NetCommWireless

OpenVPN
Technical Support Guide

Copyright

⚠ **Please note:** This document is subject to change without notice.

DOCUMENT VERSION	DATE
1.0 - Initial document release	7 December, 2015

Table 1 - Document Revision History

Table of Contents

Applicable devices

This document is applicable to the following NetComm Wireless devices:

- NTC-6908
- NTC-6908-02
- NTC-6520
- NTC-6200
- NTC-30WV
- NTC-30WV-02
- NTC-40WV
- NTC-140W
- NWL-11
- NWL-15
- NWL-25

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.

NetComm Wireless M2M 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 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 considered 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:

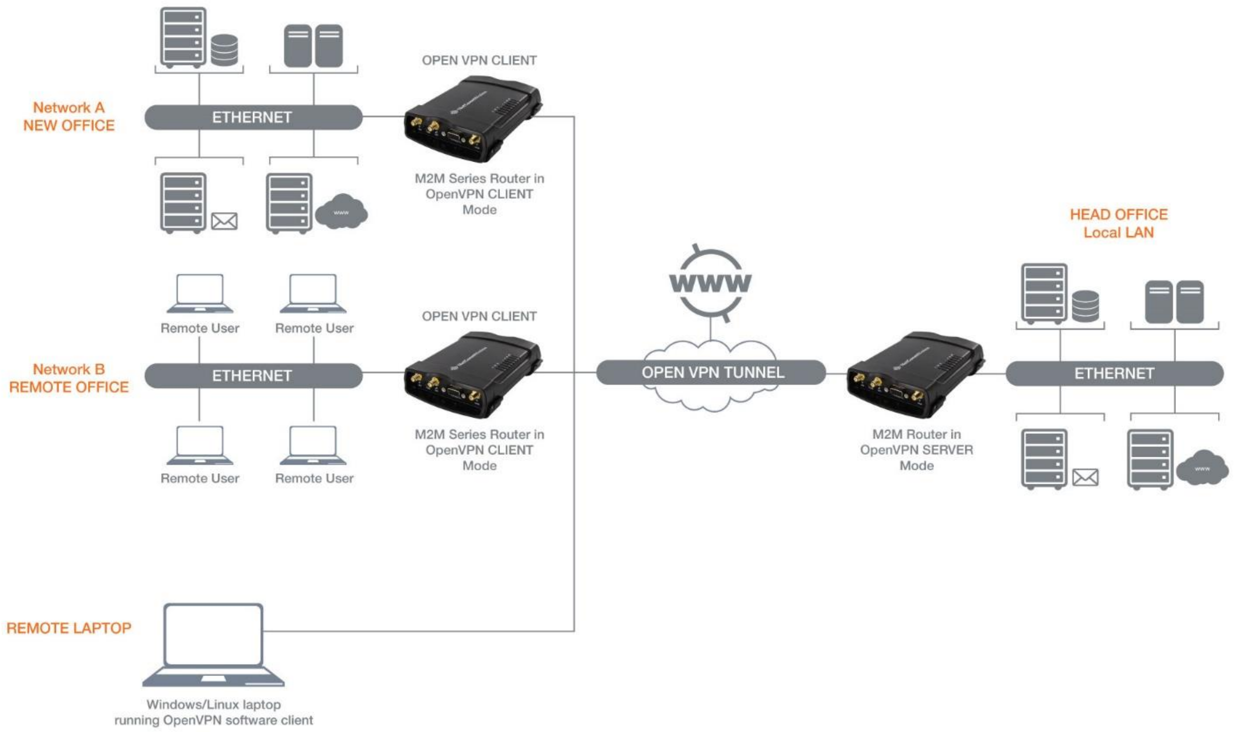
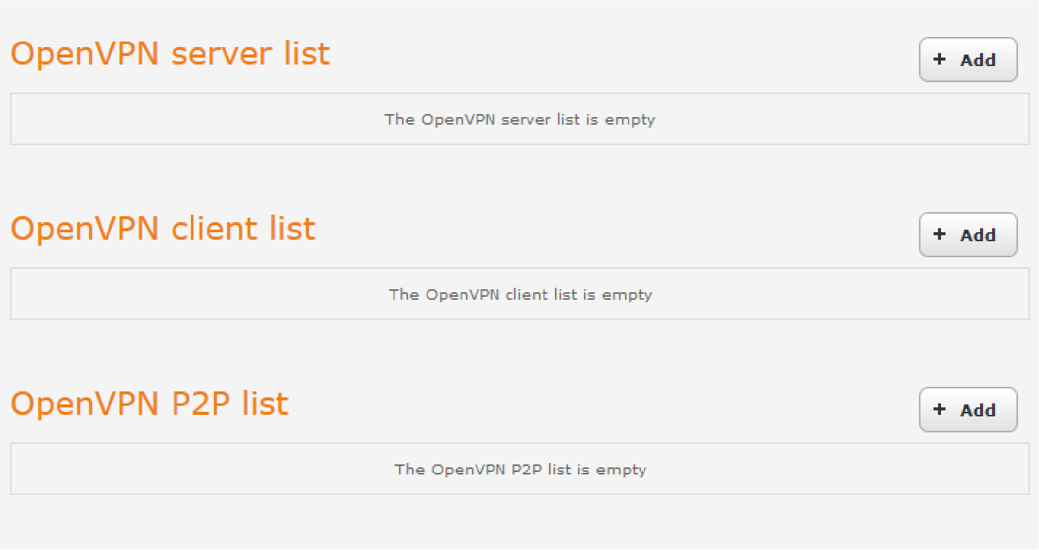


Figure 1 - OpenVPN Server Mode Diagram

Configuring an OpenVPN Server

1. Log in to your NetComm Wireless M2M router using the “root” account. Refer to your device’s User Guide for further details performing this.
2. Click on **Networking**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



OpenVPN server list

+ Add

The OpenVPN server list is empty

OpenVPN client list

+ Add

The OpenVPN client list is empty

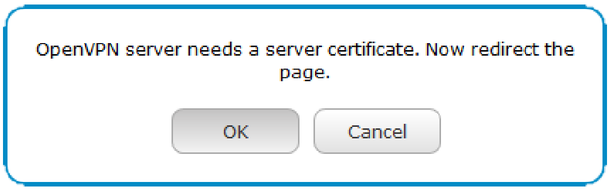
OpenVPN P2P list

+ Add

The OpenVPN P2P list is empty

Figure 2 - OpenVPN List

3. Next to **OpenVPN server list**, click the **+Add** button. If you have not yet generated a server certificate, the following message is displayed:

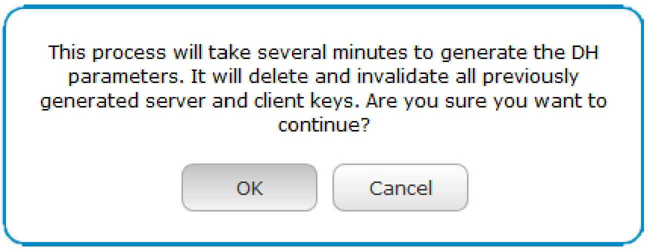


OpenVPN server needs a server certificate. Now redirect the page.

Figure 3 - Server certificate prompt

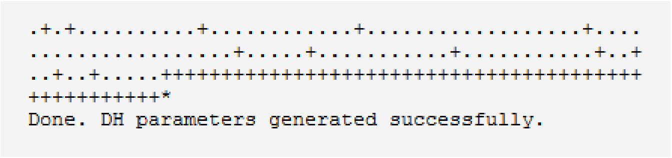
Click the **OK** button. If you have already generated a server certificate, you may skip to step 7.

