# OpenVPN Configuration

# Whitepaper

NetComm Wireless Limited • 18-20 Orion Road, Lane Cove NSW 2066, Sydney Australia
t +61 (2) 9424 2000 f +61 (2) 9424 2010 • www.netcommwireless.com • ACN 002 490 486

# Table of Contents

| DOCUMENT VERSION | DATE |
|---|---|
| - Initial document release | October 2012 |

*Table 1 - Document Revision History*

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.

# Introduction

A VPN (Virtual private network) is a secure connection between two or more endpoints. It can also be seen as an extension to a private network.

There are two key types of VPN scenarios:

- Site to Site VPN
- Remote Access VPN.

In a site to site VPN, data is encrypted from one VPN gateway to the other, providing a secure link between two sites over a third party insecure network like the Internet.

In a remote access VPN scenario, a secure connection would be made from an individual computer to a VPN gateway. This would enable a user to access their e-mail, files and other resources at work from wherever they may be, providing they have an Internet connection.

Many NetComm M2M Seriers routers support three types of Virtual Private Network (VPN) technologies:

- Point-to-Point Tunnelling Protocol (PPTP) VPN
- Internet Protocol Security (IPsec) VPN
- OpenVPN.

OpenVPN is an open source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. NetComm Wireless M2M routers support three different OpenVPN modes:

- OpenVPN Server
- OpenVPN Client
- OpenVPN Peer-to-Peer VPN connection.

This document describes how to configure the different OpenVPN types on NetComm Wireless M2M routers.

Important notes about OpenVPN on NetComm Wireless M2M Series Routers

- When using two NetComm Wireless M2M routers in a Server-Client scenario, you should change the LAN IP Address of the devices so that they are on different subnets, otherwise you may find it impossible to access the web-interface of one of the routers when an OpenVPN connection is established.
- A NetComm Wireless M2M router acting as a Server must be connected to an APN that provides a publicly routable IP address.
- OpenVPN Certificates and Secret Keys are dependent on the time on each router being in synchronisation. If the time is not correct on the router due to NTP not working or for any other reason, the certificate or secret key timestamp may be expired and hence will not be useable.
- If both the OpenVPN Server and OpenVPN Client are in a private network, please ensure that the server is routable to the client and vice-versa before establishing the VPN connection.

# OpenVPN Server Mode

In OpenVPN Server Mode, a NetComm Wireless M2M Series Router acts as a host allowing M2M Routers in client mode or Windows/Linux software clients to establish a virtual private network connection. In order to establish a secure communications channel, a cryptographic key is exchanged between the server and the client using the Diffie-Hellman method of key exchange. Once a shared secret is established, certificates identifying each client node are issued which can be used as a means of authentication.

OpenVPN authentication is achieved through first establishing a public key infrastructure. The public key infrastructure includes:

1. A public and private key for the server and each client
2. A master Certificate Authority (CA) certificate and the key used to sign each of the server and client certificates.

This authentication method results in several benefits:

- The server only needs its own certificate and key. It does not need to have every certificate of every client that may connect to it.
- The server will only accept clients with certificates that were signed by the master certificate authority.
- If the security of a client certificate is compromised, that individual certificate can be revoked without requiring a new public key infrastructure to be generated.
- The server can enforce access rights for specific clients based on the certificate fields.

While certificate authentication is the more secure and desirable means of authentication, it is also possible to use a username and password for authentication. Username and password authentication is not used in conjunction with certificates.

An OpenVPN Server allows for one or many client routers to establish secure communication tunnels as illustrated below:

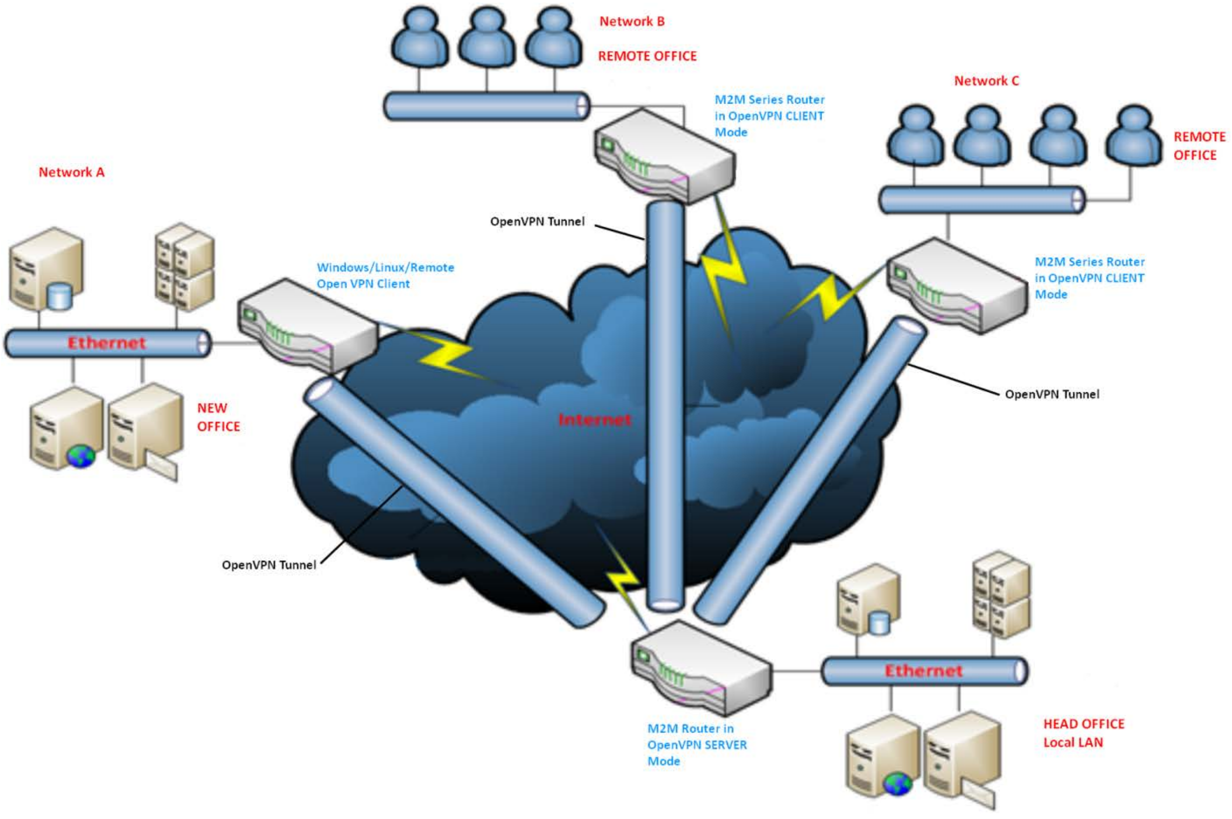
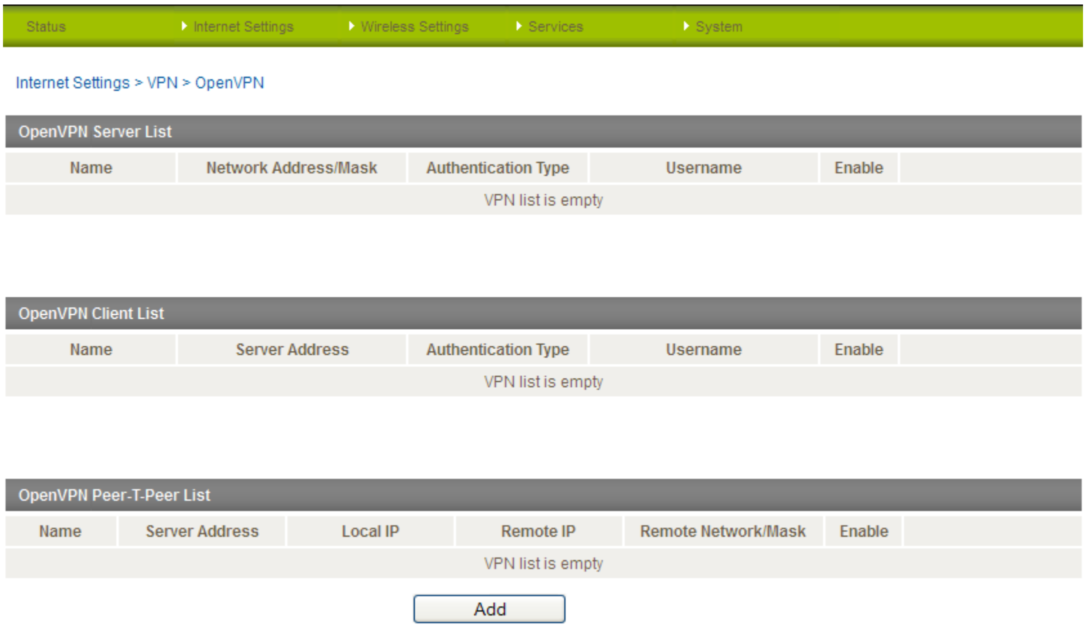


Figure 1 - OpenVPN Server Mode Diagram

## Configuring an OpenVPN Server

1. Login to your NetComm Wireless M2M Series Router using the “root” account.
2. Click on **Internet Settings**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



Internet Settings > VPN > OpenVPN

OpenVPN Server List

| Name | Network Address/Mask | Authentication Type | Username | Enable | |
|---|---|---|---|---|---|
| VPN list is empty | | | | | |

OpenVPN Client List

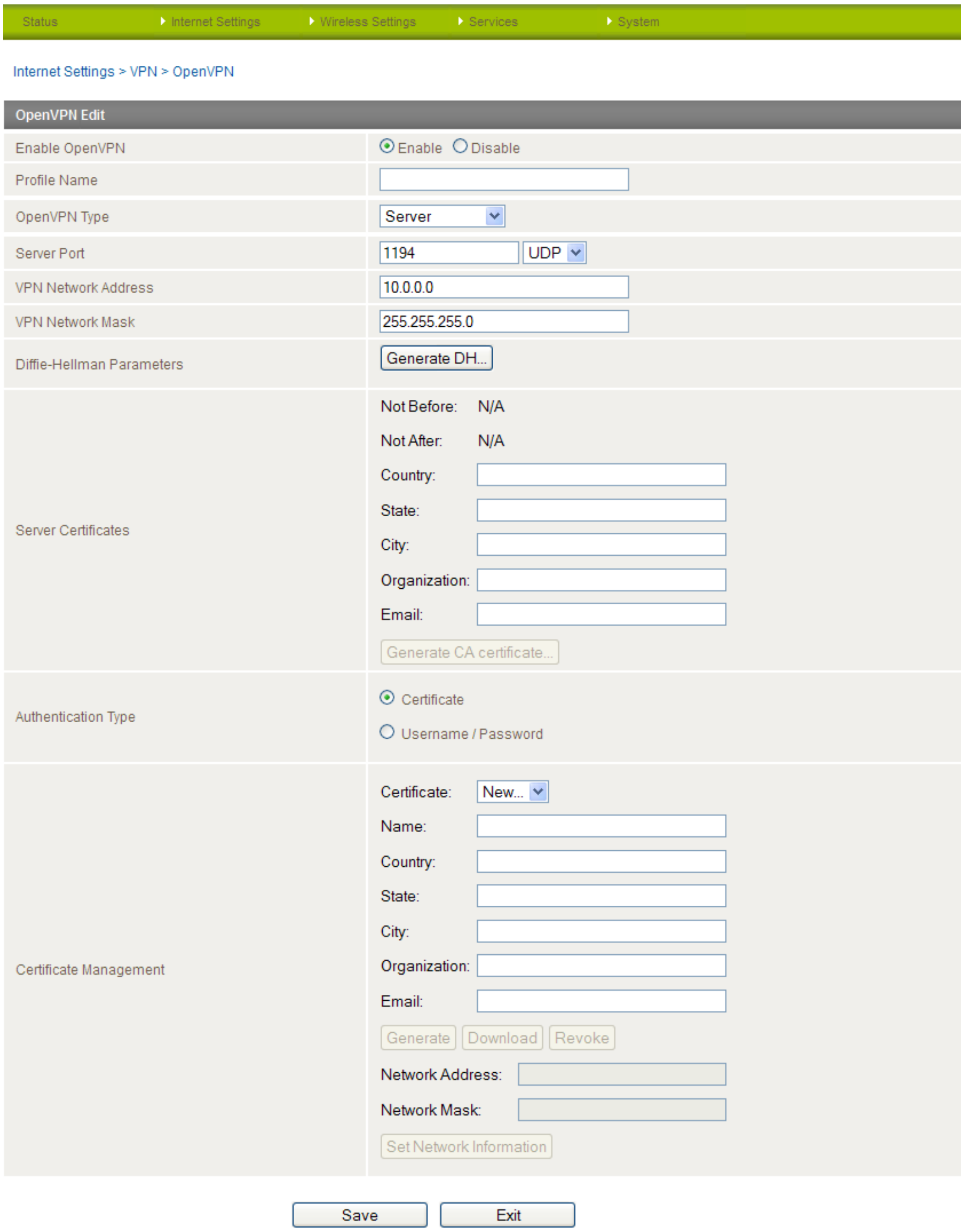
| Name | Server Address | Authentication Type | Username | Enable | |
|---|---|---|---|---|---|
| VPN list is empty | | | | | |

