 networks. When IPv6 hosts configure their network interfaces, they broadcast router solicitation (RS) requests onto the network to discover available routers. The radvd software answers requests with router advertisement (RA) messages. In addition, radvd periodically broadcasts RA packets to the attached link to update network hosts. The router advertisement messages contain the routing prefix used on the link, the link maximum transmission unit (MTU), and the address of the responsible default router.
Stateless	IPv6 hosts can configure themselves automatically when connected to a routed IPv6 network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. This type of configuration is suitable for small organizations and individuals. It allows each host to determine its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address.
Stateful	This configuration requires some human intervention as it makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for installation and administration of nodes over a network. The DHCPv6 server maintains a list of nodes and the information about their state to know the availability of each IP address from the range specified by the network administrator.
Enable MLD Snooping	Select whether to enable or disable MLD Snooping on the router. The Multicast Listener Discovery (MLD) snooping function constrains the flooding of IPv6 multicast traffic on VLANs on the router.

NAT

Virtual Servers

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

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------------	--------

Click the **Add** button to add a virtual server.

NAT -- Virtual Servers

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.
NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".
 Remaining number of entries that can be configured:32

Use Interface:

Service Name:

Select a Service:

Custom Service:

Enable LAN Loopback

Server IP Address:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

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

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

Port Triggering

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

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

NAT – Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application Name	Trigger				Open			WAN Interface	Remove
	Protocol	Port Range		Protocol	Port Range				
		Start	End		Start	End			

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

NAT – Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click "Save/Apply" to add it.

Remaining number of entries that can be configured:32

Use Interface:

Application Name:

Select an application:

Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾
		TCP ▾			TCP ▾

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

DMZ Host

The NF12 will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

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

NAT -- DMZ Host

The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

Enter the computer's IP address and click 'Apply/Save' to activate the DMZ host.

Clear the IP address field and click 'Apply/Save' to deactivate the DMZ host.

Enable DMZ host.
DMZ Host IP Address:

Enable LAN Loopback

Apply/Save

Security

IP Filtering

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

Outgoing IP Filtering

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

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

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

Add IP Filter -- Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

Apply/Save

Enter the following parameters:

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

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

Incoming IP Filtering

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

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

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

Add IP Filter -- Incoming

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

IP Version:

Protocol:

Source IP address[/prefix length]:

Source Port (port or port:port):

Destination IP address[/prefix length]:

Destination Port (port or port:port):

WAN Interfaces (Configured in Routing mode and with firewall enabled) and LAN Interfaces

Select one or more WAN/LAN interfaces displayed below to apply this rule.

- Select All
- pppoe_eth0/ppp0.1
- br0/br0

Apply/Save

Enter the following parameters:

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

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

MAC Filtering

The NF12 offers the ability to use MAC Address filtering on ATM PVCs. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow connections which match the criteria.

MAC Filtering Setup

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

MAC Filtering Policy For Each Interface (maximum 32 entries):

WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Interface	Policy	Change
-----------	--------	--------

Change Policy

Choose Add or Remove to configure MAC filtering rules.

Interface	Protocol	Destination MAC	Source MAC	Frame Direction	802.1p Priority	VLAN ID	Remove
<div style="display: flex; justify-content: center; gap: 20px;"> Add Remove </div>							

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

Add MAC Filter

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click 'Apply' to save and activate the filter.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

802.1p Priority:

Tag VLAN ID [0-4094]:

WAN Interfaces (Configured in Bridge mode only)

Save/Apply

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

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

Parental Control

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

Time Restriction

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

Access Time Restriction -- A maximum 16 entries can be configured.

Rule name	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>											

Figure 1: Advanced - Parental Control – Time Restriction

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

Access Time Restriction

This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the 'Other MAC Address' button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type 'ipconfig /all'.