4. Next to Diffie-Hellman parameters, click the **Generate** button. The following dialog is displayed.



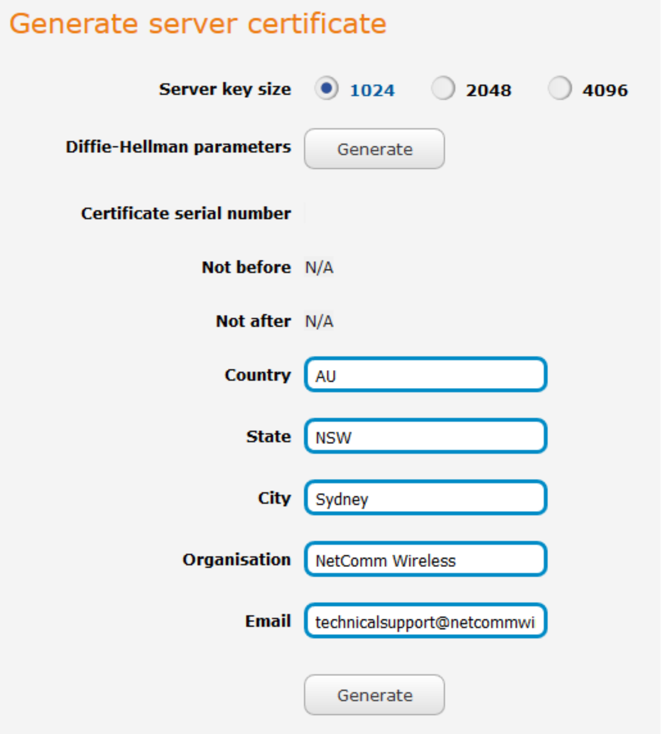
This process will take several minutes to generate the DH parameters. It will delete and invalidate all previously generated server and client keys. Are you sure you want to continue?

Click the **OK** button. The Diffie-Hellman parameters are generated. When complete the bottom section of the screen shows the following.



```
.+.+..........+............+..................+....
.................+.....+...........+...........+..+
..+..+.....++++++++++++++++++++++++++++++++++++++++
+++++++++++*
Done. DH parameters generated successfully.
```

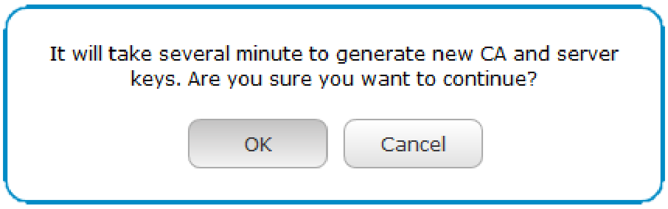
5. Enter the details in the fields provided to create a certificate for this router then click the Generate button at the bottom of the screen.



Generate server certificate

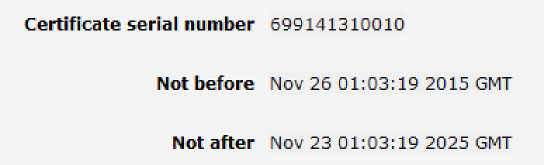
Server key size	● 1024 ○ 2048 ○ 4096
Diffie-Hellman parameters	Generate
Certificate serial number	
Not before	N/A
Not after	N/A
Country	AU
State	NSW
City	Sydney
Organisation	NetComm Wireless
Email	technicalsupport@netcommwi

The router displays a warning that the keys will take a few minutes to generate. Click the **OK** button.



It will take several minute to generate new CA and server keys. Are you sure you want to continue?

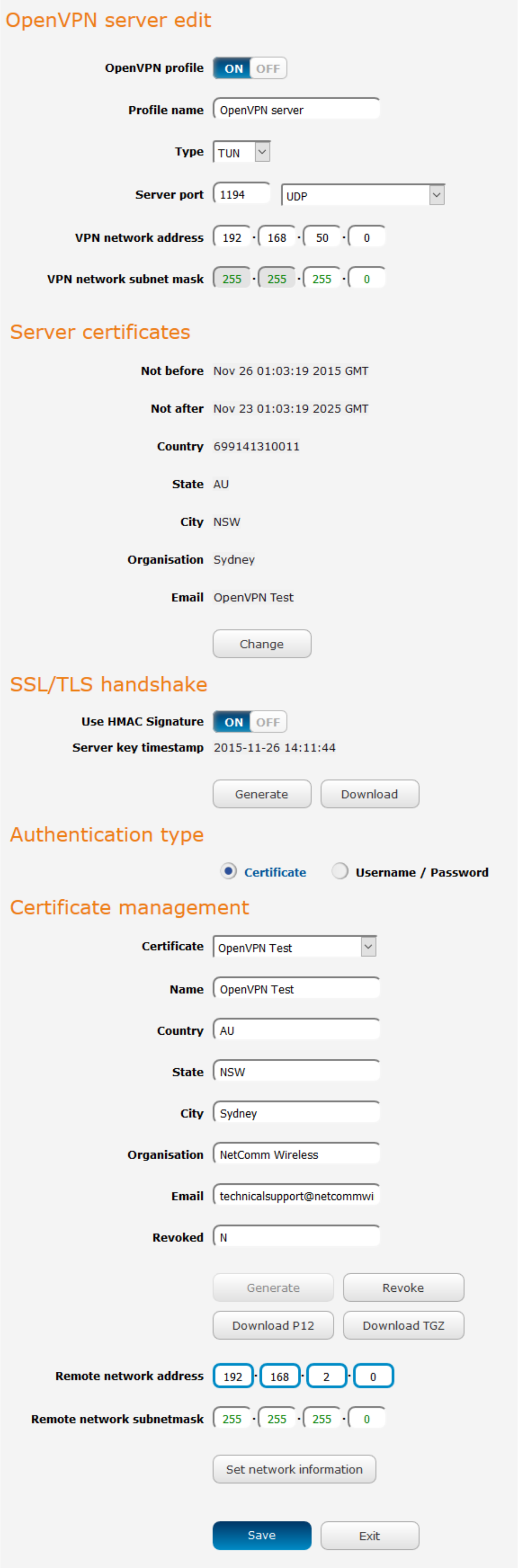
When it is complete, a certificate serial number and expiry date appear above the certificate fields.



Certificate serial number	699141310010
Not before	Nov 26 01:03:19 2015 GMT
Not after	Nov 23 01:03:19 2025 GMT

6. Navigate to the OpenVPN page again (**Networking -> VPN -> OpenVPN**)

7. Under OpenVPN server, click on the **Add** button. The **OpenVPN server edit** page is displayed.



OpenVPN server edit

OpenVPN profile	ON
Profile name	OpenVPN server
Type	TUN
Server port	1194 · UDP
VPN network address	192 . 168 . 50 . 0
VPN network subnet mask	255 . 255 . 255 . 0

Server certificates

Not before	Nov 26 01:03:19 2015 GMT
Not after	Nov 23 01:03:19 2025 GMT
Country	699141310011
State	AU
City	NSW
Organisation	Sydney
Email	OpenVPN Test

SSL/TLS handshake

Use HMAC Signature	ON
Server key timestamp	2015-11-26 14:11:44

Authentication type

● Certificate ○ Username / Password

Certificate management

Certificate	OpenVPN Test
Name	OpenVPN Test
Country	AU
State	NSW
City	Sydney
Organisation	NetComm Wireless
Email	technicalsupport@netcommwi
Revoked	N

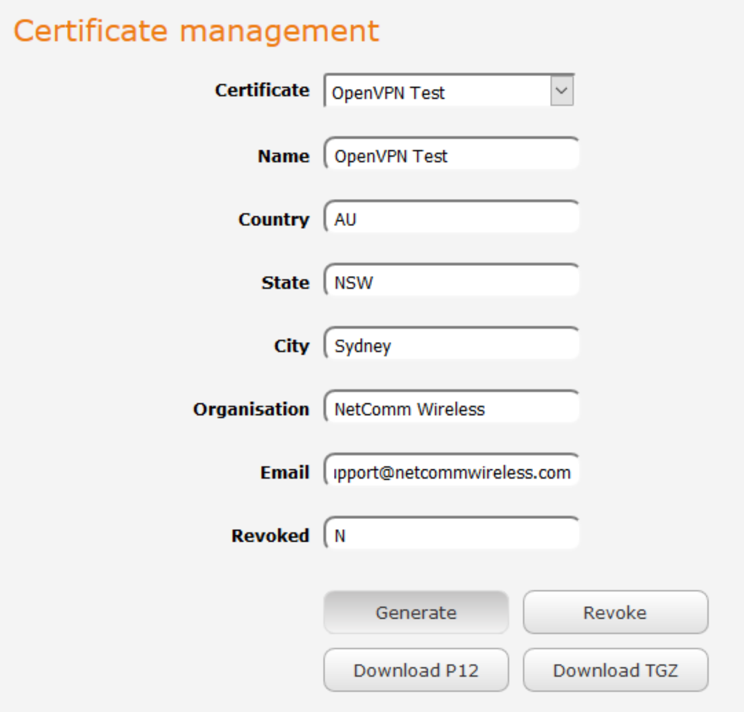
Remote network address	192 . 168 . 2 . 0
Remote network subnetmask	255 . 255 . 255 . 0

