

User Guide

CloudMesh Gateway - NF20MESH



Doc No. AA01349

Important notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. NetComm Wireless accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the NetComm Wireless CloudMesh Gateway - NF20MESH to transmit or receive such data.

Copyright

Copyright© 2025 NetComm Wireless Pty Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Pty 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 Pty Limited.

Trademarks and registered trademarks are the property of NetComm Wireless Pty Limited or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



Note – This document is subject to change without notice.

Document history

This document relates to the following product:

NetComm CloudMesh Gateway - NF20MESH

Ver.	Document description	Date
v1.0	First document release	25 June 2021
v1.01	<ul style="list-style-type: none"> - Added Wi-Fi AutoPilot description - Added notes about setting network names and passwords 	15 July 2021
v1.02	Updated the description of the <i>Backup</i> and <i>Update</i> features	9 August 2021
v1.03	Updated the Device info screenshot	11 November 2022
v2.00	Updated for new WebUI – Firmware version R6B031 onwards.	13 March 2024
V2.01	Hostname update on page 73	30 July 2024
V2.02	Update branding and remove mobile app reference	13 June 2025
V2.03	Update copyright statement	2 September 2025

Table i. – Document revision history

Contents

Overview.....	7
Introduction.....	7
Prerequisites	7
Notation	7
Product overview	8
Wi-Fi AutoPilot	8
Setting up your Internet connection.....	9
Before you begin	9
Ethernet WAN	9
Here's how things connect for Ethernet WAN connections	9
ADSL or VDSL.....	10
Here's how things connect for ADSL/VDSL connections.....	10
Configuring your gateway.....	10
Connecting with Wi-Fi.....	11
Turning Wi-Fi and lights on or off	11
Connecting a telephone.....	12
Interfaces	13
Front view.....	13
LED indicators.....	13
Rear view	14
Side view.....	15
Safety and product care.....	16
Transport and handling	16
Placement of your CloudMesh Gateway	16
Avoiding obstacles and interference	17
Cordless phones.....	17
Configuring the Gateway	18
Setup wizard	20
Setup Wizard - Internet.....	20
ADSL – VPI and VCI	20
PPPoE.....	21
PPPoA (ADSL only).....	21
Dynamic IP.....	22
Static IP.....	22
Bridge	22
Setup Wizard – Wireless	23
Network Name.....	23

Security Key Type	23
Wi-Fi Password	23
Setup Wizard – Phone	24
Phone service	24
Phone Line settings	24
Setup Wizard – Timezone	25
Setup Wizard – Summary	26
Gateway Interface	27
Left navigation	27
Quick tasks bar	28
Summary	28
Gateway	29
Internet information	30
Wireless 2.4GHz	31
Wireless 5GHz	32
USB devices	33
Phone	34
Wired devices	35
Internet	36
Edit a service	36
Create a new connection	37
Wireless	38
More settings	39
Phone	41
More settings	42
Parental Control	44
Time restriction	44
URL filter	45
Content sharing	47
Available shares	47
Sharing Options	47
UPnP	47
DLNA	48
Samba (SMB)	48
Advanced	49
Diagnostics	49
Routing	49
Management	49
Local Network	49
Phone	49
System	50
QoS	50
Security	50
Diagnostics	51
Diagnostics – Information	51
Device Info	51
WAN	52
Route	53
ARP	53
NAT Mapping Table	54
Diagnostic – Statistics	55
LAN	55

WAN Service.....	55
xTM Interface.....	56
xDSL.....	57
CPU & Memory.....	57
Diagnostics – Troubleshooting.....	58
Connection tests.....	58
Ping Diagnostic.....	59
Traceroute Diagnostic.....	59
Sniffer.....	59
Diagnostics – Logs.....	60
System Logs.....	60
Security Logs.....	62
Routing.....	63
NAT.....	63
Port Forwarding.....	63
Port Triggering.....	65
DMZ Host.....	66
ALG.....	67
Routing.....	69
Static Route.....	69
RIP Configuration.....	70
DDNS.....	71
DNS Proxy.....	72
Management.....	73
TR-069 Client.....	73
Passwords.....	74
Requirements.....	74
Restrictions.....	74
LED control.....	75
Timeout.....	75
SNMP.....	76
Local Network.....	77
Local Area Network.....	77
IPv4 LAN Auto Configuration.....	77
DHCP.....	78
IPv6 LAN Auto Configuration.....	80
VLAN.....	82
Wireless Advanced Settings.....	83
MAC Filter.....	83
Advanced.....	84
Phone.....	87
SIP Settings.....	87
Digitmap Settings (configuring a VoIP dial plan).....	88
System.....	90
Settings.....	90
Backup.....	90
Update.....	90
Factory Reset.....	91
Scheduled Reboot.....	91
Update Firmware.....	92
Device Time.....	93
QoS.....	95
Basic.....	95

Queue	95
Add queue	97
View WLAN Queue Setup	98
Classification	99
Traffic classification rule list	99
Add Network Traffic Class Rule	100
Port Shaping	102
Port Shaping Example	102
Calculation of shaping rate and burst size	103
Security	104
Firewall	104
Add firewall rule	104
MAC Filtering	106
Access Control	107
Services access control list (SCL)	107
Access List	108

Overview

Introduction

This document provides a detailed description of the device, including instructions on configuring and using the NetComm CloudMesh Gateway.

Prerequisites

To configure your CloudMesh Gateway, you will require a computing device with a web browser and either a wired or wireless network adapter.

Notation

The following symbols may be used in this document:



Note – This note contains useful information.



Important – This is important information that may require your attention.



Warning – This is a warning that may require immediate action in order to avoid damage or injury.

Product overview

- Fully featured VDSL2 / ADSL2+ gateway
- 4 x Gigabit Ethernet 10/100/1000 LAN ports
- nbn and UFB ready – ultra-fast connection to nbn and UFB fibre network - 1 x 10/100/1000 Gigabit Ethernet WAN port
- VoIP feature for HD quality voice calls - connect up to 2 telephones
- Next generation Wi-Fi 802.11ax, dual band concurrent, for multiple high-speed wireless connections
- A WPS push button for the quick and easy connection of wireless devices on both 2.4GHz and 5GHz bands
- Access and share media and file content across the wireless home network
- Device performance monitoring and management through TR-069
- Intuitive user interface for a streamlined configuration and management experience

Wi-Fi AutoPilot

CloudMesh™ Wi-Fi AutoPilot is an application that operates locally on your CloudMesh Gateway, which constantly scans and analyses the WiFi environment. If any detrimental changes are detected, the WiFi AutoPilot will adjust the gateway WiFi parameters. Any action taken is based on a patented and weighted algorithm ensuring that the Internet connection experience is not compromised. The WiFi AutoPilot is constantly synchronised with the WiFi analytics cloud that is using sophisticated machine learning techniques to detect and recognise historical patterns and then apply WiFi changes, preventing future interference.

Setting up your Internet connection



Note –

If you received your gateway from your service provider and they have provided you with their own instructions, refer to those to complete the setup. In some cases, the gateway has been pre-configured for you and is ready to use. Otherwise, you will need to complete the setup yourself.

Before you begin

Ensure that you have the following information from your service provider:

- How your Internet service will physically connect to your gateway
- The Settings specific to your type of service.

There are two ways to connect your gateway to the Internet service:

Ethernet WAN

This is the most common access type in Australia and New Zealand and covers fixed line technologies such as nbn™ FTTP, HFC, FTTC as well as UFB Fixed Wireless and Sky Muster™ satellite services.

This type of Internet service uses the red WAN port on the back of the gateway to connect to the dedicated connection box installed by your access network provider.

Here's how things connect for Ethernet WAN connections

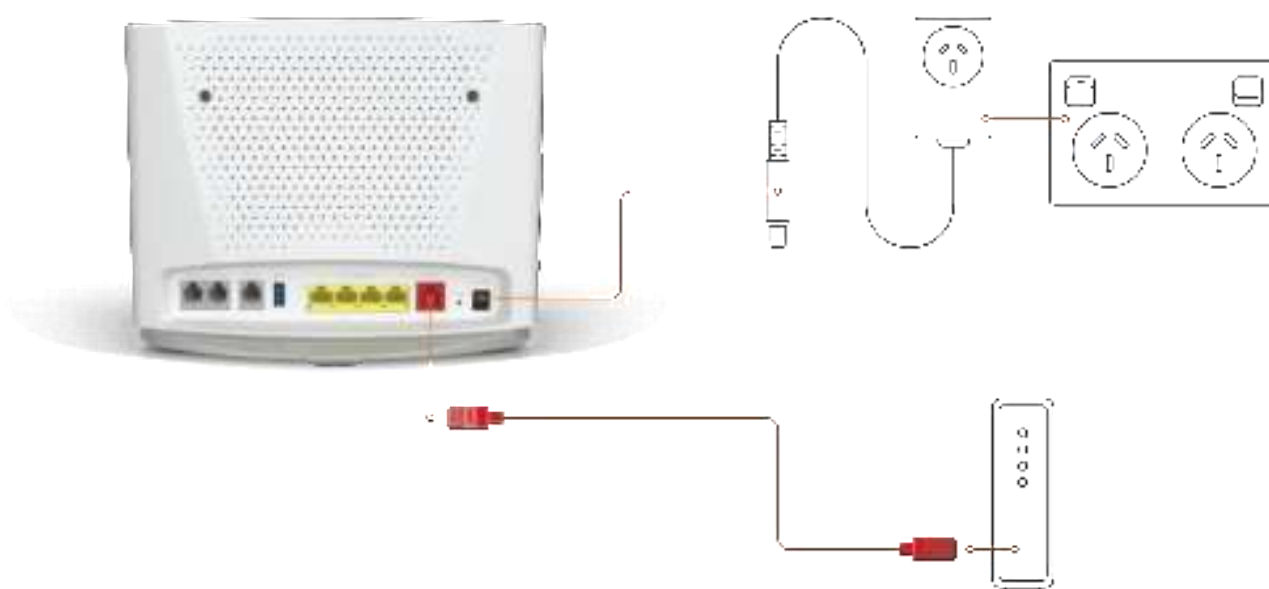


Figure 1 - Ethernet WAN connection summary

ADSL or VDSL

These access types are provided by nbn™ FTTB, FTTN or ADSL/VDSL over a traditional telephone line.

This connection uses the grey DSL port on the back of the gateway.

Here's how things connect for ADSL/VDSL connections

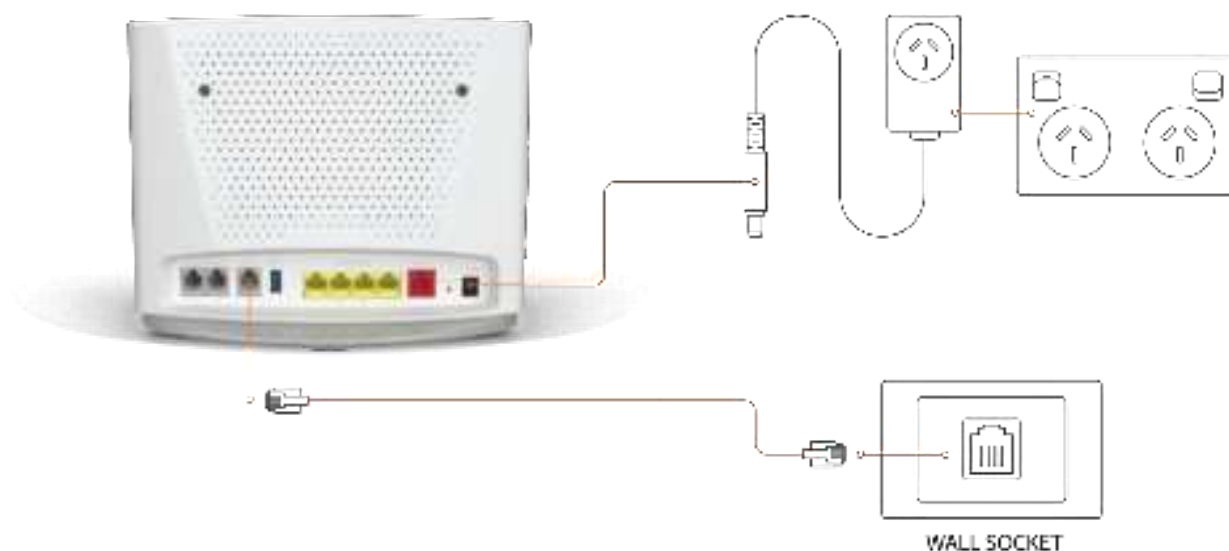


Figure 2 - ADSL/VDSL connection summary

Configuring your gateway

To complete the setup, you will need the following information from your service provider:

- Internet service type (ADSL/VDSL/Ethernet WAN)
- Connection type (PPPoE/PPPoA/Dynamic IP/Static IP)
- Other specifics depending on your connection type including 802.1P priority, VLAN Tag, WAN IP Address, Subnet Mask and DNS Servers
- VoIP settings from your service provider if you intend to use a phone with your service.

When you have the necessary information, follow these steps:

- 1 Push the power button on the side of the CloudMesh Gateway to turn it on. Wait a few minutes for it to complete starting up.
- 2 Open a web browser and type **192.168.20.1** into the address bar, then press **Enter**.
- 3 At the login screen, type **admin** into the Username field. In the Password field, type the unique password printed on the label on the bottom of the gateway, then Select on the **Login >** button
- 4 Follow the Basic Setup to complete the configuration.

Connecting with Wi-Fi

Your Wi-Fi Security Card includes your unique network name and password. Type the information into your wireless device when connecting or scan the QR code that is printed on the card.



Figure 3 - Connecting with Wi-Fi

Turning Wi-Fi and lights on or off

Hold the WIFI or WPS/LED buttons down for 6 seconds to toggle the Wi-Fi radio or LED indicators on or off.

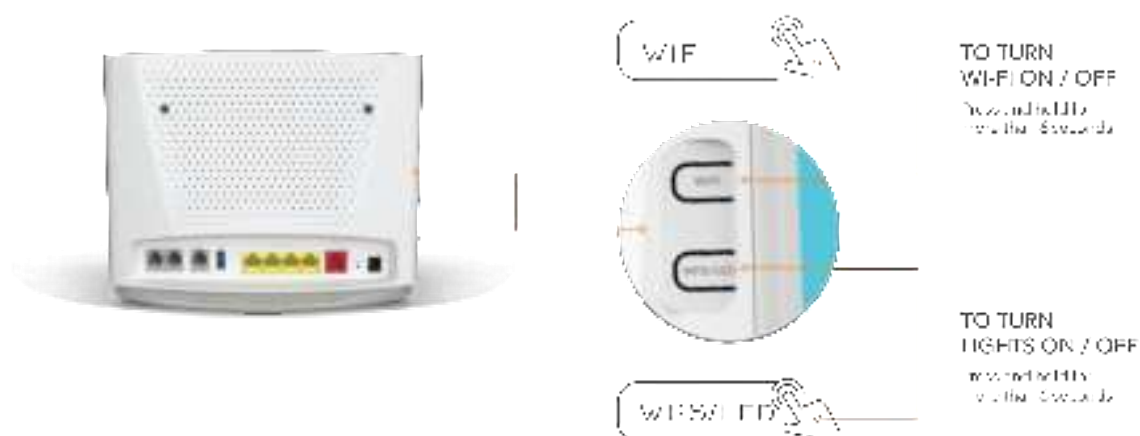


Figure 4 - Turning the Wi-Fi and lights on or off

Connecting a telephone

Connect a regular telephone handset to the CloudMesh Gateway as shown below. To use the phone, you will need to have a VoIP service from your carrier, complete the setup wizard and enter your VoIP settings.

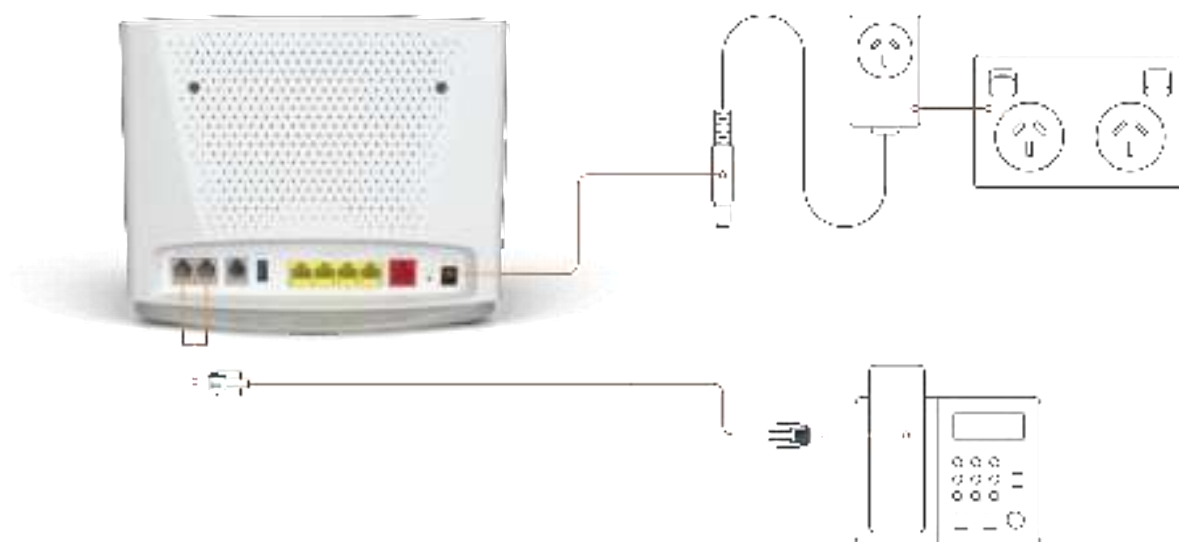


Figure 5 - Telephone connection diagram

Interfaces

The CloudMesh Gateway is designed to be placed on a desktop with the front facing outward. All of the cables exit from the rear for easy organization and the power ON/OFF and WPS buttons on the side.

Front view

The LED display visible on the front of the CloudMesh Gateway provides you with information about network activity and the device status.



Figure 6 - LED icons

LED indicators

The following table contains an explanation of each of the indicator lights on the front of the CloudMesh Gateway.