OpenVPN Peer-T-Peer List

| Name | Server Address | Local IP | Remote IP | Remote Network/Mask | Enable | |
|---|---|---|---|---|---|---|
| VPN list is empty | | | | | | |

Figure 2 - OpenVPN List

3. Click the **Add** button. The configuration window is displayed.



Internet Settings > VPN > OpenVPN

**OpenVPN Edit**

| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | |
| OpenVPN Type | Server |
| Server Port | 1194 UDP |
| VPN Network Address | 10.0.0.0 |
| VPN Network Mask | 255.255.255.0 |
| Diffie-Hellman Parameters | Generate DH... |
| Server Certificates | Not Before: N/A<br>Not After: N/A<br>Country:<br>State:<br>City:<br>Organization:<br>Email:<br>Generate CA certificate... |
| Authentication Type | ● Certificate<br>○ Username / Password |
| Certificate Management | Certificate: New...<br>Name:<br>Country:<br>State:<br>City:<br>Organization:<br>Email:<br>Generate Download Revoke<br>Network Address:<br>Network Mask:<br>Set Network Information |

Figure 3 - OpenVPN Server configuration page

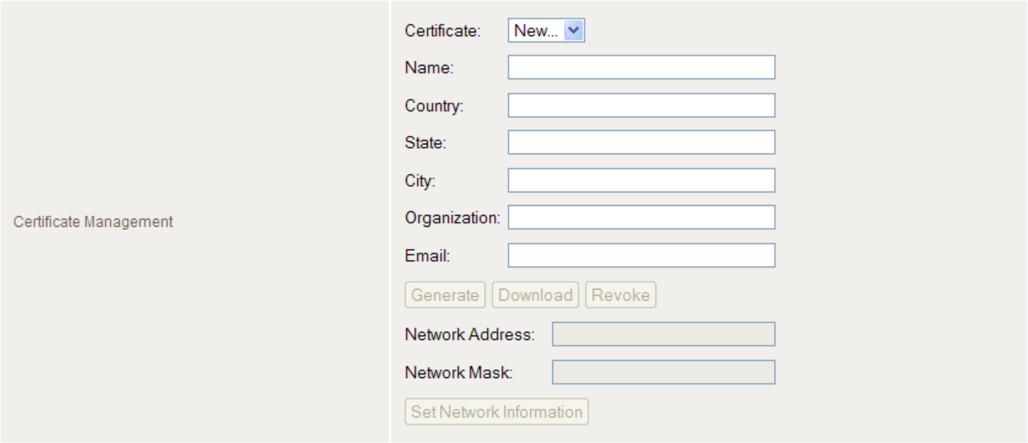
4. Set OpenVPN to **Enable.**
5. Type a name for the OpenVPN Server profile you are creating.
6. From the OpenVPN Type drop down list, select **Server**.
7. Select a port number and packet type to use for your OpenVPN Server. The default OpenVPN port is 1194 and default packet type is UDP.
8. In the VPN Network Address and VPN Network Mask fields, enter the IP address and network mask to assign to your VPN. This is ideally an internal IP address which differs from your existing address scheme. The default settings may be used if you wish.
9. Next to Diffie-Hellman Parameters, click the **Generate DH** button. This will create an encryption key to secure your OpenVPN connection.

Note: The Diffie-Hellman parameters can take up to 10 minutes to generate. Please be patient.

10. Under Server Certificates, enter the required details. All fields must be completed. The Country field must consist of two characters only. When the details have been entered, click the **Generate CA certificate** button to generate the Certificate Authority (CA) certificate based on this information.
11. Select the Authentication Type that you would like to use for the OpenVPN Server.

### Certificate Authentication

a) In the Certificate Management section, enter the required details to create a client certificate. All fields are required. When you have finished entering the details, click the **Generate** button. The certificate should only take a moment to generate.


Certificate Management

Certificate: New...

Name:

Country:

State:

City:

Organization:

Email:

Network Address:

Network Mask:

Figure 4 - OpenVPN Server - Certificate Management section

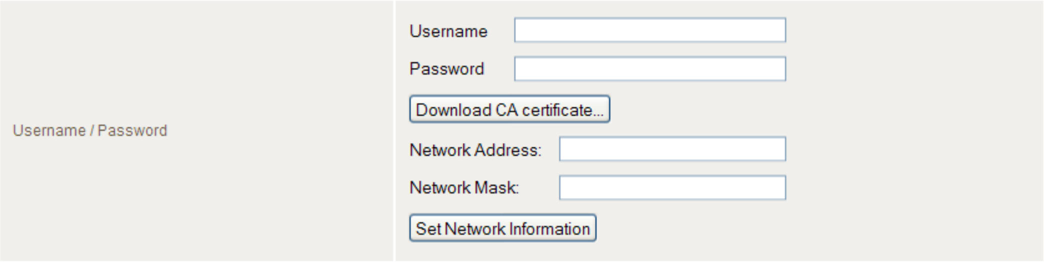
b) When it is done, you can click the **Download** button to save the certificate file. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the **Revoke** button to disable it.

c) **Optional:** To inform the OpenVPN Server of the network address scheme of the currently selected certificate, enter the Network Address and Network Mask in the respective fields. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client’s subnet.

### Username / Password Authentication

a) In the username/password section, enter the username and password you would like to use for authentication on the OpenVPN Server. Click the **Download CA certificate** button to save the **ca.crt** file. This file will need to be provided to the client.

Note: If you wish to have more than one client connect to this OpenVPN Server, you must use Certificate Authentication mode as Username/Password only allows for a single client connection.


Username / Password

Username

Password

Network Address:

Network Mask:

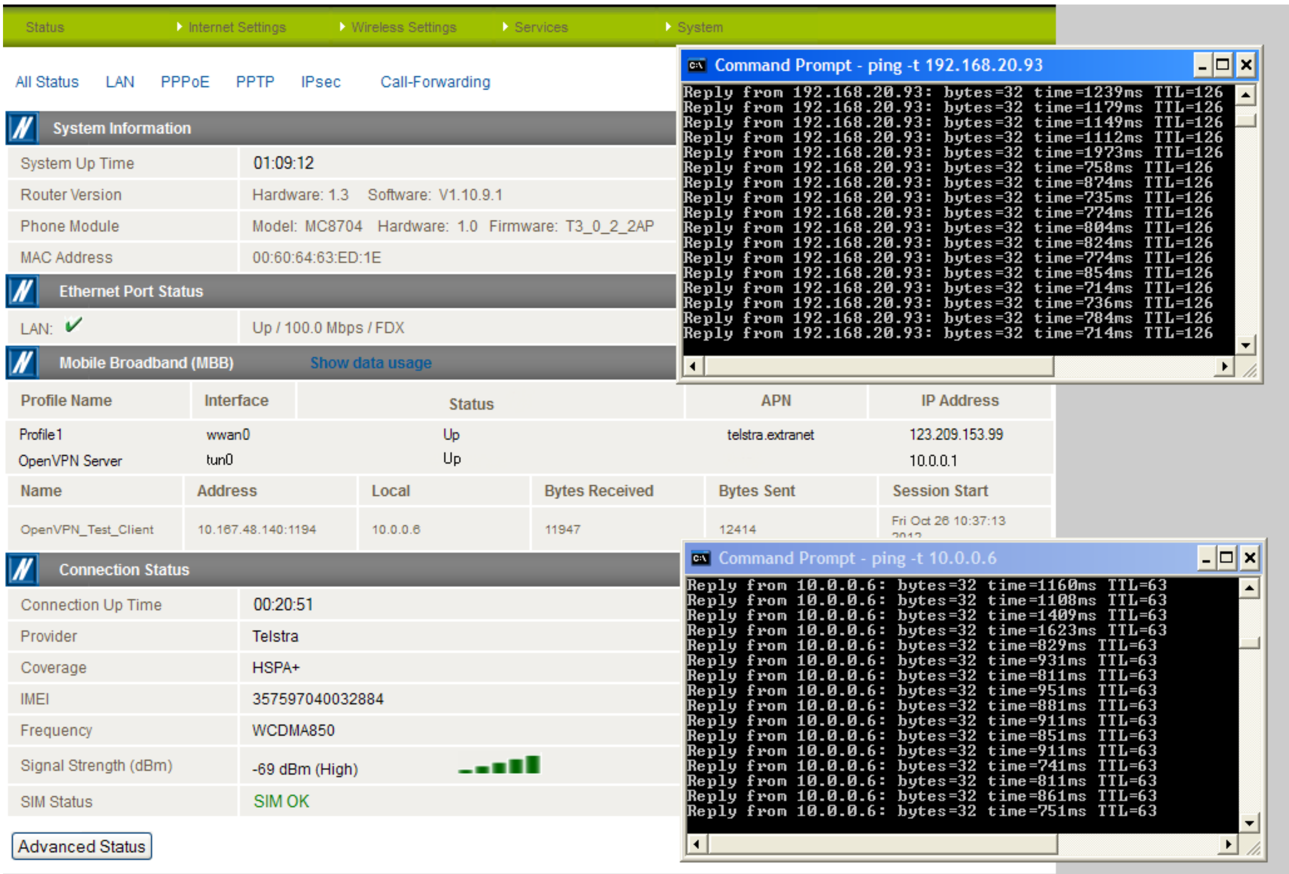
Figure 5 - OpenVPN Server - Username/Password section

b) **Optional:** To inform the OpenVPN Server of the network address scheme of the currently selected certificate, enter the Network Address and Network Mask in the respective fields. If you do not enter the remote subnet here, any packet requests from the server to the client will not be received by the client network because it is not aware of the remote client's subnet.

12. When you have finished entering all the required information, click **Save** to finish configuring the OpenVPN Server.

## Verifying the OpenVPN Connection Status

Open a command prompt and ping a client in the remote subnet and the OpenVPN Gateway address assigned to the remote router. See the screenshot below for an example.