Figure 4 - OpenVPN Server configuration page

8. In the **Profile name** field, type a name for the OpenVPN Server profile you are creating.
9. From the **Type** drop down list, select whether to use **TUN** (tunnel) or **TAP** (virtual TAP interface). A TAP interface can be bridged with an Ethernet connection.
10. 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.
11. 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.
12. HMAC or Hash-based Message Authentication Code is a means of calculating a message authentication code through the use of a cryptographic hash function and a cryptographic key. If you wish to use the HMAC signature as an additional key and level of security, under the SSL/TLS handshake section, click the **Use HMAC Signature** toggle key so that it is in the **ON** position, then click the **Generate** button so that the router can randomly generate the key. The Server key timestamp field is updated with the time that the key was generated. Click the **Download** button to download the key file so that it can be uploaded on the client.
13. 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	OpenVPN Test
Name	OpenVPN Test
Country	AU
State	NSW
City	Sydney
Organisation	NetComm Wireless
Email	ıpport@netcommwireless.com
Revoked	N

Figure 5 - OpenVPN Server - Certificate Management section

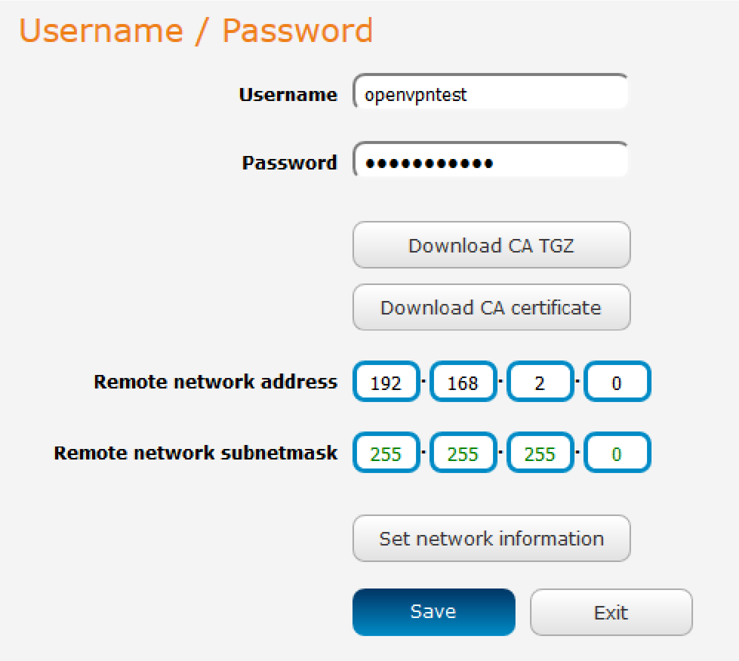
b) When it is done, you can click the **Download P12** or **Download TGZ** buttons to save the certificate file. You may select the format required by the remote router. NetComm Wireless routers support both formats. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the **Revoke** button to disable it.

c) 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** or **Download CA TGZ** button to save the certificate. Choose the format supported by your client router. NetComm Wireless routers support both formats.

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: openvpntest

Password: ●●●●●●●●●●●

Remote network address: 192 . 168 . 2 . 0

Remote network subnetmask: 255 . 255 . 255 . 0

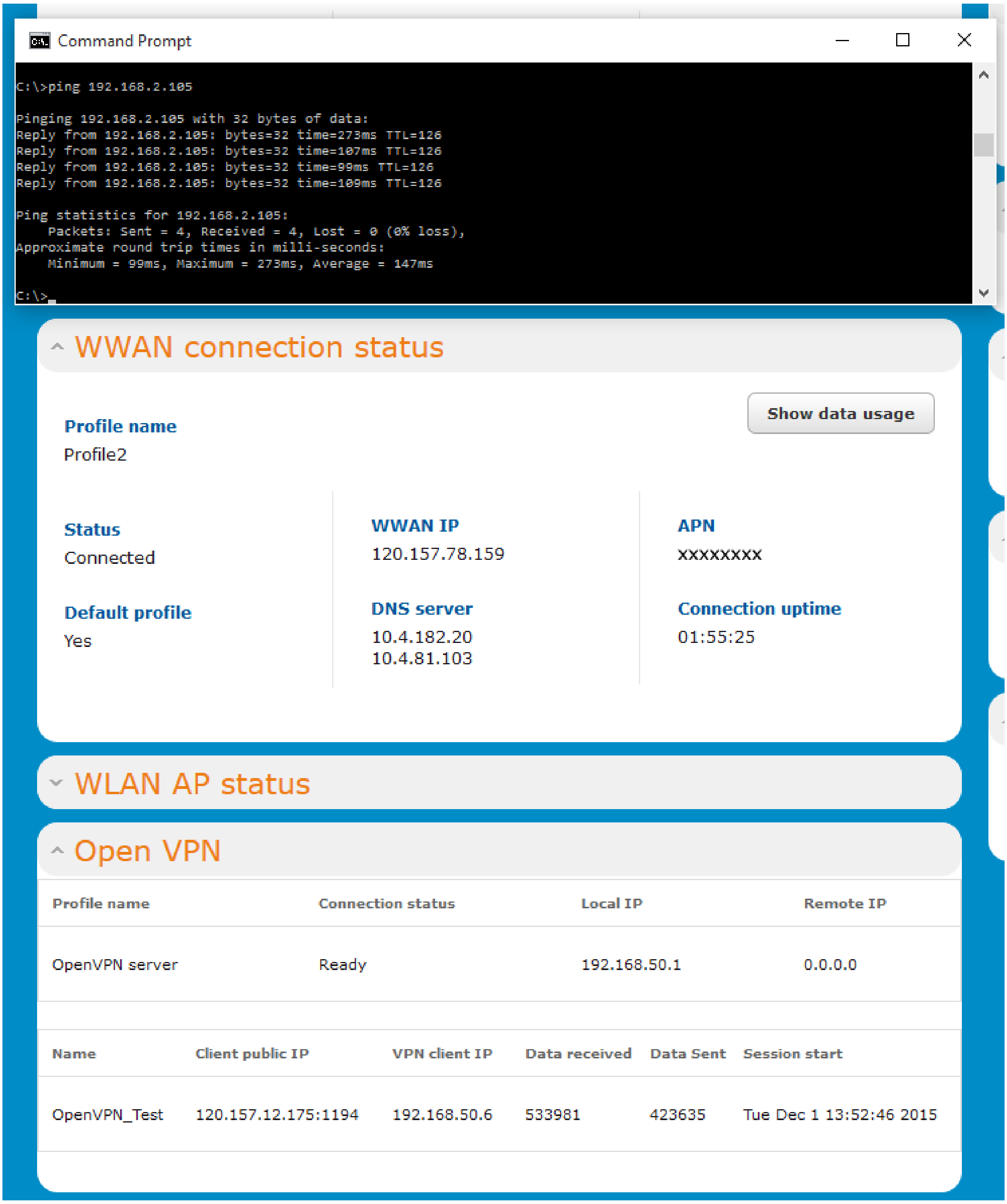
Figure 6 - OpenVPN Server - Username/Password section

b) 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.

14. 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 remote client IP address. See the screenshot below for an example.



```
C:\>ping 192.168.2.105

Pinging 192.168.2.105 with 32 bytes of data:
Reply from 192.168.2.105: bytes=32 time=273ms TTL=126
Reply from 192.168.2.105: bytes=32 time=107ms TTL=126
Reply from 192.168.2.105: bytes=32 time=99ms TTL=126
Reply from 192.168.2.105: bytes=32 time=109ms TTL=126

Ping statistics for 192.168.2.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 273ms, Average = 147ms

C:\>_
```

WWAN connection status

Profile name
Profile2

Status
Connected

Default profile
Yes

WWAN IP
120.157.78.159

DNS server
10.4.182.20
10.4.81.103

APN
xxxxxxxx

Connection uptime
01:55:25

WLAN AP status

Open VPN

Profile name	Connection status	Local IP	Remote IP
OpenVPN server	Ready	192.168.50.1	0.0.0.0

Name	Client public IP	VPN client IP	Data received	Data Sent	Session start
OpenVPN_Test	120.157.12.175:1194	192.168.50.6	533981	423635	Tue Dec 1 13:52:46 2015

Figure 7 - OpenVPN Server connection verification

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.

