

Vodafone MachineLink

Port Forwarding / DMZ Configuration Guide



Document history

This guide covers the following products:

- Vodafone MachineLink 3G (NWL-10)
- Vodafone MachineLink 3G Plus (NWL-12)
- Vodafone MachineLink 4G (NWL-22)

| Ver. | Document description | Date |
|--------|--|----------------|
| v. 1.0 | Initial document release. | March 2013 |
| v. 2.0 | Revised content based on current firmware. | September 2016 |

Table i - Document revision history



Note – Before performing the instructions in this guide, please ensure that you have the latest firmware version installed on your router. Visit <http://vodafone.netcommwireless.com> to download the latest firmware.



Note – The functions described in this document require that the router is assigned with a publicly routable IP address. Please ensure that your mobile carrier has provided you with a publicly routable IP address before performing the instructions in this document.

Copyright

Copyright© 2016 NetComm Wireless Limited. All rights reserved.

Copyright© 2016 Vodafone Group Plc. All rights reserved.

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

Trademarks and registered trademarks are the property of NetComm Wireless Limited or Vodafone Group 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.

Contents

| | |
|---|-----------|
| Introduction | 4 |
| Adding a Port Forwarding Rule | 5 |
| Verifying the Port Forwarding rule | 8 |
| Placing a device in the Demilitarized Zone (DMZ) | 10 |
| Verifying the DMZ | 12 |

Notation

The following symbols are used in this user guide:



The following note requires attention.



The following note provides a warning.



The following note provides useful information.

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.



Note – 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.



Note – 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.

This document explains how to configure port forwarding and DMZ on the Vodafone MachineLink router so that a computer running Microsoft Remote Desktop Server can be accessed remotely. This is one example of how port forwarding and the demilitarized zone may be used, however there are many other uses for these features. The diagram below illustrates the example scenario.



Figure 1 – Example network diagram

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 the MachineLink router. The default is <http://192.168.1.1>.

Log in to the router with the following credentials:

Username: **root**

Password: **admin**

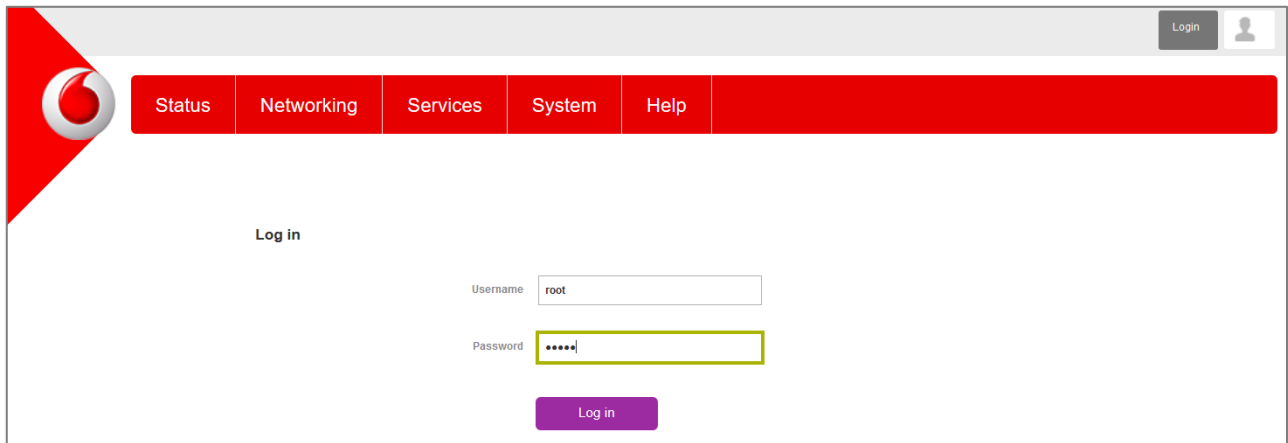


Figure 2 – Login page

- From the menu bar along the top of the screen, click on **Networking** then click the **Routing** item on the left and finally click the **Port forwarding** link.