Rule Name

Browser's MAC Address
 Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week	Mon	Tue	Wed	Thu	Fri	Sat	Sun
Click to select	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Figure 2: Advanced - Parental Control - Add Time Restriction

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

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

Table 1: Advanced - Parental Control - Add Time Restriction Settings

URL Filter

With the URL filter, you are able to add certain websites or URLs to a safe or blocked list. This will provide you added security to ensure any website you deem unsuitable will not be able to be seen by anyone who is accessing the Internet via the NF12.

Select the 'To block' or 'To allow' option and then click Add to enter the URL you wish to add to the URL Filter list.

URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured.

URL List Type: Black List White List

Address	Port	Remove

Figure 3: Advanced - Parental Control - URL Filter

Once you have chosen to add a URL to the list you will be prompted to enter the address. Simply type it in and select the **Apply/Save** button.

Parental Control -- URL Filter Add

Enter the URL address and port number then click 'Apply/Save' to add the entry to the URL filter.

URL Address:

Port Number: (Default 80 will be applied if leave blank.)

Figure 4: Advanced - Parental Control - Add URL Filter

Quality of Service

Quality of Service offers a defined level of performance in a data communications system - for example the ability to guarantee that video traffic is given priority over other network traffic to ensure that video streaming is not disrupted by other network traffic. This means that if you are streaming video and someone else in the house starts downloading a large file, the download won't disrupt the flow of video traffic.

QoS -- Queue Management Configuration

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

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

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Enable QoS

Figure 5: Advanced - Enable QoS

To enable QoS select the **Enable QoS** checkbox, and set the **Default DSCP (Differentiated Services Code Point) Mark**. Then press the **Apply/Save** button.

QoS Queue

QoS Queue Setup

In ETH mode, maximum 8 queues can be configured.
 For each Ethernet interface, maximum 4 queues can be configured.
 If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Scheduler	Precedence	DSL Latency	Enable	Remove
WMM Voice Priority	1	wl0	SP	1		Enabled	
WMM Voice Priority	2	wl0	SP	2		Enabled	
WMM Video Priority	3	wl0	SP	3		Enabled	
WMM Video Priority	4	wl0	SP	4		Enabled	
WMM Best Effort	5	wl0	SP	5		Enabled	
WMM Background	6	wl0	SP	6		Enabled	
WMM Background	7	wl0	SP	7		Enabled	
WMM Best Effort	8	wl0	SP	8		Enabled	

Figure 6: Advanced - QoS Queue Setup

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

QoS Queue Configuration

This screen allows you to configure a QoS queue and assign it to a specific layer2 interface. The scheduler algorithm is defined by the layer2 interface.

Note: For SP scheduling, queues assigned to the same layer2 interface shall have unique precedence. Lower precedence value implies higher priority for this queue relative to others

Click 'Apply/Save' to save and activate the queue.

Name:

Enable: ▾

Interface:

Figure 7: Advanced - QoS - Add QoS Queue

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

NOTE: Precedence level 1 relates to higher priority while precedence level 3 relates to lower priority.

QoS Classification

QoS Classification Setup -- A maximum 32 entries can be configured.

Choose Add or Remove to configure network traffic classes.
 If you disable WMM function in Wireless Page, classification related to wireless will not take effects
 The QoS function has been disabled. Classification rules would not take effects.

		CLASSIFICATION CRITERIA												CLASSIFICATION RESULTS								
Class Name	Order	Class Interface	Ethernet Type	Source MAC/ Mask	Destination MAC/ Mask	Source IP/Prefix Length	Destination IP/Prefix Length	Protocol	Source Port	Destination Port	DSCP Check	TOS/TC Check	802.1P Check	Queue Key	DSCP Mark	TOS/TC Mark	802.1P Mark	VlanID Tag	Rate Control	Enable	Remove	

Figure 8: Advanced - QoS Classification Setup

Click the **Add** button to configure network traffic classes.

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the rule.

Traffic Class Name:

Rule Order: ▾

Rule Status: ▾

Specify Classification Criteria
A blank criterion indicates it is not used for classification.