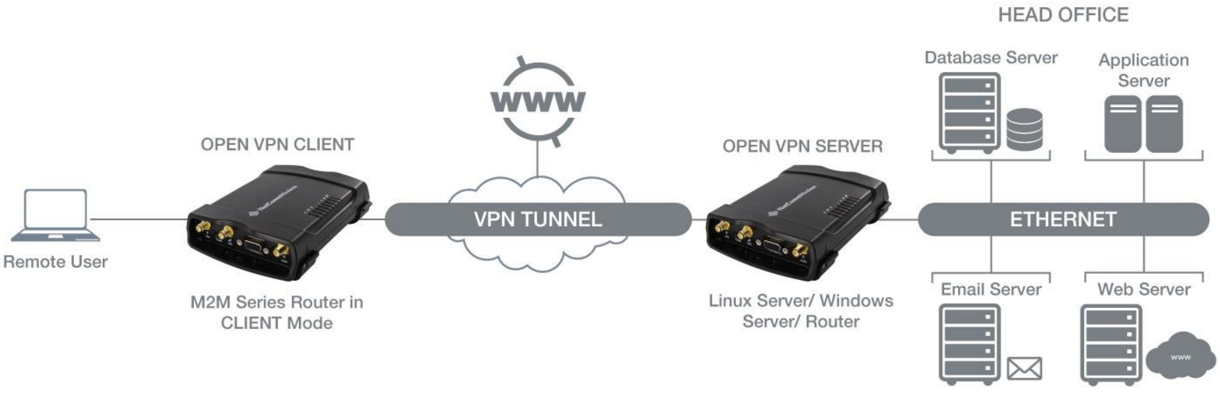


Figure 8 - OpenVPN Client Diagram

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.