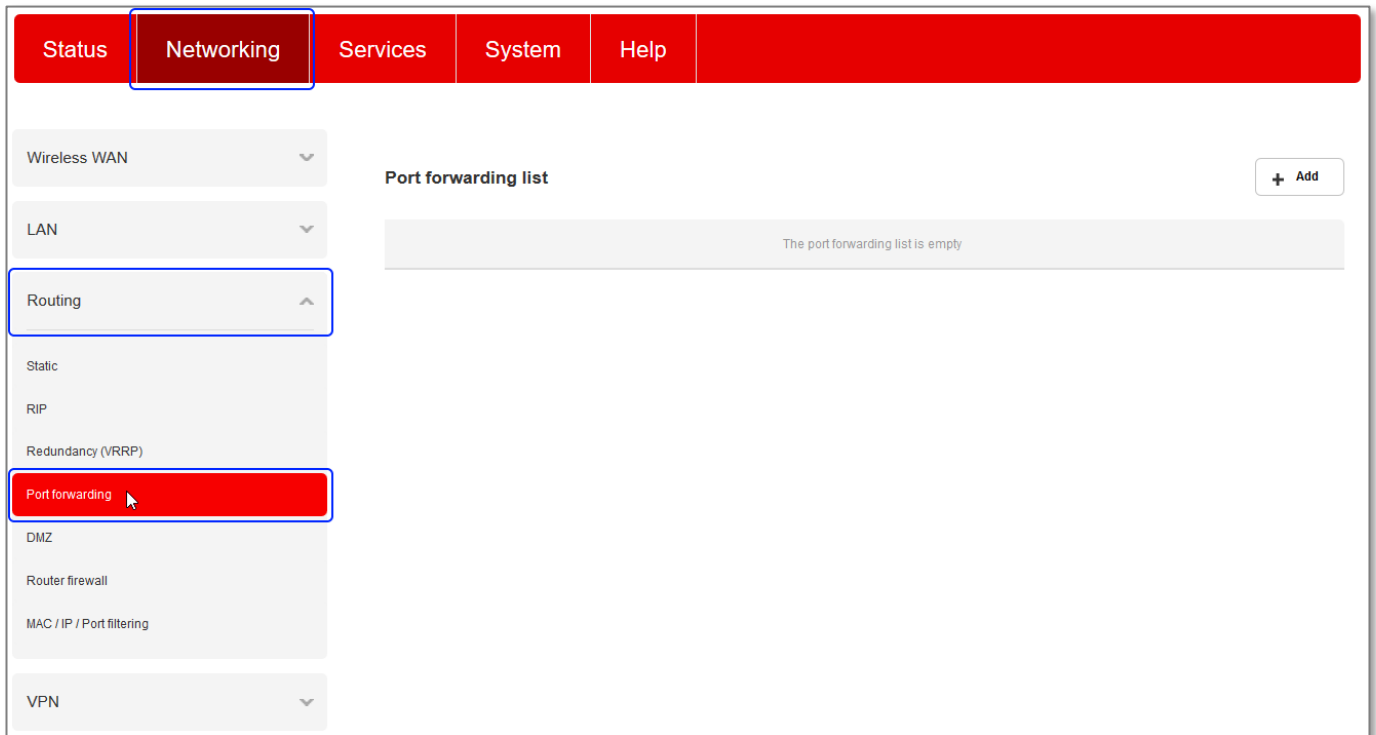


Figure 3 – Internet Settings - Routing – NAT

- Click the **+Add** button to begin configuring a new port forwarding rule.

