

Port Forwarding / DMZ Setup

Introduction

Port forwarding enables programs or devices running on your LAN to communicate with the internet as if they were directly connected. Many internet services and applications use designated ports and when packets arrive at the router, they will be lost unless they are directed to the appropriate destination. Port forwarding works by forwarding a specific TCP or UDP port or range of ports from the modem/router to the computer or device you are using.

There might also be times when you wish to place a device connected to your router in the “demilitarized zone” or “DMZ”. A device placed in the DMZ will have all port numbers forwarded to it, giving it unrestricted access to the internet.



Each service or application generally uses different TCP or UDP ports. Refer to the documentation for the service or application to find out which ports need to be forwarded.



You can only forward a port or range of ports to a single destination (IP address). In some cases, this may cause issues where multiple LAN devices attempt to use a service simultaneously. Where possible, use an alternate port for any subsequent connections after the first device. Please consult your service provider or application developer for assistance with this.



Note: Before performing the instructions in this guide, please ensure that you have the latest firmware version on your router. Visit <http://www.netcommwireless.com/products/m2m-wireless> to find your device and download the latest firmware.

Adding a Port Forwarding Rule

This guide will take you through the steps required to add a port forwarding rule to your router.

1. Open a web browser and navigate to the LAN IP address of your router. For the NTC-6000 Series, the default is <http://192.168.20.1>. For NTC-30 and NTC-40 Series, the default is <http://192.168.1.1>.

Login to the router with the following credentials:

Username: **root**
Password: **admin**

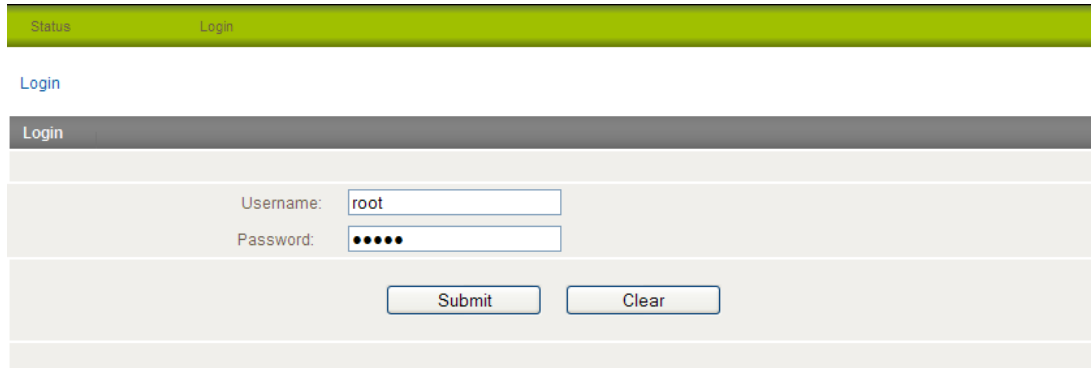


Figure 1: Login page

2. From the menu bar along the top of the screen, navigate to **Internet Settings > Routing > NAT**.

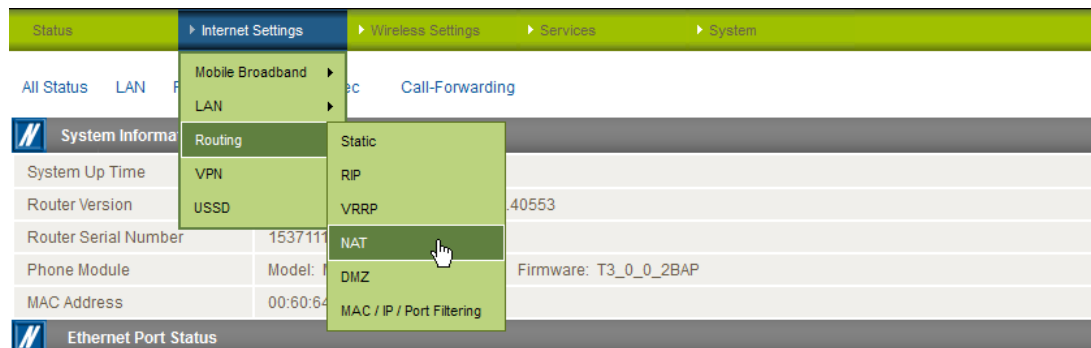


Figure 2: Internet Settings - Routing - NAT

3. Using the Protocol drop down list, select the protocol type to use for the rule. You can select **TCP**, **UDP** or **Both**.