Label	Icon	Colour	Definition
Power		Red	The CloudMesh Gateway is powered on and initialising.
		Green	The CloudMesh Gateway is powered on and operating normally.
		Off	The power is off.
DSL		Off	No DSL signal detected.
		Green Blinking	Syncing
		Green	DSL synchronized.
Internet		Green	The CloudMesh Gateway is connected to an Internet service.
		Green Blinking	Data is being transmitted to or from the Internet. Note that this will only blink for Ethernet WAN connections. Other connection types will show a steady green status.
		Off	The CloudMesh Gateway is not connected to the Internet.
WAN		Green	A device is connected to the Ethernet WAN port.
		Green Blinking	Data is being transmitted to or from the WAN.
		Off	No device is connected to the Ethernet WAN port.
Ethernet		Green	A device is connected to the Ethernet LAN port.
		Green Blinking	Data is being transmitted to or from the Ethernet LAN port.
		Off	No device is connected to the Ethernet LAN port.
Wi-Fi		Green	Wi-Fi is enabled.

		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	Wi-Fi is disabled.
	5G	Green	Wi-Fi is enabled.
		Green Blinking	Data is being transmitted to or from the Wireless interface.
		Off	Wi-Fi is disabled.
WPS		Blue	WPS (Wi-Fi Protected Setup) is enabled.
		Blue Blinking	WPS pairing is triggered.
		Off	WPS is disabled.
USB		Green	A USB device is connected.
		Green Blinking	Data is being transmitted through the USB interface.
		Off	No USB device is connected to the USB interface.
Telephone		Green	A handset is registered.
		Green Blinking	Incoming call or the handset is in use.
		Off	No handset registered

Table 1 - LED icon descriptions

Rear view

The following interfaces are available on the rear panel of the CloudMesh Gateway:



Figure 7 – CloudMesh Gateway rear view

Interface	Description
Telephone 1 and 2	Connect a regular analogue telephone handset here for use with a VoIP service.
DSL	Use the provided telephone cable to connect the router to the telephone line operating your xDSL service.
USB	Connect an external USB storage device here to use the Network Attached Storage (NAS) feature of the CloudMesh Gateway.

Ethernet 1–4	Gigabit Ethernet LAN ports. Connect your Ethernet based devices to one of these ports for high-speed internet access.
WAN	Gigabit capable WAN port for connection to a WAN network. Connect to your Network Termination Device (NTD) for high-speed internet access.
Reset button	Reset unit to Default by holding the Reset button down for 10 seconds when unit is powered on.
Power supply jack	Connection point for the included power adapter. Connect the power supply here.

Table 2 – Interface descriptions

Side view



Figure 8 - Side view

Interface	Description
Wi-Fi button	Hold the WiFi button down for six (6) seconds and then release it to toggle the Wi-Fi radio on or off. When turned off, the wireless access point will not operate. This is useful for times when you want to disable wireless access completely.
WPS/LED button	This is a multifunctional button that will trigger the Wi-Fi Protected Setup (WPS) function when held down for approximately three (3) seconds and toggle the LED indicators on or off when held for approximately six (6) seconds.

On/Off button	Toggles the power on and off.
---------------	-------------------------------

Table 3 - Side buttons

Safety and product care

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

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

Transport and handling

When transporting the gateway, we recommend returning the product in its original packaging. This helps to reduce the risk of damage to the product.



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

Placement of your CloudMesh Gateway

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

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



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

Try not to place the CloudMesh Gateway near a cordless telephone that operates at the same radio frequency as the CloudMesh Gateway (2.4GHz/5GHz).

Avoiding obstacles and interference

Avoid placing your CloudMesh Gateway 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
- 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 CloudMesh Gateway).

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 CloudMesh Gateway and your wireless-enabled computers.

Unplug and remove the battery from any cordless phone that operates on the 2.4GHz or 5GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the CloudMesh Gateway.

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. See your phone's user manual for detailed instructions.

If necessary, consider switching to a 900MHz or 1800MHz cordless phone.

Configuring the Gateway

To perform configuration of the CloudMesh Gateway, you can access its web interface.

- 1 Push the power button on the side of the CloudMesh Gateway to turn it on. Wait a few minutes for it to complete starting up.
- 2 Open a web browser and type **192.168.20.1** into the address bar, then press **Enter**.
- 3 At the login screen, type **admin** into the Username field. In the Password field, type the unique password printed on the label on the bottom of the gateway, then Select on the **Login >** button. If you have changed the password, enter your chosen password instead.



Figure 9 – Login page

- 4 If you have not yet set up your Gateway, or it was not preconfigured from your ISP, you will be presented with the setup screen.

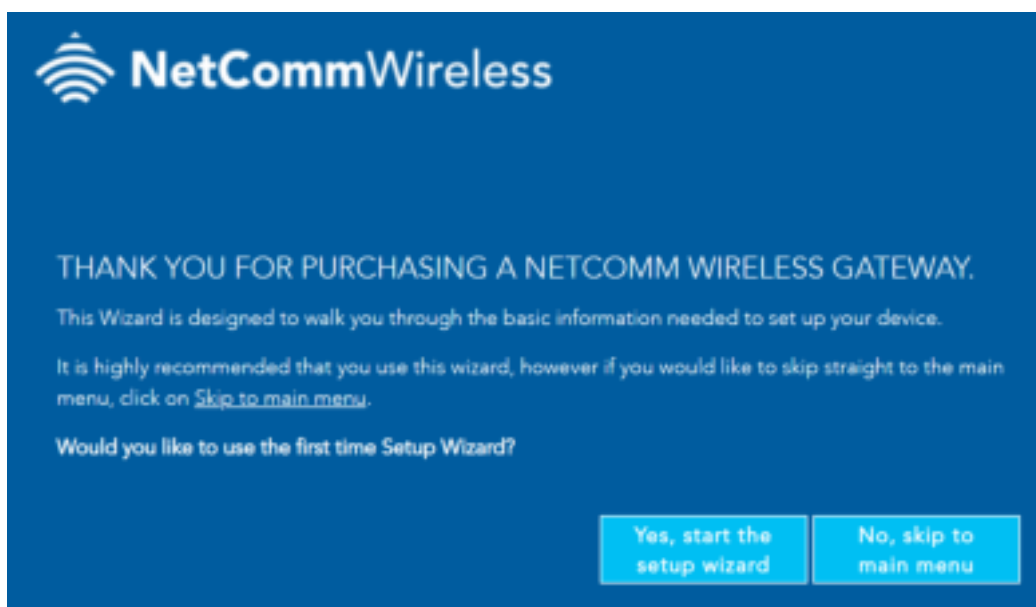


Figure 10 – Setup Wizard

Two options are available:

- a **Start the setup wizard**, where you will be guided through a step-by-step process to set up your device. We recommend that you use this wizard as it covers all the basic settings. See the next section, **Setup Wizard**, for a detailed description of how to use the wizard.
- b **Go to the Main Menu**. Select this option to skip the wizard and configure the NF20MESH from the **Advanced** screen.

Setup wizard

The NF20MESH's Setup Wizard will open the INTERNET connection page. The current step of the wizard is indicated at the top of the page:



Figure 11 – Setup Wizard - Steps

Setup Wizard - Internet

The **INTERNET** setup wizard page prompts you to select the WAN connection type that you will be using and to enter all the parameters required to enable the service.

First select your **INTERNET SERVICE: ADSL, VDSL or Ethernet WAN**

Then select from the available range of **CONNECTION TYPES** for that type of service.

Your ISP (Internet Service Provider) will have advised you which service and connection type and the required details you will be using.

VDSL (Very-high-bit-rate Digital Subscriber Line) and second-generation VDSL2, are digital subscriber line (DSL) technologies providing data transmission faster than asymmetric digital subscriber line (ADSL). VDSL services may or may not be available from your ISP or in your area. Check with your ISP.

Ethernet WAN services are normally employed when part of the internet connection is cable or fibre optic or other very high-speed services, such as NBN.

ADSL (Asymmetric Digital Subscriber Line). There are several variations of ADSL, for example ADSL2 and ADSL2+. For purposes of this manual ADSL refers to all these related service types.

The following section details the different connection types available for each service:

ADSL – VPI and VCI

If you are using an ADSL connection, each of the ADSL connection types will include a **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier) field. These fields are set to **8** (VPI) and **35** (VCI) by default. If your ISP has given you different details, change these fields to those values.

Figure 12 – Setup Wizard – VPI / VCI

PPPoE

CONNECTION TYPE

☒ PPPoE
 ☐ Dynamic IP
 ☐ Static IP
 ☐ Bridge

Username:

Password:

802.1P: (0-7)

VLAN Tag: (0-4094)

To use **PPPoE**, you will require a **Username** and **Password**, which will be advised by your ISP.

You may also need to change the **802.1P** and **VLAN Tag** value. Refer to your ISP configuration to confirm.

PPPoA (ADSL only)

CONNECTION TYPE

☐ PPPoE
 ☒ PPPoA
 ☐ Dynamic IP
 ☐ Static IP
 ☐ Bridge

VPI:

VCI:

Username:

Password:

802.1P: (0-7)

VLAN Tag: (0-4094)

To use **PPPoA**, you will require a **Username** and **Password**, which will be advised by your ISP.

VPI (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier) are commonly **8** and **35** respectively.

You may also need to change the **802.1P** and **VLAN Tag** value. Refer to your ISP configuration to confirm.

Dynamic IP

CONNECTION TYPE

☐ PPPoE
 ☒ Dynamic IP
 ☐ Static IP
 ☐ Bridge

802.1P: (0-7)

VLAN Tag: (0-4094)

Dynamic IP automatically assigns an IP from your ISP.

You may need to change the **802.1P** and **VLAN Tag** value. Refer to your ISP configuration to confirm.

Static IP

CONNECTION TYPE

☐ PPPoE
 ☐ Dynamic IP
 ☒ Static IP
 ☐ Bridge

WAN IP Address:

WAN Subnet Mask:

WAN Gateway IP Address:

Primary DNS server:

Secondary DNS server:

802.1P: (0-7)

VLAN Tag: (0-4094)

To use **Static IP**, enter the WAN IP address, subnet mask, gateway IP address and primary and secondary DNS servers.

These details will be supplied by your ISP.

You may need to change the **802.1P** and **VLAN Tag** value. Refer to your ISP configuration to confirm.

Bridge

CONNECTION TYPE

☐ PPPoE
 ☐ Dynamic IP
 ☐ Static IP
 ☒ Bridge

802.1P: (0-7)

VLAN Tag: (0-4094)

To use a **Bridge** connection you may need to change the **802.1P** and **VLAN Tag** value. Refer to your ISP configuration to confirm.

Select the **Next** button when you have completed the configuration on this page.

Setup Wizard – Wireless

The **Wireless** setup wizard page allows you to configure your wireless connection. The wireless connection can be disabled if required, by setting the **Off** button.

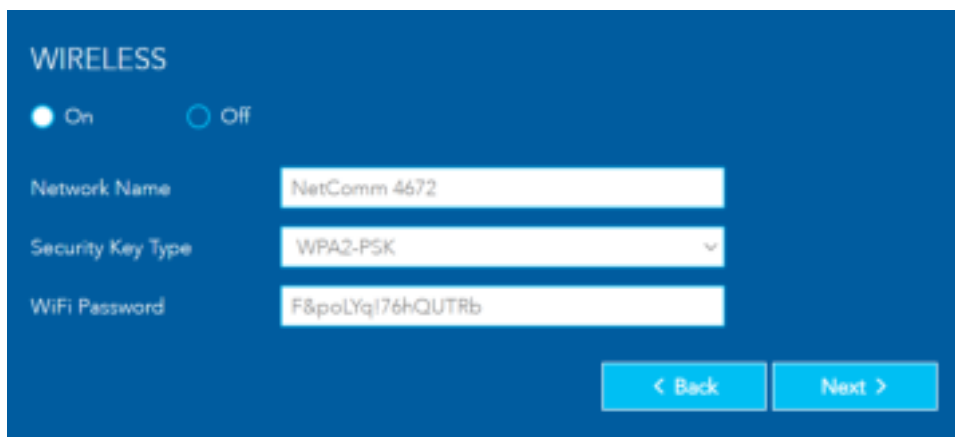


Figure 13 – Setup Wizard - Wireless

Network Name

The **Network Name** field is configured to use the default Wi-Fi name, which is printed on the Gateway label. You can change this name to be something more recognisable, or if you are replacing an existing Wi-Fi router, your existing Wi-Fi name.

Security Key Type

The **Security Key Type** field adjusts the security of your Wi-Fi network.

The default Security Key Type is **WPA2-PSK**. The recommended key type is **Mixed WPA3/WPA2-PSK** which offers high-grade security whilst maintaining good compatibility with devices.

- Choosing **WPA-PSK** offers a low level of security, you should only choose this if you have a legacy device which requires this level.
- We do not recommend selecting **Open**, as this leaves your network completely unprotected from intrusion via the Wi-Fi network.

Wi-Fi Password

The **Wi-Fi Password** field is by default configured to use the secure password on the Gateway label. You can change this password to be more recognisable, or match your previous Wi-Fi network's details.

Select the **Next** button when you have completed the configuration on this page.

Setup Wizard – Phone

The **Phone** setup wizard page allows you to configure VoIP (Voice over Internet Protocol) telephone functionality. Using the telephone functionality is **Optional**. If you do not wish to connect a phone to your Gateway, select the **Next** button to skip this step.

You can connect one or two phones via the TELEPHONE sockets located at the back of the router, labelled as **1** and **2**. Each phone line is separately defined in the Gateway. Connect a standard or the base station of your cordless phone directly into the telephone sockets.

Phone service

Your ISP will generally pre-configure **TEL1** port to work as the primary telephone port so it connects to their phone network. They will also supply you with your phone number.

If the device is not pre-configured, then you will have to get the SIP details from your ISP and enter them at this stage in the Basic Setup Wizard.

If the configuration is correctly set up and the router is connected to the internet, then the phone should work as soon as its plugged in.

Phone Line settings

 **Note** – Often ISPs will preconfigure these settings prior to the delivery of your NF20MESH Gateway.

Enter your VoIP service settings as supplied by your VoIP provider. Each of the required fields are detailed in the table below. If you are unsure about a specific setting, or have not been supplied information for a particular field, please contact your VoIP provider to verify if the setting is required.

Field	Description
Phone Number	Enter the telephone number supplied by your VoIP service provider (VSP)
SIP Username	If not preconfigured, enter the Username supplied by your VSP.
SIP Password	If not preconfigured, enter the Password supplied by your VSP.
SIP CID Number	If not preconfigured, enter the SIP CID number supplied by your VSP.
SIP Proxy Server	If not preconfigured, enter the IP address of the proxy supplied by your VSP.
SIP Registrar Server	If not preconfigured, enter the IP address of the Registrar Server supplied by your VSP.
SIP Outbound Proxy	If this optional field is required, and if not preconfigured, enter the IP address of the outbound proxy supplied by your VSP. Leave blank if this information is not supplied by your VSP.

Select the **Next** button when you have completed the configuration on this page.

Setup Wizard – Timezone

The **Timezone** setup wizard page asks you to set the time zone of the Gateway. Setting the correct time zone is important for any time based features of the Gateway, such as Parental Control.

Select the correct time zone for your location from the dropdown menu:



Figure 14 – Timezone

Select the **Next** button when you have completed the configuration on this page.

Setup Wizard – Summary

The **Summary** setup wizard page displays the settings that were configured throughout the Setup Wizard. Review the page for any errors, and then select **Finish** to finalise the setup.

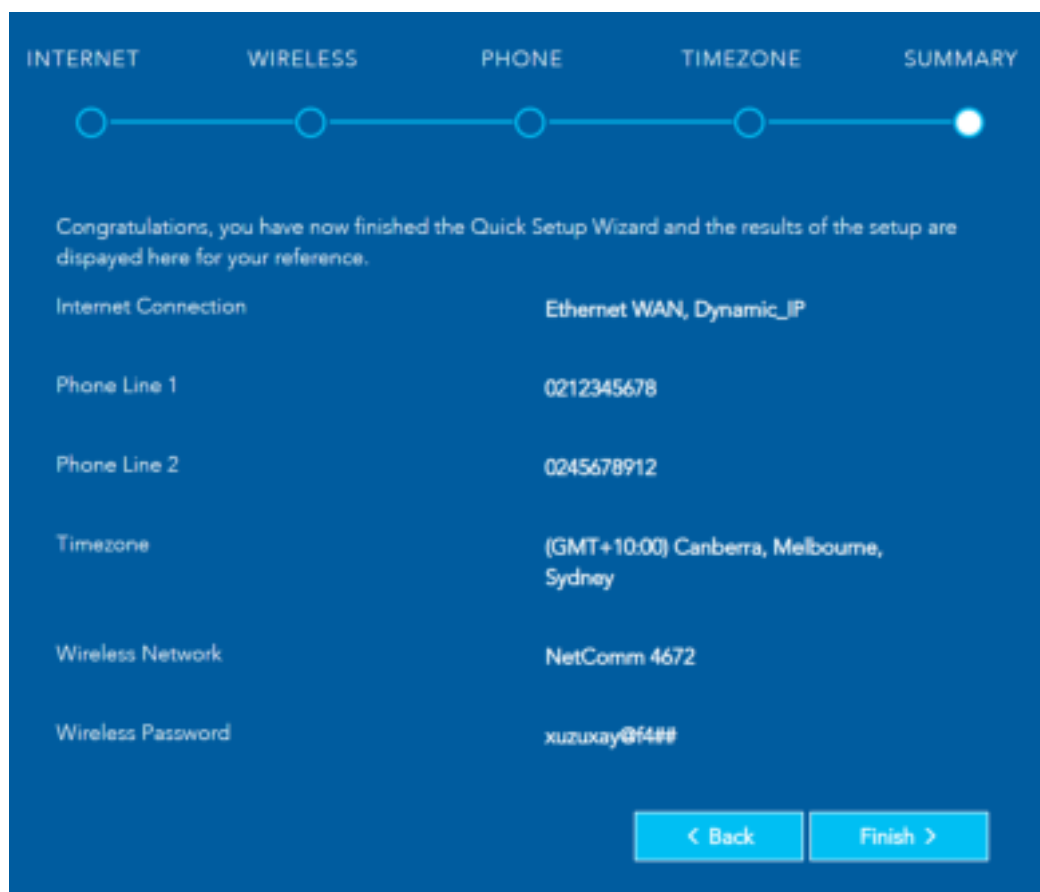


Figure 15 – Setup Wizard - Summary

The wizard will apply the settings.