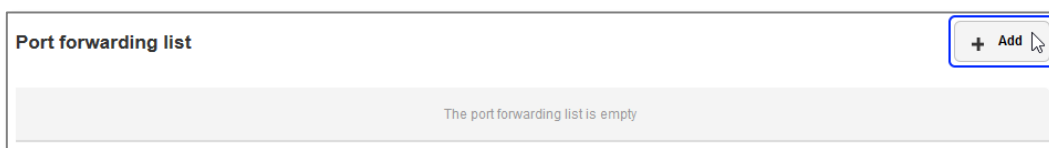
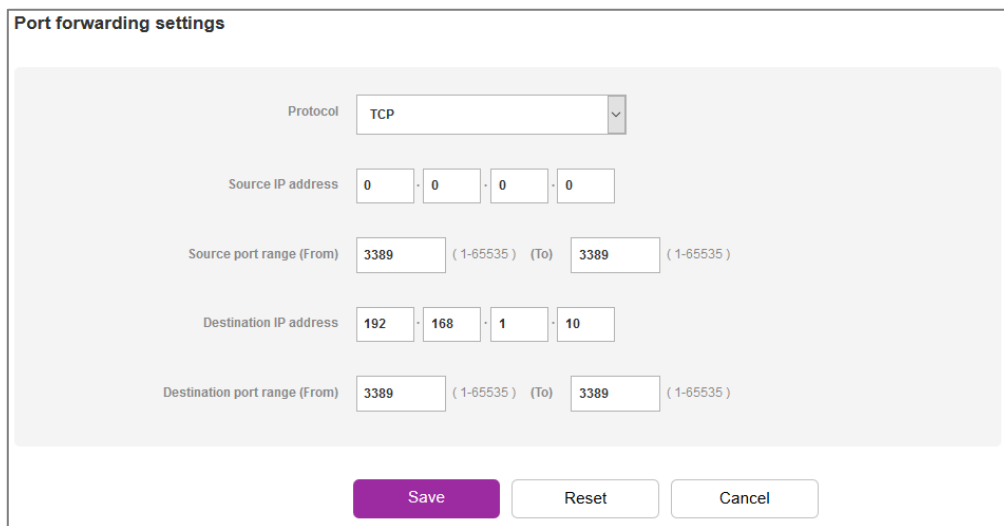


Figure 4 – Add new Port forwarding list

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



Port forwarding settings

Protocol: **TCP**

Source IP address: 0 . 0 . 0 . 0

Source port range (From): 3389 (1-65535) (To): 3389 (1-65535)

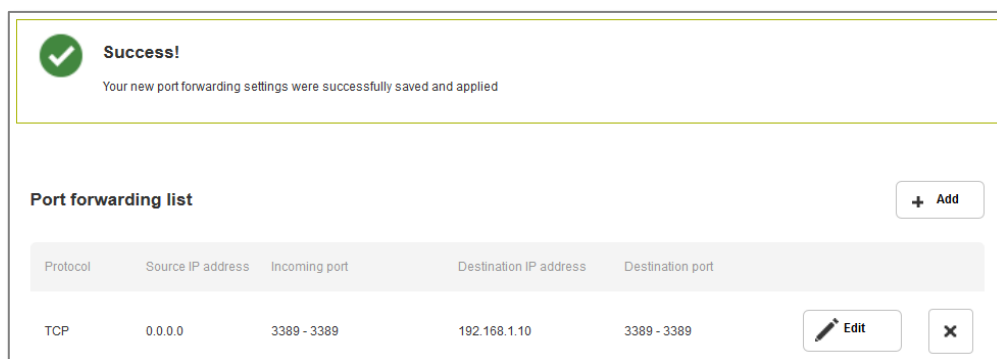
Destination IP address: 192 . 168 . 1 . 10

Destination port range (From): 3389 (1-65535) (To): 3389 (1-65535)

Buttons: Save, Reset, Cancel

Figure 5 – Port forwarding settings

- 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 have set the Source IP address to 0.0.0.0 which allows connections from anywhere.
- In the **Source port range** fields, enter the range of ports to forward from the source. 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.
- In the **Destination IP address** field, enter the local IP address of the LAN client to which port traffic will be forwarded.
- In the **Destination port range** fields, enter the port range for the destination. In many cases these ports will be the same as the Source port range. If you wish to specify a single port, enter the same port number in both the first and the second fields.
- Click the **Save** button. The port forwarding rule is displayed at the bottom of the screen as highlighted in Figure 6 below.