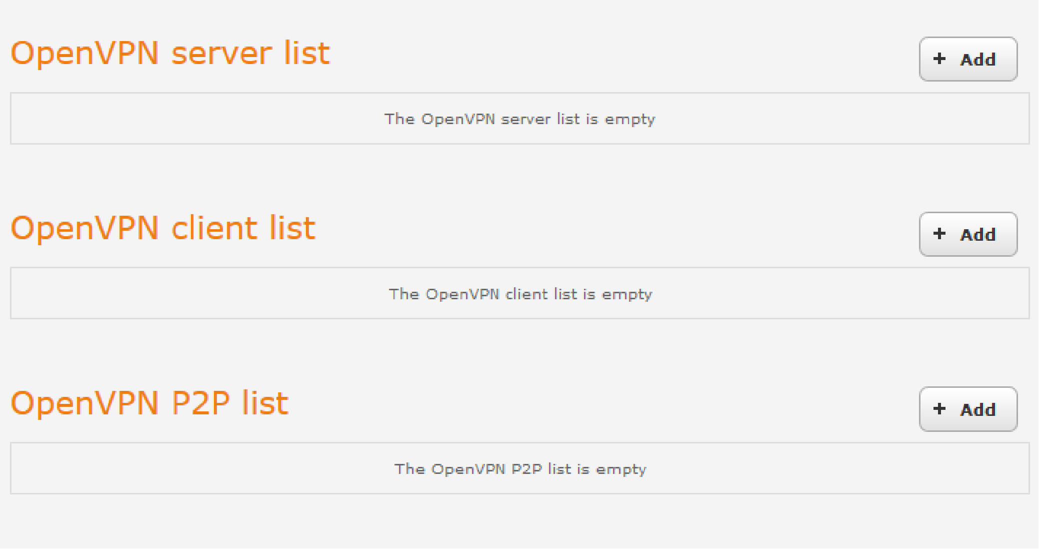
You can perform this in Linux by using the command:

```
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 **Networking**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



OpenVPN server list

The OpenVPN server list is empty

OpenVPN client list

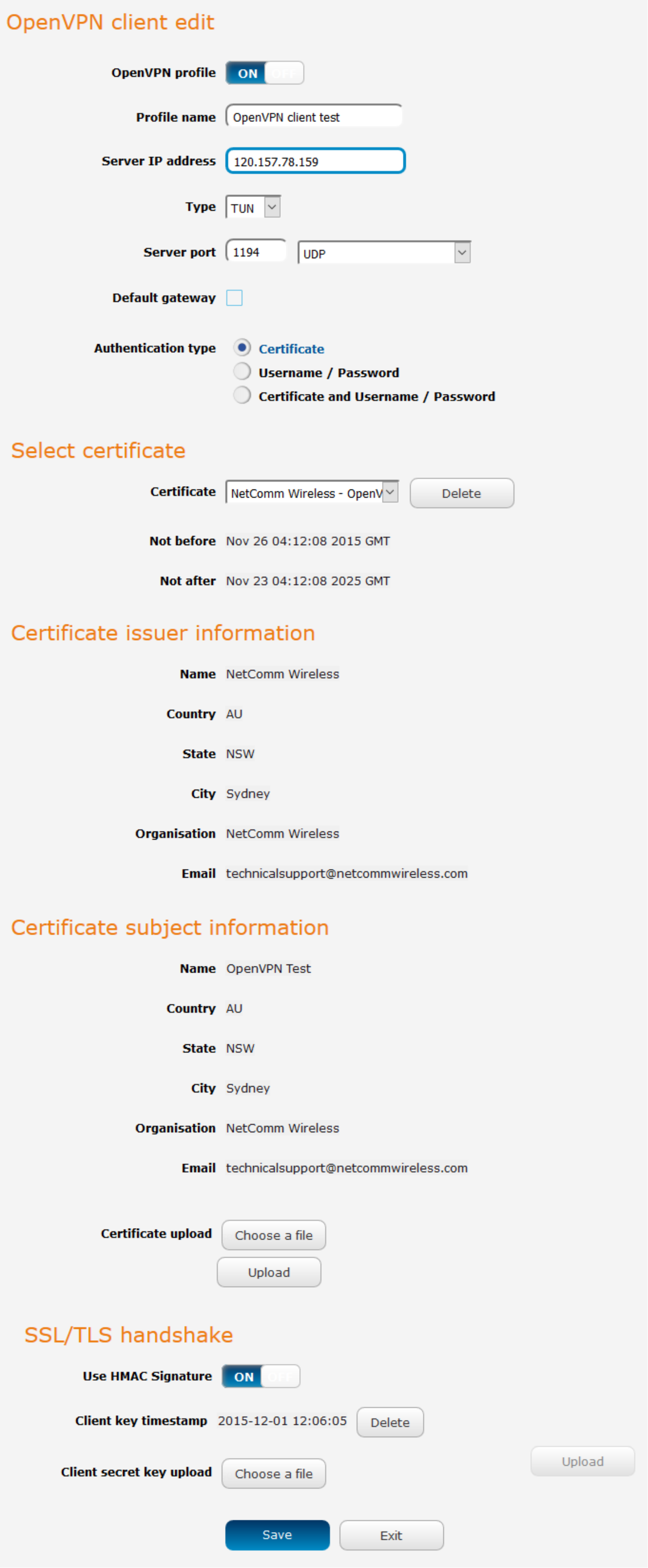
The OpenVPN client list is empty

OpenVPN P2P list

The OpenVPN P2P list is empty

Figure 9 - OpenVPN List

3. Next to **OpenVPN client list**, click the **+Add** button. The configuration window is displayed.



OpenVPN client edit

OpenVPN profile: ON

Profile name: OpenVPN client test

Server IP address: 120.157.78.159

Type: TUN

Server port: 1194 UDP

Default gateway: □

Authentication type:
- ● Certificate
- ○ Username / Password
- ○ Certificate and Username / Password

Select certificate

Certificate: NetComm Wireless - OpenV

Not before: Nov 26 04:12:08 2015 GMT

Not after: Nov 23 04:12:08 2025 GMT

Certificate issuer information

Name: NetComm Wireless

Country: AU

State: NSW

City: Sydney

Organisation: NetComm Wireless

Email: technicalsupport@netcommwireless.com

Certificate subject information

Name: OpenVPN Test

Country: AU

State: NSW

City: Sydney

Organisation: NetComm Wireless

Email: technicalsupport@netcommwireless.com

Certificate upload

SSL/TLS handshake

Use HMAC Signature: ON

Client key timestamp: 2015-12-01 12:06:05

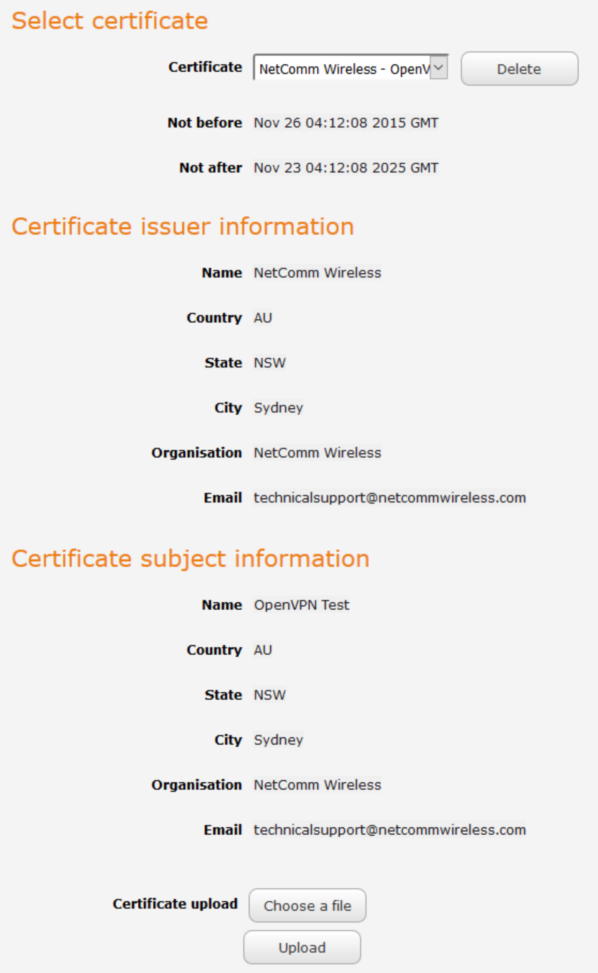
Client secret key upload

Figure 9 - OpenVPN Client - Configuration page

4. Set **OpenVPN profile** to **Enable.**
5. Type a name for the OpenVPN Client profile you are creating.
6. In the **Server IP address** field, type the WAN IP address of the OpenVPN Server.
7. From the **Type** drop down list, select **TUN** or **TAP**. TAP is used with Ethernet bridging. In this example, we have selected **TUN.**
8. Enter the **Server Port** and **packet type** to use for the connection.
9. If the "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 subject information** section at the bottom of the screen, click the **Choose a file / Browse** button and locate the certificate file you downloaded when you configured the OpenVPN Server. This may be either the P12 or TGZ file. When it has been selected, click the **Upload** button to send it to the router.



Select certificate

Certificate: NetComm Wireless - OpenV

Not before: Nov 26 04:12:08 2015 GMT

Not after: Nov 23 04:12:08 2025 GMT

Certificate issuer information

Name: NetComm Wireless

Country: AU

State: NSW

City: Sydney

Organisation: NetComm Wireless

Email: technicalsupport@netcommwireless.com

Certificate subject information

Name: OpenVPN Test

Country: AU

State: NSW

City: Sydney

Organisation: NetComm Wireless

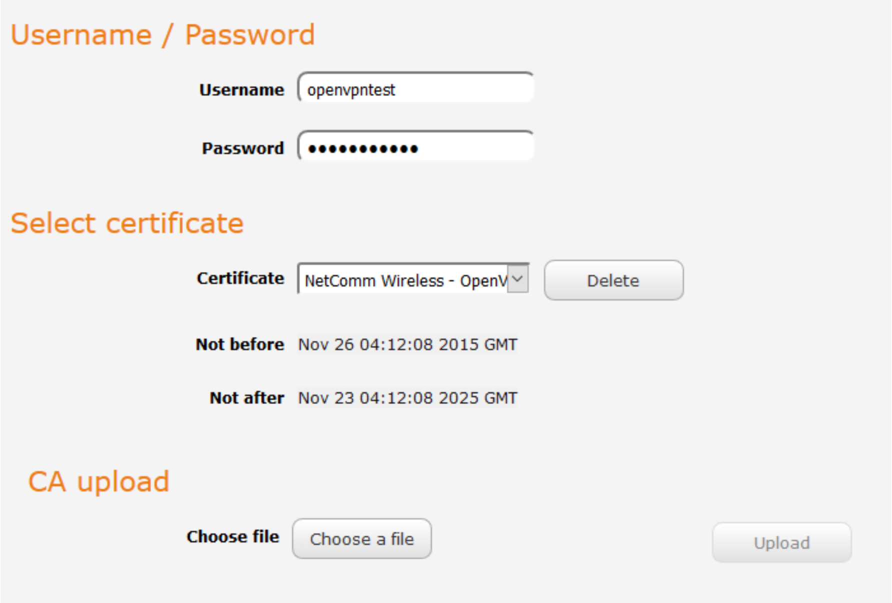
Email: technicalsupport@netcommwireless.com

Certificate upload

Figure 10 - OpenVPN Client - Certificate Authentication section

Username / Password Authentication

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



Username / Password

Username: openvpntest

Password: •••••••••••

Select certificate

Certificate: NetComm Wireless - OpenV

Not before: Nov 26 04:12:08 2015 GMT

Not after: Nov 23 04:12:08 2025 GMT

CA upload

Choose file

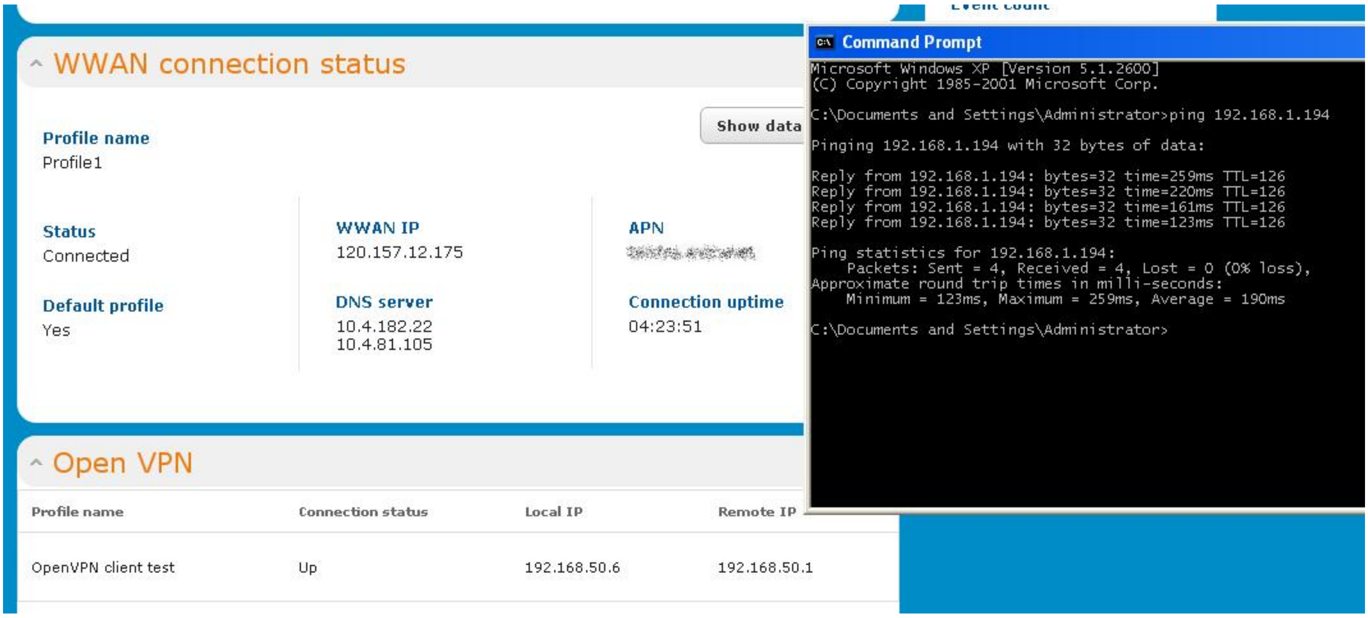
Figure 11 - OpenVPN Client - Username/Password section

b) Use the **Choose a file/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 a computer on the remote network. See the screenshot below for an example.



WWAN connection status

Profile name: Profile1

Status: Connected

WWAN IP: 120.157.12.175

APN: [redacted]

Default profile: Yes

DNS server: 10.4.182.22, 10.4.81.105

Connection uptime: 04:23:51

Open VPN

Profile name	Connection status	Local IP	Remote IP
OpenVPN client test	Up	192.168.50.6	192.168.50.1

Command Prompt

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.1.194

Pinging 192.168.1.194 with 32 bytes of data:

Reply from 192.168.1.194: bytes=32 time=259ms TTL=126
Reply from 192.168.1.194: bytes=32 time=220ms TTL=126
Reply from 192.168.1.194: bytes=32 time=161ms TTL=126
Reply from 192.168.1.194: bytes=32 time=123ms TTL=126

Ping statistics for 192.168.1.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 123ms, Maximum = 259ms, Average = 190ms

C:\Documents and Settings\Administrator>
```

Figure 12 - OpenVPN Client verification of connection

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.