**System Information**

| | |
|---|---|
| System Up Time | 01:09:12 |
| Router Version | Hardware: 1.3 Software: V1.10.9.1 |
| Phone Module | Model: MC8704 Hardware: 1.0 Firmware: T3_0_2_2AP |
| MAC Address | 00:60:64:63:ED:1E |

**Ethernet Port Status**

| | |
|---|---|
| LAN: ✓ | Up / 100.0 Mbps / FDX |

**Mobile Broadband (MBB)**

| Profile Name | Interface | Status | APN | IP Address |
|---|---|---|---|---|
| Profile1 | wwan0 | Up | telstra.extranet | 123.209.153.99 |
| OpenVPN Server | tun0 | Up | | 10.0.0.1 |

| Name | Address | Local | Bytes Received | Bytes Sent | Session Start |
|---|---|---|---|---|---|
| OpenVPN_Test_Client | 10.167.48.140:1194 | 10.0.0.6 | 11947 | 12414 | Fri Oct 26 10:37:13 2012 |

**Connection Status**

| | |
|---|---|
| Connection Up Time | 00:20:51 |
| Provider | Telstra |
| Coverage | HSPA+ |
| IMEI | 357597040032884 |
| Frequency | WCDMA850 |
| Signal Strength (dBm) | -69 dBm (High) |
| SIM Status | SIM OK |

Command Prompt - ping -t 192.168.20.93

```
Reply from 192.168.20.93: bytes=32 time=1239ms TTL=126
Reply from 192.168.20.93: bytes=32 time=1179ms TTL=126
Reply from 192.168.20.93: bytes=32 time=1149ms TTL=126
Reply from 192.168.20.93: bytes=32 time=1112ms TTL=126
Reply from 192.168.20.93: bytes=32 time=1973ms TTL=126
Reply from 192.168.20.93: bytes=32 time=758ms TTL=126
Reply from 192.168.20.93: bytes=32 time=874ms TTL=126
Reply from 192.168.20.93: bytes=32 time=735ms TTL=126
Reply from 192.168.20.93: bytes=32 time=774ms TTL=126
Reply from 192.168.20.93: bytes=32 time=804ms TTL=126
Reply from 192.168.20.93: bytes=32 time=824ms TTL=126
Reply from 192.168.20.93: bytes=32 time=774ms TTL=126
Reply from 192.168.20.93: bytes=32 time=854ms TTL=126
Reply from 192.168.20.93: bytes=32 time=714ms TTL=126
Reply from 192.168.20.93: bytes=32 time=736ms TTL=126
Reply from 192.168.20.93: bytes=32 time=784ms TTL=126
Reply from 192.168.20.93: bytes=32 time=714ms TTL=126
```

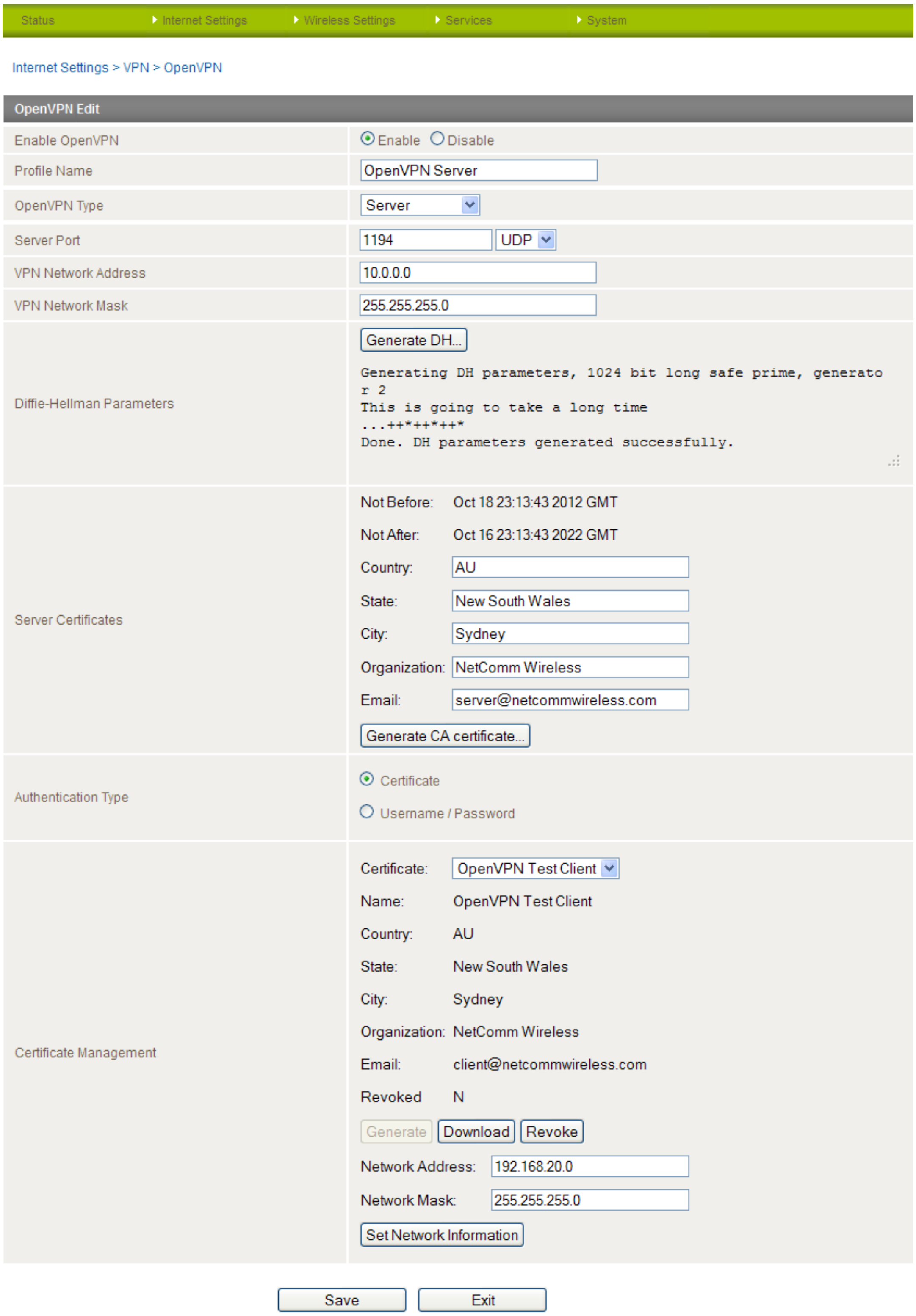
Command Prompt - ping -t 10.0.0.6

```
Reply from 10.0.0.6: bytes=32 time=1160ms TTL=63
Reply from 10.0.0.6: bytes=32 time=1108ms TTL=63
Reply from 10.0.0.6: bytes=32 time=1409ms TTL=63
Reply from 10.0.0.6: bytes=32 time=1623ms TTL=63
Reply from 10.0.0.6: bytes=32 time=829ms TTL=63
Reply from 10.0.0.6: bytes=32 time=931ms TTL=63
Reply from 10.0.0.6: bytes=32 time=811ms TTL=63
Reply from 10.0.0.6: bytes=32 time=951ms TTL=63
Reply from 10.0.0.6: bytes=32 time=881ms TTL=63
Reply from 10.0.0.6: bytes=32 time=911ms TTL=63
Reply from 10.0.0.6: bytes=32 time=851ms TTL=63
Reply from 10.0.0.6: bytes=32 time=911ms TTL=63
Reply from 10.0.0.6: bytes=32 time=741ms TTL=63
Reply from 10.0.0.6: bytes=32 time=811ms TTL=63
Reply from 10.0.0.6: bytes=32 time=861ms TTL=63
Reply from 10.0.0.6: bytes=32 time=751ms TTL=63
```

Figure 6 - OpenVPN Server connection verification

## OpenVPN Server Examples

### OpenVPN Server Mode – Certificate Authentication



**OpenVPN Edit**

Enable OpenVPN: ● Enable ○ Disable

Profile Name: OpenVPN Server

OpenVPN Type: Server

Server Port: 1194 UDP

VPN Network Address: 10.0.0.0

VPN Network Mask: 255.255.255.0

Diffie-Hellman Parameters:

```
Generating DH parameters, 1024 bit long safe prime, generato
r 2
This is going to take a long time
...++*++*++*
Done. DH parameters generated successfully.
```

Server Certificates:

| | |
|---|---|
| Not Before: | Oct 18 23:13:43 2012 GMT |
| Not After: | Oct 16 23:13:43 2022 GMT |
| Country: | AU |
| State: | New South Wales |
| City: | Sydney |
| Organization: | NetComm Wireless |
| Email: | server@netcommwireless.com |

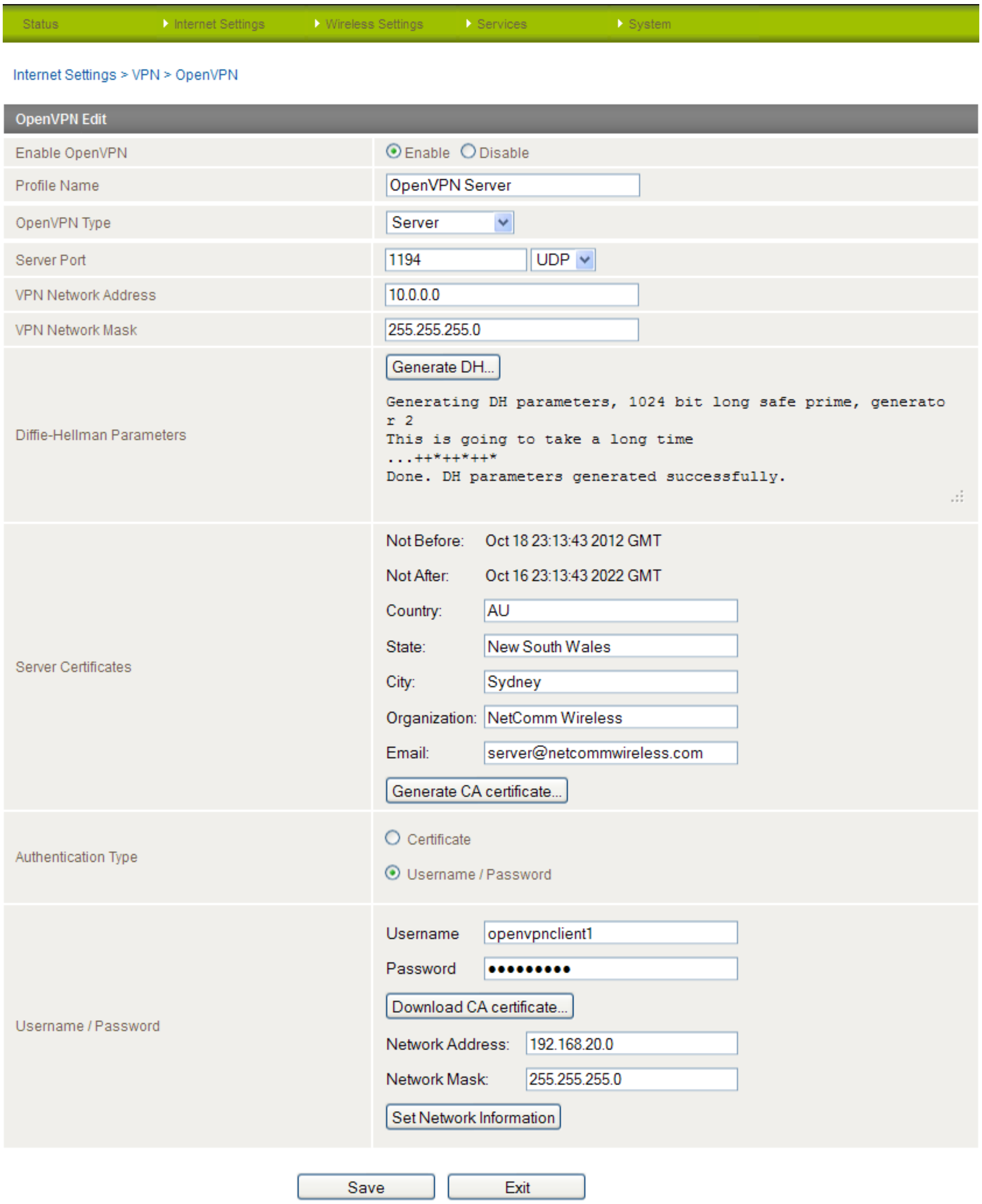
Authentication Type: ● Certificate ○ Username / Password

Certificate Management:

| | |
|---|---|
| Certificate: | OpenVPN Test Client |
| Name: | OpenVPN Test Client |
| Country: | AU |
| State: | New South Wales |
| City: | Sydney |
| Organization: | NetComm Wireless |
| Email: | client@netcommwireless.com |
| Revoked | N |
| Network Address: | 192.168.20.0 |
| Network Mask: | 255.255.255.0 |

Figure 7 - OpenVPN Server - Certificate Authentication Example page

## OpenVPN Server Mode – Username / Password Authentication



Internet Settings > VPN > OpenVPN

**OpenVPN Edit**

| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | OpenVPN Server |
| OpenVPN Type | Server |
| Server Port | 1194 UDP |
| VPN Network Address | 10.0.0.0 |
| VPN Network Mask | 255.255.255.0 |
| Diffie-Hellman Parameters | Generate DH... |
| Server Certificates | Not Before: Oct 18 23:13:43 2012 GMT<br>Not After: Oct 16 23:13:43 2022 GMT<br>Country: AU<br>State: New South Wales<br>City: Sydney<br>Organization: NetComm Wireless<br>Email: server@netcommwireless.com |
| Authentication Type | ○ Certificate<br>● Username / Password |
| Username / Password | Username: openvpnclient1<br>Password: ●●●●●●●●●<br>Network Address: 192.168.20.0<br>Network Mask: 255.255.255.0 |

```
Generating DH parameters, 1024 bit long safe prime, generato
r 2
This is going to take a long time
...++*++*++*
Done. DH parameters generated successfully.
```

Figure 8 - OpenVPN Server - Username / Password Authentication Example page

# OpenVPN Client Mode

NetComm M2M Series Routers may be configured to operate as an OpenVPN Client and connect to an OpenVPN Server running on another NetComm Wireless M2M Series Router or a software OpenVPN Server on a computer.