Success!
Your new port forwarding settings were successfully saved and applied

Port forwarding list + Add

| Protocol | Source IP address | Incoming port | Destination IP address | Destination port | |
|----------|-------------------|---------------|------------------------|------------------|----------------------------------|
| TCP | 0.0.0.0 | 3389 - 3389 | 192.168.1.10 | 3389 - 3389 | Edit × |

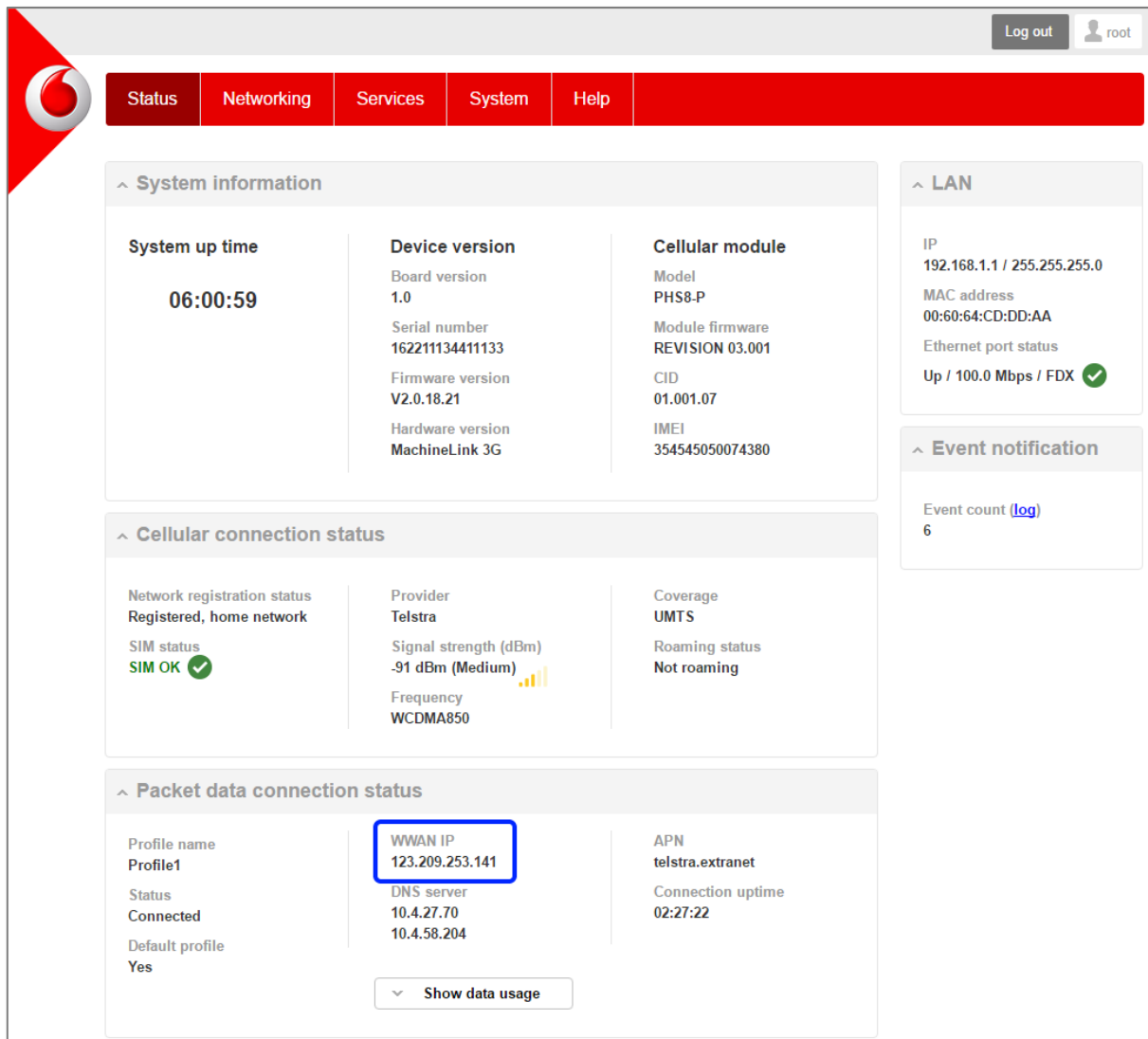
Figure 6 – Port forwarding rule added successfully.