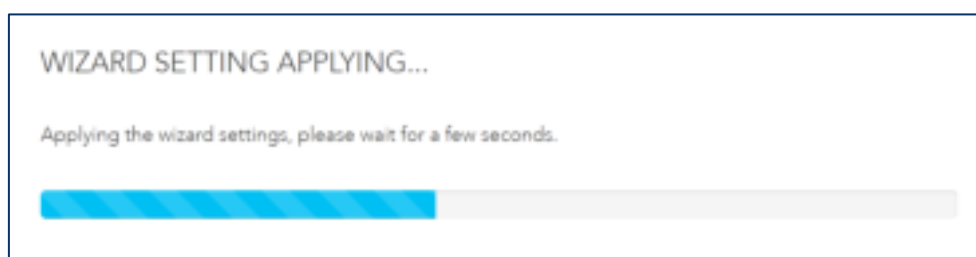


Figure 16 – Setup Wizard - Applying

On completion of the wizard the **Summary** page is shown. Initial setup of the Gateway is complete.

Gateway Interface

After the initial configuration is completed, and a network connection established, the **Gateway WebUI** is displayed.



Figure 17 – Interface

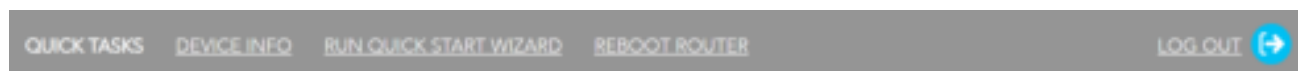
Left navigation

At the left of the window is navigation for further information and configuration of the Gateway:

Navigation Item	Description
Summary	Displays the summary page
Internet	Displays configuration information related to the internet connection
Wireless	Displays information and basic configuration settings about the Wi-Fi connection
Phone	Display the VoIP configuration
Parental control	Displays parental controls for the Gateway
Content sharing	Displays settings to share content from a mass storage device connected to the USB port of the Gateway
Advanced	Opens the Advanced configuration page of the Gateway

Quick tasks bar

At the top of the window is a quick tasks bar, allowing you to quickly complete tasks such as rebooting the Gateway or displaying information about the Gateway for support.



Summary

The **Summary** page is displayed when first logging in to the Gateway. It displays information about the status of the Gateway, including internet connection status, wired and wireless clients, and phone line information. Select an icon to change the information dialog to the right of the summary diagram.

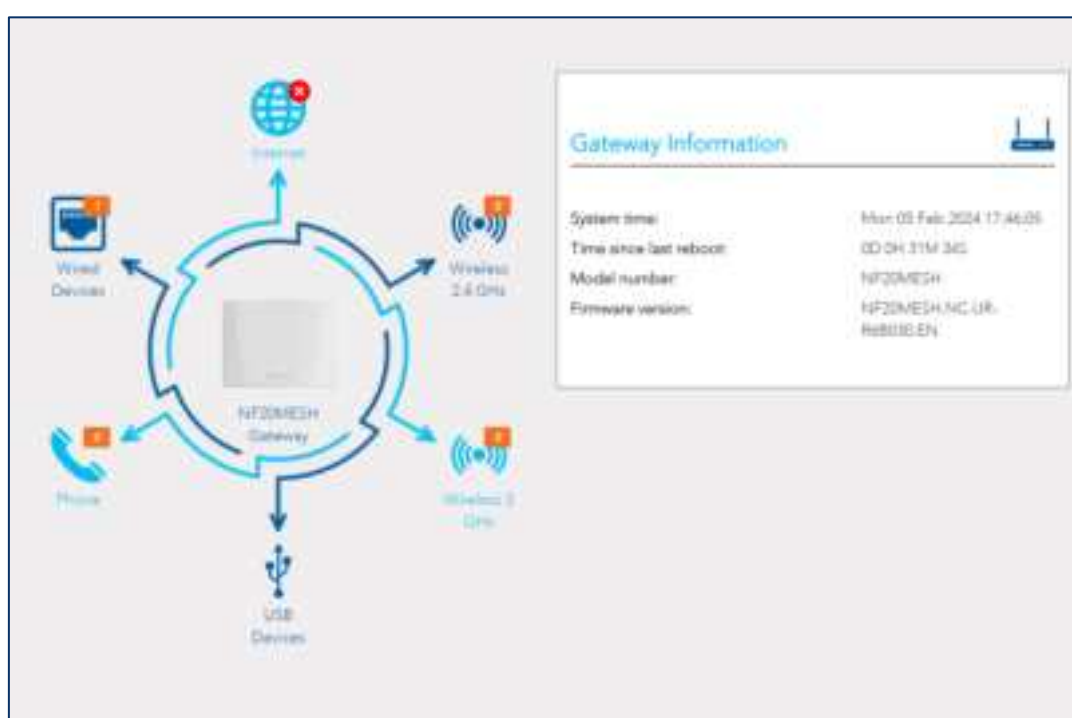


Figure 18 – Summary

Information about each icon is detailed below:

Gateway

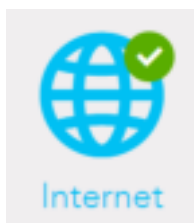


Gateway Information

System time:	Mon 05 Feb 2024 18:18:47
Time since last reboot:	0D 1H 4M 17S
Model number:	NF20MESH
Firmware version:	NF20MESH.NC.UR-R6B030.EN

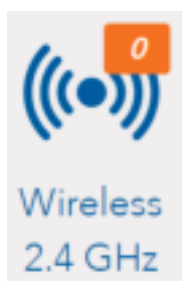
Item	Description
System time	The time retrieved from the NTP (Network Time Protocol) server when <input checked="" type="checkbox"/> Automatically synchronize with Internet time servers. is selected on the Advanced > System > Internet Time page. If your area observes daylight savings time, ensure that <input checked="" type="checkbox"/> Enable Daylight Saving Time is selected as well.
Time since last reboot	The time that has elapsed since the last time the gateway was 'rebooted', normally meaning when it was last turned off and then on.
Model number	The full model number of the gateway.
Firmware version	The currently installed firmware version number.

Internet information



Item	Description
Connection type	<p>The current connection type or status of your connection. The possible Connection types that can be displayed are:</p> <ul style="list-style-type: none"> ● ETH – Ethernet WAN connection ● PTM – VDSL connection ● ATM – ADSL connection, or ● No Connection – no WAN interface set up or no connection to the Internet.
Line rate - upstream	The current speed of data being uploaded from the NF20MESH.
Line rate - downstream	The current speed of data being downloaded into the NF20MESH.
WAN Gateway IP Address	IP address of the WAN Gateway
WAN IP Address	IP address of the WAN
Primary DNS Server	IP address of the Primary DNS Server
Secondary DNS Server	IP address of the Secondary DNS Server

Wireless 2.4GHz



Wireless 2.4 GHz

Wireless network:

Enabled

Wireless network name:

NetComm-4672

Channel:

11

Bandwidth:

20MHz

Security:

WPA2-PSK

Wireless network:

Disabled

Wireless network name:

wifi-Quartf

Security:

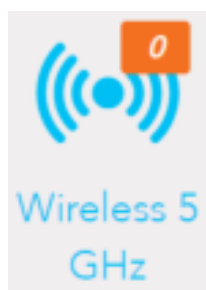
Open

Wireless Clients:

Name	SSID	IP Address	MAC Address
<div>Edit</div>			

Item	Description
Wireless network status	Enabled or Disabled
Wireless network name	The name of the wireless network
Channel	The current channel the wireless network is broadcasting on
Bandwidth	The current bandwidth of the wireless network
Security	The current security in use on the wireless network
Wireless Clients	
Name	The wireless client's name
SSID	The Wi-Fi network name identifier that the client is connected to
IP Address	The current IP address of the device
MAC Address	The device's unique MAC address, used to identify the device on the network

Wireless 5GHz



Wireless 5 GHz

Wireless network:

Enabled

Wireless network name:

NetComm 4672

Channel:

157

Bandwidth:

80MHz

Security:

WPA2-PSK

Wireless network:

Disabled

Wireless network name:

all_Guest

Security:

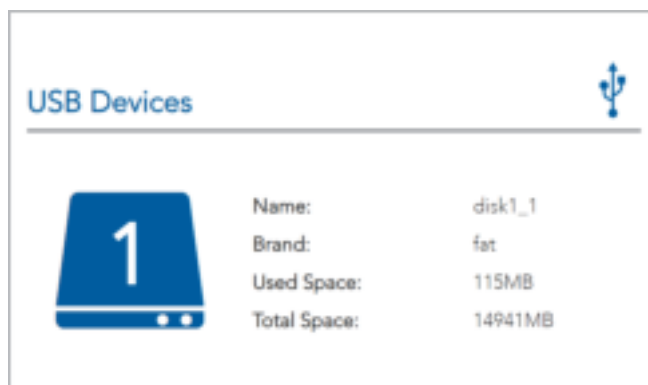
Open

Wireless Clients

Name	SSID	IP Address	MAC Address
<div>Edit</div>			

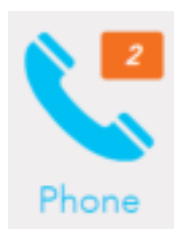
Item	Description
Wireless network status	Enabled or Disabled
Wireless network name	The name of the wireless network
Channel	The current channel the wireless network is broadcasting on
Bandwidth	The current bandwidth of the wireless network
Security	The current security in use on the wireless network
Wireless Clients	
Name	The wireless client's name
SSID	The Wi-Fi network name identifier that the client is connected to
IP Address	The current IP address of the device
MAC Address	The device's unique MAC address, used to identify the device on the network

USB devices



Item	Description
Name	The name given to the USB drive (often the manufacturer's default name)
File System	Type of file system. The NF20MESH supports: FAT16, FAT32, NTFS, EXT2 and EXT3 (Linux).
Used Space	Amount of space used.
Total Space	Total amount of space on the USB.

Phone



Phone Details

Phone 1 Provider: Ring Central

Number: 09 2424 7576

Registration Status: Up

Phone 2 Provider: Ring Central

Number: 09 2424 7577

Registration Status: Up

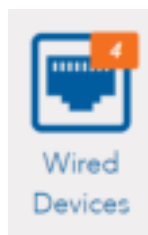
Call History

From	To	Duration	Direction	Date - Time
00 4584 3326	0475 337 159	00:09:12	Inbound	29/5/24 - 12:40:02
00 4584 3326	0475 337 159	00:09:12	Inbound	29/5/24 - 12:40:02
00 4584 3326	0475 337 159	00:09:12	Inbound	29/5/24 - 12:40:02

Edit

Item	Description
Phone Provider	The name of the VoIP service provider.
Number	The number assigned to this phone.
Registration Status	Status of the telephone service.
Call history details	
From	Telephone number of the caller.
To	Telephone number of the answering party.
Port used	The port used by the phone.
Duration	Duration of the call.
Direction	Indicates whether the call was: IN or OUT
Timestamp	Time stamp when call started

Wired devices



Wired Devices		
Name	IP Address	MAC Address
	192.168.20.2	

Item	Description
Name	Name assigned by the manufacturer or administrator to the device.
IP Address	The IP Address of the device.
MAC Address	The MAC address of the attached device.

Internet

The **Internet** page displays details of all current connections to the internet.



Figure 19 – Internet

The following information is provided for each connection:

Item	Description
Description	The name of the connection.
Internet Service	The service type: ADSL, VDSL or Ethernet WAN
Connection Type	The connection type differs depending on the service type.
VLAN ID	The VLAN tag if used by this connection type.

Edit a service

To edit a connection, select the button underneath the **Description** column which is applicable to your connection. The **Edit existing** screen is shown to the right of the Internet Service Information screen.



Figure 20 – Edit service

Some fields cannot be edited, as they are configured as part of the initial connection configuration. Select the **More Options** button to see further configuration settings. Select the **Update** button to apply the configuration. Select the **Delete** button to delete the connection.

Create a new connection

Select the **Create New** button to create a new connection. The **Create new Internet Service connection** page is displayed to the right of the Internet Service Information screen.

Create new Internet Service connection

Description: (0-32 characters)

Internet Service: ☒ ADSL ☐ VDSL ☐ Ethernet WAN

Connection Type: ☒ PPPoE ☐ PPPoA ☐ Dynamic IP ☐ Static IP ☐ Bridge

VPI: (0-255) VCI: (0-65535)

Username: Password:

BQ2.1P: (0-1) VLAN Tag: (0-4094)

Apply **More Options**

Figure 21 – Internet – Create new service

The settings used to create a new internet service connection are covered in the **Setup Wizard – Internet** section. Select the appropriate settings and apply them here. Select the **Apply** button when you have finished entering the required details. The connection will appear in the **Internet Service Information** window.

Current Connections			
Description	Interface	Connection Type	VLAN ID
Ethernet WAN	eth4.1	Dynamic IP	-

Figure 22 – Internet - Current connections

Wireless

The **Wireless** page shows information about the Wi-Fi connection of the NF20MESH. The NF20MESH gateway supports both 2.4GHz and 5GHz wireless bands.

Figure 23 – Wireless

The NF20MESH will automatically select the correct band for connected Wi-Fi devices when the Wi-Fi Name and password are set the same on both 2.4 GHz and 5 GHz screens.

Alternatively, the NF20MESH gateway can be set up to maintain separate wireless settings for each of the 2.4GHz and 5GHz wireless services. Both wireless bands can transmit simultaneously, and it is up to each client to decide which service to use. In this case the set the Name and Password fields to be different to each other.

You can also create optional **Guest** accounts for the 2.4GHz and/or 5GHz wireless networks.

Turn **On** the guest network band you will use and enter a recognisable Name so that guest devices can identify the network.





If the Authentication setting is not **Open** a password is required. We recommend that you change the default password and select **Save** to apply the new Name and Password.

More settings

Select the **More Settings** button to display all available settings for the selected wireless band (2.4GHz or 5GHz). All settings are the same between bands with the exception of **Beam forming**, which is only available on the 5GHz band.

Figure 24 – Wireless – More settings

Item	Description
Channel Bandwidth	Select the bandwidth for the network: 20MHz , 40MHz , or 80MHz (5GHZ only) In high wireless activity/interference environment, reduce the bandwidth to 20MHz for greater stability.
Max. Connected Devices	Enter the maximum number of wireless devices able to simultaneously connect to the wireless network. Usually this is 32 (default setting) for consumer devices.
Device Isolation	Select <input checked="" type="checkbox"/> On to prevent devices on the wireless network being able to access each other, the wireless devices can only access the Internet. The default <input checked="" type="checkbox"/> Off setting allows every device connected to the router (wirelessly or by cable) to be considered part of the same local network and can communicate with each other device (e.g. servers, printers, PCs, wireless devices, etc.) on that network.
Hide SSID	By default, the NF20MESH broadcasts its SSID (network name), to nearby computers and other devices. Select Hide SSID <input checked="" type="checkbox"/> On to hide the network from appearing in client device network lists.

Beamforming Transmission	Enables Beamforming Transmission.
Beamforming Reception	Enables Beamforming Reception.
WPS Function	Set the WPS button to  On to enable WPS.
WPS Mode	 Router to connect a wireless device using the Router PIN , see below.  Device to connect a wireless device using the Device's PIN , see below.  Push Button to connect without a PIN using the physical WPS button on the side of the Router.
WPS connect button	<p>When Router or Device WPS Mode is selected choose this button to establish the connection using the PIN you have previously entered.</p> <p>When Push Button is selected you can either use this button or the physical WPS button on the side of the Router.</p>

Phone

The **Phone** page shows information about any configured VoIP services that are configured on the NF20MESH.

Figure 25 – Phone

To connect a phone, you will need to connect a phone to the **TELEPHONE** ports labelled **1** and **2** on the rear of the Gateway. You can configure each separate line in the gateway configuration. Select the **Line 1** or **Line 2** button at the top of the page to choose the line you want to configure.

If your gateway is preconfigured by your ISP, they will generally configure port **1** with their configuration details, and your ISP will supply your phone number.

If your gateway is not preconfigured, you will need to obtain your SIP details from your VoIP provider, and enter the details here.

Once the configuration is complete and the gateway is connected to the internet, then the phone should work as soon as it is plugged in.

The following information is required to create a VoIP connection:

Item	Description
SIP Username	The username as defined by your ISP
SIP Password	The password supplied by your ISP
Line Number	The telephone number supplied by your ISP.
CID Name	
SIP Proxy	The IP address of the proxy.
SIP Proxy Port	The port that this proxy is listening on. By default, the port value is 5060.

SIP Registrar	Enter the IP address of the SIP registrar.
SIP Registrar Port	The port that SIP registrar is listening on. By default, the port value is 5060.
SIP Outbound Proxy	Enter the IP address of the outbound proxy.
SIP Outbound Proxy Port	The port that the outbound proxy is listening on. By default, the port value is 5060.
Apply button	Select to save and apply any changes.

More settings

Select the **More Settings** button to enable additional features which may be supported by your VoIP provider:

Line 1

Features below can be enabled if it's supported by your Phone provider

Call Waiting: ☒ Enable ☐ Disable

Call Return: ☒ Enable ☐ Disable

Call Transfer: ☒ Enable ☐ Disable

Call Conference: ☒ Enable ☐ Disable

Call Forwarding Unconditional: ☒ Enable ☐ Disable

Unconditional Number:

Call Forwarding Busy: ☒ Enable ☐ Disable

Busy Number:

Call Forwarding No Answer: ☒ Enable ☐ Disable

No Answer Number:

Message Waiting Indicator: ☐ Enable ☒ Disable

Anonymous Call Blocking: ☒ Enable ☐ Disable

Anonymous Calling: ☒ Enable ☐ Disable

Anonymous Calling Mode:

Do Not Disturb: ☒ Enable ☐ Disable

Apply/Save

Figure 26 – Phone – More Settings

Item	Description
Call Waiting	Select <input checked="" type="radio"/> Enable if your VoIP Service Provider has enabled Call Waiting on your SIP account.
Call Return	Select <input checked="" type="radio"/> Enable if your VoIP Service Provider has enabled Call Return on your SIP account.

