# Vodafone MachineLink

## OpenVPN 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

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

# Contents

## Notation

The following symbols are used in this user guide:

⚠ The following note requires attention.

⚡ The following note provides a warning.

ℹ The following note provides useful information.

# 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.

The Vodafone MachineLink router supports 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. The Vodafone MachineLink router supports 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 the Vodafone MachineLink router.

## Important notes about OpenVPN on the Vodafone MachineLink router

- When using two MachineLink 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 MachineLink 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 MachineLink 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:

- A public and private key for the server and each client
- 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:

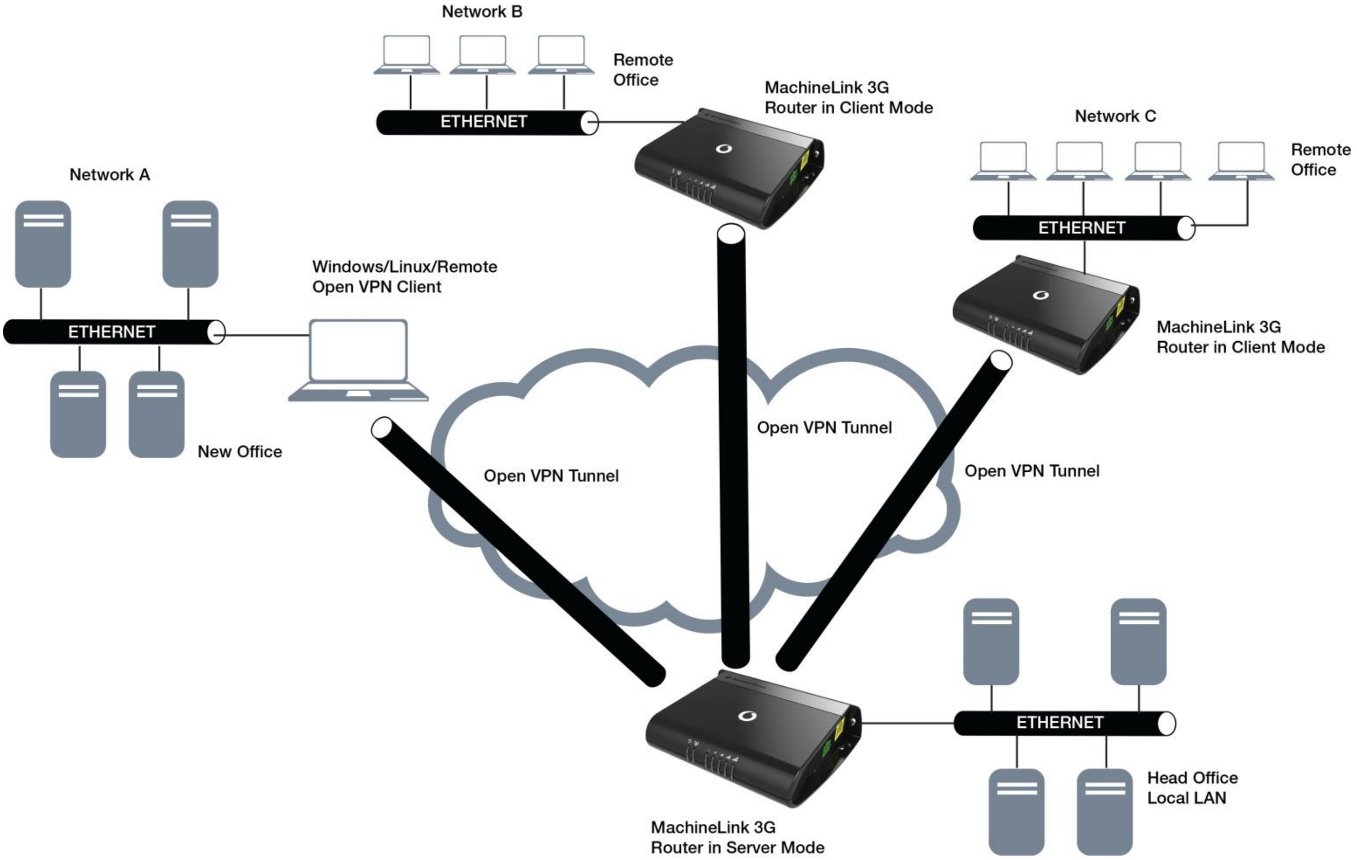


*Figure 1 - OpenVPN Server Mode Diagram*

# Configuring an OpenVPN Server

1 Login to your MachineLink router using the “root” account.

2 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **Open VPN** item.