Class Interface: ▾

Ether Type: ▾

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results
Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue: ▾

▾

Mark 802.1p priority: ▾

Figure 9: Advanced - Add QoS Network Traffic Classification

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

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

Routing

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

Default Gateway

Select your preferred WAN interface from the available options.

Routing -- Default Gateway

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Selected Default Gateway Interfaces:

Available Routed WAN Interfaces:

Select a preferred wan interface as the system default IPv6 gateway.

Selected WAN Interface: ▾

Figure 10: Advanced - Routing - Default Gateway

Static Route

The Static Route screen displays the configured static routes. Click the **Add** or **Remove** buttons to change settings.

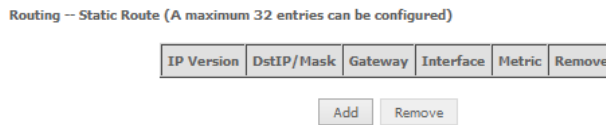


Figure 11: Advanced - Routing - Static Route

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

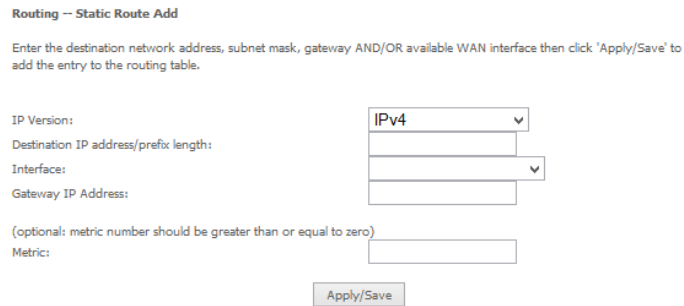


Figure 12: Advanced - Routing - Add Static Route

Enter the Destination Network Address, Subnet Mask, Gateway IP Address and/or WAN Interface. Then click Apply/Save to add the entry to the routing table.

RIP (Routing Information Protocol)

To activate this option, select the Enabled checkbox.

To configure an individual interface, select the desired RIP version and operation, and select the Enabled checkbox for that interface. Click **Apply/Save** to save the configuration.

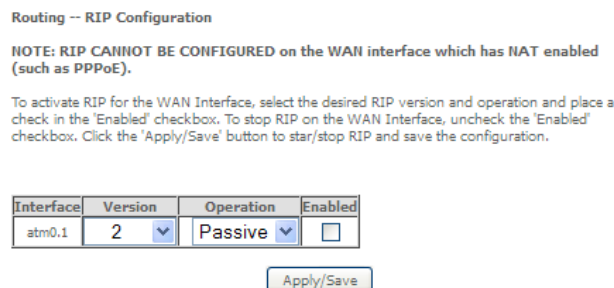


Figure 13: Advanced - Routing - RIP

DNS

DNS Server

This page allows you to enable automatic DNS settings detected from the Internet Service Provider or specify your own DNS server address manually.

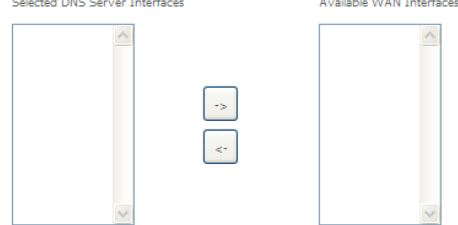
DNS Server Configuration

Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Select DNS Server Interface from available WAN interfaces:

Selected DNS Server Interfaces Available WAN Interfaces



Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Figure 14: Advanced - DNS Server

Dynamic DNS

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

Dynamic DNS

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

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove

Figure 15: Advanced - DNS - Dynamic DNS



Note: The Add/Remove buttons will be displayed only if the router has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and the following screen will display.