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 (192.168.1.10) 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 (192.168.1.10).

Retrieving the WAN IP address

The WAN IP Address can be found by viewing the Status page of the Vodafone MachineLink router as shown below:



The screenshot displays the 'Status' page of a Vodafone MachineLink router. The page is organized into several sections:

- System information:**
 - System up time:** 06:00:59
 - Device version:** Board version 1.0, Serial number 162211134411133, Firmware version V2.0.18.21, Hardware version MachineLink 3G
 - Cellular module:** Model PHS8-P, Module firmware REVISION 03.001, CID 01.001.07, IMEI 354545050074380
- Cellular connection status:**
 - Network registration status:** Registered, home network
 - SIM status:** SIM OK (with green checkmark)
 - Provider:** Telstra
 - Signal strength (dBm):** -91 dBm (Medium) (with signal strength icon)
 - Frequency:** WCDMA850
 - Coverage:** UMTS
 - Roaming status:** Not roaming
- Packet data connection status:**
 - Profile name:** Profile1
 - Status:** Connected
 - Default profile:** Yes
 - WWAN IP:** 123.209.253.141 (highlighted with a blue box)
 - DNS server:** 10.4.27.70, 10.4.58.204
 - APN:** telstra.extranet
 - Connection uptime:** 02:27:22
 - Show data usage:** (button)
- LAN:**
 - IP:** 192.168.1.1 / 255.255.255.0
 - MAC address:** 00:60:64:CD:DD:AA
 - Ethernet port status:** Up / 100.0 Mbps / FDX (with green checkmark)
- Event notification:**
 - Event count:** 6 (with [log](#) link)

Figure 7 – The Status page showing the WAN IP Address

Connect to remote PC via remote desktop connection

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

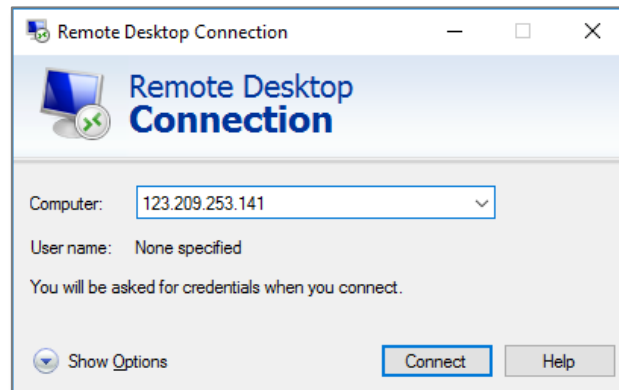


Figure 8 – RDP Connection screen

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 the MachineLink router. The default is <http://192.168.1.1>.

Log in to the router with the following credentials:

Username: **root**

Password: **admin**

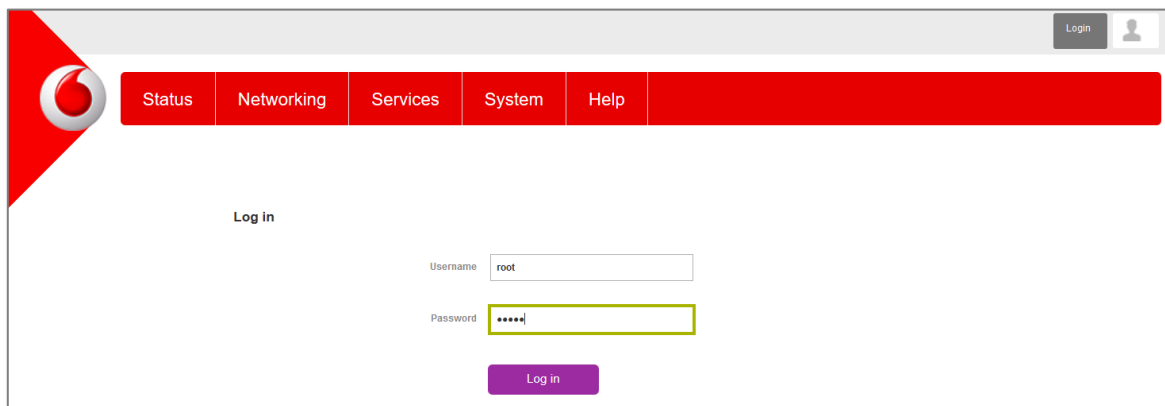


Figure 9 – Login page

- 2 From the menu bar along the top of the screen, click on **Networking** then click the **Routing** item on the left and finally click the **DMZ** link.

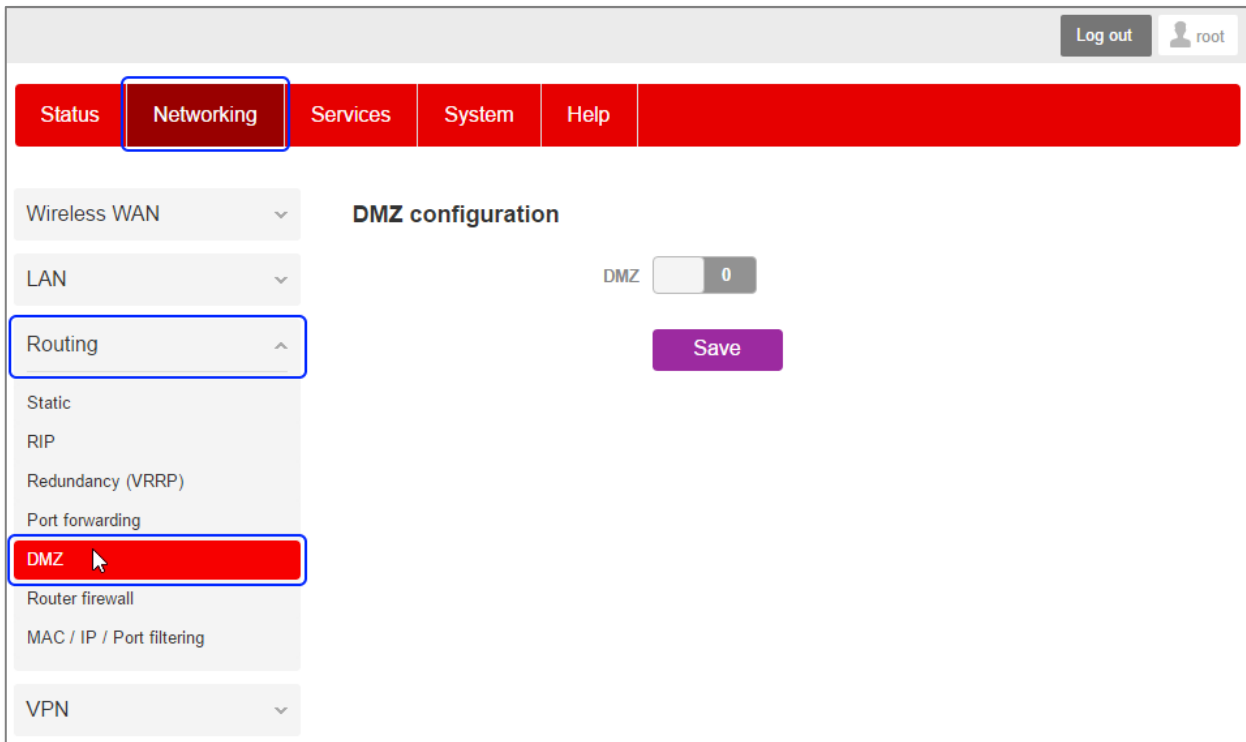


Figure 10 – Internet Settings - Routing – NAT

- 3 Click the **DMZ** toggle key to switch it to the **ON** position.