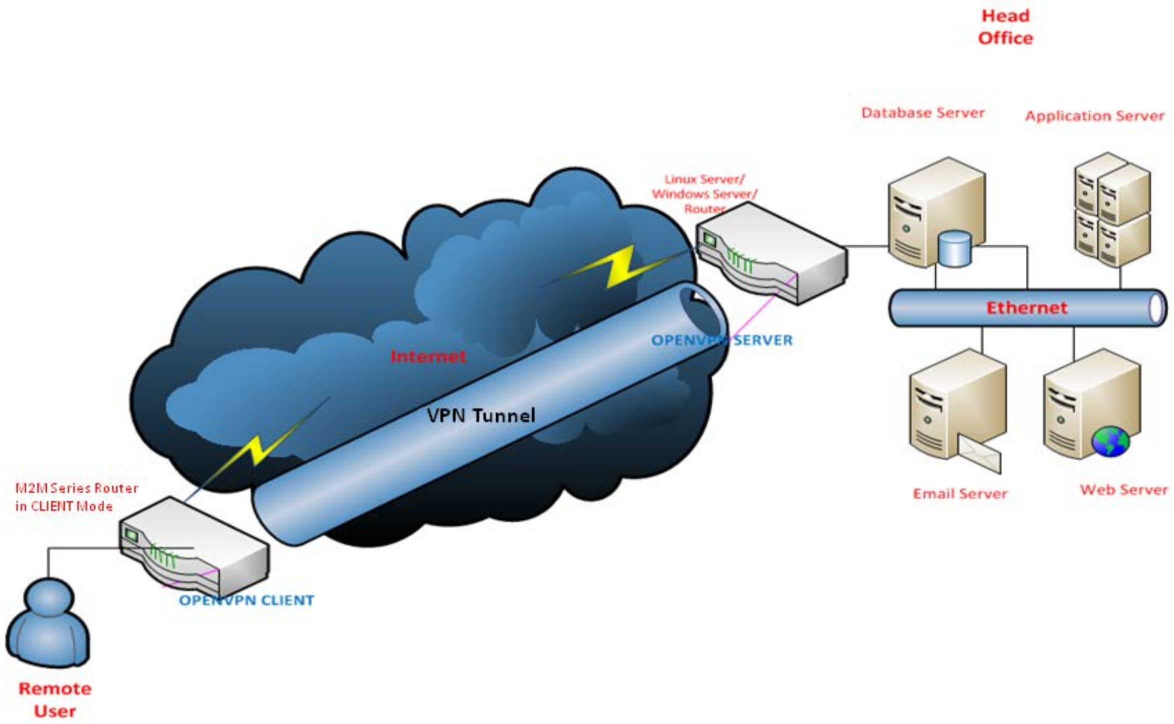


Figure 9 - OpenVPN Client Diagram

## Certificate Files

When using two NetComm Wireless M2M Routers to establish an OpenVPN connection, the certificate generated by the server will be recognised by the client and will not require modification.

In situations where you are using another third-party OpenVPN Server to generate certificates, the NetComm Wireless M2M Router will expect a tar archive compressed using GZip. There are three files that the OpenVPN client in a NetComm Wireless router will expect to see within a .tgz file:

- The master Certificate Authority (CA) certificate file named ca.crt
- Client certificate file (e.g., OpenVPN Test Client.crt)
- Client key file (e.g., OpenVPN Test Client.key)

If you have used a third-party OpenVPN Server to generate certificates and keys, you will need to archive these three files in a .tgz file to provide the OpenVPN Client on your NetComm Wireless M2M Router.

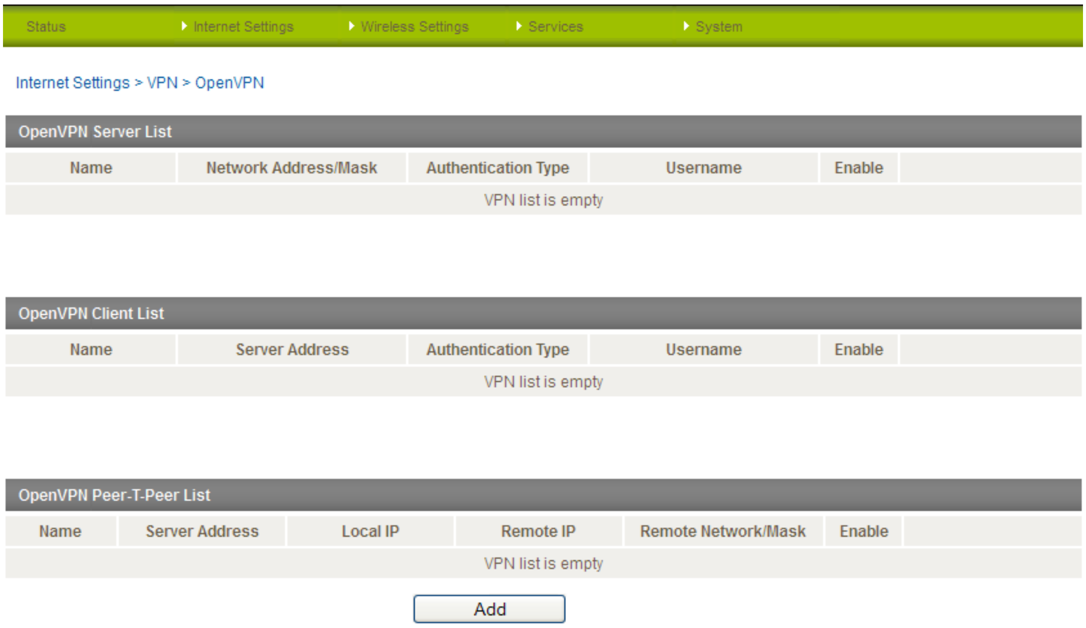
You can perform this in Linux by using the command:

```
tar –zcvf netcommclient.tgz netcommclient.crt netcommclient.key ca.crt
```

For more information on creating .tgz files, please refer to http://www.cs.duke.edu/~ola/courses/programming/tar.html

## Configuring an OpenVPN Client

1. Login to your NetComm Wireless M2M Series Router using the “root” account.
2. Click on **Internet Settings**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



OpenVPN Server List

| Name | Network Address/Mask | Authentication Type | Username | Enable | |
|---|---|---|---|---|---|
| VPN list is empty | | | | | |

OpenVPN Client List

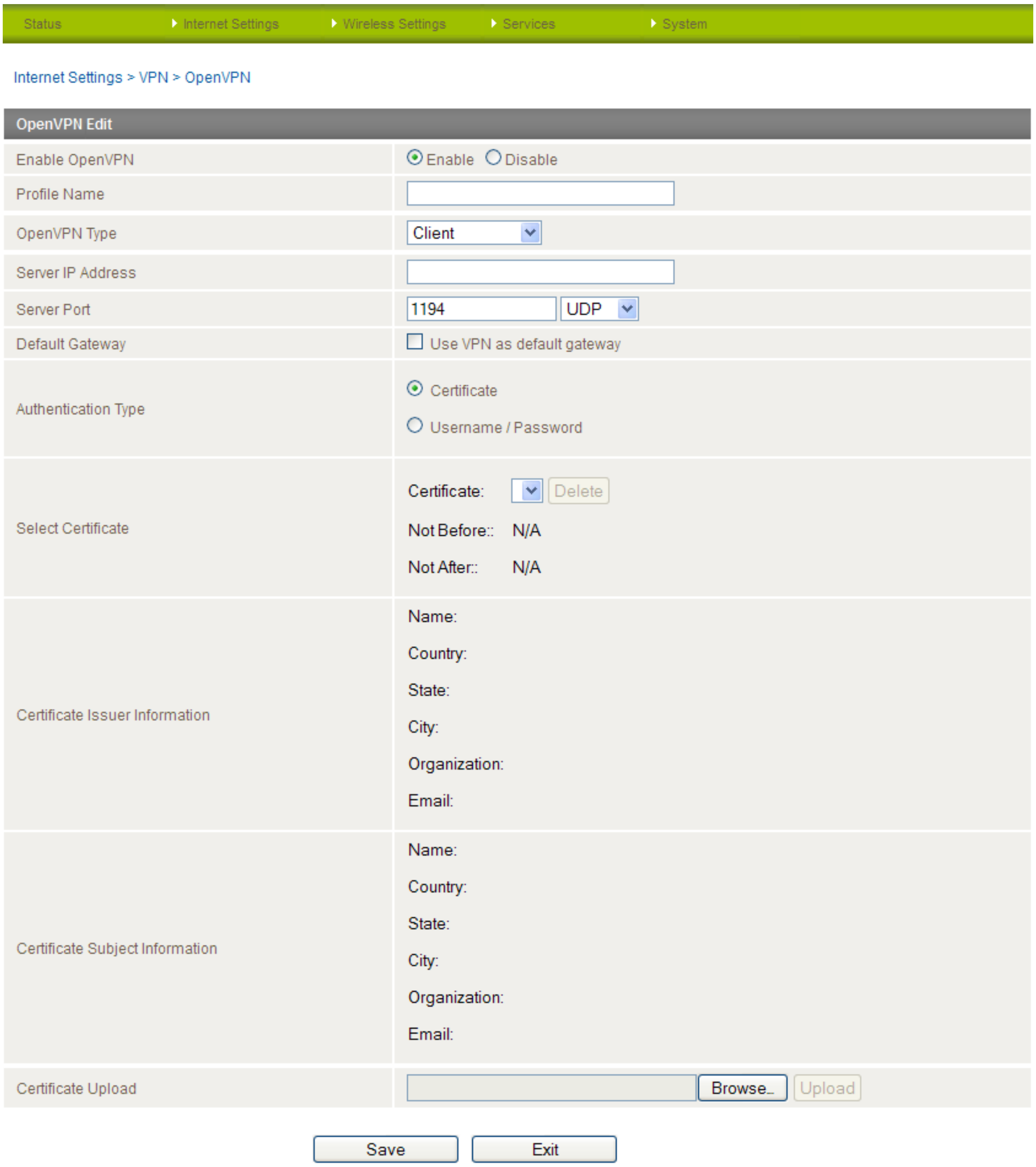
| Name | Server Address | Authentication Type | Username | Enable | |
|---|---|---|---|---|---|
| VPN list is empty | | | | | |

OpenVPN Peer-T-Peer List

| Name | Server Address | Local IP | Remote IP | Remote Network/Mask | Enable | |
|---|---|---|---|---|---|---|
| VPN list is empty | | | | | | |