Add Dynamic DNS

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

D-DNS provider

Hostname

Interface

DynDNS Settings

Username

Password

Figure 16: Advanced - DNS - Add Dynamic DNS Account

FIELD	DESCRIPTION
D-DNS Provider	Select the dynamic DNS provider from the list.
Host Name	The name of the dynamic DNS provider.
Interface	Select the interface from the list.
Username	Enter the Dynamic DNS account username.
Password	Enter the Dynamic DNS account password.

Table 2: Advanced - DNS - Add Dynamic DNS Account Settings

UPnP

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

UPnP Configuration

NOTE: UPnP is activated only when there is a live WAN service with NAT enabled.

Enable UPnP

Figure 17: Advanced – UPnP

DNS Proxy

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

DNS Proxy Configuration

Enable DNS Proxy

Host name of the Broadband Router:

Domain name of the LAN network:

Figure 18: Advanced - DNS Proxy

The Host Name and Domain name are combined to form a unique label that is mapped to the router IP address. This can be used to access the user interface of the router with a local name rather than by using the router IP address.

Interface Grouping

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

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

Interface Grouping -- A maximum 16 entries can be configured

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Group Name	Remove	WAN Interface	LAN Interfaces
Default		ppp0.1	LAN1
			LAN2
			LAN3
			LAN4
			wlan0
			wl0_Guest1
			wl0_Guest2
			wl0_Guest3

Click **Add** to create an Interface group.

Interface grouping Configuration

To create a new interface group:

1. Enter the Group name and the group name must be unique.
2. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.
3. Click Save/Apply button to make the changes effective immediately.

Group Name:

Grouped Interfaces

->

<-

Available Interfaces

pppoe_eth0/ppp0.1

LAN1

LAN2

LAN3

LAN4

wlan0

wl0_Guest1

wl0_Guest2

wl0_Guest3

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

IP Tunnel

The IP Tunnelling feature allows you to configure tunnelling of traffic between IPv6 and IPv4 networks.
IPv6inIPv4

IP Tunneling -- 6in4 Tunnel Configuration

Name	Wan	Lan	Dynamic	IPv4 Mask Length	6rd Prefix	Border Relay Address	Remove
------	-----	-----	---------	------------------	------------	----------------------	--------

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

IP Tunneling -- 6in4 Tunnel Configuration

Currently, only 6rd configuration is supported.

Tunnel Name:

Mechanism:

6RD

Associated WAN Interface:

Associated LAN Interface:

LAN/br0

Manual
 Automatic

IPv4 Mask Length:

6rd Prefix with Prefix Length:

Border Relay IPv4 Address:

IPv4inIPv6

IP Tunneling -- 4in6 Tunnel Configuration

Name	Wan	Lan	Dynamic	Remote IPv6 Address	Remove
<input type="button" value="Add"/> <input type="button" value="Remove"/>					

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

IPSec Tunnel Mode Connections

Add, edit or remove IPSec tunnel mode connections from this page.

Tunnel Name:

Mechanism: ▼

Associated WAN Interface: ▼

Associated LAN Interface: ▼

Manual
 Automatic

Remote IPv6 Address:

Certificate

Local

Local Certificates

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

Name	In Use	Subject	Type	Action
<input type="button" value="Create Certificate Request"/> <input type="button" value="Import Certificate"/>				

Trusted CA

Trusted CA (Certificate Authority) Certificates

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

Name	Subject	Type	Action
<input type="button" value="Import Certificate"/>			

Multicast (IGMP Configuration)

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is a protocol only used on the network between a host and the router. It allows a host to inform the router whenever that host needs to join or leave a particular multicast group. IGMP provides for more efficient allocation of resources when used with online gaming and video streaming.

IGMP Configuration

Enter IGMP protocol configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="2"/>
Query Interval (s):	<input type="text" value="125"/>
Query Response Interval (1/10s):	<input type="text" value="100"/>
Last Member Query Interval (1/10s):	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="25"/>
Maximum Multicast Data Sources (for IGMPv3):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="25"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

MLD Configuration

Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default values shown below.