3 The three types of OpenVPN lists are displayed.

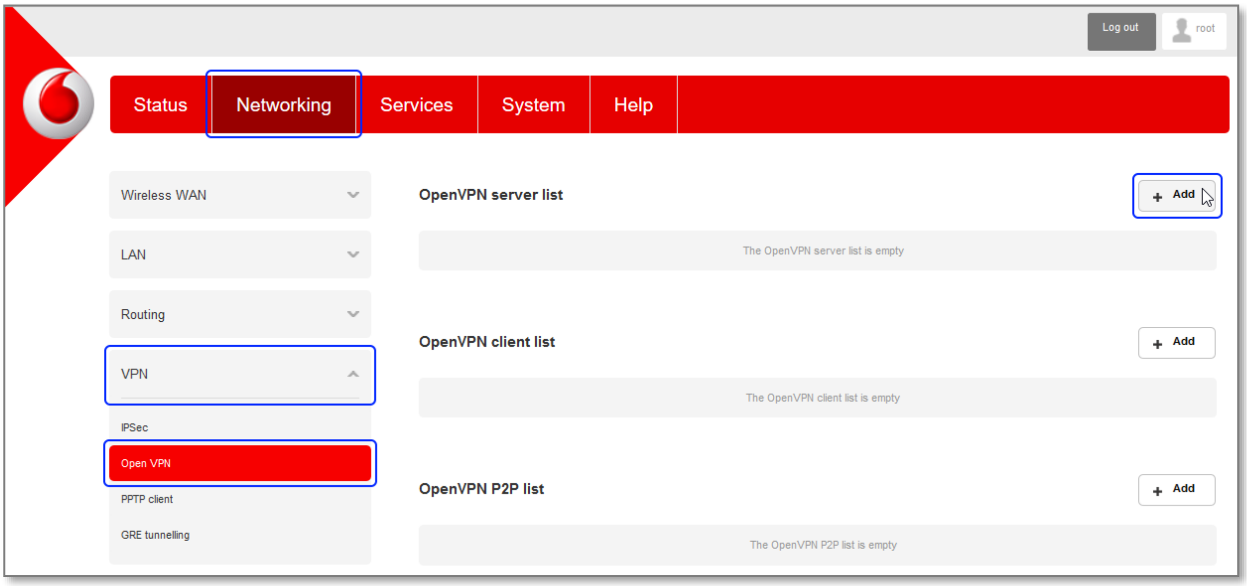
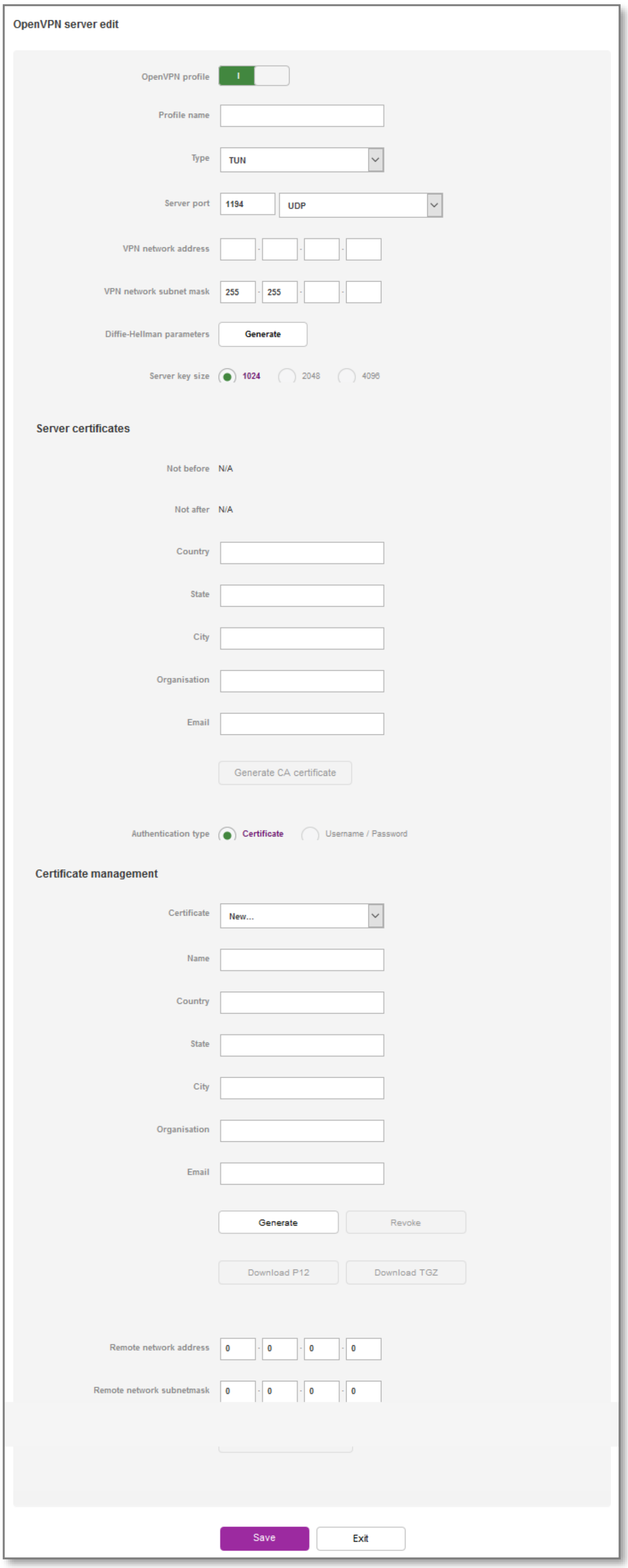