Call Transfer	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled Call Transfer on your SIP account and you wish to use this feature.
Call Conference	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled Call Conferencing on your SIP account and you wish to use this feature.
Call Forwarding Unconditionally	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled Call Forwarding Unconditionally (i.e. no wait, no busy signal, immediate forwarding) on your SIP account and you wish to use this feature.
Unconditionally Number	Enter the phone number to forward a call to if the primary telephone number is busy.
Call Forwarding Busy	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
Busy Number	Enter the phone number to forward a call to if the primary telephone number is busy.
Call Forwarding No Answer	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled Call Forwarding on your SIP account and you wish to use this feature.
No Answer Number	Enter the phone number to forward a call to if the call is not answered.
Message Waiting indicator	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled MWI (Message Waiting Indicator) on your SIP account and you wish to use this feature.
Anonymous Call Blocking	Select <input checked="" type="checkbox"/> Enable to block incoming calls that do not provide a caller id.
Anonymous Calling	Select <input checked="" type="checkbox"/> Enable if you would like all outgoing calls to hide your caller id.
Anonymous Calling mode	When set to Display anonymous, the modem hides your caller ID. When set to All anonymous, the modem hides both caller ID and the SIP URL of the originating call.
Do Not Disturb	Select <input checked="" type="checkbox"/> Enable if your VoIP Service Provider has enabled DND (Do Not Disturb) on your SIP account and you wish to use this feature.
Apply button	Select to save and apply the changes you have made to these settings.

Parental Control

The parental control page allows you to configure time and URL based blocking on your network. These controls can be used to ensure internet access is paused for specific devices at certain times of the day, such as when a child is going to bed.



Important –

Parental controls on the gateway are only one part providing safe internet browsing for children. Time scheduling and internet blocking may not work well across devices, especially those with increased privacy protections in place. You should use these tools alongside other things, such as inbuilt device parental control apps and supervising your children when online.

Time restriction

The **Time Restriction** function allows you to configure times when certain devices are blocked from connecting to the internet. Devices are identified using their MAC address. The same device can have multiple time restrictions applied.



Figure 27 – Parental Control – Time restriction

To add a device to the time restriction list:

- 1 At the bottom right of the window, select the **Add** button. The **Access Time Restriction** configuration window is shown.

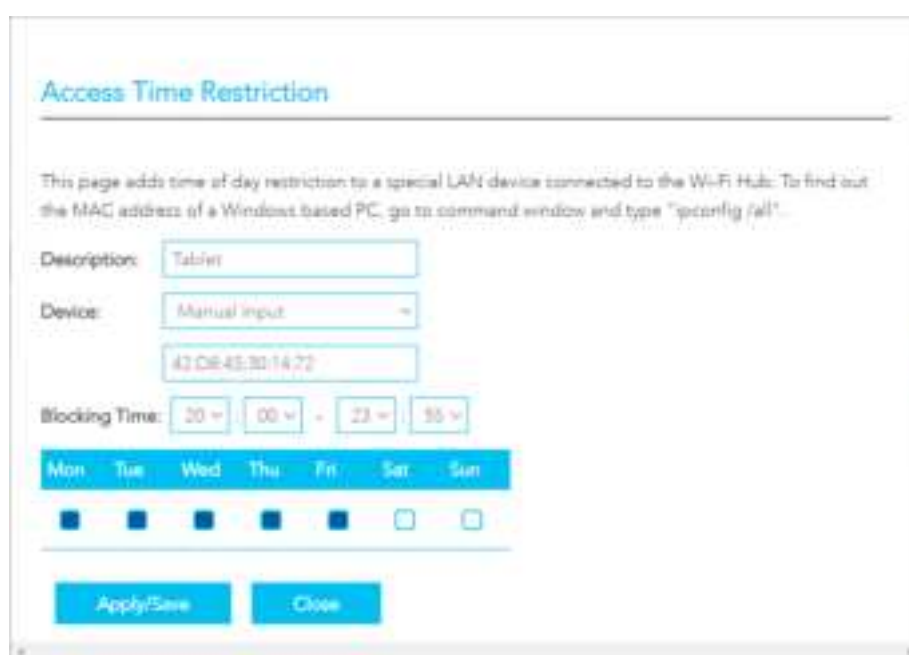


Figure 28 – Parental Control – Time restriction

- 2 In the **Description** field, enter a name which will help you to identify the device later.
- 3 The **Device** field offers two options, **Manual Input** or a list of devices currently on the network. If you can identify your device, select it here. Else, select **Manual Input**, then enter the MAC address of the device you wish to block
- 4 Enter the times of day that the device should be blocked. To create an overnight block which crosses from one day to the next, create two individual blocking rules.
- 5 Select the days that the block should apply.
- 6 Select the **Apply / Save** button.

URL filter

The URL filter is used to filter URLs on your client devices.

To use the URL filter, select the button which is appropriate to the type of filtering you would like:

Whitelist: If using a whitelist, users will only be able to access URLs which are on the list.

Blacklist: If using a blacklist, then users will not be able to access the URLs on the list.

Disable: Switch off the URL filter.

URL Filter

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

URL List Type: ☐ White list ☒ Black list ☐ Disable

URL	Port	Remove
demosite.com	443	

Add

Figure 29 – Parental Control – URL Filter

To add a URL to the filter list:

- 1 Select the **Add** button. The **URL Filter Add** dialog is shown.

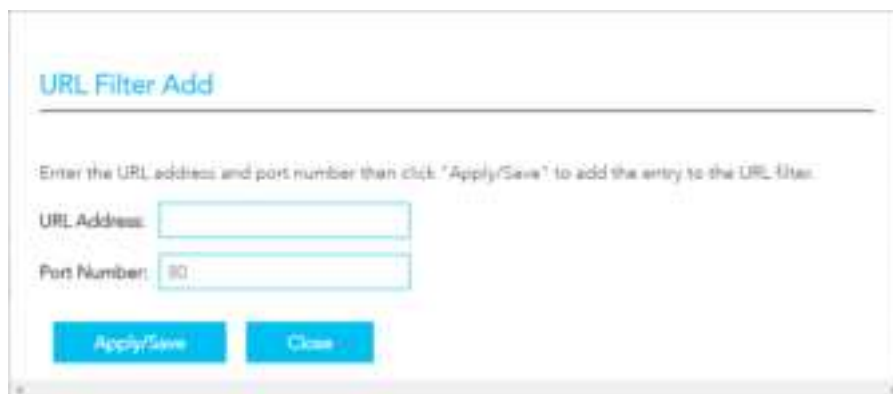


Figure 30 – Parental Control – URL Filter Add

- 2 In the **URL address** field, enter the URL address of the address that should be filtered.
- 3 In the **Port Number** field, enter the port that should be filtered. To filter HTTP traffic, enter port 80. To filter HTTPS traffic, enter port 443. If you are unsure, you should add both ports by adding a second URL filter.
- 4 Select the **Apply / Save** button.

Content sharing

The Content sharing page allows you to share an external drive which is connected to the NF20MESH.

Figure 31 – Content sharing

Available shares

The NF20MESH has one USB port located on the back of the router.

Insert a USB and the following details will display:

USB Device Name – The name given to the USB drive.

USB File System – The NF20MESH supports: FAT16, FAT32, NTFS, EXT2 and EXT3 (Linux).

USB Sharing Support – Yes means that the USB's contents can be shared with other devices connected to the NF20MESH. Note that USB ports will only provide 5V 1Amp, if your storage device exceeds this, please use USB power injector hubs.

Sharing Options

UPnP

Universal Plug and Play (UPnP) is a set of networking protocols that can allow networked devices, such as computers, printers, gaming console, 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.

■ **Enable UPnP** to allow automatic port forwarding configuration detection for your UPnP devices.

DLNA

DLNA (Digital Living Network Alliance) setting allows you to ■ **Enable** and configure the digital media server. This allows digital media stored on an external USB hard drive connected to the NF20MESH to be accessible to other devices on your network.

Samba (SMB)

■ **Enable** the Samba Server Message Block (SMB) to access the USB content from other connected devices. Samba requires authentication. Enter a **Username** and **Password** then select the **Apply** button. The Username will appear in the **Current Users** list.

Multiple Samba users are supported.

To remove a user, select the ■ button and then select the **OK** button in the confirmation dialog.

Advanced

The **Advanced** page contains eight groups of tools accessing a wide range of specialised settings.



Figure 32 – Advanced

Diagnostics

Monitor the performance of your gateway and troubleshoot its behaviour using a range of tests, real-time statistical analysis and activity logs.

Routing

Configure and control the flow and routing of data in to and out of your gateway.

Management

Enable and configure remote access and control for your gateway in a secure environment and control the LED light display.

Local Network

Access all configuration options for IPv4, IPv6, VLAN and your wireless services.

Phone

View and configure all the advanced features of your VoIP telephones.

System

Keep your system up to date and save your settings.

QoS

Manage and customise data priority for different services on the network.

Security

Control access and set up firewalls to prevent intrusion or define filters to allow specific access.

Diagnostics

Diagnostics – Information

The **Diagnostics – Information** page contains **Device Info** such as hardware and software versions, etc. as well as the current status of the WAN connection. The lower part of the page contains **WAN** connection, **Route** and **ARP** (Address Resolution Protocol) details.

Device Info

The **Device Info** section displays basic information about the gateway.

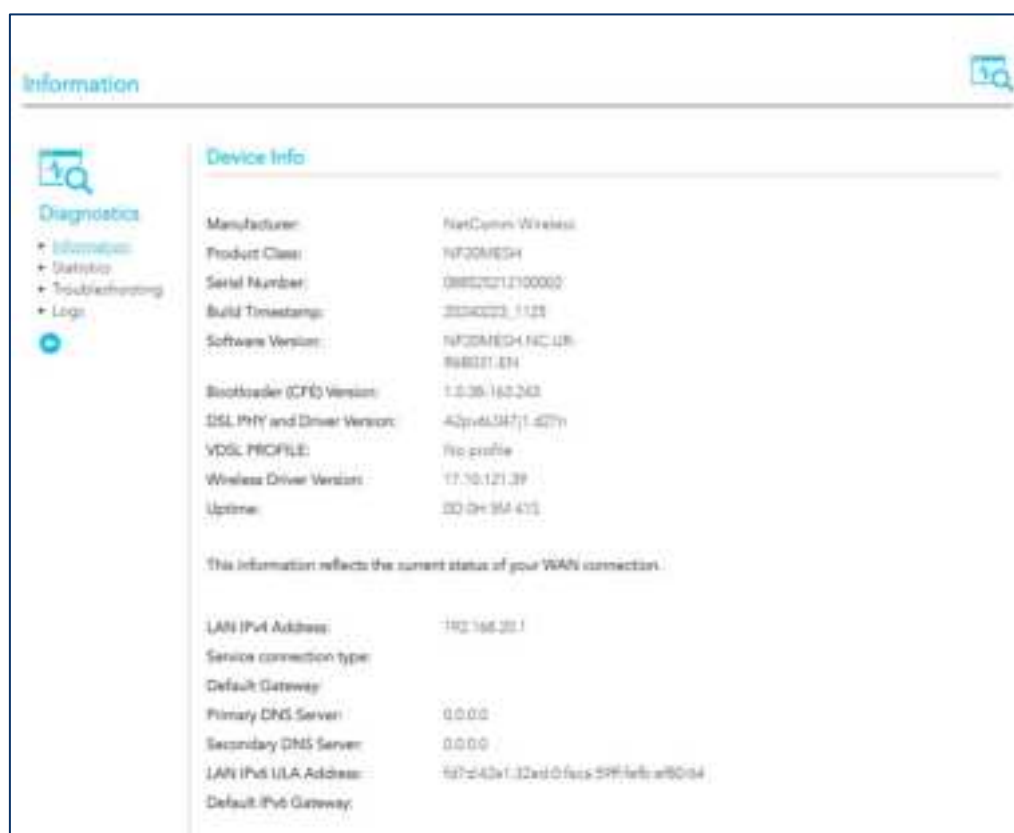


Figure 33 – Diagnostics - Information

The **Device Info** section contains the following information:

Item	Description
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.
Bootloader (CFE) Version	The current boot loader version installed on the router.

DSL PHY and Driver Version	The driver version of the on-board DSL chip.
VDSL PROFILE	The VDSL profile in use.
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	"Voice" is the only option currently available.
Uptime	The number of days, hours and minutes that the router has been running.
Line Rate – Upstream (Kbps)	The current synchronisation upstream speed of the DSL connection in Kbps (Kilobits per second).
Line Rate – Downstream (Kbps)	The current synchronisation upstream speed of the DSL connection in Kbps (Kilobits per second).
LAN IPv4 Address	The current IPv4 LAN IP address assigned to the router.
Service connection type	Displays whether the WAN connection is ADSL/VDSL or Ethernet WAN.
Default Gateway	The current default gateway address of the WAN interface.
Primary DNS Server	The current primary DNS server in use
Secondary DNS Server	The current secondary DNS server is use.
LAN IPv6 ULA Address	The current IPv6 LAN IP address in use if assigned.
Default IPv6 Gateway	The current IPv6 default gateway if assigned.

WAN

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

Interface	Description	Type	VLAN Mux ID	IPv6	IGMP Phy	IGMP Src Enbl	MLD Phy	MLD Src Enbl	NAT	Firewall	IPv4 Status	IPv4 Address	IPv6 Status
eth4.1	ETH WAN	IPoE	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	Enabled	ServiceDown		ServiceDown

Figure 34 – Diagnostics - WAN

Item	Description
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.
IPv6	The status of IPv6.

IGMP Pxy	Details the status of IGMP on each WAN connection. IGMP is only used with IP v4 connections. IGMP proxy enables the router to issue IGMP host messages on behalf of hosts that the router discovered through standard IGMP interfaces, allowing NAT transversal of Multicast traffic.
IGMP Source Enable	Details the status of IGMP Src on each WAN connection. IGMP Sources function send a membership report that includes a list of IGMP source addresses.
MLD Pxy	Shows the status of the Multicast Listener Discovery protocol when IPv6 is in use. Multicast Listener Discovery (MLD) proxy enables the router to issue MLD host messages on behalf of hosts that the router discovered through standard MLD interfaces.
MLD Source Enable	Details the status of MLD Src on each WAN connection. MLD Sources function can send a membership report that includes a list of MLD source addresses.
NAT	The NAT status of the WAN connection.
Firewall	The status of the router firewall across the WAN connection.
Status	The status of the WAN connection.
IPv4 Address	The current IP v4 address of the WAN interface.
IPv6 Address	The current IP v6 address of the WAN interface.

Route

The **Route** table displays details of displays any routes that the router has created.

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.20.0	0.0.0.0	255.255.255.0	U	0	cpe-pintf-1	b0
192.168.255.0	0.0.0.0	255.255.255.0	U	0		v40
255.0.0.0	0.0.0.0	255.0.0.0	U	0	cpe-pintf-1	b0

Figure 35 – Diagnostics - Route

ARP

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

ARP

IP address	Flags	HW Address	Device
192.168.20.2	Complete	54:05:db:dc:e2:80	br0
160.254.36.251	Complete	54:05:db:dc:e2:80	br0

NAT Mapping Table

The NAT Mapping Table displays any NAT address mappings. Each host on the network is shown, alongside the number of connections per host. Select the **Download** button to download a CSV document listing the complete NAT address mapping.

NAT Mapping Table

The NAT Mapping Table displays the current NAT address mapping.

Connections Per Host

Host Name	IP Address	Number of Connections
...	192.168.20.2	141

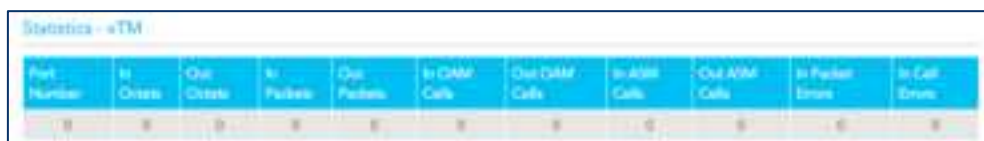
[Download](#) the complete NAT address mapping table in CSV format

Figure 36 – Diagnostics – NAT Mapping Table

	Drops	Rx/Tx (receive/transmit) packets with drops.
--	-------	--

xTM Interface

The **Statistics – xTM** section shows details related to the xTM (ATM/PTM) interface of the router.



Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packets Errors	In Cell Errors
1	0	0	0	0	0	0	0	0	0	0

Figure 39 – Diagnostics – xTM Interface

Item	Description
Port Number	The port number used by the xTM interface.
In Octets	The number of data packets in octets received over the ATM interface.
Out Octets	The number of data packets in octets transmitted over the ATM interface.
In Packets	The number of data packets received over the ATM interface.
Out Packets	The number of data packets transmitted over the ATM interface.
In OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
Out OAM Cells	Operation, Administration, and Maintenance (OAM) Cell is the ATM Forum specification for cells used to monitor virtual circuits.
In ASM Cells	The number of Any Source Multicast (ASM) cells received over the interface.
Out ASM Cells	The number of Any Source Multicast (ASM) cells transmitted over the interface.
In Packets Errors	The number of packets with errors detected over the xTM interface.
In Cell Errors	The number of cells with errors detected over the xTM interface.

xDSL

The **Statistics – XDSL** section provides advanced diagnostic information about the DSL interface of the gateway.