Default Version:	<input type="text" value="2"/>
Query Interval (s):	<input type="text" value="125"/>
Query Response Interval (1/10s):	<input type="text" value="100"/>
Last Member Query Interval (1/10s):	<input type="text" value="10"/>
Robustness Value:	<input type="text" value="2"/>
Maximum Multicast Groups:	<input type="text" value="10"/>
Maximum Multicast Data Sources (for mldv2):	<input type="text" value="10"/>
Maximum Multicast Group Members:	<input type="text" value="10"/>
Fast Leave Enable:	<input checked="" type="checkbox"/>

Apply/Save

FIELD	DEFINITION
Default Version	The version IGMP in use by the router.
Query Interval	The hosts on the segment report their group membership in response to the router's queries. The query interval timer is also used to define the amount of time a router will store particular IGMP state if it does not hear any reports on the group. The query interval is the time in seconds between queries sent from the router to IGMP hosts.
Query Response Interval	When a host receives the query packet, it starts counting to a random value, less the maximum response time. When this timer expires, the host replies with a report, provided that no other host has responded yet. This accomplishes two purposes: a) Allows controlling the amount of IGMP reports sent during a time window. b) Engages the report suppression feature, which permits a host to suppress its own report and conserve bandwidth.
Last Member Query Interval	IGMP uses this value when router hears IGMP Leave report. This means that at least one host wants to leave the group. After router receives the Leave report, it checks that the interface is not configured for IGMP Immediate Leave (single-host on the segment) and if not, it sends out an out-of-sequence query.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. You can also click the scroll arrows to select a new setting. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	The maximum number of multicast groups that the router can control at any one time.
Maximum Multicast Data Sources	The maximum number of data sources a multicast group can have.
Maximum Multicast Group Members	The maximum number of hosts a multicast group can have.
Fast Leave Enable	With IGMP fast-leave processing, which means that the router immediately removes the interface attached to a receiver upon receiving a Leave Group message from a IGMP host.

Wireless

Basic

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

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click 'Apply/Save' to configure the basic wireless options.

- Enable Wireless
- Hide Access Point
- Clients Isolation
- Disable WMM Advertise
- Enable Wireless Multicast Forwarding (WMF)
- Support WPS v2.0

SSID:

BSSID: 64:D9:54:10:BC:EE

Country:

Max Clients:

Wireless - Guest/Virtual Access Points:

Enabled	SSID	Hidden	Isolate Clients	Enable WMM Advertise	Enable WMF	Max Clients	BSSID
<input type="checkbox"/>	<input type="text" value="WLAN_Guest1"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A
<input type="checkbox"/>	<input type="text" value="WLAN_Guest2"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A
<input type="checkbox"/>	<input type="text" value="WLAN_Guest3"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="32"/>	N/A

Figure 19: Wireless - Basic

The following parameters are available:

PARAMETER	DEFINITION
Enable Wireless	Select to enable or disable the wireless network function
Hide Access Point	Select to hide or display the wireless network when an SSID scan is performed
Clients Isolation	Select to prevent clients on the wireless network being able to access each other
Disable WMM Advertise	Select to prevent the NF12 advertising its WMM function
Enable Multicast Forwarding (WMF)	Select to enable Wireless Multicast Forwarding. This can reduce latency and improve throughput for wireless clients
Max Clients	Enter the maximum number of wireless clients able to connect to the wireless network
Wireless Guest Network	Select to enable a separate Wireless Guest network, the same options are available for a Guest network as with the main system wireless network.

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

Security

The NF12 supports all encryptions within the 802.11 standard. The factory default is WPA2-PSK. The NF12 also supports WPA, WPA-PSK, WPA2, WPA2-PSK. You can also select to enable WPS mode.