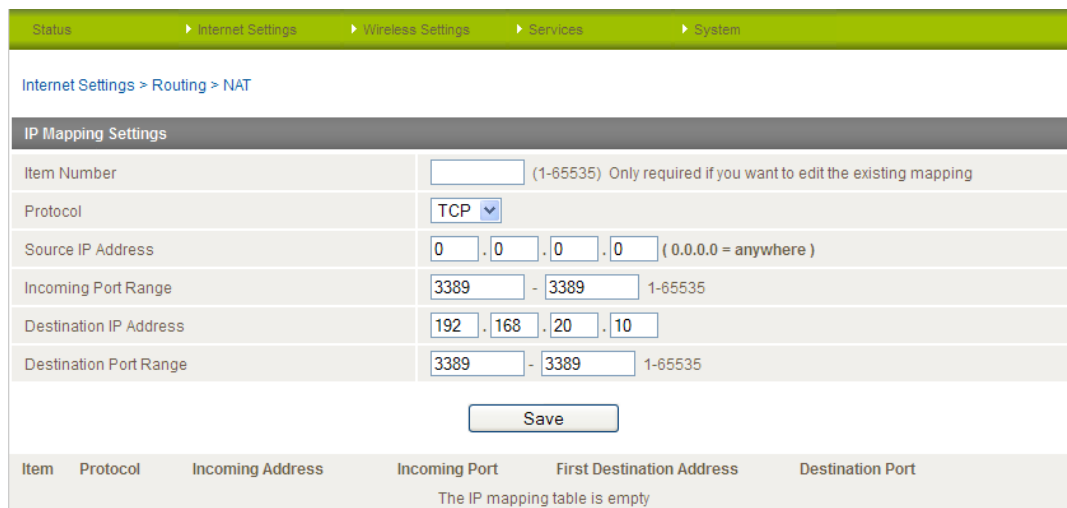


Figure 3: Entering the port forwarding rule details

4. In the Source IP Address field, enter the address from which the traffic will originate. This is usually a WAN IP address originating from the internet. In this example, we are setting the Source IP Address to 0.0.0.0 which allows connections from anywhere.
5. In the Incoming Port Range fields, enter the range of ports to forward. For example, entering 6881 in the first field and 6999 in the second field will forward the 19 ports between and including 6881 and 6999. If you wish to forward a single port, enter the same port number in both the first and the second fields.
6. In the Destination IP Address field, enter the local IP address of the LAN client to which port traffic will be forwarded.
7. In the Destination Port Range fields, enter the port range for the destination. In many cases these ports will be the same as the Incoming Port Range. If you wish to specify a single port, enter the same port number in both the first and the second fields.
8. Click the **Save** button. The port forwarding rule is displayed at the bottom of the screen as highlighted in Figure 4 below.

