

Port Forwarding Setup Guide

NF18MESH



Doc No. FA01253

Copyright

Copyright© 2020 Casa Systems, Inc. All rights reserved.

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

Trademarks and registered trademarks are the property of Casa Systems, Inc or their respective subsidiaries. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

Previous versions of this document may have been issued by NetComm Wireless Limited. NetComm Wireless Limited was acquired by Casa Systems Inc on 1 July 2019.

 **Note** – This document is subject to change without notice.

Document history

This document relates to the following product:

Casa Systems NF18MESH

Ver.	Document description	Date
v1.0	First document release	23 June 2020

Table i. – Document revision history

Port Forwarding Overview

Port forwarding enables programs or devices running on your LAN to communicate with the internet as if they were directly connected. This is most commonly used for remotely accessing DVR/NVR Controller, IP Cameras, Web Server or online gaming (via game console or computer).

Port forwarding works by “forwarding” a specific TCP or UDP port from the NF18MESH to the computer or device you are using.

Prerequisite

Prior to setting the port forwarding function you must know which ports need to be opened. If you are not sure, contact the application vendor or developer.

Add a Port Forwarding Rule

Open web interface

- 1 Open a web browser (such as Internet Explorer, Google Chrome or Firefox), type following address into the address bar and press enter.

<http://cloudmesh.net> or <http://192.168.20.1>

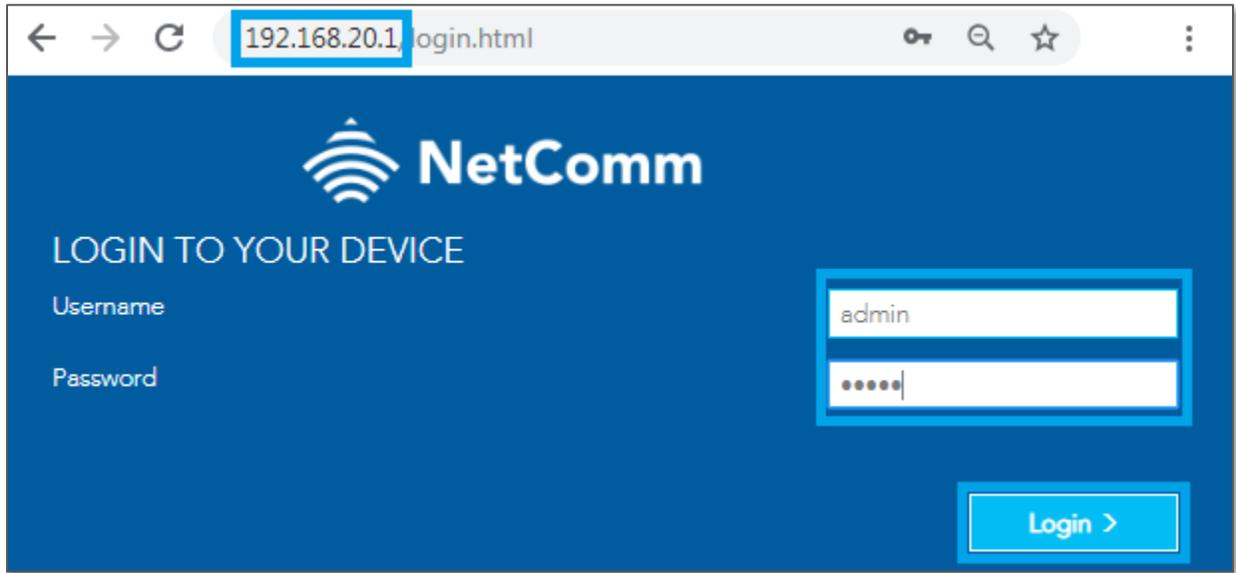
Enter the following credentials:

Username: admin

Password: <The password printed on the back of the modem>

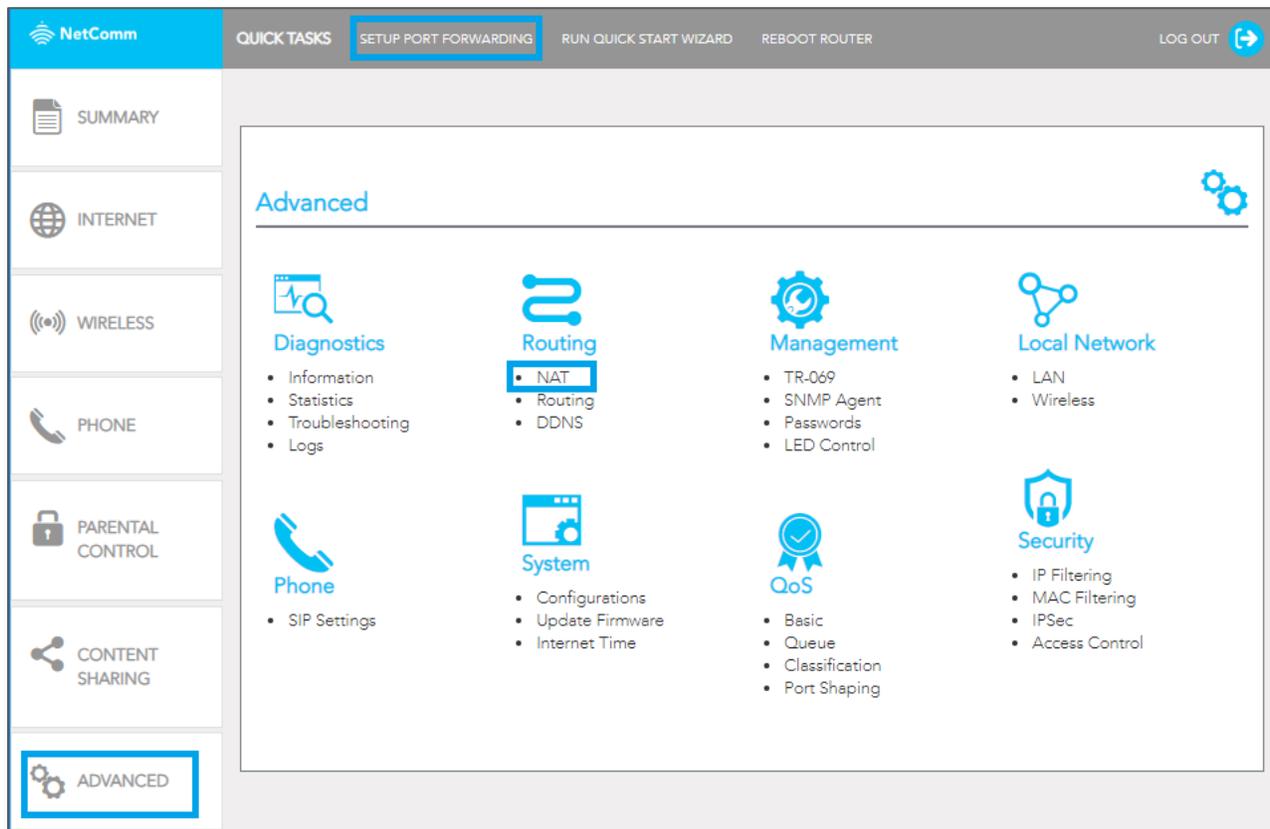
then click the **Login** button.

NOTE – Some Internet Service Providers use custom password. If login fails, contact your Internet Service Provider. Use your own password if it is changed.



Set up Port forwarding (Virtual Server)

- 2 SETUP PORT FORWARDING option is available on the QUICK TASK bar. Alternatively, available in the **Advanced** menu, under **Routing** click on the option **NAT**.



3 Then under the **Port forwarding** section, click the **Add** button to add a new port forwarding rule.

Port Forwarding

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Action	Delete
<input type="button" value="Add"/>										

4 The **Add Port Forwarding Rule** pop up window will appear.

A sample configuration for allowing Remote desktop toward a LAN side device is provided below.

Add Port Forwarding Rule

Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server.

NOTE: The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port Start".

Remaining number of entries that can be configured: 32

Use Interface: **4**

Service Name: **5**

LAN Loopback: **6**

Server IP address: **7**

Status: **8**

External Port Start: **9**

External Port End:

Protocol: **10**

Internal Port Start:

Internal Port End:

- 5 Select the correct Interface in the **Use Interface** field as a misconfiguration will end up failing to forward anything.
- 6 The correct interface can be checked from the **Internet** page.
- 7 The **Service Name** needs to be unique, so provide something meaningful for future references.
- 8 **LAN Loopback** needs to be enabled. This is important if you want to access resources using public IP address even when you are connected to the same network. A good example can be DVR security systems. You may watch your camera feed from anywhere in the world using the public IP address. Now if you are in the local network, with this option enabled, you do not need to change DVR IP address.
- 9 Configure the Private IP address of the device (e.g. Computer, DVR, Gaming Console) you wish to port forward to in the **Server IP Address** field.
- 10 This will be a local IP address in the subnet 192.168.20.xx (by default); where xx can be equal to 2 to 254.
- 11 Open the **Status** drop down list and select **Enable**.
- 12 Enter the port number or port range into the **External Port Start** and **External Port End** fields.
- 13 If you only want to open one port, then enter the same number in **Start** and **End** port fields, but if you want to open range of ports, then enter the start number in **Port Start** field and end number in **Port End** field.
- 14 *Note that the **Internal Port Start** and **Internal Port End** fields will automatically populate with the same port numbers.*
- 15 Select the **Protocol** to be used for the port forwarding rule: **TCP**, **UDP** or **TCP/UDP both**.
- 16 Click the **Apply/Save** button.
- 17 The port forwarding rule will now be added to the list.
- 18 This example created in this user document is displayed below.

Port Forwarding

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

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	LAN Loopback	Action	Delete
Remote Desktop	3389	3389	TCP	3389	3389	192.168.123.5	undefined	Enabled	Disable	Delete

Add

Port forwarding is now configured.

You may also **Enable/Disable, Delete** any rule existing rule from this window.

Please note

- ▲ We recommend that you **set a Static IP address** on the end device, **instead of obtaining one automatically**, to make sure that the request is forwarded to the appropriate machine every individual time.
- ▲ You **can only forward a port to one location** (IP address). In some cases, this may cause issues when multiple LAN devices (computers, game consoles, or VOIP ATAs) attempt to use online gaming at the same time or make multiple VOIP service connections. In these cases, you will need to use an alternate port for any subsequent connections after the first device. Please consult your VOIP provider or game manufacturer for assistance with this.
- ▲ Similarly, **remote access and the webserver must have unique port numbers.**
- ▲ For example, you cannot host a web server accessible through port 80 of your public IP and enable remote http administration of the NF18MESH through port 80, you must provide both with unique port numbers.
- ▲ Note also that **ports 22456 to 32456 are reserved for RTP protocol in VOIP services.**
- ▲ Do not use any of these ports for any other service.