Wireless -- Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually
OR
through WiFi Protected Setup(WPS)
Note:When both STA PIN and Authorized MAC are empty, PBC is used.AP PIN set is always valid.If Hide Access Point enabled or Mac filter list is empty with 'allow' chosen, WPS2 will be disabled

WPS Setup

Enable WPS:

AddClient

WPSv1 worked with WPA2-PSK,WPA/WPA2-PSK,WPA-PSK mode.
WPSv2 worked with WPA2-PSK,WPA/WPA2-PSK mode.

Push-Button Enter STA PIN USE AP PIN

Set WPS AP Mode:

AP PIN: 30254749 [Help](#)

Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Apply/Save' when done.

Select SSID:

Network Authentication:

WPA/WAPI passphrase: [Click here to display](#)

WPA Group Rekey Interval:

WPA/WAPI Encryption:

Figure 20: Wireless - Security

The following parameters are available:

PARAMETER	DEFINITION
Enable WPS	Select to enable or disable the WPS function of the NF12.
Select SSID	Select the SSID to apply the security settings to.
Network Authentication	Select the Wireless security type to use with the wireless network.
WPA/WAPI passphrase	Enter the security key to use with the wireless network.
WPA Group Rekey Interval	Enter the group rekey interval. This should not need to change.
WPA/WAPI Encryption	Select the type of encryption to use on the wireless network.
WEP Encryption	Select to utilise WEP encryption on the wireless network connection.

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

MAC Filter

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

Wireless -- MAC Filter

Select SSID:

MAC Restrict Mode: Disabled Allow Deny

Click **Add** to add a MAC Address Filter.

Wireless -- MAC Filter

Enter the MAC address and click 'Apply/Save' to add the MAC address to the wireless MAC address filters.

MAC Address:

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

Wireless Bridge

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

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.

Click "Refresh" to update the remote bridges. Wait for few seconds to update.
Click "Apply/Save" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Select the mode for the Wireless Access Point built into the NF12. You can specify which wireless networks will be allowed to connect to the NF12 by using the 'Bridge Restrict' option and then entering the applicable MAC Addresses of the other wireless access points.

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

Advanced

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

Wireless -- Advanced

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click 'Apply/Save' to configure the advanced wireless options.

Band:	<input type="text" value="2.4GHz"/>	
Channel:	<input type="text" value="Auto"/>	Current: 6(interference: acceptable)
Auto Channel Timer(min)	<input type="text" value="0"/>	
802.11n/EWC:	<input type="text" value="Auto"/>	
Bandwidth:	<input type="text" value="40MHz"/>	Current: 40MHz
Control Sideband:	<input type="text" value="Lower"/>	Current: Upper
802.11n Rate:	<input type="text" value="Auto"/>	
802.11n Protection:	<input type="text" value="Auto"/>	
Support 802.11n Client Only:	<input type="text" value="Off"/>	
RIFS Advertisement:	<input type="text" value="Off"/>	
OBSS Co-Existence:	<input type="text" value="Disable"/>	
RX Chain Power Save:	<input type="text" value="Disable"/>	Power Save status: Full Power
RX Chain Power Save Quiet Time:	<input type="text" value="10"/>	
RX Chain Power Save PPS:	<input type="text" value="10"/>	
54g Rate:	<input type="text" value="1 Mbps"/>	
Multicast Rate:	<input type="text" value="Auto"/>	
Basic Rate:	<input type="text" value="Default"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
DTIM Interval:	<input type="text" value="1"/>	
Beacon Interval:	<input type="text" value="100"/>	
Global Max Clients:	<input type="text" value="32"/>	
XPress Technology:	<input type="text" value="Enable"/>	
Transmit Power:	<input type="text" value="100%"/>	
WMM(Wi-Fi Multimedia):	<input type="text" value="Enabled"/>	
WMM No Acknowledgement:	<input type="text" value="Disabled"/>	
WMM APSD:	<input type="text" value="Enabled"/>	

Click **Apply/Save** to save any changes to the wireless network settings configuration.