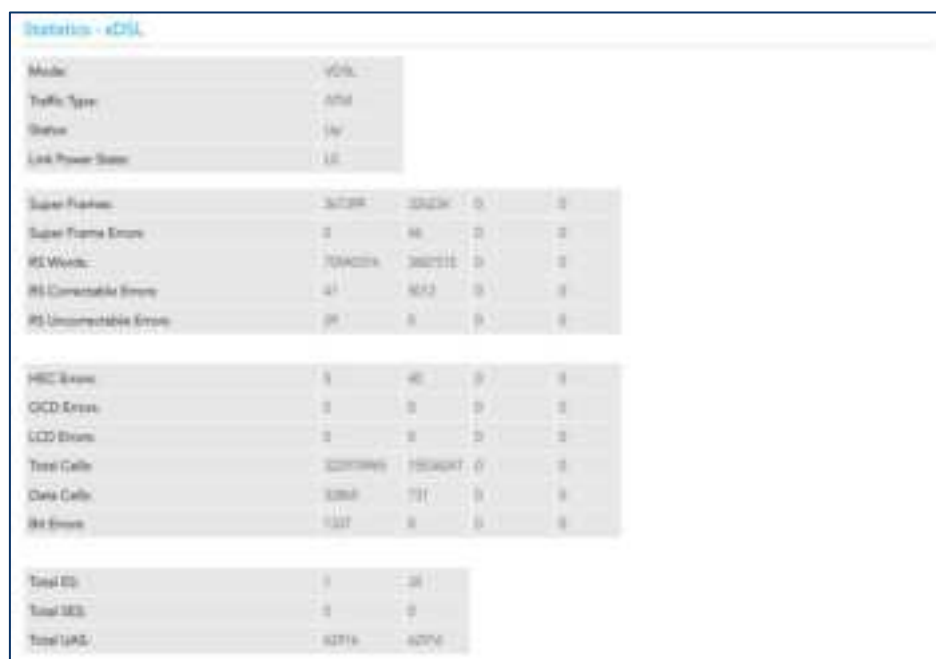


Figure 40 – Diagnostics - xDSL

CPU & Memory

The **Statistics – CPU & Memory** section shows real-time graphs charting the physical memory usage and the workload of the CPU.

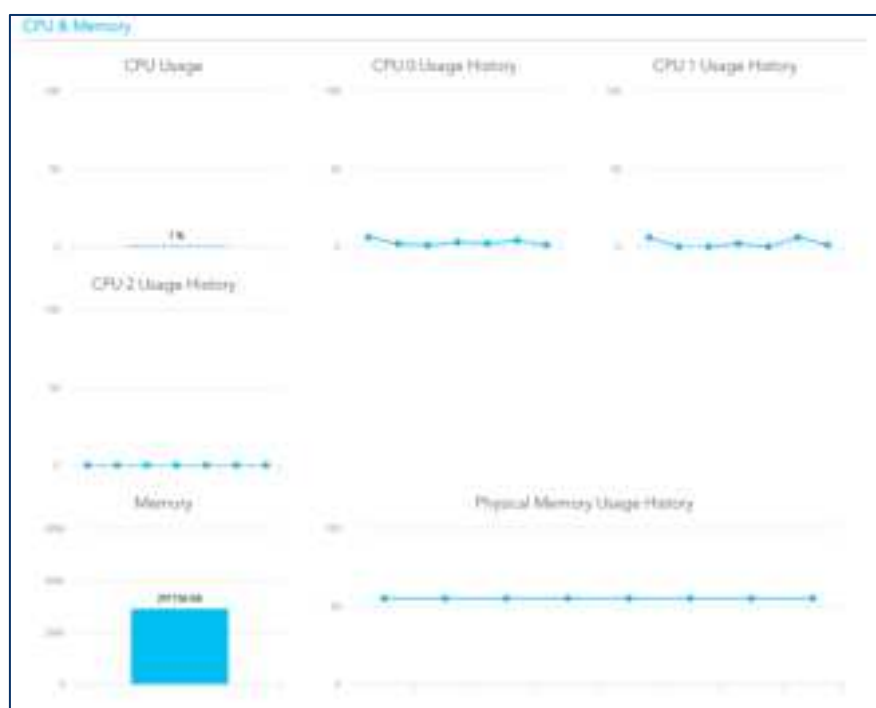


Figure 41 – Diagnostics – CPU and Memory

Diagnostics – Troubleshooting

The **Diagnostics – Troubleshooting** page contains a number of predefined tests with test results and other diagnostic settings.

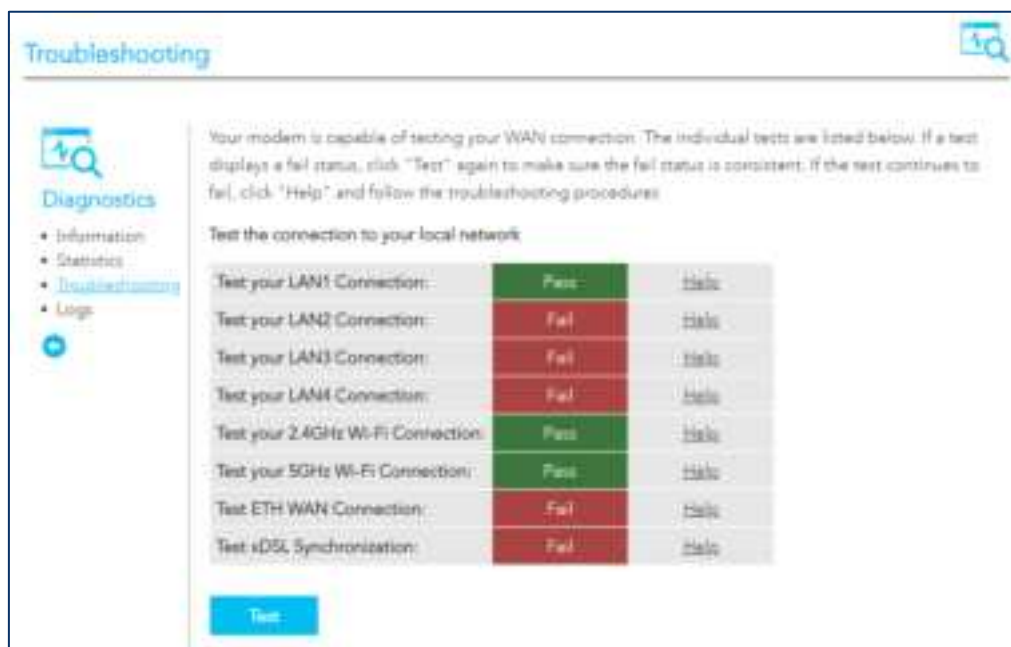


Figure 42 – Diagnostics - Troubleshooting

Connection tests

The connection tests section contains the result of several tests to check the status of your connection to your local network and the connection to your Internet service provider.

Diagnose the connection by selecting the **Test** button.

The following indicators display for each test:



A Pass icon displays when the connection is operating correctly.

Select [Help](#) to see the criteria for success for this test.



A Fail icon indicates that the test was unsuccessful.

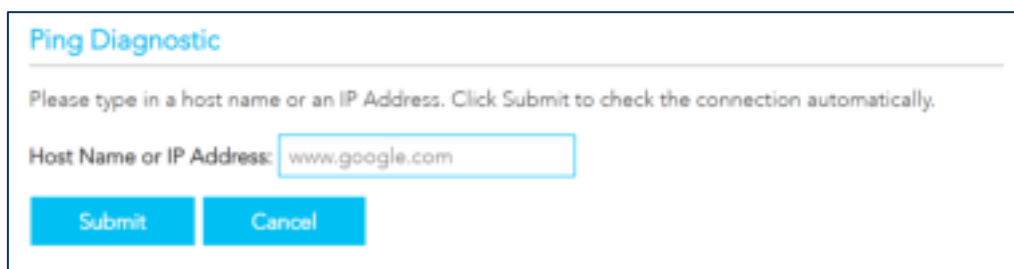
Select [Help](#) to see the possible reasons for the failure.

In the Help screen there are also Troubleshooting suggestions specific to that particular type of test which may be able to rectify the problem.

Select the **Rerun Diagnostic Tests** button after the troubleshooting has been completed.

Ping Diagnostic

The ping test lets you ping a remote IP address or hostname in order to test your internet connection.



Ping Diagnostic

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

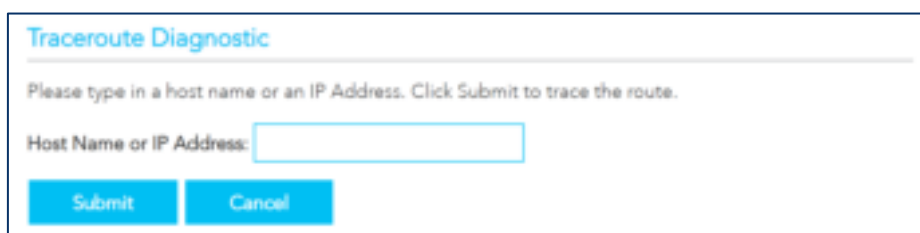
Host Name or IP Address:

Figure 43 – Diagnostics – Ping Diagnostic

To ping, type in a **Host Name** or **IP Address** and select the **Submit** button.

Traceroute Diagnostic

Perform a traceroute to a remote IP address or host name, to display the route used from your gateway to the remote host.



Traceroute Diagnostic

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


Host Name or IP Address:

Figure 44 – Diagnostic – Traceroute Diagnostic

To trace a route, type in a **Host Name** or **IP Address** and select the **Submit** button.

Sniffer

The Sniffer function is used to capture packets as they transit the gateway. The sniffer requires a USB storage device to be attached to the gateway to store the captured file.



Sniffer

The Sniffer is for capture packet. You need to set the "file name", "interface", "filter", "packet number" and "file size" when you can click "start" button to start capture.

USB storage	<input type="text" value="usb1:1"/>	
File Name	<input type="text" value="capture"/>	string
Interface	<input type="text" value="eth0.1"/>	
Protocol Filter	<input type="text" value="ALL"/>	
Packet Number	<input type="text" value="1000"/>	1-11
File Size(MB)	<input type="text" value="1"/>	1-100
Option	<input type="text" value="none"/>	
File		

After complete you can click the File to download the File.

Figure 45 – Diagnostic - Sniffer

Diagnostics – Logs

The **System Log** page allows you to view the log of the NF20MESH.

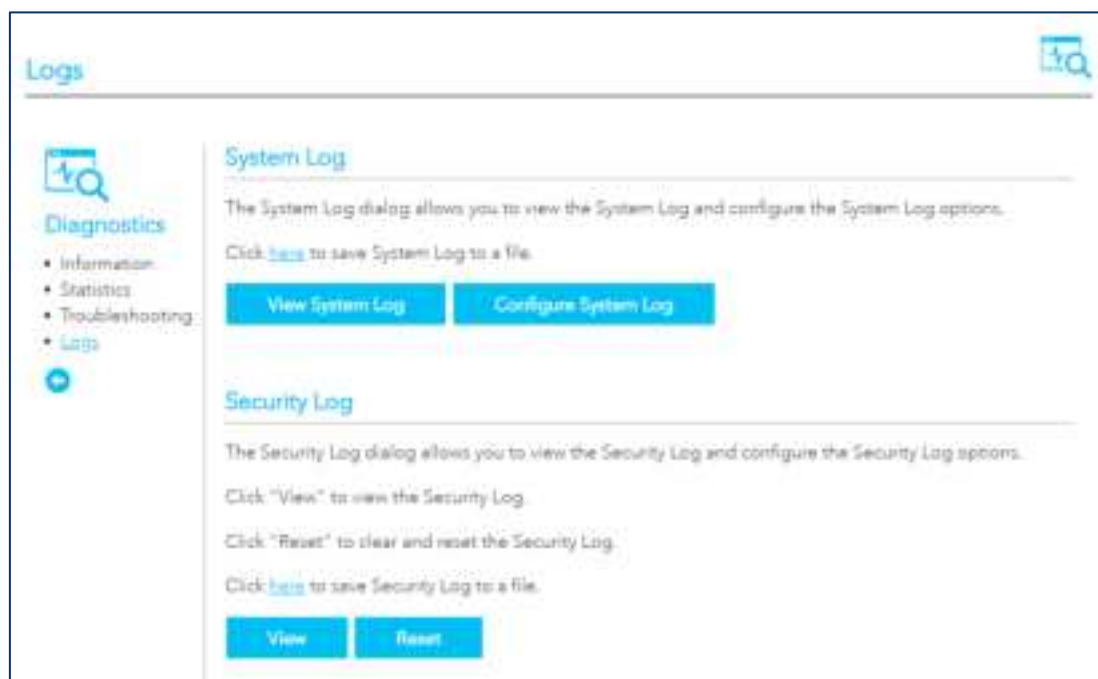


Figure 46 – Diagnostic – System Log

System Logs

To view the system log as it is currently configured, select the **View System Log** button.

System Logs			
Date/Time	Facility	Severity	Message
Feb 23 14:29:34	user	info	kernel: eth0 (vrt switch port: 0) (Logical Port: 0) (physid: 8) Link Up at 1000 mbps full duplex
Feb 23 14:38:16	daemon	err	smnbd[2741]: (2024/02/23 14:38:16.163959.0) ./source3/printing/print_standard.c#rstd_pcap_cache_reload
Feb 23 14:38:16	daemon	err	smnbd[2741]: Unable to open printcap file /etc/printcap for read!
Feb 23 15:56:20	daemon	err	smnbd[2741]: (2024/02/23 15:56:20.995559.0) ./source3/printing/print_standard.c#rstd_pcap_cache_reload
Feb 23 15:56:20	daemon	err	smnbd[2741]: Unable to open printcap file /etc/printcap for read!
Close			

Figure 47 – Diagnostic – System Logs

The results are displayed in a table in which each log record contains the following data fields: **Date/Time** stamp, **Facility**, **Severity** and a **Message**

The range of messages displayed can be defined, select the **Configure System Log** button to access the display settings.

Configure System Log

To configure the system log, select the **Configure System Log** button. When you have set the configuration, select the **Apply / Save** button to apply the changes.

Figure 48 – Diagnostic – System Log - Configuration

Item	Description
Log	When enabled the system will begin to log all the selected events.
Log Level	<p>The Log Level drop down list is arranged from most critical at the top (Emergency), the lowest level event at the bottom (Debugging).</p> <p>The following log levels are available: Emergency, Alert, Critical, Error, Warning, Notices, Informational, Debugging.</p> <p>Select a Log Level and all events above or equal to the selected level will be logged to a log file.</p>
Display Level	<p>Select a Display Level and, all logged events above or equal to the selected level will be displayed on the System Logs page.</p> <p>The range displayed is set using the same settings as described for the Log Level settings, see previous item.</p> <p>To view the System Logs page, select the View System Log button on the Logs page:</p> <p>View System Log</p>
Mode	<p>The default setting, Local, saves the log only to the local memory on the NF20MESH.</p> <p>The Remote mode allows you to save the log on a remote server.</p> <p>If the selected mode is Remote you must specify the IP address and UDP port of the remote syslog server to which the log will be sent.</p>

	If Both is selected you must specify the IP address and UDP port of the remote syslog server and events will be recorded in the local memory as well as the remote server.
Server IP Address	Specify the IP address of the remote syslog server. (Remote and both only.)
Server UDP Port	Specify the UDP port of the remote syslog server. (Remote and both only.)

Security Logs

Select the **View** button to display the security log. The security log contains details of login attempts to the gateway.

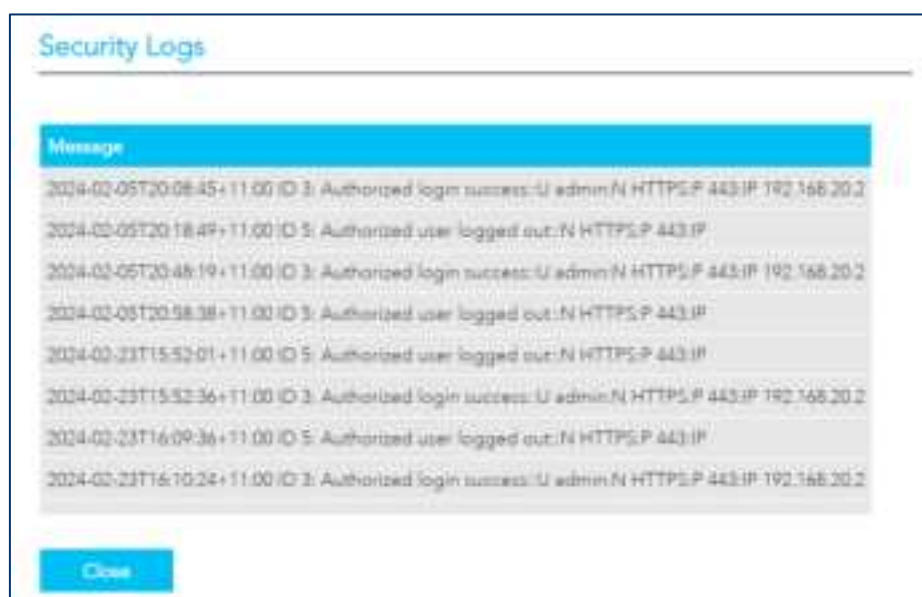


Figure 49 – Diagnostic – System Log – Security Log

Select the **Reset** button to clear the existing records from the log and reset the **Security Log**.

Select the **Click here** link to save the current log file to a .txt file.

Routing

NAT

The **Routing – NAT** page contains three sections: Port Forwarding, DMZ Host and ALG.

Port Forwarding

Port forwarding allows you to direct incoming traffic from the WAN side to the Internal network host with a private IP address on the LAN side.



Figure 50 – Routing – Port Forwarding

The following parameters are displayed in the port forwarding section:

Item	Description
External Port Start	The starting external port number (when custom server is selected). When a service is connected this field will be completed automatically.
External Port End	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	The starting internal port number (when custom server is selected). When a service is connected this field will be completed automatically.
Internal Port End	The ending internal port number (when custom server is selected). When a service is connected this field will be completed automatically.
Server IP Address	The IP address of the local server.
WAN Interface	Describes the type of target interface: ETH , WAN , VDSL , custom, etc.
WAN Loopback	Indicates current WAN Loopback status: Enabled or Disabled
Enable	Enables the rule
Delete button	Select the Delete button to permanently remove a Port Forwarding rule.
Add button	Select Add to open the Add Virtual Servers page.

Add a port forwarding rule

To add a port forwarding rule select the **Add** button. The **Add Port Forwarding Rule** window is shown:

Figure 51 – Routing – Add port forwarding rule

Enter the following details to create the rule:

Item	Description
Use Interface	The interface type to be used by the rule.
Service Name	Enter a descriptive name for the service that the rule will apply to.
LAN Loopback	Select Enable to allow the LAN host to access another LAN host/server via the external IP Address of the gateway. When Disable is selected you must use the internal IP address of the device when on the LAN side.
Server IP Address	Enter the IP address of the local server/host.
Status	Select Enable to allow the rule to be accessible. Select Disable to save the rule in an inactive state.
External Port Start	Enter the starting internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically
External Port End	Enter the ending internal port number range (when custom server is selected).