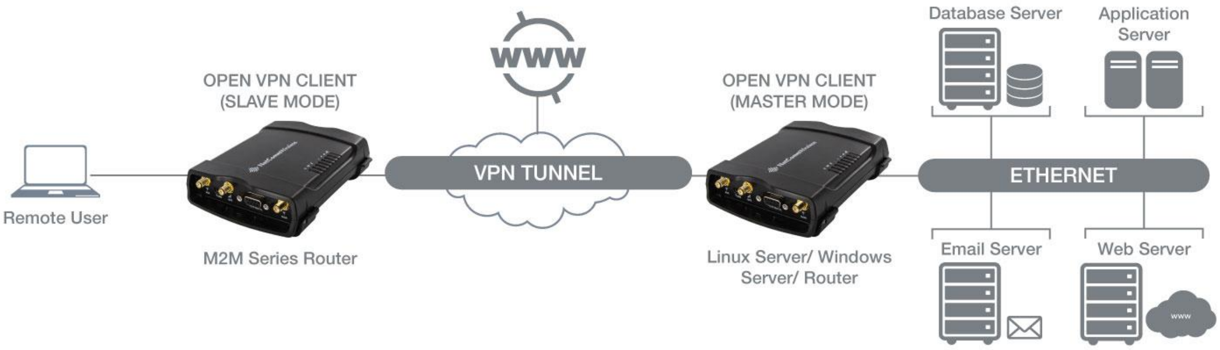
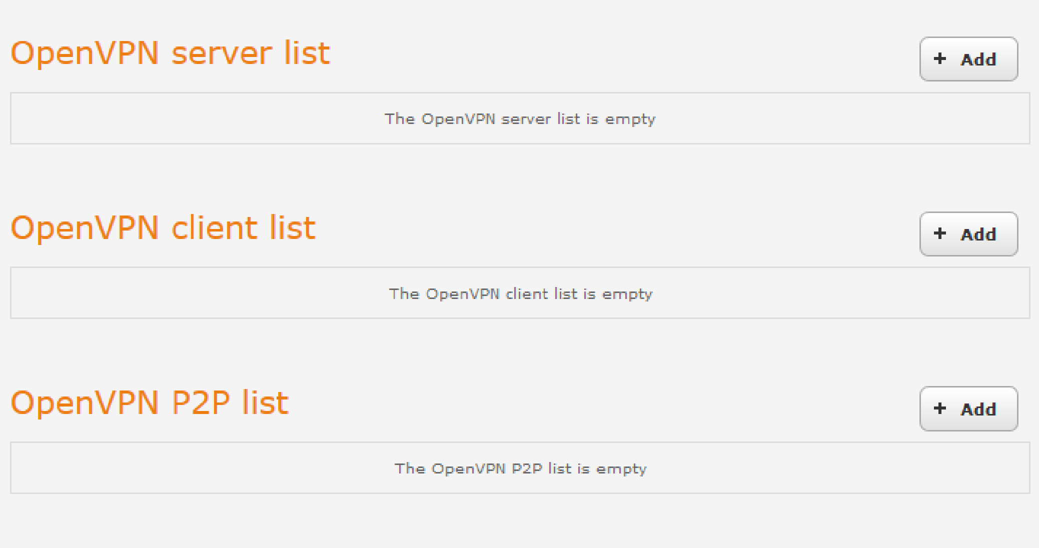


Figure 13 - OpenVPN Peer-To-Peer Mode Diagram

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 **Networking**, **VPN**, then **OpenVPN.** The OpenVPN List is displayed.



OpenVPN server list

+ Add

The OpenVPN server list is empty

OpenVPN client list

+ Add

The OpenVPN client list is empty

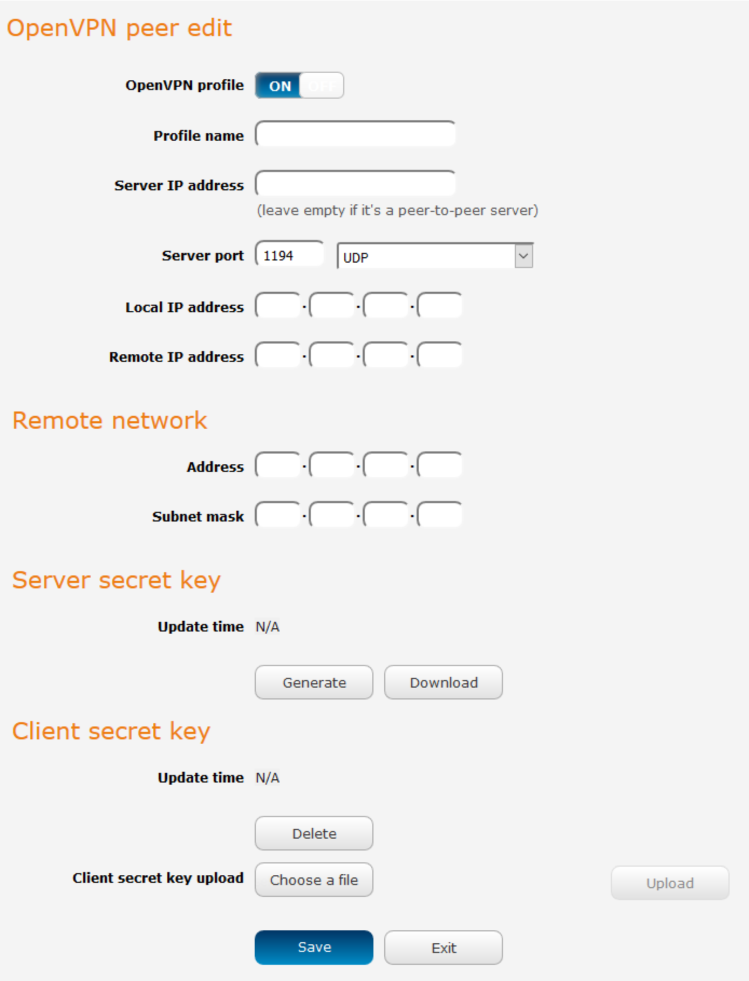
OpenVPN P2P list

+ Add

The OpenVPN P2P list is empty

Figure 14 - OpenVPN List

3. Next to **OpenVPN P2P list**, click the +**Add** button. The configuration window is displayed.



OpenVPN peer edit

OpenVPN profile: ON

Profile name:

Server IP address:
(leave empty if it's a peer-to-peer server)

Server port: 1194 UDP

Local IP address: . . .

Remote IP address: . . .

Remote network

Address: . . .

Subnet mask: . . .