*Figure 2 - OpenVPN profile list*

4 Click the **+Add** button next to the **OpenVPN server list**. The configuration window is displayed.



OpenVPN server edit

OpenVPN profile: I

Profile name:

Type: TUN

Server port: 1194 UDP

VPN network address: . . .

VPN network subnet mask: 255 . 255 . .

Diffie-Hellman parameters: Generate

Server key size: ● 1024 ○ 2048 ○ 4096

Server certificates

Not before: N/A

Not after: N/A

Country:

State:

City:

Organisation:

Email:

Generate CA certificate

Authentication type: ● Certificate ○ Username / Password

Certificate management

Certificate: New...

Name:

Country:

State:

City:

Organisation:

Email:

Generate Revoke

Download P12 Download TGZ

Remote network address: 0 . 0 . 0 . 0

Remote network subnetmask: 0 . 0 . 0 . 0

Save Exit

*Figure 3 - OpenVPN Server configuration page*

5 Set the OpenVPN profile option to **ON.**

6 In the **Profile name** field, type a name for the OpenVPN Server profile you are creating. This is used to identify the OpenVPN connection on the router.

7 Use the **Server port** fields to enter a port number and select a 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 Under **Server key size**, select the size of the key. A larger key will result in higher security but will also take longer to generate the key.

10 Next to **Diffie-Hellman Parameters**, click the **Generate** 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.

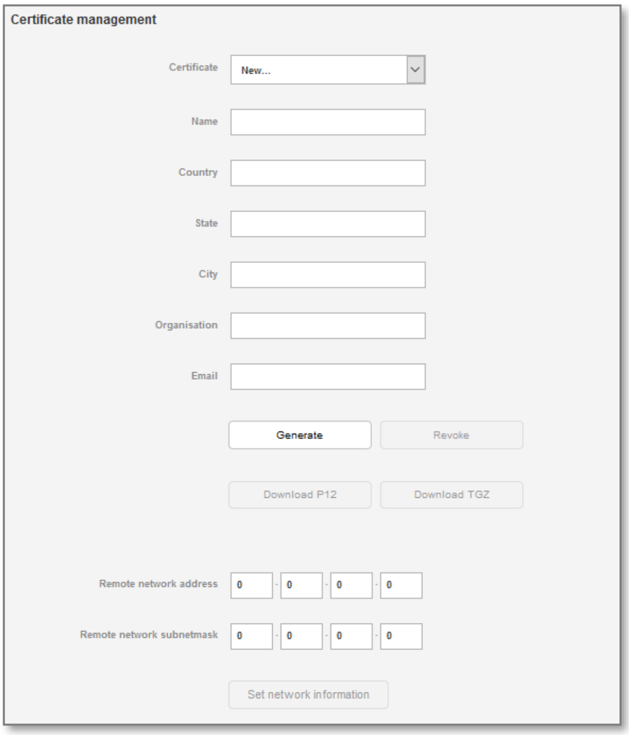
11 Under **Server Certificates**, enter the required details. All fields must be completed. The **Country** field must consist of one of the country codes listed in the Appendix. When the details have been entered, click the **Generate CA certificate** button to generate the Certificate Authority (CA) certificate based on this information.