	When a predefined service is selected this field will be completed automatically.
Protocol	The options are: TCP, UDP or TCP/UDP
Internal Port Start	Enter the starting internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
Internal Port End	Enter the ending internal port number range (when custom server is selected). When a predefined service is selected this field will be completed automatically.
Apply/Save button	Select to save and enable the rule. Up to 32 rules can be defined.

Port Triggering

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

The Gateway 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 of 32 entries can be configured.

This is a list of specific ports in the router's firewall that are open for access by remote parties.



Figure 52 – Routing – Port Triggering

Select the **Add** button to configure the port settings to add a port triggering rule. The **Add Port Forwarding Rule** window is shown.

Add Port Forwarding Rule

Name:

Use Interface:

Trigger Protocol:

Trigger Port Start:

Trigger Port End:

Open Protocol:

Open Port Start:

Open Port End:

Figure 53 – Routing – Add Port Forwarding Rule

The following information is required to configure the Port Forwarding rule. Select the **Apply / Save** button to create the rule.

Field	Description
Name	Enter the name of the rule.
Use Interface	The interface that the rule should be valid on.
Trigger Protocol	Options include TCP, UDP or TCP/UDP.
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.
Open 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.

DMZ Host

When the DMZ host is enabled, the NF20MESH 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 or being used in the Virtual Server table to the DMZ host.

Enter the **DMZ Host IP address** and select **Apply** to activate the DMZ host. To deactivate the DMZ Host function, clear the IP address field and select the **Save/Apply** button.

Figure 54 – Routing – DMZ

Enable LAN Loopback

Note that ☒ **Enable LAN Loopback** can also be selected.

LAN Loopback allows the LAN host to access another LAN host/server via the external IP Address of the router.

Without NAT loopback you must use the internal IP address of the device when on the LAN side.



Important –

Enabling LAN loopback will present your DMZ server to the Internet without a router firewall. This may pose a security risk to your network.

ALG

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

Figure 55 – Routing – ALG

The following ALG settings are configurable. Select the **Apply / Save** button to apply any changes.

Item	Description
<input checked="" type="checkbox"/> FTP Enable	Select to allow File Transfer Protocol (FTP) services.
<input checked="" type="checkbox"/> SIP Enable	Session Initiation Protocol (SIP) is a signalling protocol used by communications applications and services between two or more endpoints on IP networks.
<input checked="" type="checkbox"/> TFTP Enable	Select to allow Trivial File Transfer Protocol (TFTP) services. TFTP provides a simpler file transfer protocol than FTP using UDP, without user authentications, etc..
<input checked="" type="checkbox"/> H323 Enable	H.323 is a protocol standard for multimedia communications that supports real-time transfer of audio and video data over packet networks like IP.
<input checked="" type="checkbox"/> IRC Enable	Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in the form of text.
<input checked="" type="checkbox"/> Port Triggering Enable	Port Triggering is a configuration option on NAT-enabled routers that provides access to services outside the network or on the Internet.
<input checked="" type="checkbox"/> PPTP Enable	Point-to-Point Tunnelling Protocol (PPTP) is a protocol used to implement virtual private network.
<input checked="" type="checkbox"/> IPsec Enable	Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data sent over an IPv4 network.
<input checked="" type="checkbox"/> RTSP Enable	Real Time Streaming Protocol (RTSP) is a network control protocol designed to establish and control streaming media sessions in entertainment and communications applications.
<input checked="" type="checkbox"/> SNMP Enable	Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions in a local area network (LAN) or wide area network (WAN).

Routing

The **Routing – NAT** page contains two sections: **Static Route** and **RIP Configuration**

Static Route

The **Static Route** table displays a list of the configured static routes.



Static Route

A maximum 32 entries can be configured.

IP Version	Destination IP/Mask	Gateway	Interface	Metric	Delete
	192.168.20.10/32	192.168.20.1	br0	0	<button>Delete</button>

Add

Figure 56 – Routing – Static Route

Select the **Add** button to add a static route definition. The **Add Static Route** window is shown.



Add Static Route

Enter the destination network address, subnet mask, gateway IP and/or available WAN interface then click "Apply/Save" to add the entry to the routing table.

IP Version: ☒ IPv4 ☐ IPv6

Destination IP address/prefix length:

Gateway:

Interface:

Metric: (optional; metric number should be greater than or equal to zero)

Apply/Save Close

Figure 57 – Routing – Static Route – Add Static Route

Enter the following details to configure a new static route. Select the **Apply / Save** button to apply any changes.

Item	Description
IP Version	Select <input checked="" type="radio"/> IPv4 or <input type="radio"/> IPv6.
Destination IP/Mask	Enter the Destination Network Address and its subnet mask in CIDR notation, for example 192.168.20.10/32.
Gateway	Enter the Gateway IP Address and/or an available WAN Interface .
Interface	
Metric	The Metric field is used to set a priority for this route, the lower the number the higher the priority.

RIP Configuration

The **Routing Information Protocol (RIP)** allows routers to exchange network topology information. This information allows the automatic creation and updating of routing tables.

Interface	Version	Operation	Enabled
eth4.1	2	Passive	<input checked="" type="checkbox"/>

Apply/Save

Figure 58 – Routing – RIP Configuration

The following information is required to configure RIP:

Item	Description
Interface	The network interface that the RIP settings apply to.
Version	1: Use RIPv1 to support classful routing. 2: Use RIPv2 to support subnet information gathering and Classless Inter-Domain Routing. Both: RIP will use both RIPv1 & RIPv2, and will multicast and broadcast to all adjacent routers.
Operation	Passive: RIP will only respond to “Request Message” queries on the RIP enabled interface. Active: RIP will broadcast and respond to “Request Message” queries on the RIP enabled interface.
Enabled	Select Enable to activate the RIP routing service on the selected Interface .



Important –

RIP cannot be selected for a WAN interface which is NAT enabled, such as PPPoE.

Go to Basic Setup and select Ethernet WAN, click Next and then select IP over Ethernet (IPoE). The RIP option will now be available.

DDNS

Dynamic DNS (DDNS) allows your Gateway to associate an easy-to-remember domain name, such as [yourdomainname].com with the regularly changing IP address assigned by your ISP. This feature allows you to connect remotely more easily to your home network.



Note –

DDNS is one component of connecting remotely to your home network. For complete connectivity, you will need to add port forwarding rules for the relevant application in the firewall. Some ISPs block common ports, such as 80 and 443, so you may need to contact your internet provider to allow traffic from your ISP to your gateway. Refer to your ISP documentation for further information.



Figure 59 – Routing – DDNS

To add a Dynamic DNS connection, select the **Add** button. The **Add Dynamic DNS** window is shown:

Figure 60 – Routing – Add DDNS

The following information is required to configure a Dynamic DNS entry. Select the **Apply / Save** button to apply the changes.

Item	Description
D-DNS provider	Select the DDNS service provider from the D-DNS provider .
Hostname	Enter your chosen dynamic DNS Hostname .
Interface	Select the interface that the service operates on.
Username / Password	Enter the Username and Password of your dynamic DNS account.

DNS Proxy

You can define an easy to remember proxy name for the standard URL of the Gateway (192.168.20.1) to provide more convenient access the gateway's Web UI.

Select **Enable DNS Proxy** and then enter the proxy **Host name of the Broadband Router** and the proxy **Domain name of the LAN network**, as in the example shown below. Select **Apply / Save** to continue.

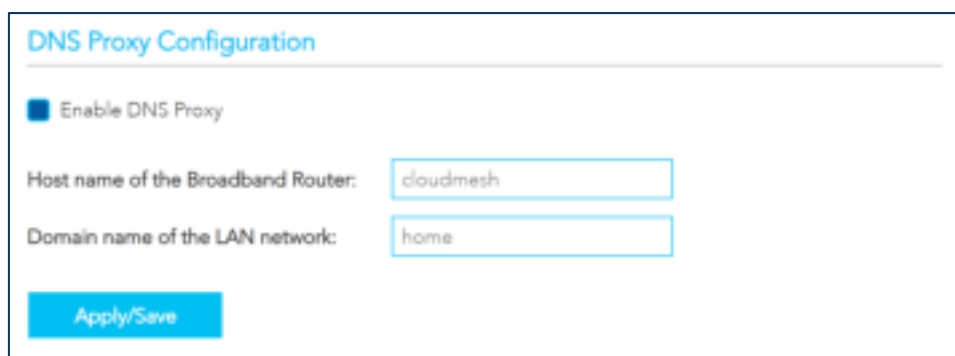


Figure 61 – Routing – DNS Proxy

The **Host name** and **Domain name** are combined to form a unique label that is mapped to the gateway IP address. This can be used to access the user interface of the gateway with a local name rather than by using the gateway IP address. In the example above you will now be able to access your gateway by entering the proxy name **http://cloudmesh.home** into your web browser.


Proxy names can also be custom: quick.uiaccess, goto.gatewayui, etc.

Management


TR-069 Client

The **TR-069 Client** page is used to enable **TR-069** on the gateway, providing provisioning, auto-configuration or diagnostics to be automatically performed if supported by your Internet Service Provider (ISP).

Figure 62 – Management –TR-069 Client

 **Important** – Changing or removing these settings may cause you to lose ISP remote support and automatic firmware upgrade services.

The following settings can be configured on the TR-069 page:

Item	Description
Inform	Set to enable to TR-069 client inform session initialization.
Inform interval	Time in seconds that inform session data is sent to the Auto-Configuration Server (ACS).
ACS URL	The address where the ACS server is located.
ACS Username	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 interface connection used to send and receive data to the ACS server.
Display SOAP messages on serial console	Select  Enable to view the SOAP messages on a command prompt screen.

Apply/Save button	Select to save your settings and start the TR-069 services.
Get RPC Methods button	Select to retrieve Remote Procedure Call (RPC) Methods .
Connection Request Username	Enter the username to be used by the ACS to initiate the connection for a TR-069 session with the NF20MESH.
Connection Request Password	Enter the password to be used by the ACS to initiate the connection for a TR-069 session with the NF20MESH.
Connection Request Port	Enter the Port number to be used by the ACS when connecting to the NF20MESH for a TR-069 session.
Connection Request URL	Enter the URL address to be used by the ACS for a TR-069 session with the NF20MESH.

Passwords

The **Passwords** page is used to manage the password used to log in to the gateway.

Figure 63 – Management - Passwords

There are a number of requirements and restrictions for passwords on the gateway:

Requirements

- Both username and password can be between 1 to 16 characters.
- Characters can be either letters, numerals and/or special characters.
- Letters are case-sensitive.

Restrictions

- Usernames and passwords cannot exceed 16 characters in length.
- They must not include spaces or punctuation marks.
- Characters cannot be symbols.

LED control

In some locations the LED lights on the front of the NF20MESH may cause an unwanted distraction, for example in a small apartment or bedroom.

Use the **LED Control** settings to switch the display of the LED lights on or off.



Figure 64 – Management – LED control

Timeout

The **Timeout** page allows you to configure the amount of inactive / idle time before the web interface is logged out. To update, enter the amount of time, in seconds, then select the **Save / Apply** button.




Figure 65 – Management - Timeout

SNMP

The **SNMP** page allows for the configuration of Simple Network Management Protocol (SNMP), which 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 Gateway (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.

Figure 66 – Management – SNMP Agent

The following information is required to configure an SNMP configuration:

Item	Description
SNMP Agent	Select  Enable to start this service.
Read Community	Enter the password to read device SNMP values or accept the default: public
Set Community	Enter the password to sset device SNMP values or accept the default: private
System Name	Enter a recognisable system name or accept the default: NF20MESH
System Location	Enter a system location or accept the default: unknown
System Contact	Enter a system location or accept the default: unknown
Trap Manager IP	Enter the IP address of the trap manager.

Local Network

Local Area Network

The **Local Area Network** page is used to configure your local area network, such as IP addresses, DHCP and DNS. The page is broken up into multiple sections, and individual setting pages – **IPv4**, **IPv6** and **VLAN**.

IPv4 LAN Auto Configuration

Figure 67 – Local Network - LAN

Item	Description
IP Address	Enter the Local IP Address to use for the NF18MESH.
Subnet Mask	Enter the subnet mask to define the subnet of the Local Network.
DHCP	Select <input checked="" type="radio"/> On to enable the DHCP server.
DHCP Start Range	Enter the start IP address for the DHCP IP Address pool.
DHCP End Range	Enter the end IP address for the DHCP IP Address pool.
Primary DNS Server	Enter the IP address of the primary DNS server.
Secondary DNS Server	Enter the IP address of the secondary DNS server.
DHCP Lease Time (Hour)	Assigned IP addresses will be dropped after this time period and the address may be assigned to a different device on the network. Default is 24 hours.

<input type="checkbox"/> Enable IGMP Snooping	<p>Enable IGMP (Internet Group Management Protocol) Snooping and select the IGMP Snooping mode to use.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Standard Mode – Allows all multicast traffic to LAN clients. <input type="checkbox"/> Blocking Mode – Only allows multicast subscribed clients to receive multicast packets.
<input type="checkbox"/> Enable LAN side firewall	Enable the LAN side firewall to restrict traffic between LAN host-LAN hosts and WiFi clients.
<input type="checkbox"/> Enable DHCP Server Relay	Disable the DHCP server defined above and relay requests to the external server specified in the DHCP server IP address text box.
DHCP Server IP Address	When you select <input checked="" type="checkbox"/> Enable DHCP Server Relay this text box becomes available. Enter the address of the external DHCP server that you want to use instead of the DHCP server specified above. Note that it is no longer available.

DHCP

The screenshot displays the DHCP configuration page. It includes three main sections:

- Static IP Lease Set:** A table with columns 'Description', 'MAC Address', 'IP Address', and 'Delete'. It contains one entry with a MAC address '2819C0845-B0C8-4D28-B020-...' and a 'Delete' button.
- DHCP Option Setup:** A table with columns 'Option ID', 'Value', 'Address Pool', 'Enabled', and 'Delete'. It contains one entry 'Curler (1:254)' and an 'Add' button.
- DHCP Option ID Setup:** A table with columns 'Option ID', 'Vendor ID', 'IP Address', 'Subnet Mask', 'Primary DNS', 'Secondary DNS', 'Gateway', 'DHCP Lease Time', 'Enabled', and 'Delete'. It contains one entry '1' and an 'Add' button.

Figure 68 – Local Network - DHCP

DHCP Static IP

Use the **DHCP Static IP Lease** facility to reserve DHCP Addresses for specific hosts.

Select the **Add Entries** button to open the **DHCP Static IP Lease** dialog.

Enter the **MAC Address** of the chosen host and **Static IP Address** and then select the **Apply/Save** button.

Up to 32 **Static IP Leases** can be created and managed at the same time.

To manage the lease list, select the **Delete** button to permanently remove a lease from the list.

DHCP Option Setup

Select the **Add** button to open the **DHCP Option Setup** dialog.

Select the **State** as ☒ **Enable** to allow custom DHCP codes.

If the **State** as ☐ **Disable** the option will remain in the list, but no be active.

Enter a **Code** of 1 to 254.

Enter a **Value**, maximum length is 255.

Select the **Apply/Save** button to apply and save the changes.

To manage the option list, select the **Delete** button to permanently remove an option from the list.

DHCP Port setup

The DHCP port allows you to enable or disable DHCP on specific ports. Select the ports you would like DHCP enabled on, then select the **Apply / Save** button.



Figure 69 – Local Network – DHCP Port Setup

IPv6 LAN Auto Configuration

IPv6 LAN Auto Configuration

1. Successful 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 "0002" instead of "2".

2. Unique local address must start with "fd". The prefix length must be 64.

Static LAN IPv6 Address Configuration

Interface Address (prefix length is required):

IPv6 LAN Applications

RADVD: ☒ On ☐ Off

ULA Prefix Advertisement: ☒ On ☐ Off

☒ Automatically Generate ☐ Manually Configure

DHCP: ☒ On ☐ Off

Auto-Configuration: ☒ Stateless ☐ Stateless

MLD: ☒ On ☐ Off

☒ Standard Mode ☐ Blinking Mode

DHCPv6 Relay: ☐ On ☒ Off

Figure 70 – Local Network – IPv6 LAN Configuration

The following settings are configurable on the IPv6 LAN Auto Configuration page:

Item	Description
Interface Address	Enter an IPv6 address for the gateway.
IPv6 LAN Applications	
RADVD	<p>The Router Advertisement Daemon (RADVD) is used by system administrators in stateless auto-configuration methods of network hosts on IPV6 networks.</p> <p>The Router Advertisement Daemon (RADVD) is used in stateless auto-configuration on IPv6 networks.</p> <p>The RADVD is an open-source software agent that allows link-local advertisements of IPv6 router information using the Neighbour Discovery Protocol (NDP) as specified in RFC 2461.</p> <p>When IPv6 hosts first connects, they broadcast router solicitation (RS) requests onto the network to discover available routers. The RADVD agent answers requests with Router Advertisement (RA) messages. In addition, RADVD periodically broadcasts RA packets to update network hosts.</p> <p>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.</p>

ULA Prefix Advertisement	<p>Select <input checked="" type="checkbox"/> On to enable the use of unique local addresses. The router will advertise the IPv6 /64 prefix to new devices on the network.</p> <p><input checked="" type="checkbox"/> Randomly Generate – Randomly generates the unique local addresses and the prefix.</p> <p><input checked="" type="checkbox"/> Statically Configure – Enter a static IPv6 address for the router if one has been assigned to you by your Internet Service Provider (ISP).</p>
DHCP	Select <input checked="" type="checkbox"/> On to enable a DHCPv6 service.
Auto-Configuration	<p><input checked="" type="checkbox"/> Stateless – IPv6 hosts can generate the 64-bit Interface ID automatically using Internet Control Message Protocol version 6 (ICMPv6) 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.</p> <p><input checked="" type="checkbox"/> Stateful – This configuration makes use of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Similar to IPv4 implementation, 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.</p>
MLD	<p>Select <input checked="" type="checkbox"/> On to enable MLD (Multicast Listener Discovery) snooping and select the MLD Snooping mode to use.</p> <p><input checked="" type="checkbox"/> Standard Mode – Allows all multicast traffic to LAN clients.</p> <p><input checked="" type="checkbox"/> Blocking Mode – Only allows multicast subscribed clients to receive multicast packets.</p>
DHCPv6 Relay	<p>Select <input checked="" type="checkbox"/> Enable to relay DHCP messages between DHCPv6 clients and DHCPv6 servers on different IPv6 networks.</p> <p>The following DHCPv6 related settings are required:</p> <p>DHCPv6 Server IP Address – Enter the relay destination.</p> <p>Selected WAN Interface – Select the type of interface to be used.</p> <p>Hop limit – Set the number of hops (each time a data packet passes through a network device on its way from its source to its destination) a packet is allowed before being discarded.</p>

VLAN

VLAN Setup

Select a LAN port: eth0

☒ Enable VLAN Mode

Apply/Save

VLAN ID	Pbits	Delete
1	1	Delete

Add

Figure 71 – Local Network – VLAN Setup

Item	Description
Select a LAN port	Select the port you would like to enable VLAN settings.
<input checked="" type="checkbox"/> Enable VLAN Mode	Select if you want to configure VLAN.
VLAN ID	Enter a VLAN value between 0 and 4094.
Pbits	Enter a value from 0-7 indicating the priority bits that dictates the priority of the VLAN.
Add button	Click to create an additional VLAN port.
Delete button	Select the delete button to remove the VLAN configuration.