Server secret key

Update time: N/A

Generate Download

Client secret key

Update time: N/A

Delete

Client secret key upload: Choose a file Upload

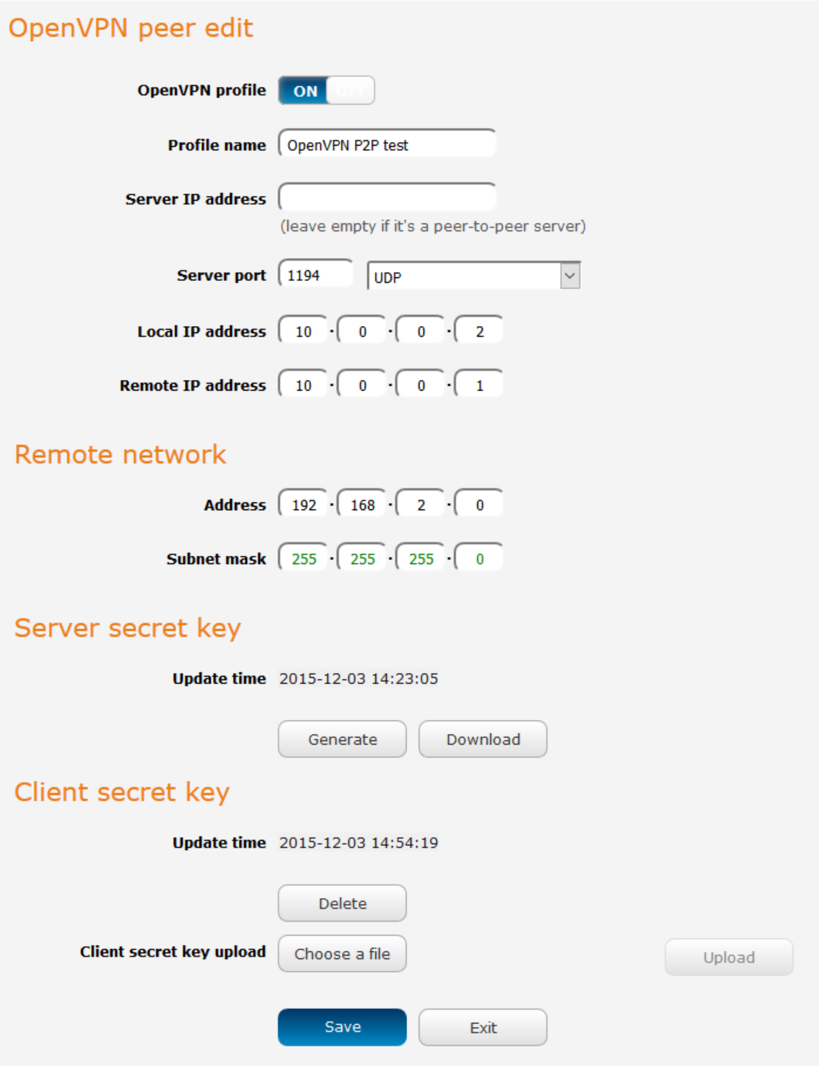
Save Exit

Figure 9 - OpenVPN Peer-To-Peer Mode

4. Set **OpenVPN profile** to **Enable.**
5. In the Profile name field, type a name for the OpenVPN Peer-To-Peer profile you are creating.
6. 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.
7. Enter the Server Port and packet type to use for the connection.
8. Enter the **Local IP address** and **Remote IP address** to use for the OpenVPN tunnel. The slave should have the reverse settings of the master.
9. Under the **Remote network** section, enter the **Network address** and **Subnet mask**. The Network address and Subnet mask fields inform the Master node of the LAN address scheme of the Slave.
10. Under the **Server secret key** section, 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.
11. 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.
12. 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 peer edit

OpenVPN profile: ON

Profile name: OpenVPN P2P test

Server IP address:

(leave empty if it's a peer-to-peer server)

Server port: 1194 UDP

Local IP address: 10 . 0 . 0 . 2

Remote IP address: 10 . 0 . 0 . 1

Remote network

Address: 192 . 168 . 2 . 0

Subnet mask: 255 . 255 . 255 . 0

Server secret key

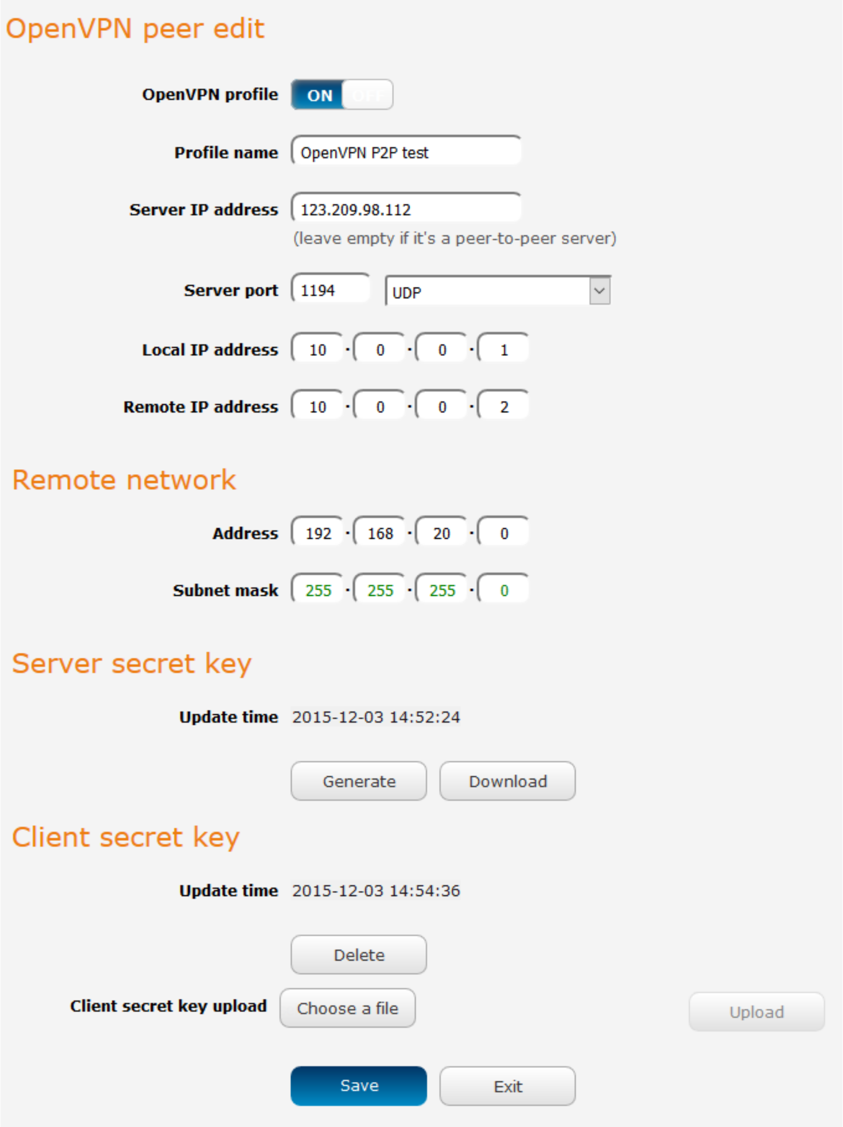
Update time: 2015-12-03 14:23:05

Client secret key

Update time: 2015-12-03 14:54:19

Figure 15 - OpenVPN Peer-To-Peer Master Example

OpenVPN Peer-To-Peer Slave



OpenVPN peer edit

OpenVPN profile	ON
Profile name	OpenVPN P2P test
Server IP address	123.209.98.112 (leave empty if it's a peer-to-peer server)
Server port	1194 UDP
Local IP address	10 . 0 . 0 . 1
Remote IP address	10 . 0 . 0 . 2