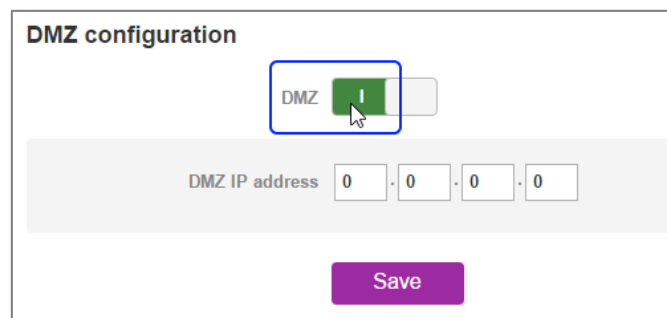


Figure 11 – Enable DMZ Settings

- 4 Enter the Local IP address of the device that you want to place in the demilitarized zone.

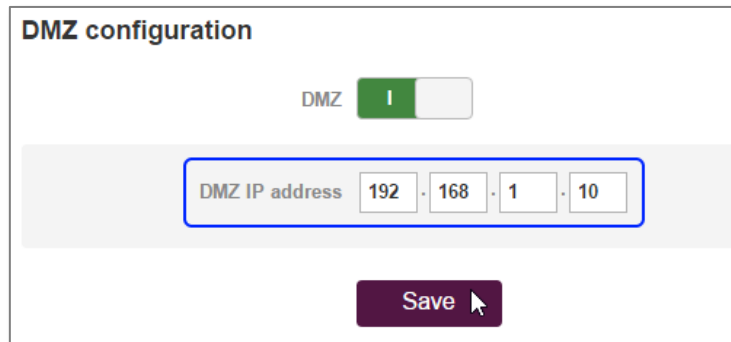
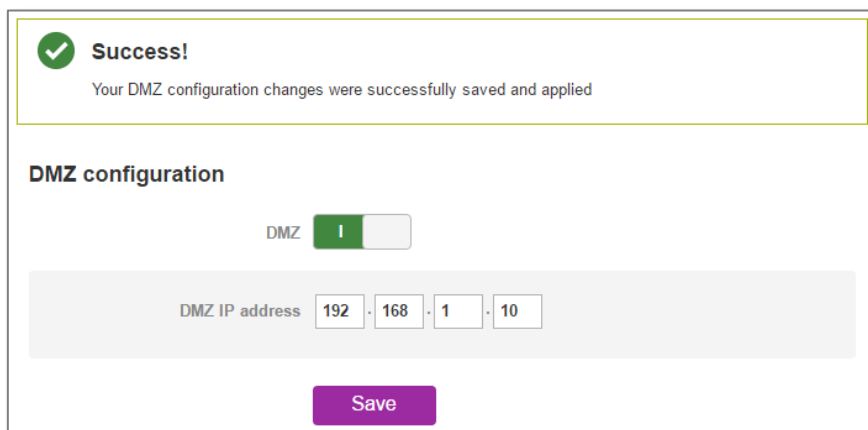


Figure 12 – Enter DMZ IP Address

- 5 Click the **Save** button.
- 6 The IP address you entered will have all ports forwarded to it:



Verifying the DMZ

In the example above, we placed the client machine on 192.168.1.10 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 Vodafone MachineLink router as shown below:

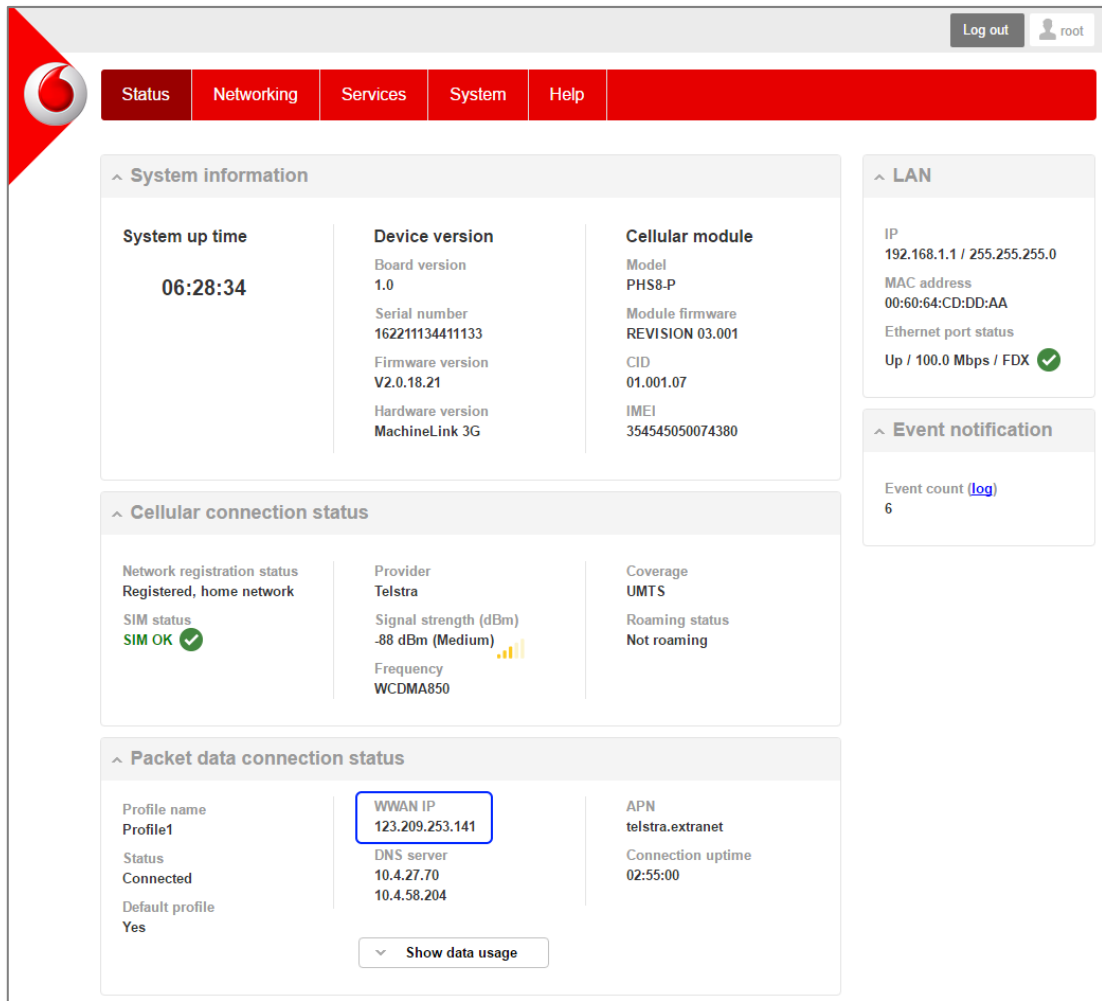


Figure 13: The Status page showing the WAN IP Address

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

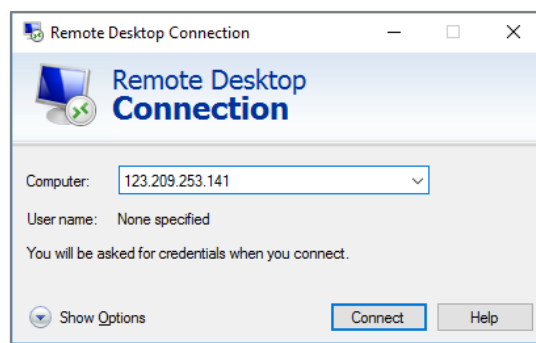


Figure 14 - RDP Connection screen

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