Wireless Advanced Settings

The **Wireless Advanced Settings** page includes two sections for configuring advanced settings of the Wi-Fi: MAC Filter and Advanced.

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.

Select  **MAC Filter** to configure this service.

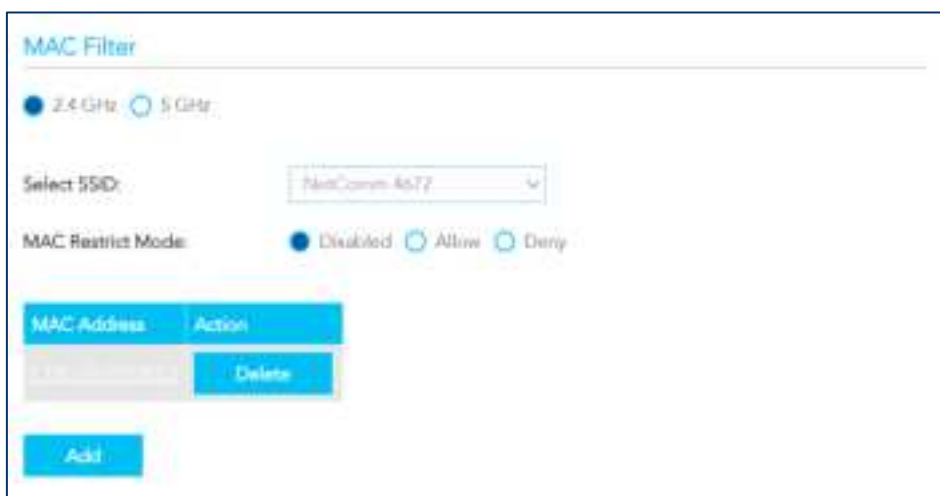




Figure 72 – Local Network – Wireless - MAC Filter

Item	Description
Select a frequency	Select  2.4GHz or  5GHz to separately define the MAC Filter settings for each. Note that you must click the Apply/Save button before switching frequencies or the changes made to the first will be lost.
Select SSID	Select the wireless network you wish to configure.
MAC Restrict Mode	Specify which wireless networks will be allowed to connect to the NF18MESH by using the three Bridge Restrict options. Disabled – This will keep the MAC Addresses that you have added but turn off the MAC Filter functionality. Allow – Select to allow the listed MAC Addresses access to the wireless network. Deny – Select to prevent the listed MAC Addresses from having access to the wireless network.
MAC Address	Click the Add button to include additional MAC Addresses in the list. Enter MAC address in the format of: aa:bb:cc:11:22:33
Delete button	Click permanently remove the MAC Address from the list.

Advanced

Use the **Wireless Advanced Settings** page access highly technical advanced settings for the Wi-Fi.

Advanced

☒ 2.4 GHz ☐ 5 GHz

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.

Bandwidth:	20MHz	Current: 20 MHz
Channel:	Auto	Current: 2
Control Sideband:	Auto	
802.11n Protection:	Auto	
Support 802.11n Client Only:	Off	
54g Mode:	54g Auto	
Rate:	Auto	
Basic Rate:	Default	
Multicast Rate:	Auto	
OBSS Co-Existence:	Enable	
Fragmentation Threshold:	2346	
RTS Threshold:	2347	
DTIM Interval:	1	
Beacon Interval:	100	
XPress Technology:	Enable	
WMM(Wi-Fi Multimedia):	Auto	
WMM No Acknowledgement:	Disable	
Beamforming Transmission (BFR):	Enable	
Beamforming Reception (BFR):	Enable	
Band Steering:	Disable	

Apply/Save

Figure 73 – Local Network – Wireless – Advanced

The following settings are configurable on this page:

Item	Description
Bandwidth	Bandwidth Select the bandwidth for the network: For 2.4GHz this may be 20MHz or 40MHz. For 5GHz and 6GHz this may be 20MHz, 40MHz, 80MHz.
Channel	The best channel is automatically chosen for your network.

Control Sideband	Always set to Auto.
802.11n Protection	Select 802.11n Protection functionality to be either: Disabled or Auto These settings will enable or disable 802.11n service, resorting to 802.11a/b/g service.
Support 802.11n Client Only	If the network should only support 802.11n clients only.
54g Rate	Allows you to specify the maximum bandwidth of the 802.11g network.
Basic Rate	Limits the connection minimum rate for 802.11a/b/g service.
Multicast Rate	Select the multicast transmission rate in Mbps for the network. The rate of data transmission should be set depending on the speed of your wireless network. Available settings are: Auto, 6, 9, 12, 18, 24, 36, 48, 54 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 .
OBSS Co-Existence	Enable or disable OBSS Co-Existence, which assists to reduce interference with other wireless networks.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. 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. The default setting is: 2346
RTS Threshold	The RTS Threshold is the minimum size in bytes for which the Request to Send/Clear to Send (RTS/CTS) channel contention mechanism is used. The router sends 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 setting (which is the maximum value): 2347 In a network with significant radio interference or large number of wireless devices on the same channel, reducing the RTS Threshold might help in reducing frame loss.
DTIM Interval	A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. Enter a value between 1 and 255 seconds for the DTIM interval between messages.
Beacon Interval	SSID information is broadcast in specific intervals. The beacon interval may be adjusted in milliseconds (ms). The default (100 ms) is recommended.
XPress Technology	Select Enable to turn on this is special frame-bursting accelerating technology for IEEE802.11g. The default is Enable .
WMM (WiFi Multimedia)	WMM (WiFi Multimedia) maintains the priority of audio, video and voice, over other applications which are less time critical by ensuring that data from applications

	<p>that require better throughput and performance are inserted in queues with higher priority.</p> <p>Select whether WMM is: Auto, Disabled or Enabled</p>
WMM No Acknowledgement	<p>This setting is only available when WMM (WiFi Multimedia) is set to Auto or Enabled.</p> <p>By default, the 'Ack Policy' for each access category is set to Disabled, meaning that an acknowledgement packet <u>is</u> returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance.</p> <p>Select Enabled to turn off the acknowledgement request. This can be useful for Voice transmissions where speed of transmission is important and packet loss is tolerable to a certain degree.</p>
Beamforming Transmission (BFR)	Enables Beamforming Transmission.
Beamforming Reception (BFE)	Enables Beamforming Reception.
Band Steering	<p>Select Enable to detect if the client has the ability to use all bands.</p> <p>When enabled, the less congested 5GHz network is selected (by blocking the client's 2.4GHz network).</p>

Phone

SIP Settings

The **SIP settings** page provides advanced functionality for managing your VoIP connection.



Figure 74 – Local Network – SIP Settings

The following configuration items can be updated on this page. Select the **Apply / Save** button when you have finished configuring the connection to save your changes.

Item	Description
Interface Selecting	
Bound Interface Name	Select the correct Bound Interface Name from your Internet WAN Service Connection or you can select or Any_WAN
Fax Setting	
Fax negotiate mode	Select: Auto Switch , Negotiate or V.152
Bypass Codec	Select the codec used for FAX sending, check with your VoIP Provider for codec and FAX over VoIP support. Select: G711_A , G711_MU or T.38
Settings	
Enable T38 Redundancy Support	If you wish to send or receive faxes via VoIP and have a fax machine capable of using the T38 fax over VoIP protocol select this function to enable T.38 Codec redundancy. T.38 packet payloads are repeated for each packet.
Enable VAD redundancy support	Enables the Voice Activated Detection (VAD) function of the modem. When enabled, no data is transmitted during periods of silence or low volume, reducing the data usage.
VAD mode in signal	Select: None , Silencsupp or Annexa Annb VAD
Enable RTCP Flow Control	RTP Control Protocol (RTCP) provides out-of-band statistics and packet control information for an RTP session.
Enable Echo Cancellation	Enable to improve voice quality and network capacity by preventing echo from being created or removing it after it is already present.
Enable # to ASCII	Select convert phone number to ASCII format.
SIP Timer Setting	

	Set custom Timeout and Expiration times or accept the defaults.
Digitmap Setting	
Digitmap Setting	The VoIP Dialplan specifies how to interpret digit sequences dialled by the user, and how to convert those sequences into an outbound dial string. For more information refer to the <i>Configuring a VoIP dial plan</i> section on the next page.
QoS Setting	
DSCP for SIP	Select a specific Differentiated Services Code Point (DSCP) priority tag for Quality of Service (QoS) to SIP packets, the default: DEFAULT(00000)
DSCP for RTP	Select a specific Differentiated Services Code Point (DSCP) priority tag for Quality of Service (QoS) to RTP packets, the default: DEFAULT(00000)
Ethernet Priority Mark	Assign and tag packets with Class of Service (CoS) for Quality of Service at the media access control (MAC) level according to IEEE 802.1p. A value of 0-7 is accepted. Set -1 to disable CoS QoS.
Payload Setting	
RFC2198 Payload Value	Defines the RTP Payload size for Redundant Audio Data according to RFC2198 in lossy network connections. Enter a value between 97 to 127 , or accept the default of 125
Dtmf Relay setting	Select the signalling method for relaying Dual-tone Multi-frequency Relay Settings: InBand (default, used when the other two are not available), RFC2833 or SIPInfo
Call ID Setting	
Caller ID send Delay Time	Defines the delay after initial ring before CPE sends Caller ID to phone handsets. Enter a value in milliseconds (ms) between 500 to 1500ms , or accept the default of 600ms
Caller ID Message Type	Defines the Signalling method for sending caller id to phone handsets to display. Select a Caller ID Message Type: FSK_SDMF, FSK_MDMF or DTMF
FSK modulation Mode	Select the optimal Frequency-shift keying modulation mode: BellcoreGen, V23Gen or V23UK
Transport Setting	Select the appropriate SIP Transport protocol: UDP or TCP
SIP Extends	Select the appropriate PRACK (100rel) setting: Supported (default), Disabled or Required
Service Offer Setting	Select your Complementary business model: Local, Server, IMS or undefined

Digitmap Settings (configuring a VoIP dial plan)

The router comes with a default dial plan suitable for use in Australia. The dial plan tells the router to dial a number immediately when a string of numbers entered on a connected handset matches a string in the dial plan.

For example, the string 13[1-9]XXX allows the router to recognize six digit “13 numbers” allowing customers to call a business for the price of a local call anywhere in Australia. The reason it is configured as 13[1-9]XXX is because 13 numbers cannot begin with a 0 after the 13 while the last 3 digits may be any numeric digit.

You can configure the dial plan to match any string you like.

Digitmap Rules

Below are some rules for configuring a dial plan:

- Separate strings with a | (pipe) character.
- Use the letter X to define any single numeric digit.
- Use square brackets to specify ranges or subsets, for example:
 - [1-9] allows any digit from 1 to 9
 - [247] allows either 2 or 4 or 7
 - Combine ranges with other keys, for example:
[247-9*#] means 2 or 4 or 7 or 8 or 9 or * or #

Dial plan syntax

Item	Enter	Result
New dial string	(Pipe)	Separates dial strings.
Digit	0 1 2 3 4 5 6 7 8 9	Identifies a specific digit (do not use #).
Range	[digit-digit]	Identifies any digit dialled that is included in the range.
Wild card	X	X matches any single digit that is dialled.
Timer	.t (dot t)	Indicates that an additional time out period of 4 seconds should take place before automatic dialling starts.

Dial plan example: Australia Dial Plan

```
000|[*#]X[0-9*]|*#X[0-9*]|00[1-9]XX.t|014XXXXXXXX|016XXXXXXXX|0192X|0198XXXXXXXX|0[23478]XXXXXXXX|0500XXXXXXXX|11XX|123X|124XX|1251XX|1252XXX|1255X|1258XXX|1271X|130XXXXXXXX|13[1-9]XXX|1802XXX|189XX|1[8-9]XXXXXXXX|[2-9]XXXXXXX
```

Meaning

- 000 = Australia Emergency Call Service
- 0011*t = International number (After 0011 the router allows entry of arbitrary digits then and dials out after 4 seconds from the entry of the last digit.)(Note: Please ensure your VoIP provider supports international numbers for the country you are dialling.)
- 0[23478]XXXXXXXX = Landline numbers with area code 02,03,04,07,08 +XXXX XXXX and Mobile numbers with 04XXXXXXXX)
- 1[8-9]XXXXXXXX = 1800 and 1900 free call numbers
- 130XXXXXXXX = 1300 business numbers
- 13[1-9]XXX = 13 business numbers

- [2-9]XXXXXXX = Landline numbers without area code

System

The **System** pages allow you to access features such as configuration backup, scheduled reboot and firmware updates.

Settings

The **Settings** page is used to back up the current configuration of your gateway, as well as restore the gateway to factory defaults.

Backup

To create a file containing the current NF20MESH settings, select the **Backup** button, then select the **Backup Settings** button. A backup file is downloaded to the browser's default download location.

If you wish to encrypt the configuration, enter a password in the **Configuration Encryption Key** field, then select the **Apply / Save** button.

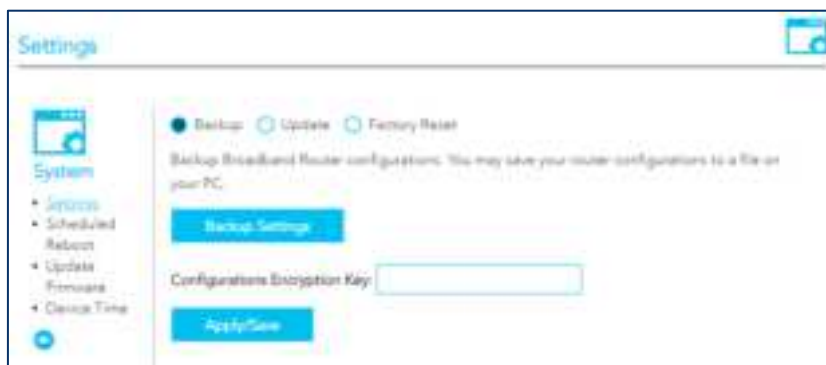


Figure 75 – System - Backup

Update

Use the **Update** page to restore the backup file created in the **Backup** section. Select the **Choose File** button, select a valid configuration file, then select the **Update Settings** button to begin the restore.

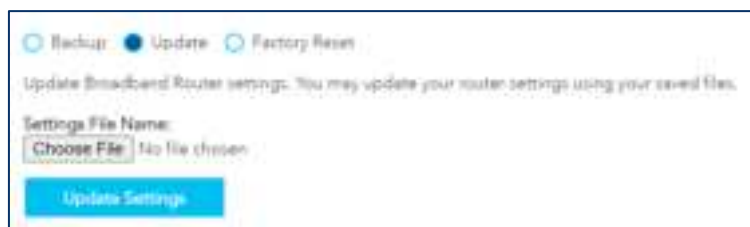


Figure 76 – System - Backup

Factory Reset

Use the **Factory Reset** page to restore the NF20MESH to its factory default settings.

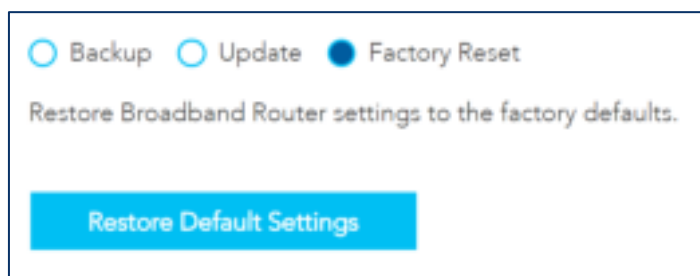


Figure 77 – System – Factory Reset

Select the **Restore Default Settings** button to restore the default settings. A **Reset to Default Settings** confirmation is shown. Select **Yes** to confirm the restore.



Figure 78 – System – Factory Reset - Confirm

Scheduled Reboot

The **Scheduled Reboot** page is used to schedule a regular time to restart the gateway.

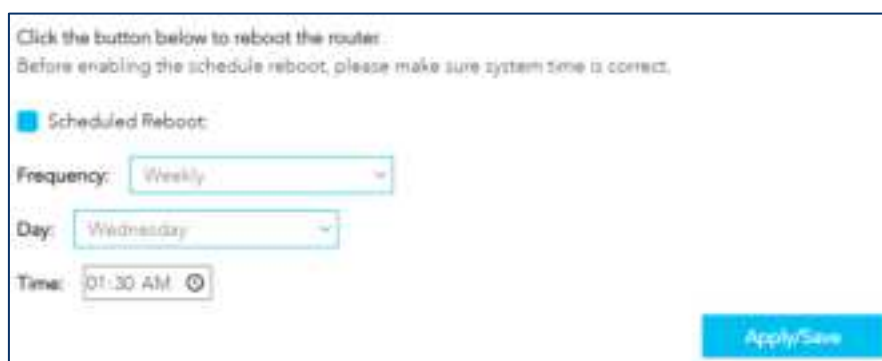


Figure 79 – System – Scheduled Reboot

To enable a scheduled reboot:

- 1 Enable the ☒ **Scheduled Reboot** check box.
- 2 Set the **Frequency** of the reboot from **Daily**, **Weekly** or **Monthly**.
- 3 If using a **Weekly** frequency, set the **Day** field to the day of the week that the gateway should reboot. If using a **Monthly** frequency, set the **Date** field to the date in the month that the gateway should reboot.
- 4 Set the **Time** of the day that the gateway should reboot.
- 5 Select the **Apply / Save** button. The gateway will reboot on the selected day and time.