Remote network

Address	192 . 168 . 20 . 0
Subnet mask	255 . 255 . 255 . 0

Server secret key

Update time 2015-12-03 14:52:24

Client secret key

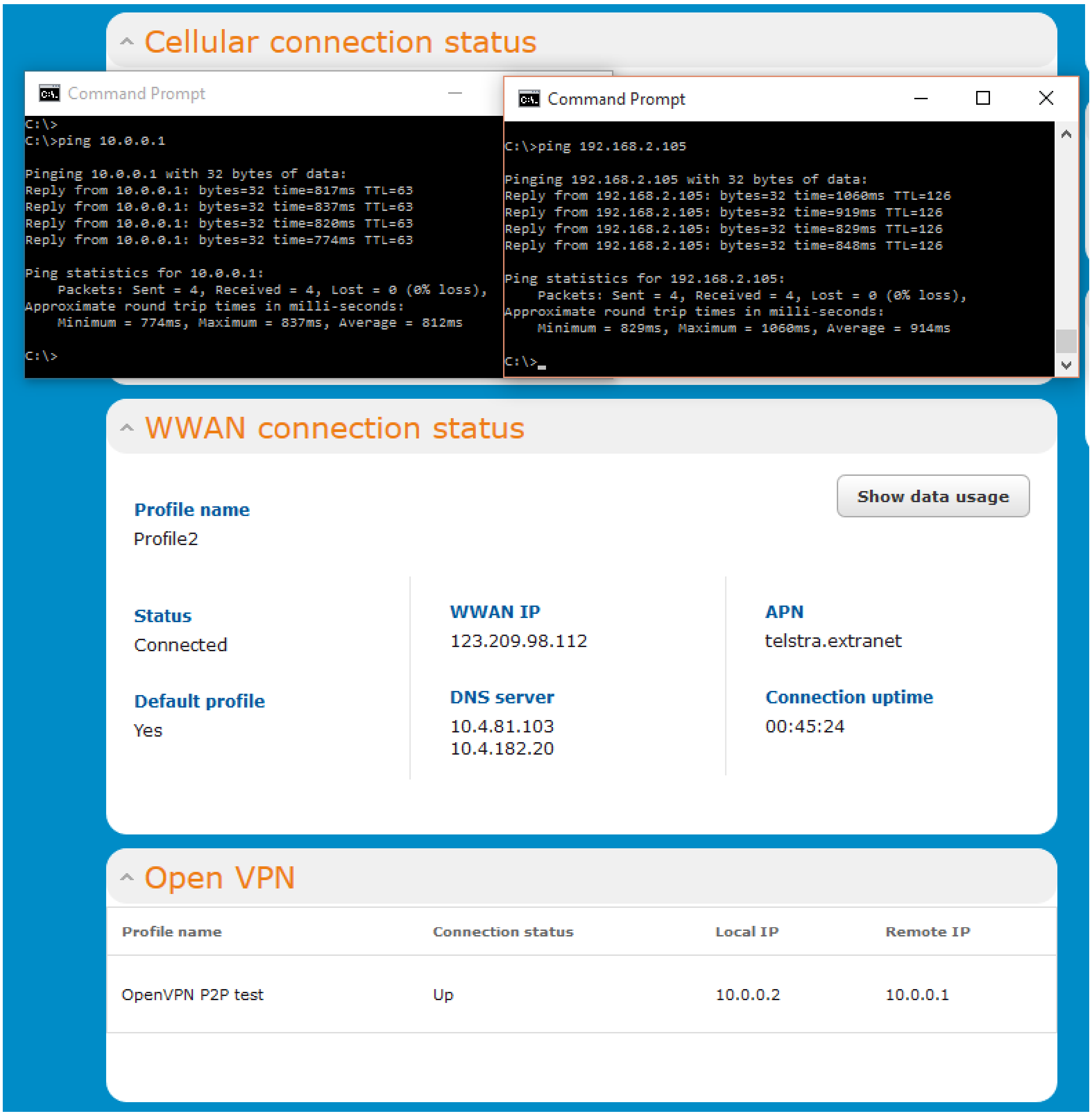
Update time 2015-12-03 14:54:36

Figure 16 - 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



Cellular connection status

Command Prompt

```
C:\>
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=817ms TTL=63
Reply from 10.0.0.1: bytes=32 time=837ms TTL=63
Reply from 10.0.0.1: bytes=32 time=820ms TTL=63
Reply from 10.0.0.1: bytes=32 time=774ms TTL=63

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 774ms, Maximum = 837ms, Average = 812ms

C:\>
```

Command Prompt

```
C:\>ping 192.168.2.105

Pinging 192.168.2.105 with 32 bytes of data:
Reply from 192.168.2.105: bytes=32 time=1060ms TTL=126
Reply from 192.168.2.105: bytes=32 time=919ms TTL=126
Reply from 192.168.2.105: bytes=32 time=829ms TTL=126
Reply from 192.168.2.105: bytes=32 time=848ms TTL=126

Ping statistics for 192.168.2.105:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 829ms, Maximum = 1060ms, Average = 914ms

C:\>_
```

WWAN connection status

Profile name
Profile2

Status
Connected

Default profile
Yes

WWAN IP
123.209.98.112

DNS server
10.4.81.103
10.4.182.20

APN
telstra.extranet

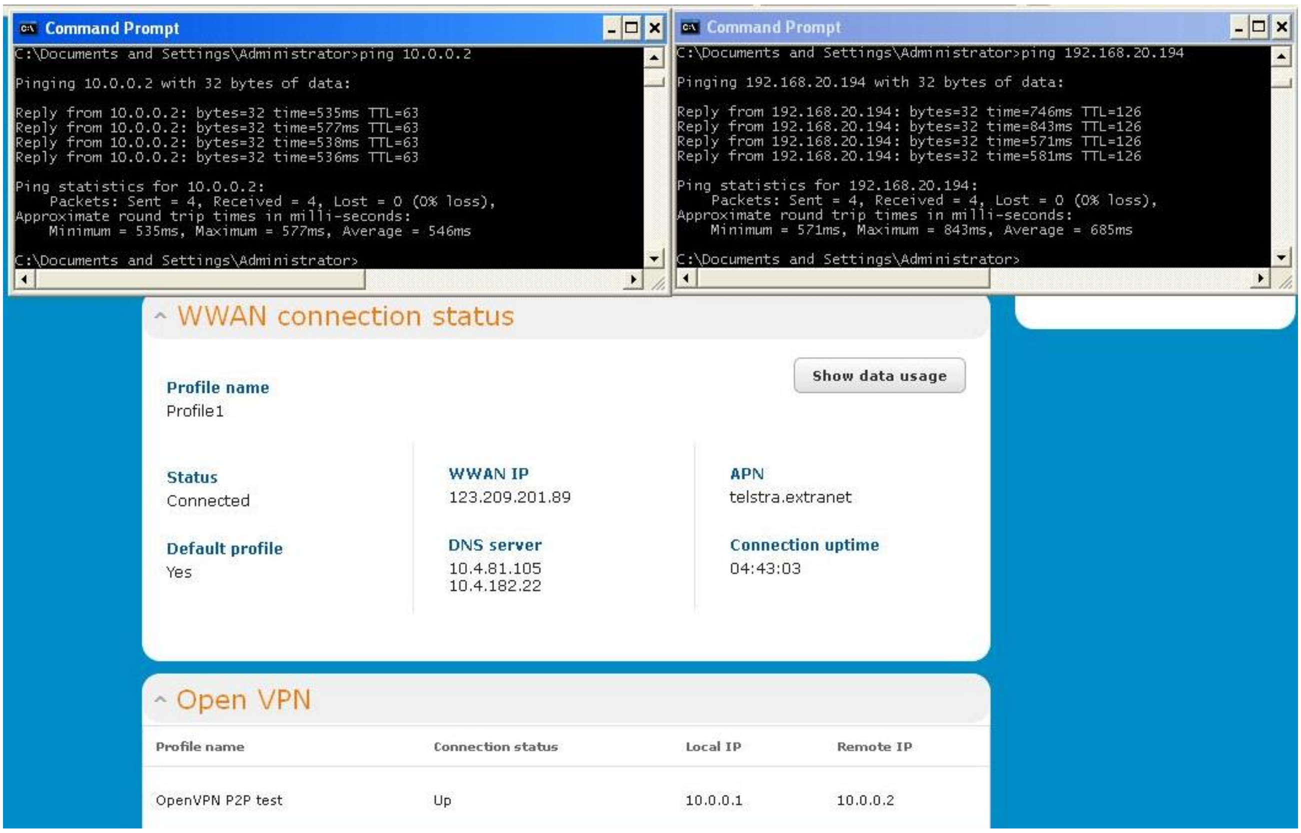
Connection uptime
00:45:24

Open VPN

Profile name	Connection status	Local IP	Remote IP
OpenVPN P2P test	Up	10.0.0.2	10.0.0.1

Figure 17 - OpenVPN Peer-To-Peer Master connection verification

OpenVPN Peer-To-Peer Slave



```
C:\Documents and Settings\Administrator>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=535ms TTL=63
Reply from 10.0.0.2: bytes=32 time=577ms TTL=63
Reply from 10.0.0.2: bytes=32 time=538ms TTL=63
Reply from 10.0.0.2: bytes=32 time=536ms TTL=63

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 535ms, Maximum = 577ms, Average = 546ms

C:\Documents and Settings\Administrator>
```

```
C:\Documents and Settings\Administrator>ping 192.168.20.194

Pinging 192.168.20.194 with 32 bytes of data:

Reply from 192.168.20.194: bytes=32 time=746ms TTL=126
Reply from 192.168.20.194: bytes=32 time=843ms TTL=126
Reply from 192.168.20.194: bytes=32 time=571ms TTL=126
Reply from 192.168.20.194: bytes=32 time=581ms TTL=126

Ping statistics for 192.168.20.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 571ms, Maximum = 843ms, Average = 685ms

C:\Documents and Settings\Administrator>
```

WWAN connection status

Profile name
Profile1

Status
Connected

Default profile
Yes

WWAN IP
123.209.201.89

DNS server
10.4.81.105
10.4.182.22

APN
telstra.extranet

Connection uptime
04:43:03

Open VPN

Profile name	Connection status	Local IP	Remote IP
OpenVPN P2P test	Up	10.0.0.1	10.0.0.2

Figure 18 - OpenVPN Peer-To-Peer Slave connection verification