12 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.

b 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 | |
| Organisation | |
| Email | |
| Remote network address | 0 . 0 . 0 . 0 |
| Remote network subnetmask | 0 . 0 . 0 . 0 |

*Figure 4 - OpenVPN Server - Certificate Management section*

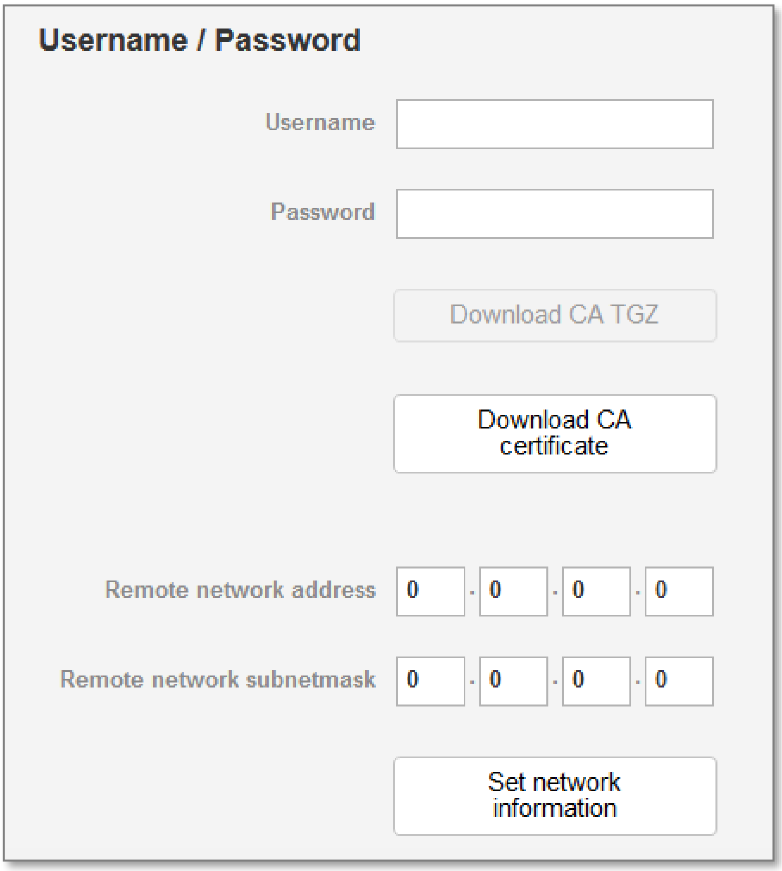
c When it is done, you can click the **Download** button to save the certificate file. If for some reason the integrity of your network has been compromised, you can return to this screen and use the Certificate drop down list to select the certificate and then press the **Revoke** button to disable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

d **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

e 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:

Remote network address: 0 . 0 . 0 . 0

Remote network subnetmask: 0 . 0 . 0 . 0

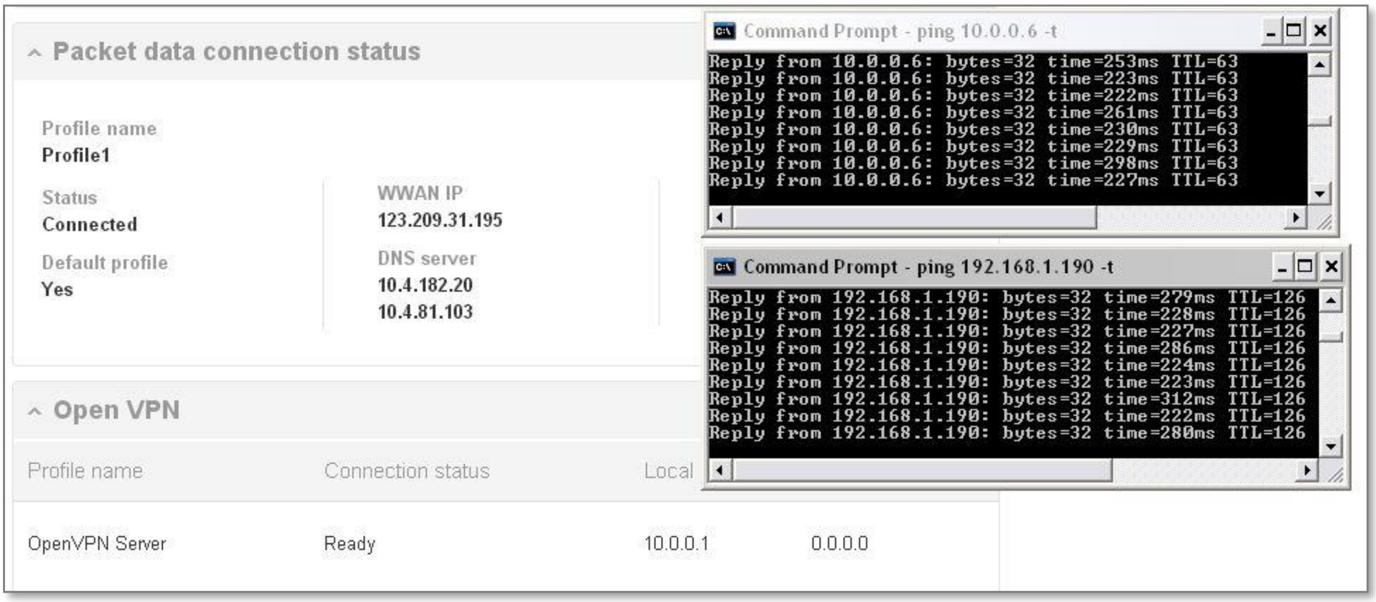
*Figure 5 - OpenVPN Server - Username/Password section*

f **Optional –** To inform the OpenVPN Server of the network address scheme of the currently selected certificate, enter the **Remote network address** and **Remote network subnetmask** 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. When done, click the **Set network information** button.

13 When you have finished entering all the required information, click the **Save** button 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.



Packet data connection status

| | |
|---|---|
| Profile name<br>Profile1 | |
| Status<br>Connected | WWAN IP<br>123.209.31.195 |
| Default profile<br>Yes | DNS server<br>10.4.182.20<br>10.4.81.103 |

Open VPN

| Profile name | Connection status | Local | |
|---|---|---|---|
| OpenVPN Server | Ready | 10.0.0.1 | 0.0.0.0 |

Command Prompt - ping 10.0.0.6 -t

```
Reply from 10.0.0.6: bytes=32 time=253ms TTL=63
Reply from 10.0.0.6: bytes=32 time=223ms TTL=63
Reply from 10.0.0.6: bytes=32 time=222ms TTL=63
Reply from 10.0.0.6: bytes=32 time=261ms TTL=63
Reply from 10.0.0.6: bytes=32 time=230ms TTL=63
Reply from 10.0.0.6: bytes=32 time=229ms TTL=63
Reply from 10.0.0.6: bytes=32 time=298ms TTL=63
Reply from 10.0.0.6: bytes=32 time=227ms TTL=63
```