▶ Status
▶ Internet Settings
▶ Wireless Settings
▶ Services
▶ System

Internet Settings > Routing > NAT

IP Mapping Settings

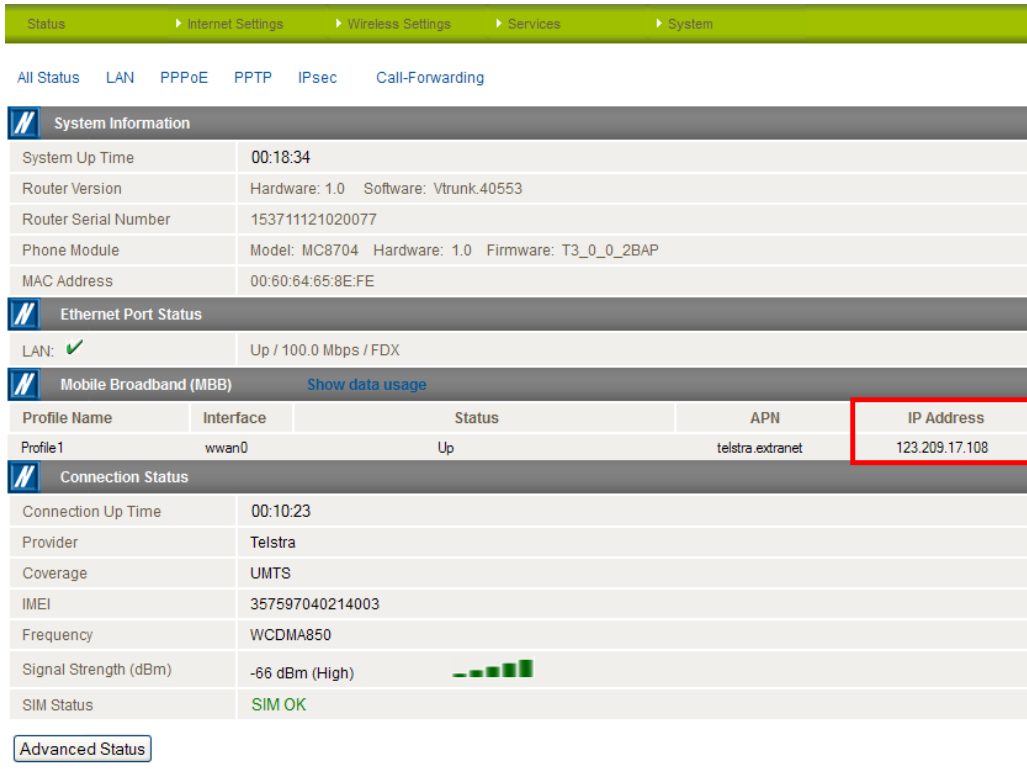
Item Number	<input type="text"/> (1-65535) Only required if you want to edit the existing mapping
Protocol	TCP ▼
Source IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> (0.0.0.0 = anywhere)
Incoming Port Range	<input type="text"/> - <input type="text"/> 1-65535
Destination IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Destination Port Range	<input type="text"/> - <input type="text"/> 1-65535

Item	Protocol	Incoming Address	Incoming Port	First Destination Address	Destination Port	
1	TCP	0.0.0.0	3389 - 3389	192.168.20.10	3389 - 3389	Delete entry

Figure 4: A completed port forwarding rule

Verifying the Port Forwarding rule

In the example above, we forwarded port 3389 which is the default port for Microsoft's Remote Desktop Protocol (RDP). The client machine (192.168.20.10) is accepting Remote Desktop connections on port 3389 so we can verify the connection by connecting to the client using RDP. We need to connect to the WAN IP address of the router and our request is forwarded on to the client (192.168.20.10). The WAN IP Address can be found by viewing the Status page of the NetComm Wireless M2M Series Router as shown below:



Profile Name	Interface	Status	APN	IP Address
Profile1	wwan0	Up	telstra.extranet	123.209.17.108

Figure 5: The Status page showing the WAN IP Address

1. Click **Start** then **Run** and type **mstsc** and press Enter.
2. Type the WAN IP address of the remote router and click **Connect**.

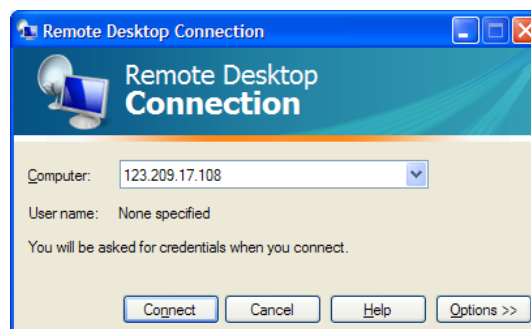


Figure 6: RDP Connection screen

3. The remote desktop opens and prompts you to login. If it does not, verify your settings and try again.

Placing a device in the Demilitarized Zone (DMZ)

A device connected to the router may be placed in the DMZ which gives it unrestricted access to the internet. All ports are forwarded to the device when it is in the DMZ. Placing a device in the DMZ can be useful for testing certain scenarios but is also risky since it puts the client device in a vulnerable position.



Note: Placing a device in the DMZ puts it in a vulnerable position and is open to potential threats from the internet. It is not recommended that you leave a device in the DMZ during normal operation.

To place a device in the DMZ:

1. Open a web browser and navigate to the LAN IP address of your router. For the NTC-6000 Series, the default is <http://192.168.20.1>. For NTC-30 and NTC-40 Series, the default is <http://192.168.1.1>.

Login to the router with the following credentials:

Username: **root**
Password: **admin**.