PARAMETER	DEFINITION
Band	You can select 2.4GHz or 5GHz.
Channel	Fill in the appropriate channel to correspond with your network settings. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto channeling functionality.
Auto Channel Timer(min)	Specifies the timer of auto channelling.
802.11n/EWC	Select disable 802.11n or Auto.
Bandwidth	Select the bandwidth for the network. You can select 20MHz in Both Bands, 20MHz in 2.4G Band and 40MHz in 5G Band, or 40MHz in Both Bands.
Control Sideband	If you select 20MHz in Both Bands or 20MHz in 2.4G Band and 40MHz in 5G Band, the service of control sideband does not work. When you select 40MHz in Both Bands as the bandwidth, the following page appears. Then you can select Lower or Upper as the value of sideband. As the control sideband, when you select Lower, the channel is 1~7. When you select Upper, the channel is 5~11.
802.11n Rate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
802.11n Protection	The 802.11n standards provide a protection method so 802.11b/g and 802.11n devices can co-exist in the same network without "speaking" at the same time.
Support 802.11n Client Only	Only stations that are configured in 802.11n mode can associate.
Multicast Rate	Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default value is Auto.
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.
RTS Threshold	This value should remain at its default setting of 2347. Should you encounter inconsistent data flow, only minor reductions are recommended. Should you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of 2347.
DTIM Interval	(Delivery Traffic Indication Message) Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM.) A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms). Default (100) is recommended.
XPress Technology	Select Enable or Disable. This is a special accelerating technology for IEEE802.11g. The default is Disabled.
Transmit Power	Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
WMM (Wi-Fi Multimedia)	Select whether WMM is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	Select whether ACK in WMM packet. By default, the 'Ack Policy' for each access category is set to Disable, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. To disable the acknowledgement can be useful for Voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	APSD is short for automatic power save delivery, Selecting enable will make it has very low power consumption. WMM Power Save is an improvement to the 802.11e amendment adding advanced power management functionality to WMM.

Station Info

This page shows the MAC address of authenticated wireless stations that are connected to the NF-12 and their status

Wireless -- Authenticated Stations

This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface
-----	------------	------------	------	-----------

Refresh

Diagnostics

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. You may diagnose the connection by clicking the **Test** button or click the **Test With OAM F4** button. If the test continues to fail, click **Help** and follow the troubleshooting procedures.

Diagnostics

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

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

Diagnostics

The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network

Test your LAN1 Connection:	FAIL	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

Rerun Diagnostic Tests

FIELD	DESCRIPTION
eth Connection	Pass: Indicates the Ethernet connection to your computer is connected to the LAN port of the router. Fail: Indicates that the router does not detect the Ethernet interface of your computer.
Test your Wireless Connection	Pass: Indicates that the wireless card is switched ON. Fail: Indicates that the wireless card is switched OFF.

Management

Settings

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

Backup

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings.

You will be prompted for the location to save the backup file to on your PC.

Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

Backup Settings

System Log

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

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click 'View System Log' to view the System Log.

Click 'Configure System Log' to configure the System Log options.

View System Log

Configure System Log

To configure the system log, click the **Configure System Log** button.

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

Apply/Save

SNMP Agent

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this, the administrator typically runs an SNMP management station program such as MIB browser on a local host to obtain information from the SNMP agent, in this case the NF1ADV (if SNMP is enabled). An SNMP 'community' performs the function of authenticating SNMP traffic. A 'community name' acts as a password that is typically shared among SNMP agents and managers.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click 'Apply' to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:	public
Set Community:	private
System Name:	NF12
System Location:	unknown
System Contact:	unknown
Trap Manager IP:	0.0.0.0

Save/Apply

TR-069 Client

TR-069 enables provisioning, auto-configuration or diagnostics to be automatically performed on your router if supported by your Internet Service Provider (ISP).