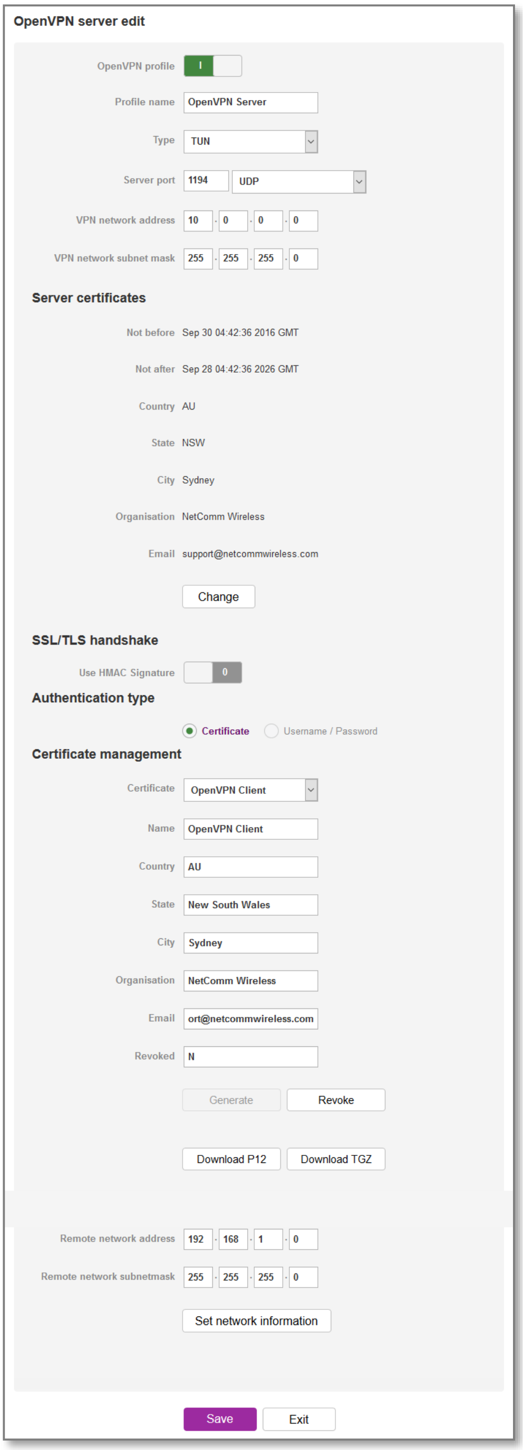
Command Prompt - ping 192.168.1.190 -t

```
Reply from 192.168.1.190: bytes=32 time=279ms TTL=126
Reply from 192.168.1.190: bytes=32 time=228ms TTL=126
Reply from 192.168.1.190: bytes=32 time=227ms TTL=126
Reply from 192.168.1.190: bytes=32 time=286ms TTL=126
Reply from 192.168.1.190: bytes=32 time=224ms TTL=126
Reply from 192.168.1.190: bytes=32 time=223ms TTL=126
Reply from 192.168.1.190: bytes=32 time=312ms TTL=126
Reply from 192.168.1.190: bytes=32 time=222ms TTL=126
Reply from 192.168.1.190: bytes=32 time=280ms TTL=126
```

*Figure 6 - OpenVPN Server connection verification*

# OpenVPN Server Examples

## OpenVPN Server Mode – Certificate Authentication



**OpenVPN server edit**

| | |
|---|---|
| OpenVPN profile | I |
| Profile name | OpenVPN Server |
| Type | TUN |
| Server port | 1194 UDP |
| VPN network address | 10 . 0 . 0 . 0 |
| VPN network subnet mask | 255 . 255 . 255 . 0 |

**Server certificates**

| | |
|---|---|
| Not before | Sep 30 04:42:36 2016 GMT |
| Not after | Sep 28 04:42:36 2026 GMT |
| Country | AU |
| State | NSW |
| City | Sydney |
| Organisation | NetComm Wireless |
| Email | support@netcommwireless.com |