Update Firmware

The Update Software page is used to manually update your Gateway's firmware.



Important –

Some ISPs may have their own custom firmware for the Gateway and manage this for you remotely. In this situation, manually updating the firmware yourself could cause issues with your router, so we recommend that you consult with your ISP before installing any software updates manually.

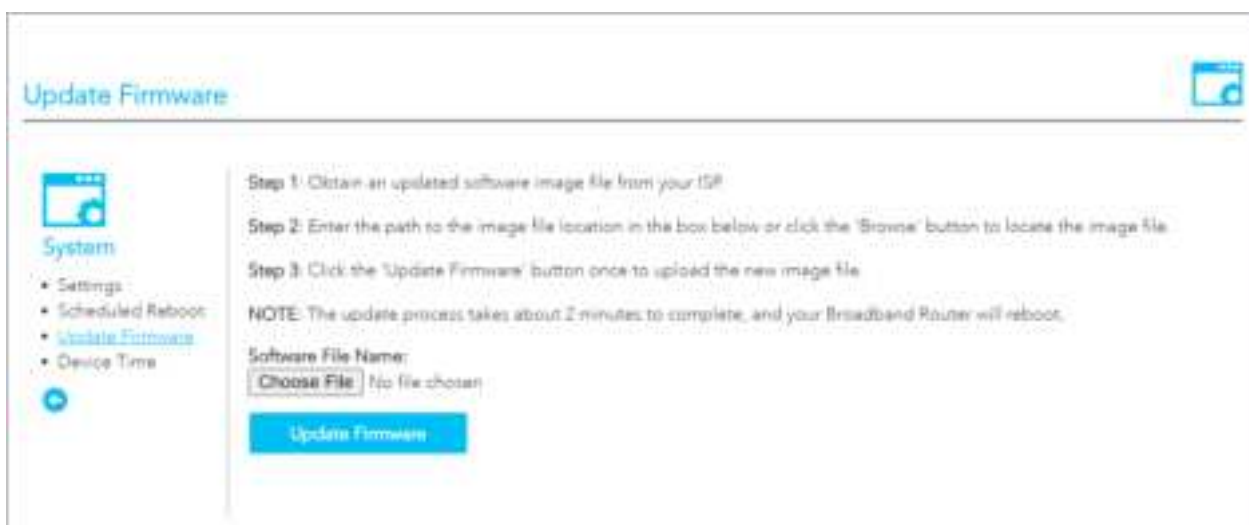


Figure 80 – System – Update Firmware

To perform a firmware upgrade:

- 1 Check for a firmware upgrade file from the NetComm Support Page for the NF20MESH - <https://support.netcommwireless.com/products/NF20MESH>. If a file is available, download it to your computer.
- 2 Select the **Choose File** button and locate the file on your computer.
- 3 Select the **Update Firmware** button to perform the firmware upgrade. The Gateway reboots on completion.



Figure 81 – System – Firmware Upgrade - Reboot

- 4 Log in to the gateway and ensure the **Firmware Version** in the **Gateway Information** section matches the firmware file which was installed.



Figure 82 – System – Firmware Upgrade – Confirm installation

Device Time

The **Device Time** page configures the gateway to use the Network Time Protocol (NTP) to synchronise time, set local time zones, etc. for the modem.





Figure 83 – System – Device Time

The following settings can be configured on this page:

Item	Description
Current Router Time	The current router time as per the settings in this page.
Automatically Synchronize	The router will periodically poll the designated NTP servers and confirm the correct time.
First, Second, Third, Fourth, Fifth NTP Server	Enter the address of the NTP servers to be used, in order of preference from 1 – 5.

Time Zone Offset	Select the preferred time zone. Normally this will be the location of the device.
Enable Daylight Savings Time	Coordinated Universal Time or Universal Time Coordinated (UTC) is not adjusted for daylight saving time. To display the Current Router Time in the actual local time where Daylight Savings Time is in effect, select <input checked="" type="checkbox"/> Enable Daylight Savings Time .

The QoS table displays the following information:

Item	Description
Name	The name applied to the queue. Custom queues will have this set in the Add Queue section (below).
Interface	Select an interface for the queue. Options include: LAN1~4 or eth4(wan)
Qid	Indicates the priority of the queue for the selected interface.
Prec/Alg/Wght	Indicates the Precedence, Algorithm and Weight used for calculating the priority of the queue.
DSL Latency	Path0 (fast) or Path1 (interleaved). This is selected while creating Interface. The default is: Path0
PTM Priority	Defines how PTM traffic packets should be handled. During congestion High priority traffic gets priority over Low.
Shaping Rate (bps)	The speed you would limit the queue to in bps (bits per second) after the burst size. Set the initial max speed traffic size before shaping the speed. This will allow packets such as Web Pages to load without being shaped, but allowing shaping to larger packets such as files transfer
Burst Size (bytes)	Set a maximum size for traffic to be sent in.
Enable button	Unselect  Enable to disable the application of a queue rule without deleting it from the list. You can then later  Enable to the queue rule without needing to redefine it.
Delete Button	To permanently remove a queue rule, select the Delete button.

Add queue

To define a new queue, select the **Add** button. The **Add Queue** page is displayed. Each of the settings correspond to the table in the previous section. Select the **Apply / Save** button to add the queue.

Add Queue

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.

Name:

Enable:

Interface:

Queue Precedence:

- The precedence list shows the scheduler algorithm configured at each precedence level.
- Note that precedence level with SP scheduler may have only one queue.
- precedence level with WRR/WFQ scheduler may have multiple queues.

Scheduler Algorithm: ☒ Weighted Round Robin ☐ Weighted Fair Queuing

Queue Weight: (1-50)

Minimum Rate: (1-965 Kbps) (-1 indicates no shaping)

Shaping Rate: (1-965 Kbps) (-1 indicates no shaping)

Shape Burst Size: (bytes) (shall be >= 1500)

PTM Priority:

DSL Latency:

Figure 86 – QoS – Add Queue

View WLAN Queue Setup

To view the WLAN Queue in order of priority, select the **View Wlan Queue Setup** button on the **QoS Queue Setup** page.

QoS WLAN Queue Setup					
Note: IF WMM function is disabled in Wireless Page, queues related to wireless will not take effects.					
Name	SSKey	Interface	Qid	Prec/Alg/Wght	Enable
WMM Voice Priority	1	wl0	8	1/5P/0	Enabled
WMM Voice Priority	2	wl0	7	2/5P/0	Enabled
WMM Video Priority	3	wl0	6	3/5P/0	Enabled
WMM Video Priority	4	wl0	5	4/5P/0	Enabled
WMM Best Effort	5	wl0	4	5/5P/0	Enabled
WMM Background	6	wl0	3	6/5P/0	Enabled
WMM Background	7	wl0	2	7/5P/0	Enabled
WMM Best Effort	8	wl0	1	8/5P/0	Enabled
WMM Voice Priority	9	wl0.1	8	1/5P/0	Enabled
WMM Voice Priority	10	wl0.1	7	2/5P/0	Enabled
WMM Video Priority	11	wl0.1	6	3/5P/0	Enabled
WMM Video Priority	12	wl0.1	5	4/5P/0	Enabled
WMM Best Effort	13	wl0.1	4	5/5P/0	Enabled
WMM Background	14	wl0.1	3	6/5P/0	Enabled
WMM Background	15	wl0.1	2	7/5P/0	Enabled

Close

Figure 87 – QoS – View WLAN Queue

Classification

The **Classification** page allows you to create traffic class rules to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS (type of service) byte.

A traffic class rule consists of a class name and at least one condition. All of the specified conditions in a classification rule must be satisfied for the rule to take effect.



Figure 88 – QoS - Classification

Traffic classification rule list

The list is displayed in a table displaying the user defined **Class Name**, whether or not it is enabled, its **Interface** and a system-defined **Order** number.

To edit a QoS Classification rule, select the Class Name. Enter your changes and select the **Apply/Save** button.

To permanently remove a rule, select the **Delete** button.

To create a new rule, click the **Add** button and define the rule in the **Add Network Traffic Class Rule** page, see next section.

Add Network Traffic Class Rule

Use the Add Network Traffic Class Rule window to add a new rule for QoS.

Add Network Traffic Class Rule

This screen creates a traffic class rule to classify the ingress traffic into a priority queue and optionally mark the DSCP or Ethernet priority of the packet.

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.

Ingress Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Source IP Address/Mask:

Destination IP Address/Mask:

Differentiated Service Code Point (DSCP) Check:

Protocol:

Specify Classification Results. (A blank value indicates no operation.)

Specify Egress Interface Required?:

Specify Egress Queue Required?:

- Packets classified into a queue that isn't through an interface for which the queue is not specified in next, will instead ingress to the default queue on the interface.

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

- Class non-qlan packets ingress to a non-qlan interface will be tagged with VID 0 and the class rule p-bits.
- Class qlan packets ingress to a non-qlan interface will have the packet p-bits re-tagged by the class rule p-bits. No additional qlan tag is added.
- Class non-qlan packets ingress to a qlan interface will be tagged with the interface VID and the class rule p-bits.
- Class qlan packets ingress to a qlan interface will be additionally tagged with the packet VID, and the class rule p-bits.

Set Rate Limit(kbps): (Kb/sec)

Figure 89 – QoS – Add Traffic Class

The following details are required to configure a rule:

Item	Description
Traffic Class Name	Enter a name (max 15 characters) reflecting the priority of the defined rule, for example: PC1HighPriority
Rule Order.	Leave as Last .
Rule Status	Set to Enable .
Ingress Interface	Set the Class Interface according to how the device connects to the router. Options are: LAN, Wireless, Local and USB
Ether Type	Set the Ether Type to IP(0x800) . Other options include ARP(0x8086) , Ipv6(0x86DD) , PPPoE_DISC(0x8863) , 8865(0x8865) , 8866(0x8866) , 8021Q(0x8100) .
Source MAC Address	Enter the Source MAC Address of the device, the unique 12-character signature with every 2 characters separated by a colon (:), that you previously entered to reserve the device's IP address.
Source MAC Mask	Enter the source MAC mask.
Destination MAC Address	Enter a Destination MAC Address if the connection is to a single device. This is useful for VPN connections. If you wish the destination MAC address to be any address leave the field blank.
Destination MAC Mask	Enter the destination MAC mask.
Source IP Address	Enter the Source IP Address of the device that you previously entered into the Static IP Lease List, in the range of 192.168.1.x
Destination IP Address	Enter a Destination IP Address if the connection is to a single device. This is useful for VPN connections. If you wish the destination IP address to be any address leave the field blank.
Differentiated Service Code Point (DSCP)	Set the Differentiated Service Code Point (DSCP) Check to EF(101110) .
Protocol	Set the Protocol to TCP . Other options include UDP, ICMP or IGMP .
Specify Egress Interface	Select the Interface that the queue should apply to.
Specify Egress Queue	Set Priority 1 for the highest priority with priority 3 being the lowest. Priority 2 is in between
Mark Differentiated Service Code Point (DSCP)	Set Mark Differentiated Service Code Point (DSCP) as AF11(001010)
Mark 802.1p Priority	The scale 0~7 , with 6 and 7 are reserved for networking performance. Set 5 as the highest priority, set 0 for lowest priority.
Set Rate Limit(kbps)	Set the rate of the queue in kbps.
Apply/Save button	Select to save the new Network Class Traffic Rule .

Port Shaping

The QoS port shaping page allows you to set shaping rates to specific interfaces. QoS port shaping supports traffic shaping of Ethernet interface, limiting continuous network speed without affecting burst traffic.

QoS port shaping supports traffic shaping of Ethernet interface.

If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.

Interface	Type	Shaping Rate (Kbps)	Burst Size (bytes)
eth4	WAN	-1	0
LAN1	LAN	-1	0
LAN2	LAN	-1	0
LAN3	LAN	-1	0
LAN4	LAN	-1	0

Apply/Save

Figure 90 – QoS – Port Shaping

The following information is set in the port shaping table:

Item	Description
Interface	Identifies the interface type.
Type	Identifies the connection type.
Shaping Rate (Kbps)	The speed you would limit the port to in Kbps (Kilobits per second) after the burst size.
Burst Size (bytes)	Burst size should be more than 10x MTU (≥ 15000 bytes).

Port Shaping Example

An example of port shaping is when your browser loads a web page, this is a type burst traffic as the browser aims to fetch small amounts of data quickly and then leaves the connection idle. Limiting port speed alone will affect the speed at which web pages are loaded, causing users to feel that their overall internet connection speed is slow.

By configuring QoS Port Shaping with a Burst size, web pages are allowed to load using the burst speed, while continuous traffic such as file downloads will be shaped at a lower rate.

Calculation of shaping rate and burst size

To identify the best way to configure shaping rate and burst size, consider the equation below:

Time window = Burst size / rate

For example, if a 200 Mbps bandwidth limit is configured with a 5 ms burst window, the calculation becomes $200 \text{ Mbps} \times 5 \text{ ms} = 125 \text{ Kbytes}$, which is approximately eighty-three (83) 1500-byte packets.

If the 200 Mbps bandwidth limit is configured on a Gigabit Ethernet interface, the burst duration is $125000 \text{ bytes} / 1 \text{ Gbps} = 1 \text{ ms}$ at the Gigabit Ethernet line rate.

Result

After 1ms of burst data at full gigabit speed, the speed is shaped to 200Mbps.

Security

Firewall

The **Firewall** page allows you to configure the firewall on the Gateway, including creating custom rules to allow specific traffic to transverse the Gateway. Select the **Enabled** checkbox to enable the Firewall. Set the **Default Policy** to accept or drop.

Firewall Setup

This function only processes forwarded packets, and does not process packets sent to the device itself.

Firewall: ☒ Enable

Default policy: ☒ Accept ☐ Drop

Choose Add or Delete to configure IP filtering rules.

IP Version	Source IP/ Prefix Length	Destination IP/ Prefix Length	Protocol	Source Port	Destination Port	Source Interfaces	Dest Interfaces	Action	Delete
IPv4	10.100.12.12/32	192.168.20.10/32	TCP/UDP	3000	3000	-	-	Drop	

Add **Apply/Save**

Figure 91 – Security - Firewall

Add firewall rule

Select the **Add** button to add a firewall rule.

Add Rule

IP Version:

Source IP address/prefix length:

Destination IP address/prefix length:

Protocol:

Source Port (port or start/end):

Destination Port (port or start/end):

Source Interfaces:

Destination Interfaces:

Action:

Done **Close**

Figure 92 – Security – Add Rule

The following settings are required to add a firewall rule:

Item	Description
IP Version	The IP version for the firewall. Either IPv4 or IPv6 .
Source IP address [prefix length]	The source IP address that initiates the request.
Destination IP address [prefix length]	The destination IP.
Protocol	The protocol that should be used for the rule.
Source Port	The source port that the connection is initiated over.
Destination Port	The destination port that is being connected to.
Source Interfaces	The source interfaces that the rule should apply to.
Destination Interfaces	The destination interface that the rule should apply to.
Action	The action the gateway should take when the traffic matches the defined rule.

MAC Filtering

The **MAC Filtering** page allows you to configure MAC address filtering. You can elect to block or allow connections based on MAC Address criteria. The default policy is to allow all connections.

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

Figure 93 – Security – MAC Filter


The following information is required to create a MAC filter:


Item	Description
Protocol Type	Select the protocol type to which the filter should apply: PPPoE (Point-to-Point Protocol over Ethernet) IPv4 IPv6 Apple Talk IPXNetBEUI (NetBIOS Extended User Interface) IGMP (Internet Group Message Protocol)
Destination MAC Address	Enter the MAC address of the device that the NF18MESH will be blocked from accessing.
Source MAC Address	Enter the MAC address of the device that the NF18MESH will block from external communication.
Frame Direction	Select the direction of communication that will be blocked. Options are: LAN<=>WAN WAN=>LAN LAN=>WAN
WAN Interface	This is configured in Bridge mode only.

Access Control

The Access Control pages are used to restrict access to your network.

Services access control list (SCL)

The Service Control List (SCL) allows you to enable or disable services running on the NF20MESH. Select  **Enable** on the service that should be enabled. Select the **Apply / Save** button to apply the changes.

 **Important** – Enabling services on the WAN side may allow access to your local network from the internet, which may allow unauthorised users on to the network. It is recommended that you do not enable any services on the WAN side.

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

Services	LAN	LAN Port	WAN	WAN Port
HTTP	<input checked="" type="checkbox"/> Enable	80	<input type="checkbox"/> Enable	80
HTTPS	<input checked="" type="checkbox"/> Enable	443	<input type="checkbox"/> Enable	443
TELNET	<input type="checkbox"/> Enable	23	<input type="checkbox"/> Enable	23
SSH	<input type="checkbox"/> Enable	22	<input type="checkbox"/> Enable	22
FTP	<input type="checkbox"/> Enable	21	<input type="checkbox"/> Enable	21
TFTP	<input type="checkbox"/> Enable	69	<input type="checkbox"/> Enable	69
ICMP	<input checked="" type="checkbox"/> Enable	0	<input type="checkbox"/> Enable	0
SNMP	<input type="checkbox"/> Enable	161	<input type="checkbox"/> Enable	161
SAMBA	<input checked="" type="checkbox"/> Enable	445	<input type="checkbox"/> Enable	445

Apply/Save

Figure 94 – Security – Access Control

Access List

The **Access List** is used to restrict management access to the specified IP addresses.

Access List

The IP Address Access Control mode, if enabled, permits access to remote management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

Access Control Mode: ☒ Enable ☐ Disable

IP Address	Subnet Mask	Delete
192.168.20.2	255.255.255.0	Delete

Add

Figure 95 – Security – Access List

- 1 Select **Enable** to activate the Access List.
- 2 Select the **Add** button to add a specific address to the restricted list.
- 3 Enter the IP Address which should be able to access the device.
- 4 Include the Subnet Mask of the address.
- 5 Select **Apply/Save** to apply the access list.