Figure 10 - OpenVPN List

3. Click the **Add** button. The configuration window is displayed.



Internet Settings > VPN > OpenVPN

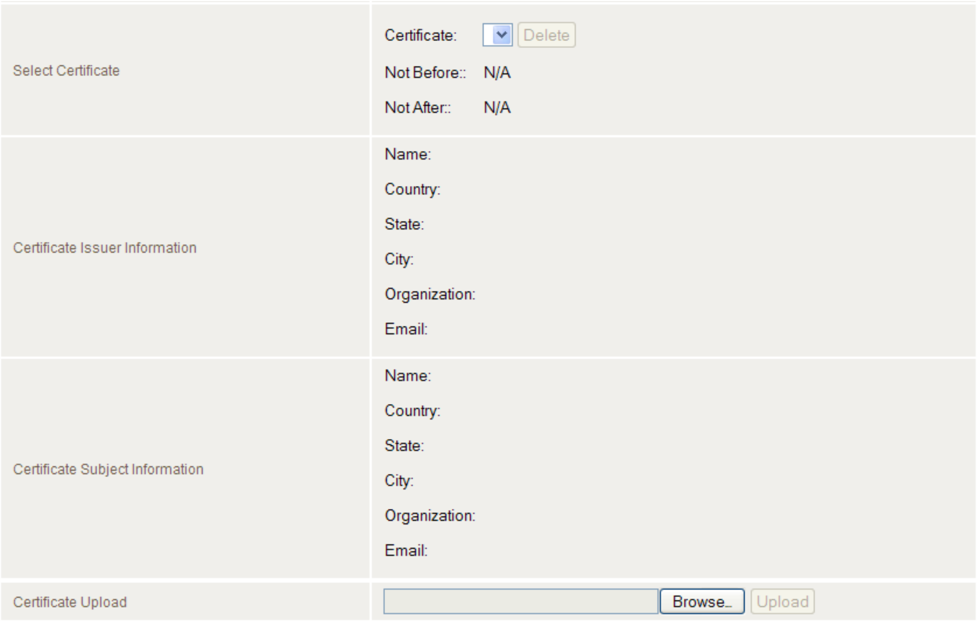
| OpenVPN Edit | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | |
| OpenVPN Type | Client |
| Server IP Address | |
| Server Port | 1194 UDP |
| Default Gateway | □ Use VPN as default gateway |
| Authentication Type | ● Certificate<br>○ Username / Password |
| Select Certificate | Certificate: Delete<br>Not Before:: N/A<br>Not After:: N/A |
| Certificate Issuer Information | Name:<br>Country:<br>State:<br>City:<br>Organization:<br>Email: |
| Certificate Subject Information | Name:<br>Country:<br>State:<br>City:<br>Organization:<br>Email: |
| Certificate Upload | Browse... Upload |

Figure 9 - OpenVPN Client - Configuration page

4. Set OpenVPN to **Enable.**
5. Type a name for the OpenVPN Client profile you are creating.
6. From the OpenVPN Type drop down list, select **Client**.
7. Type the WAN IP address of the OpenVPN Server.
8. Enter the Server Port and packet type to use for the connection.
9. If “Use VPN as default gateway” option is applied on the OpenVPN Client page, the OpenVPN Server will enable connections to be made to other client networks connected to it. If it is not selected, the OpenVPN connection allows for secure communication links between the remote office and the head office only.
10. Select the Authentication Type that you would like to use for the OpenVPN Client.

### Certificate Authentication

a) In the Certificate Upload section at the bottom of the screen, click the **Browse** button and locate the certificate file you downloaded when you configured the OpenVPN Server. When it has been selected, click the **Upload** button to send it to the router.

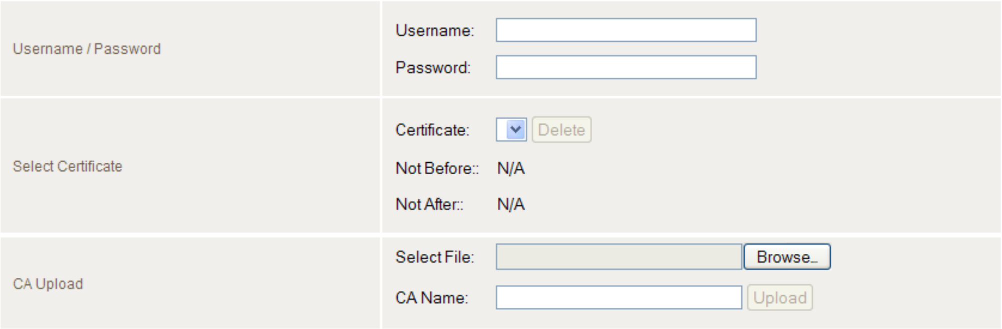


| | |
|---|---|
| Select Certificate | Certificate: ▾ Delete<br>Not Before:: N/A<br>Not After:: N/A |
| Certificate Issuer Information | Name:<br>Country:<br>State:<br>City:<br>Organization:<br>Email: |
| Certificate Subject Information | Name:<br>Country:<br>State:<br>City:<br>Organization:<br>Email: |
| Certificate Upload | Browse... Upload |

Figure 11 - OpenVPN Client - Certificate Authentication section

### Username / Password Authentication

a) Enter the username and password to authenticate with the OpenVPN Server.



| | |
|---|---|
| Username / Password | Username:<br>Password: |
| Select Certificate | Certificate: ▾ Delete<br>Not Before:: N/A<br>Not After:: N/A |
| CA Upload | Select File: Browse...<br>CA Name: Upload |

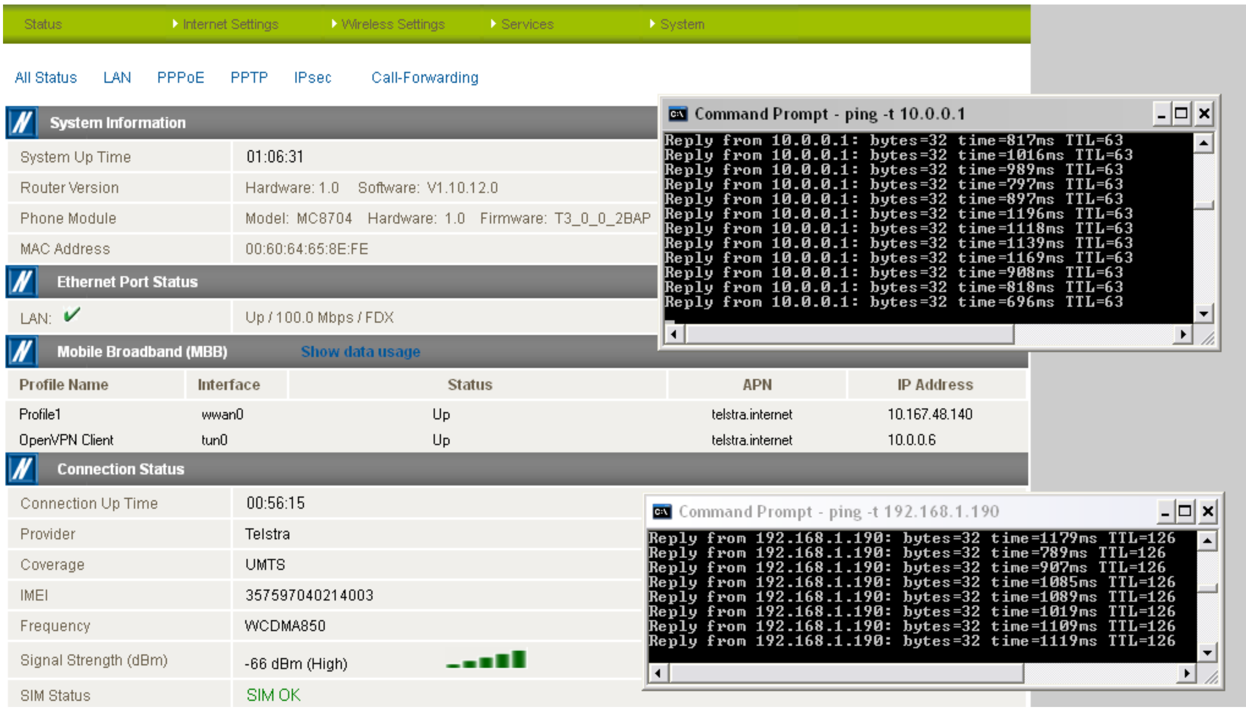
Figure 12 - OpenVPN Client - Username/Password section

b) Use the **Browse** button to locate the CA certificate file you saved from the OpenVPN Server and then press the **Upload** button to send it to the router.

11. Click the **Save** button to complete the OpenVPN Client configuration.

## Verifying the OpenVPN Connection Status

Open a command prompt and ping the OpenVPN Gateway address assigned to the remote router. See the screenshot below for an example.



**System Information**

| | |
|---|---|
| System Up Time | 01:06:31 |
| Router Version | Hardware: 1.0 Software: V1.10.12.0 |
| 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)** Show data usage

| Profile Name | Interface | Status | APN | IP Address |
|---|---|---|---|---|
| Profile1 | wwan0 | Up | telstra.internet | 10.167.48.140 |
| OpenVPN Client | tun0 | Up | telstra.internet | 10.0.0.6 |

**Connection Status**

| | |
|---|---|
| Connection Up Time | 00:56:15 |
| Provider | Telstra |
| Coverage | UMTS |
| IMEI | 357597040214003 |
| Frequency | WCDMA850 |
| Signal Strength (dBm) | -66 dBm (High) |
| SIM Status | SIM OK |

Command Prompt - ping -t 10.0.0.1

```
Reply from 10.0.0.1: bytes=32 time=817ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1016ms TTL=63
Reply from 10.0.0.1: bytes=32 time=989ms TTL=63
Reply from 10.0.0.1: bytes=32 time=797ms TTL=63
Reply from 10.0.0.1: bytes=32 time=897ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1196ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1118ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1139ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1169ms TTL=63
Reply from 10.0.0.1: bytes=32 time=908ms TTL=63
Reply from 10.0.0.1: bytes=32 time=818ms TTL=63
Reply from 10.0.0.1: bytes=32 time=696ms TTL=63
```

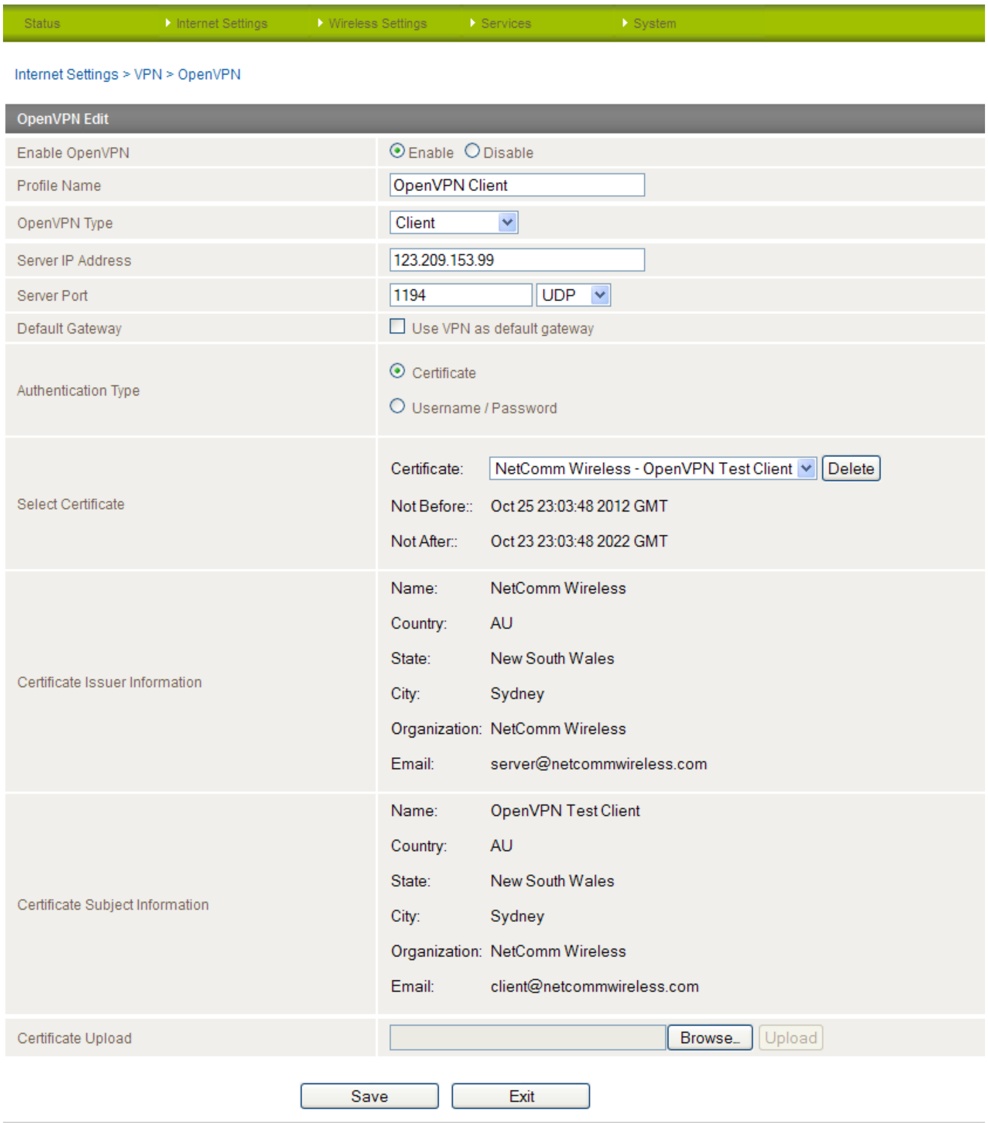
Command Prompt - ping -t 192.168.1.190

```
Reply from 192.168.1.190: bytes=32 time=1179ms TTL=126
Reply from 192.168.1.190: bytes=32 time=789ms TTL=126
Reply from 192.168.1.190: bytes=32 time=907ms TTL=126
Reply from 192.168.1.190: bytes=32 time=1085ms TTL=126
Reply from 192.168.1.190: bytes=32 time=1089ms TTL=126
Reply from 192.168.1.190: bytes=32 time=1019ms TTL=126
Reply from 192.168.1.190: bytes=32 time=1109ms TTL=126
Reply from 192.168.1.190: bytes=32 time=1119ms TTL=126
```