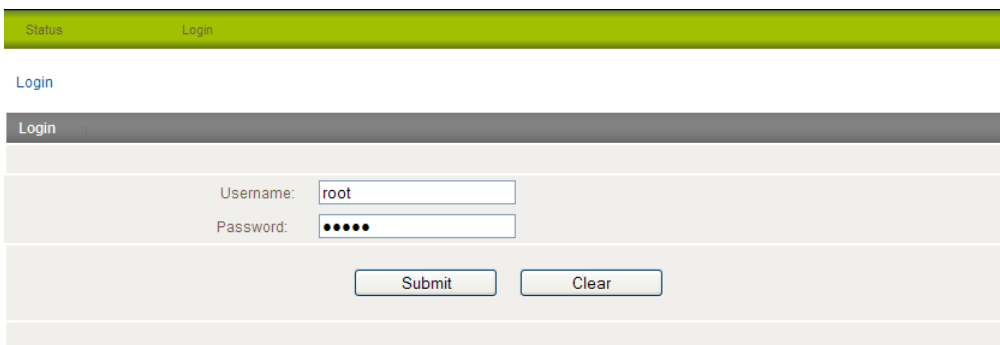


Figure 7: Login page

2. From the menu bar along the top of the screen, navigate to **Internet Settings > Routing > DMZ**.

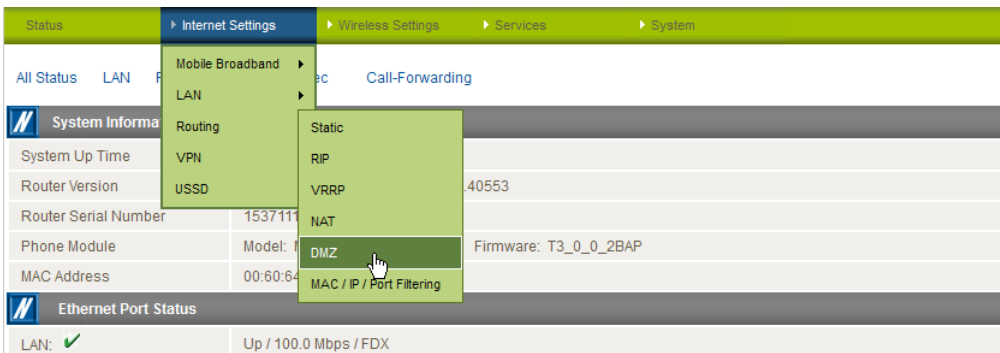


Figure 8: Internet Settings - Routing - DMZ

3. Set the **DMZ Settings** option to **Enable** and enter the IP address of the device that you want to place in the DMZ.