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

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

Inform Disable Enable

Inform Interval:	86400
ACS URL:	https://pppacs.tpg.com.a
ACS Username:	TPGACUser
ACS Password:
WAN Interface used by TR-069 client:	Any_WAN ▾

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:	TPGCPEuser
Connection Request Password:
Connection Request Port:	30005

Apply/Save

Get RPC Methods

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

Internet Time

Enable Internet Time to automatically synchronize your time with an Internet based time server. You can use up to 5 NTP servers.

Time settings

This page allows you to the modem's time configuration.

Automatically synchronize with Internet time servers

First NTP time server:	Other	0.netcomm.pool.ntp.org
Second NTP time server:	Other	1.netcomm.pool.ntp.org
Third NTP time server:	None	
Fourth NTP time server:	None	
Fifth NTP time server:	None	

Current Router Time: Sat Jan 1 04:36:01 2000

Time zone offset: (GMT+10:00) Canberra, Melbourne, Sydney



Enable Daylight Saving Time

Apply/Save

Enter your select NTP server to use for time synchronisation, select your time zone and then click Apply/Save to save the new Internet Time settings.

Access Control




The Access Control option found in the Management drop down menu configures access related parameters in the following three areas:

-  Passwords
-  Services Control

Access Control is used to control local and remote management settings for your router.

Passwords

The Passwords option configures your account access password for your modem. Access to the device is limited to the following three user accounts:

-  admin is to be used for local unrestricted access control
-  support is to be used for remote maintenance of the device
-  user is to be used to view information and update device firmware

Use the fields illustrated in the screen below to change or create your password. Passwords must be 16 characters or less with no spaces. Click the Apply/Save button after making any changes to continue.

Access Control -- Passwords

Access to your LAN router is controlled through three user accounts: admin, support and user .

The user name "admin" has unrestricted access to change and view configuration of your LAN Router.

The user name "support" is used to allow an ISP technician to access your LAN Router for maintenance and to run diagnostics.

The user name "user" can access the LAN Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 15 characters and click 'Apply/Save' to change or create passwords. Note: Password cannot contain a space.

Username:	<input type="text"/>
New Username:	<input type="text"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

Apply/Save

Services Control

The Service Control List (SCL) allows you to enable or disable your Local Area Network (LAN) or Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SAMBA, SNMP, SSH, TELNET, and TFTP. Click the **Apply/Save** button after making any changes to continue.

Access Control -- Services

Services access control list (SCL) enable or disable the running services.

Services	LAN	WAN	Port
HTTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="80"/>
TELNET	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="23"/>
SSH	<input type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="22"/>
FTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="21"/>
TFTP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="69"/>
ICMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="0"/>
SNMP	<input checked="" type="checkbox"/> enable	<input type="checkbox"/> enable	<input type="text" value="161"/>

Apply/Save

Update Firmware

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

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

Tools -- Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the 'Browse' button to locate the image file.

Step 3: Click the 'Update Firmware' button once to upload the new image file.

NOTE: The update process takes about 2 minutes to complete, and your Broadband Router will reboot.

Firmware File Name: No file selected.

Save/Reboot

This option reboots the NF12.

Click the button below to reboot the router.

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

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

Additional Product Information

Establishing a wireless connection

Windows 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 NF12 with "Connected" next to it.

Mac OSX 10.6

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



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

Troubleshooting

Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NF12 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 NF12 and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF12 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 NF12. 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 NF12'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 3 seconds and then releasing it. When the Power LED begins to blink, the defaults have been restored and the NF12 restarts. Navigate to 192.168.1.1 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 3 seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF12 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 NF12 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 NF12 and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

Legal & Regulatory Information

Intellectual Property Rights

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

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

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

Customer Information

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

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

Consumer Protection Laws

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

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

Product Warranty

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

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see the [Consumer Protection Laws](#) Section above), the Product Warranty is granted on the following conditions:

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

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

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

Limitation of Liability

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

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

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

Contact

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