Figure 13 - OpenVPN Client verification of connection

## OpenVPN Client Example

### OpenVPN Client – Certificate Authentication



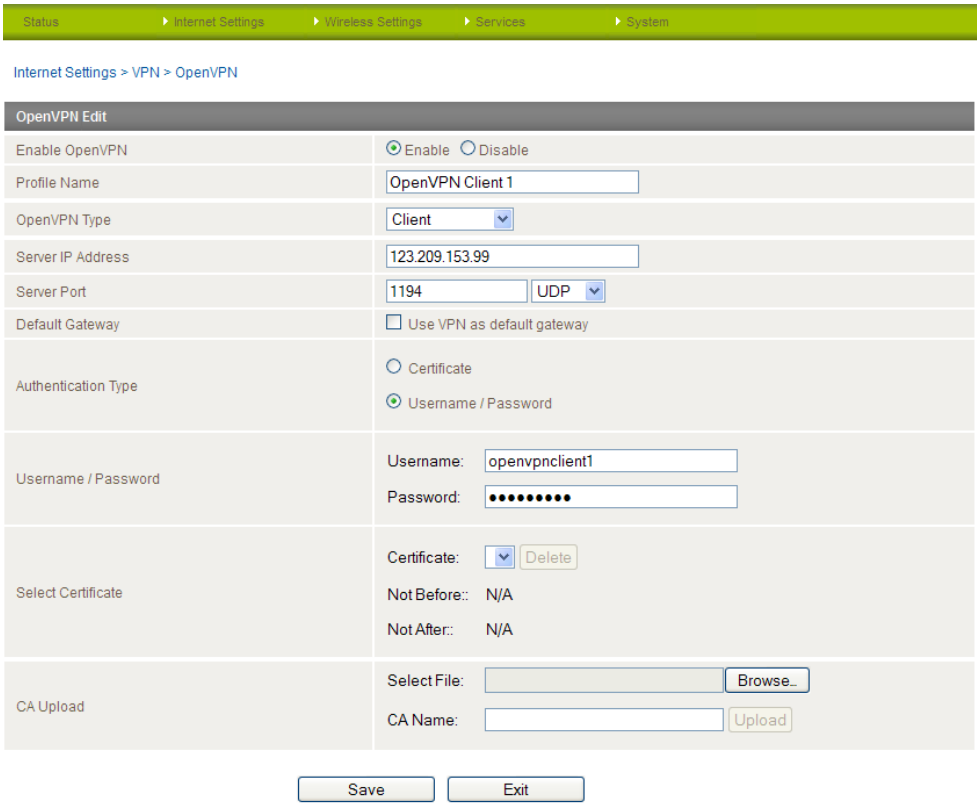
Internet Settings > VPN > OpenVPN

OpenVPN Edit

| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | OpenVPN Client |
| OpenVPN Type | Client |
| Server IP Address | 123.209.153.99 |
| Server Port | 1194 UDP |
| Default Gateway | □ Use VPN as default gateway |
| Authentication Type | ● Certificate<br>○ Username / Password |
| Select Certificate | Certificate: NetComm Wireless - OpenVPN Test Client [Delete]<br>Not Before:: Oct 25 23:03:48 2012 GMT<br>Not After:: Oct 23 23:03:48 2022 GMT |
| Certificate Issuer Information | Name: NetComm Wireless<br>Country: AU<br>State: New South Wales<br>City: Sydney<br>Organization: NetComm Wireless<br>Email: server@netcommwireless.com |
| Certificate Subject Information | Name: OpenVPN Test Client<br>Country: AU<br>State: New South Wales<br>City: Sydney<br>Organization: NetComm Wireless<br>Email: client@netcommwireless.com |
| Certificate Upload | [Browse...] [Upload] |

Figure 14 - OpenVPN Client Mode - Certificate Authentication Example

### OpenVPN Client – Username / Password Authentication



| OpenVPN Edit | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | OpenVPN Client 1 |
| OpenVPN Type | Client |
| Server IP Address | 123.209.153.99 |
| Server Port | 1194 UDP |
| Default Gateway | □ Use VPN as default gateway |
| Authentication Type | ○ Certificate<br>● Username / Password |
| Username / Password | Username: openvpnclient1<br>Password: ••••••••• |
| Select Certificate | Certificate:<br>Not Before:: N/A<br>Not After:: N/A |
| CA Upload | Select File:<br>CA Name: |

Figure 15 - OpenVPN Client Mode - Username / Password Authentication Example

# OpenVPN Peer-To-Peer Mode

OpenVPN Peer-To-Peer Mode is the quickest and easiest way to establish a secure connection between two points. In Peer-To-Peer Mode one node acts as a master and accepts a single connection from a slave.

In OpenVPN Peer-To-Peer mode, both the master and the slave generate a secret key which is then passed on to the other for authentication. This is the only form of authentication available in Peer-To-Peer mode.

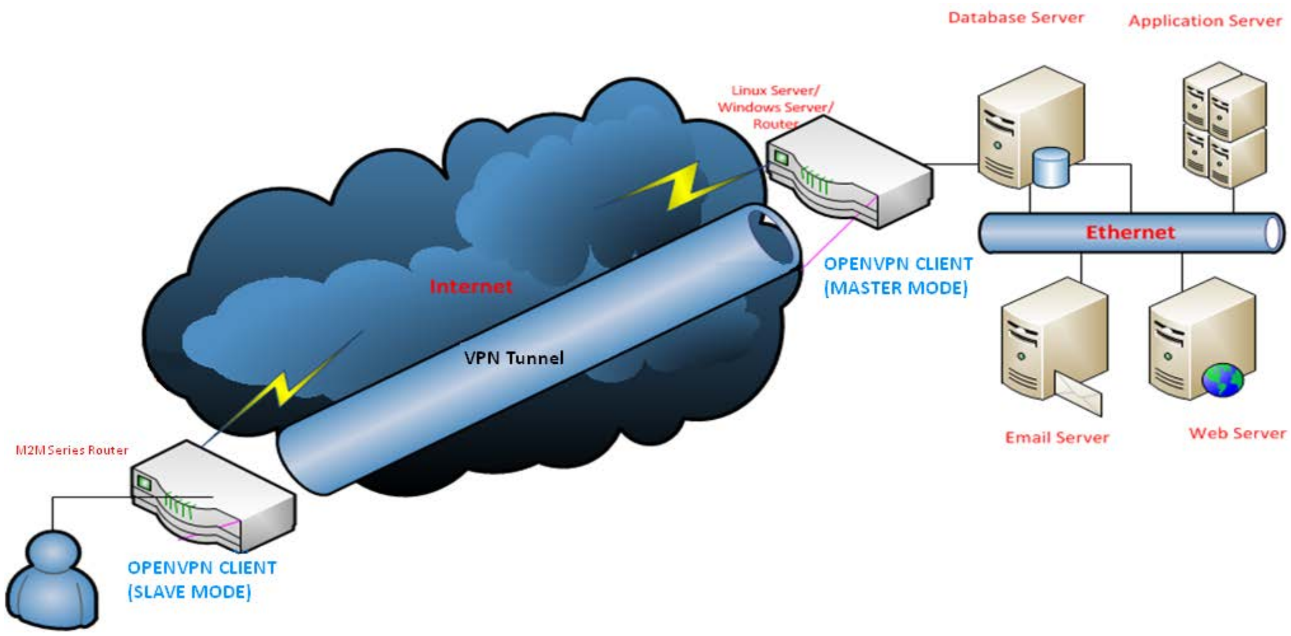
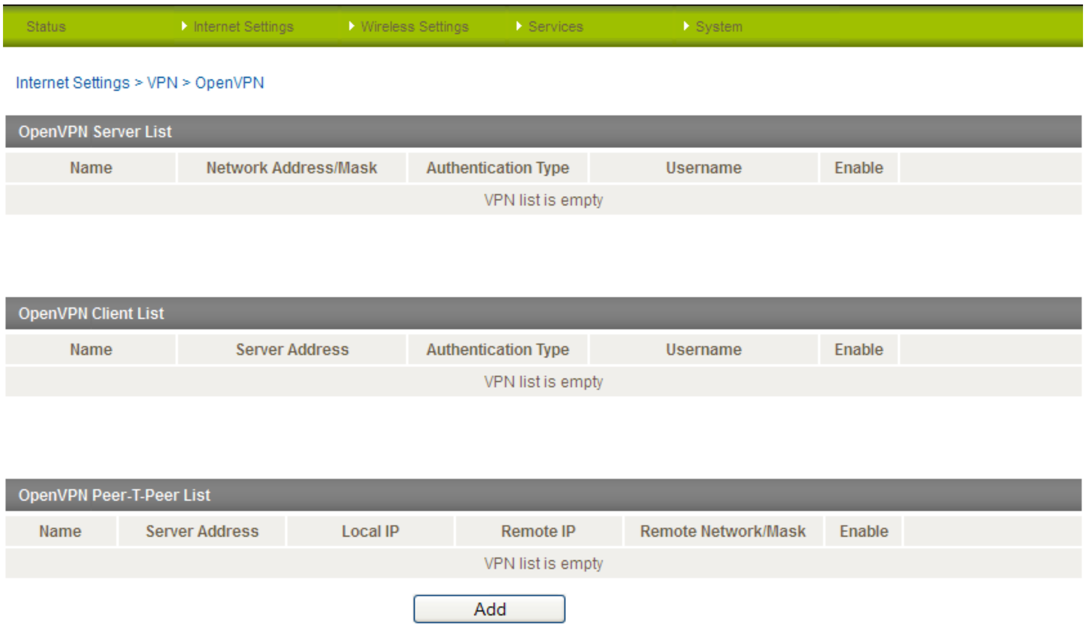


Figure 16 - OpenVPN Peer-To-Peer Mode Diagram

## Configuring an OpenVPN Peer-To-Peer Connection

Perform the following steps on two NetComm Wireless M2M Series Routers:

1. Login to your NetComm Wireless M2M Series Routers using the “root” account.
2. Click on **Internet Settings**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



OpenVPN Server List

| Name | Network Address/Mask | Authentication Type | Username | Enable |
|---|---|---|---|---|
| VPN list is empty | | | | |

OpenVPN Client List

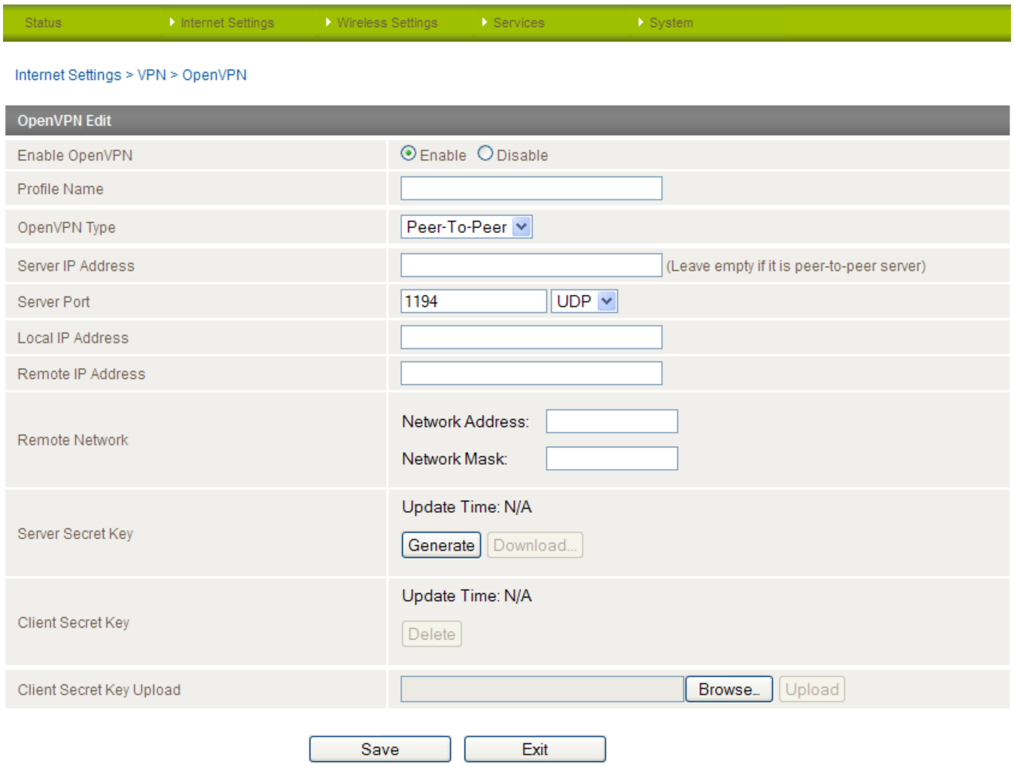
| Name | Server Address | Authentication Type | Username | Enable |
|---|---|---|---|---|
| VPN list is empty | | | | |