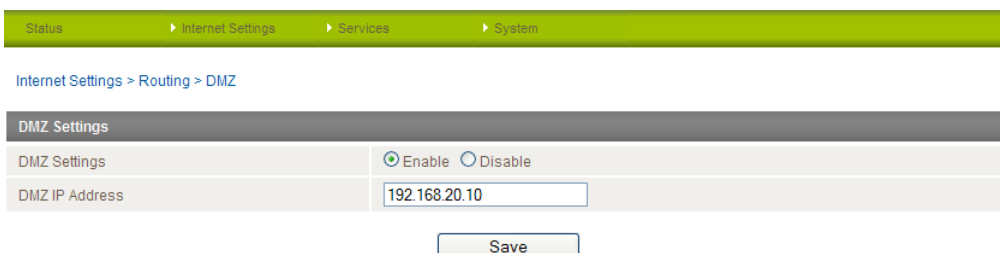
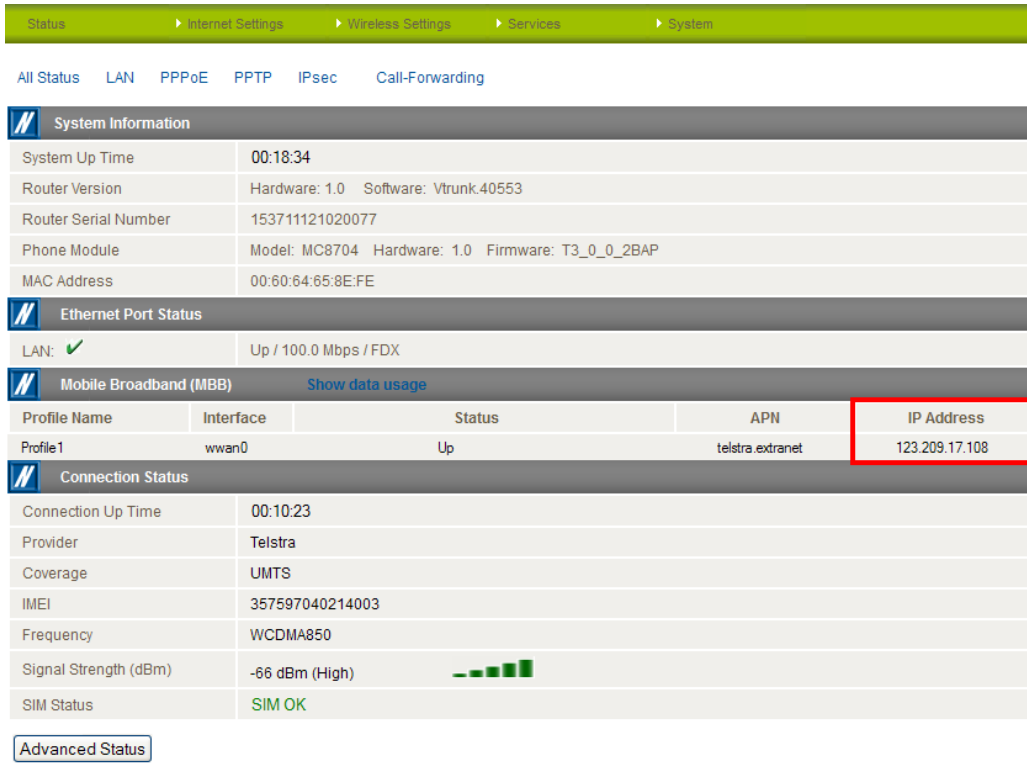


Figure 9: DMZ Settings

4. Click the **Save** button. The IP address you entered will have all ports forwarded to it.

Verifying the Port Forwarding rule

In the example above, we placed the client machine on 192.168.20.10 in the demilitarized zone. This means that all ports are forwarded directly to it. To test that it is in the DMZ, we can connect to the WAN IP Address using RDP. The WAN IP Address can be found by viewing the Status page of the NetComm Wireless M2M Series Router as shown below:



The screenshot shows the router's status page with the following sections:

- System Information:**
 - System Up Time: 00:18:34
 - Router Version: Hardware: 1.0 Software: Vtrunk.40553
 - Router Serial Number: 153711121020077
 - Phone Module: Model: MC8704 Hardware: 1.0 Firmware: T3_0_0_2BAP
 - MAC Address: 00:60:64:65:8E:FE
- Ethernet Port Status:**
 - LAN: ✓ Up / 100.0 Mbps / FDX
- Mobile Broadband (MBB):**
 - Profile Name: Profile1
 - Interface: wwan0
 - Status: Up
 - APN: telstra.extranet
 - IP Address: 123.209.17.108** (highlighted in red)
- Connection Status:**
 - Connection Up Time: 00:10:23
 - Provider: Telstra
 - Coverage: UMTS
 - IMEI: 357597040214003
 - Frequency: WCDMA850
 - Signal Strength (dBm): -66 dBm (High) ▬▬▬▬▬▬
 - SIM Status: SIM OK

Figure 10: The Status page showing the WAN IP Address

1. Click **Start** then **Run** and type **mstsc** and press Enter.
2. Type the WAN IP address of the client and click **Connect**.

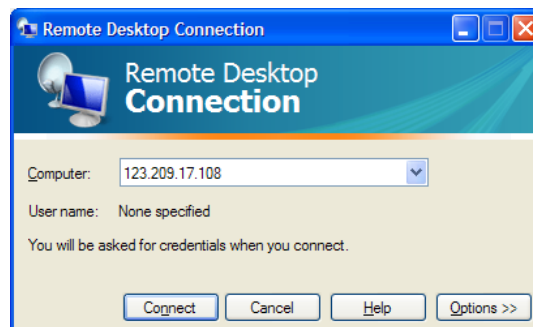


Figure 11 - RDP Connection screen

3. The remote desktop opens and prompts you to login. If it does not, verify your settings and try again.