OpenVPN Peer-T-Peer List

| Name | Server Address | Local IP | Remote IP | Remote Network/Mask | Enable |
|---|---|---|---|---|---|
| VPN list is empty | | | | | |

Figure 17 - OpenVPN List

3. Click the **Add** button. The configuration window is displayed.



OpenVPN Edit

| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | |
| OpenVPN Type | Peer-To-Peer |
| Server IP Address | (Leave empty if it is peer-to-peer server) |
| Server Port | 1194 UDP |
| Local IP Address | |
| Remote IP Address | |
| Remote Network | Network Address:<br>Network Mask: |
| Server Secret Key | Update Time: N/A<br>Generate Download... |
| Client Secret Key | Update Time: N/A<br>Delete |
| Client Secret Key Upload | Browse... Upload |

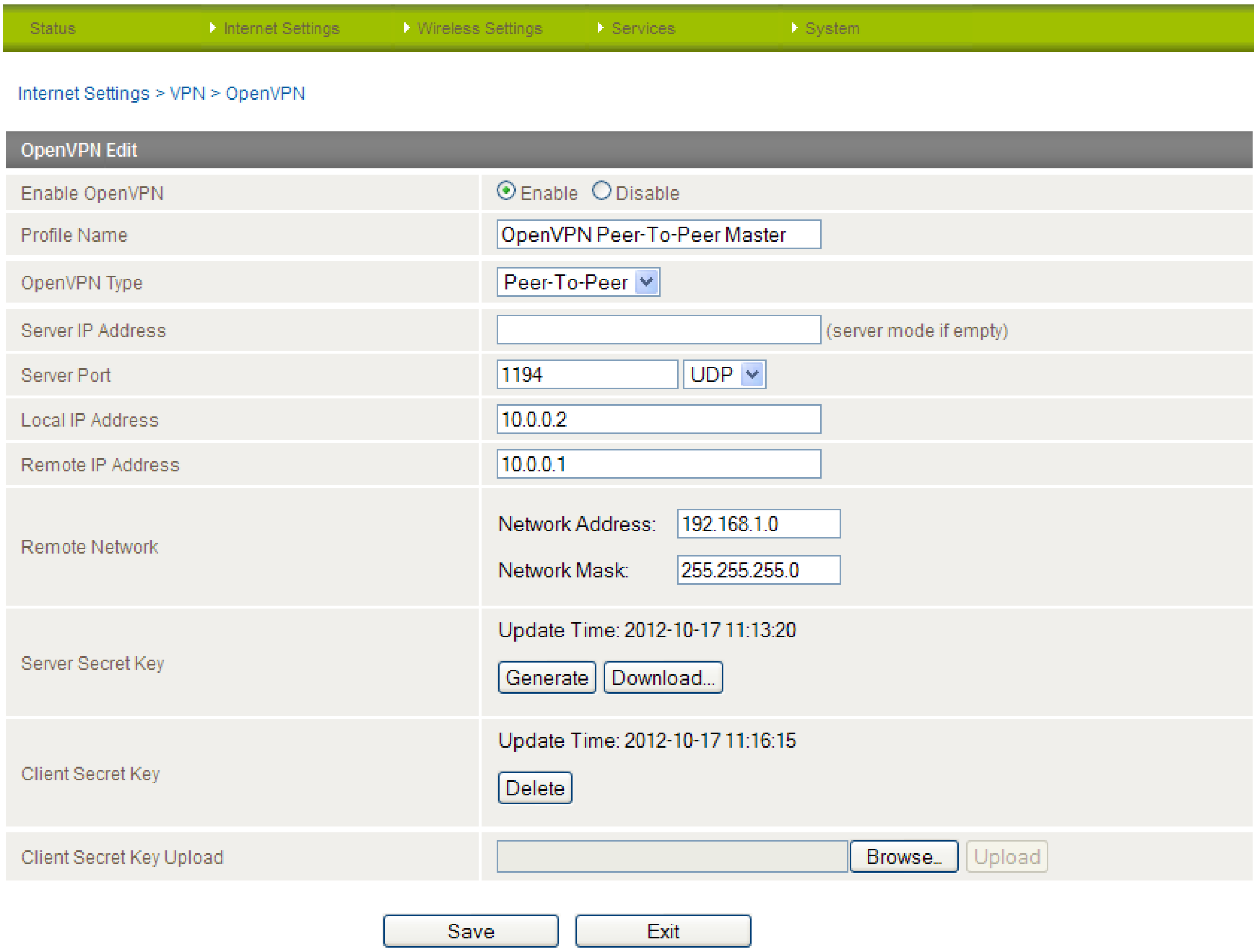
Figure 9 - OpenVPN Peer-To-Peer Mode

4. Set OpenVPN to **Enable.**

5. Type a name for the OpenVPN Peer-To-Peer profile you are creating.
6. For OpenVPN Type, select **Peer-To-Peer**
7. On the router designated as the master, leave the Server IP Address field empty. On the router designated as the slave, enter the WAN IP Address of the master.
8. Enter the Server Port and packet type to use for the connection.
9. Enter the local and remote IP addresses to use for the OpenVPN tunnel. The slave should have the reverse settings of the master.
10. Under the Remote Network section, enter the network address and network mask. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the Slave.
11. Press the **Generate** button to create a secret key to be shared with the slave. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.
12. When you have saved the secret key file on each router, use the **Browse** button to locate the secret key file for the master and then press the **Upload** button to send it to the slave. Perform the same for the other router, uploading the slave's secret key file to master.
13. When they are uploaded click the **Save** button to complete the Peer-To-Peer OpenVPN configuration.

## OpenVPN Peer-To-Peer Example

### OpenVPN Peer-To-Peer Master

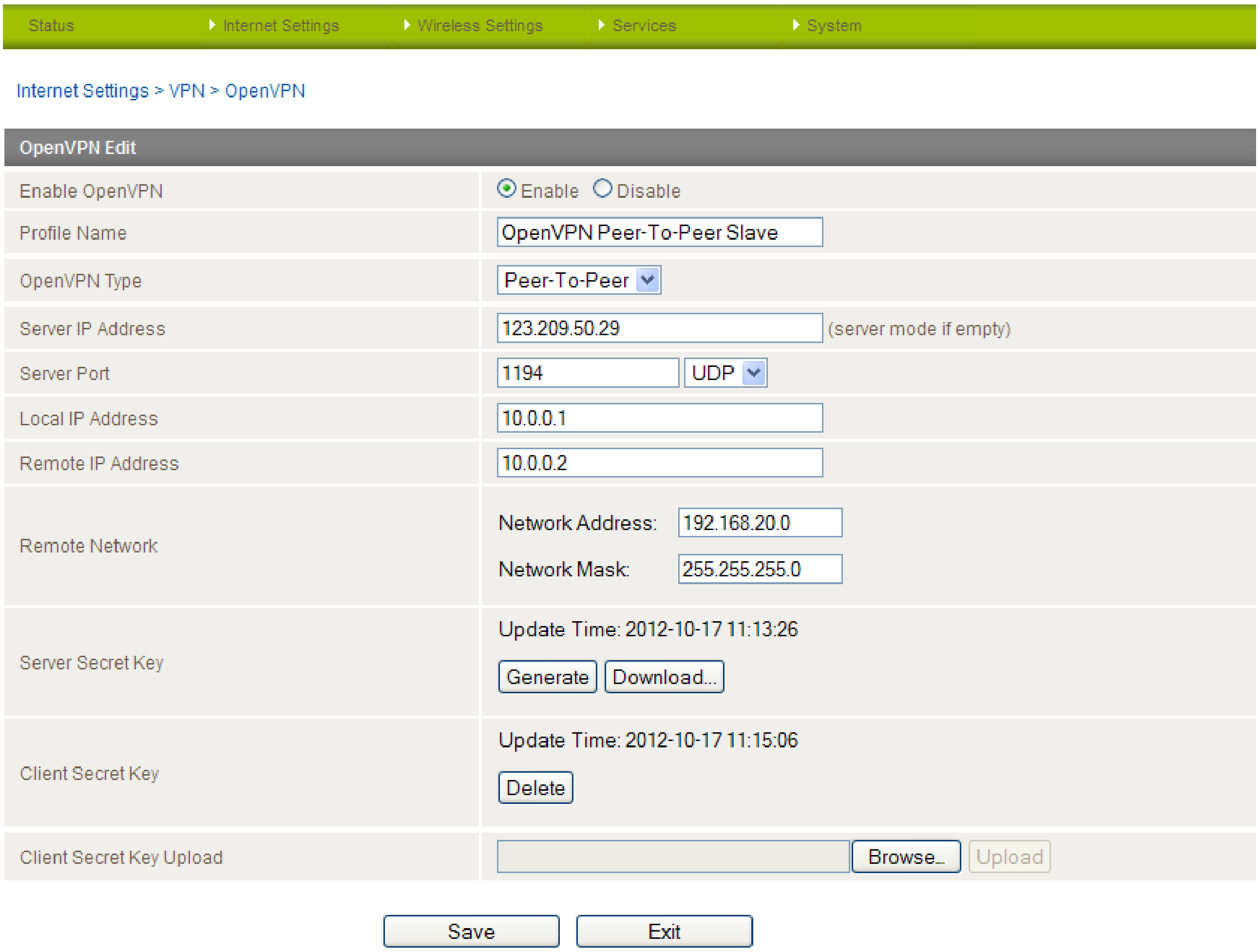


OpenVPN Edit

| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | OpenVPN Peer-To-Peer Master |
| OpenVPN Type | Peer-To-Peer |
| Server IP Address | (server mode if empty) |
| Server Port | 1194 UDP |
| Local IP Address | 10.0.0.2 |
| Remote IP Address | 10.0.0.1 |
| Remote Network | Network Address: 192.168.1.0<br>Network Mask: 255.255.255.0 |
| Server Secret Key | Update Time: 2012-10-17 11:13:20 |
| Client Secret Key | Update Time: 2012-10-17 11:16:15 |
| Client Secret Key Upload | |

Figure 18 - OpenVPN Peer-To-Peer Master Example

OpenVPN Peer-To-Peer Slave



Internet Settings > VPN > OpenVPN

**OpenVPN Edit**

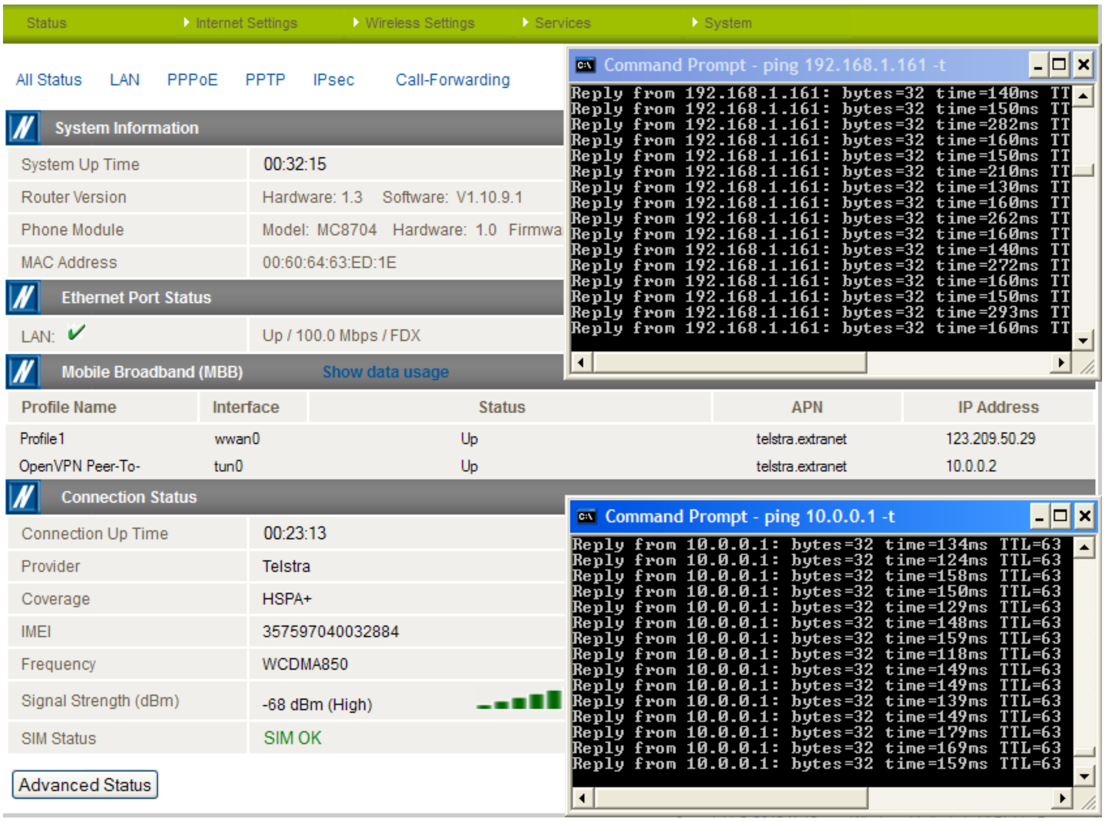
| | |
|---|---|
| Enable OpenVPN | ● Enable ○ Disable |
| Profile Name | OpenVPN Peer-To-Peer Slave |
| OpenVPN Type | Peer-To-Peer |
| Server IP Address | 123.209.50.29 (server mode if empty) |
| Server Port | 1194 UDP |
| Local IP Address | 10.0.0.1 |
| Remote IP Address | 10.0.0.2 |
| Remote Network | Network Address: 192.168.20.0<br>Network Mask: 255.255.255.0 |
| Server Secret Key | Update Time: 2012-10-17 11:13:26<br>Generate Download... |
| Client Secret Key | Update Time: 2012-10-17 11:15:06<br>Delete |
| Client Secret Key Upload | Browse... Upload |

Figure 19 - OpenVPN Peer-To-Peer Slave Example

## Verifying the OpenVPN Peer-To-Peer Connection Status

Open a command prompt on either the master or the slave and ping the OpenVPN Gateway address assigned to the remote router. See the screenshots below for an example.

### OpenVPN Peer-To-Peer Master



System Information

| | |
|---|---|
| System Up Time | 00:32:15 |
| Router Version | Hardware: 1.3 Software: V1.10.9.1 |
| Phone Module | Model: MC8704 Hardware: 1.0 Firmwa |
| MAC Address | 00:60:64:63:ED:1E |

Ethernet Port Status

| | |
|---|---|
| LAN: ✓ | Up / 100.0 Mbps / FDX |

Mobile Broadband (MBB) Show data usage

| Profile Name | Interface | Status | APN | IP Address |
|---|---|---|---|---|
| Profile1 | wwan0 | Up | telstra.extranet | 123.209.50.29 |
| OpenVPN Peer-To- | tun0 | Up | telstra.extranet | 10.0.0.2 |

Connection Status

| | |
|---|---|
| Connection Up Time | 00:23:13 |
| Provider | Telstra |
| Coverage | HSPA+ |
| IMEI | 357597040032884 |
| Frequency | WCDMA850 |
| Signal Strength (dBm) | -68 dBm (High) |
| SIM Status | SIM OK |

Command Prompt - ping 192.168.1.161 -t

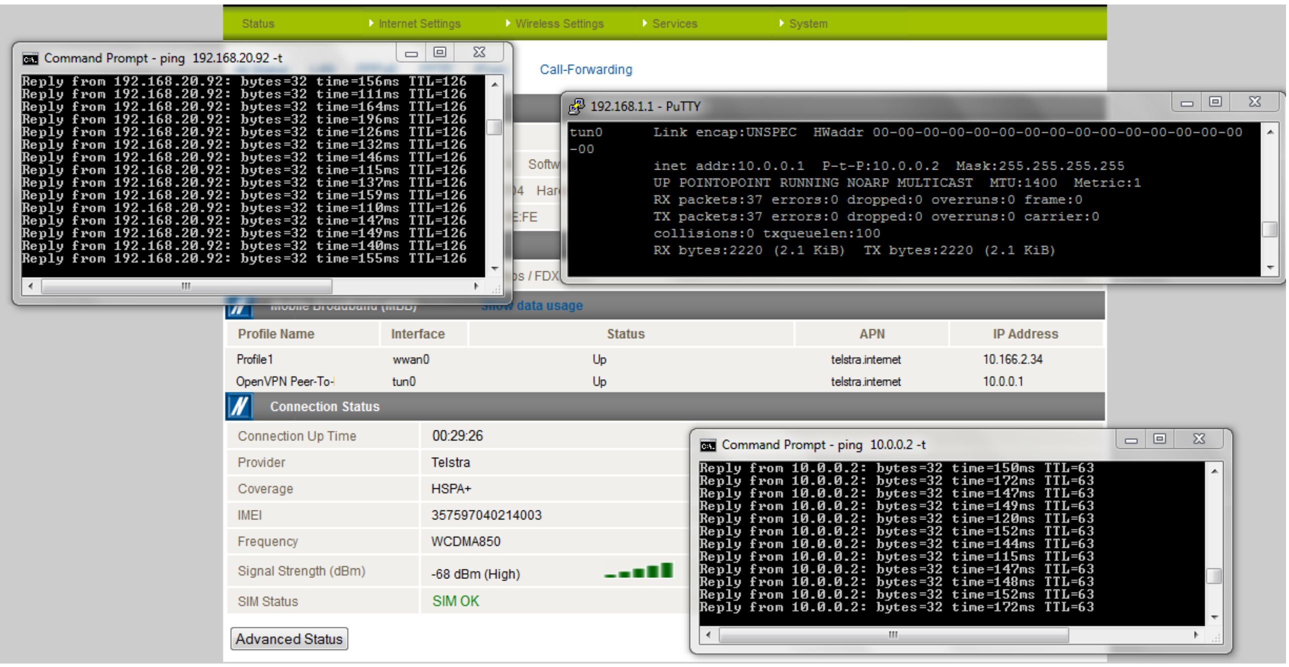
```
Reply from 192.168.1.161: bytes=32 time=140ms TT
Reply from 192.168.1.161: bytes=32 time=150ms TT
Reply from 192.168.1.161: bytes=32 time=282ms TT
Reply from 192.168.1.161: bytes=32 time=160ms TT
Reply from 192.168.1.161: bytes=32 time=150ms TT
Reply from 192.168.1.161: bytes=32 time=210ms TT
Reply from 192.168.1.161: bytes=32 time=130ms TT
Reply from 192.168.1.161: bytes=32 time=160ms TT
Reply from 192.168.1.161: bytes=32 time=262ms TT
Reply from 192.168.1.161: bytes=32 time=160ms TT
Reply from 192.168.1.161: bytes=32 time=140ms TT
Reply from 192.168.1.161: bytes=32 time=272ms TT
Reply from 192.168.1.161: bytes=32 time=160ms TT
Reply from 192.168.1.161: bytes=32 time=150ms TT
Reply from 192.168.1.161: bytes=32 time=293ms TT
Reply from 192.168.1.161: bytes=32 time=160ms TT
```

Command Prompt - ping 10.0.0.1 -t

```
Reply from 10.0.0.1: bytes=32 time=134ms TTL=63
Reply from 10.0.0.1: bytes=32 time=124ms TTL=63
Reply from 10.0.0.1: bytes=32 time=158ms TTL=63
Reply from 10.0.0.1: bytes=32 time=150ms TTL=63
Reply from 10.0.0.1: bytes=32 time=129ms TTL=63
Reply from 10.0.0.1: bytes=32 time=148ms TTL=63
Reply from 10.0.0.1: bytes=32 time=159ms TTL=63
Reply from 10.0.0.1: bytes=32 time=118ms TTL=63
Reply from 10.0.0.1: bytes=32 time=149ms TTL=63
Reply from 10.0.0.1: bytes=32 time=149ms TTL=63
Reply from 10.0.0.1: bytes=32 time=139ms TTL=63
Reply from 10.0.0.1: bytes=32 time=149ms TTL=63
Reply from 10.0.0.1: bytes=32 time=179ms TTL=63
Reply from 10.0.0.1: bytes=32 time=169ms TTL=63
Reply from 10.0.0.1: bytes=32 time=159ms TTL=63
```

Figure 20 - OpenVPN Peer-To-Peer Master connection verification

### OpenVPN Peer-To-Peer Slave



Command Prompt - ping 192.168.20.92 -t

```
Reply from 192.168.20.92: bytes=32 time=156ms TTL=126
Reply from 192.168.20.92: bytes=32 time=111ms TTL=126
Reply from 192.168.20.92: bytes=32 time=164ms TTL=126
Reply from 192.168.20.92: bytes=32 time=196ms TTL=126
Reply from 192.168.20.92: bytes=32 time=126ms TTL=126
Reply from 192.168.20.92: bytes=32 time=132ms TTL=126
Reply from 192.168.20.92: bytes=32 time=146ms TTL=126
Reply from 192.168.20.92: bytes=32 time=115ms TTL=126
Reply from 192.168.20.92: bytes=32 time=137ms TTL=126
Reply from 192.168.20.92: bytes=32 time=159ms TTL=126
Reply from 192.168.20.92: bytes=32 time=110ms TTL=126
Reply from 192.168.20.92: bytes=32 time=147ms TTL=126
Reply from 192.168.20.92: bytes=32 time=149ms TTL=126
Reply from 192.168.20.92: bytes=32 time=140ms TTL=126
Reply from 192.168.20.92: bytes=32 time=155ms TTL=126
```

192.168.1.1 - PuTTY

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.0.0.1  P-t-P:10.0.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1400  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:37 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2220 (2.1 KiB)  TX bytes:2220 (2.1 KiB)
```

Mobile Broadband (MBB) Show data usage

| Profile Name | Interface | Status | APN | IP Address |
|---|---|---|---|---|
| Profile1 | wwan0 | Up | telstra.internet | 10.166.2.34 |
| OpenVPN Peer-To- | tun0 | Up | telstra.internet | 10.0.0.1 |

Connection Status

| | |
|---|---|
| Connection Up Time | 00:29:26 |
| Provider | Telstra |
| Coverage | HSPA+ |
| IMEI | 357597040214003 |
| Frequency | WCDMA850 |
| Signal Strength (dBm) | -68 dBm (High) |
| SIM Status | SIM OK |

Command Prompt - ping 10.0.0.2 -t

```
Reply from 10.0.0.2: bytes=32 time=150ms TTL=63
Reply from 10.0.0.2: bytes=32 time=172ms TTL=63
Reply from 10.0.0.2: bytes=32 time=147ms TTL=63
Reply from 10.0.0.2: bytes=32 time=149ms TTL=63
Reply from 10.0.0.2: bytes=32 time=120ms TTL=63
Reply from 10.0.0.2: bytes=32 time=152ms TTL=63
Reply from 10.0.0.2: bytes=32 time=144ms TTL=63
Reply from 10.0.0.2: bytes=32 time=115ms TTL=63
Reply from 10.0.0.2: bytes=32 time=147ms TTL=63
Reply from 10.0.0.2: bytes=32 time=148ms TTL=63
Reply from 10.0.0.2: bytes=32 time=152ms TTL=63
Reply from 10.0.0.2: bytes=32 time=172ms TTL=63
```

Figure 21 - OpenVPN Peer-To-Peer Slave connection verification