**SSL/TLS handshake**

| | |
|---|---|
| Use HMAC Signature | 0 |

**Authentication type**

● Certificate ○ Username / Password

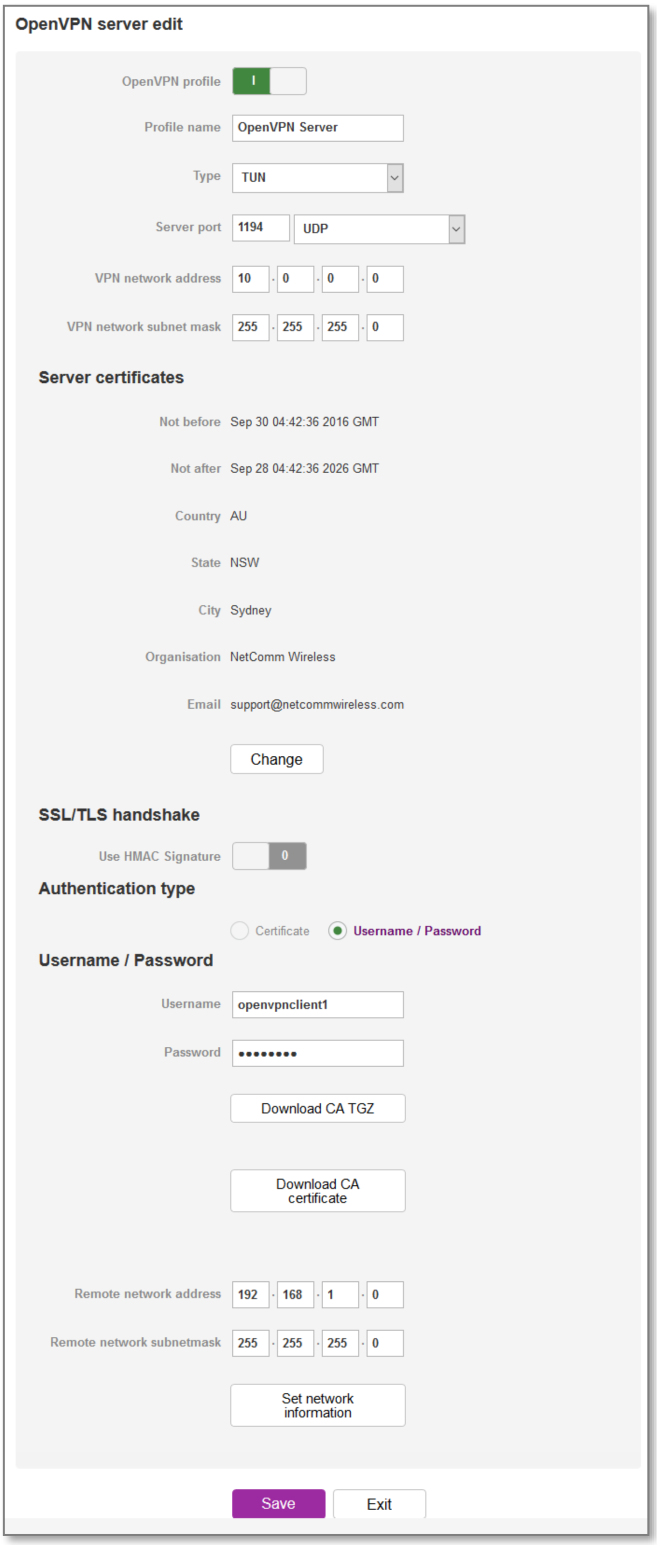
**Certificate management**

| | |
|---|---|
| Certificate | OpenVPN Client |
| Name | OpenVPN Client |
| Country | AU |
| State | New South Wales |
| City | Sydney |
| Organisation | NetComm Wireless |
| Email | ort@netcommwireless.com |
| Revoked | N |

| | |
|---|---|
| Remote network address | 192 . 168 . 1 . 0 |
| Remote network subnetmask | 255 . 255 . 255 . 0 |

*Figure 7 - OpenVPN Server - Certificate Authentication Example page*

# OpenVPN Server Mode – Username / Password Authentication



**OpenVPN server edit**

OpenVPN profile: I

Profile name: OpenVPN Server

Type: TUN

Server port: 1194 UDP

VPN network address: 10 . 0 . 0 . 0

VPN network subnet mask: 255 . 255 . 255 . 0

**Server certificates**

Not before: Sep 30 04:42:36 2016 GMT

Not after: Sep 28 04:42:36 2026 GMT

Country: AU

State: NSW

City: Sydney

Organisation: NetComm Wireless

Email: support@netcommwireless.com

**SSL/TLS handshake**

Use HMAC Signature: 0

**Authentication type**

○ Certificate ● Username / Password

**Username / Password**

Username: openvpnclient1

Password: ••••••••

Remote network address: 192 . 168 . 1 . 0

Remote network subnetmask: 255 . 255 . 255 . 0

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

# OpenVPN Client Mode

The Vodafone MachineLink router may be configured to operate as an OpenVPN Client and connect to an OpenVPN Server running on another MachineLink router or a software OpenVPN Server on a computer.

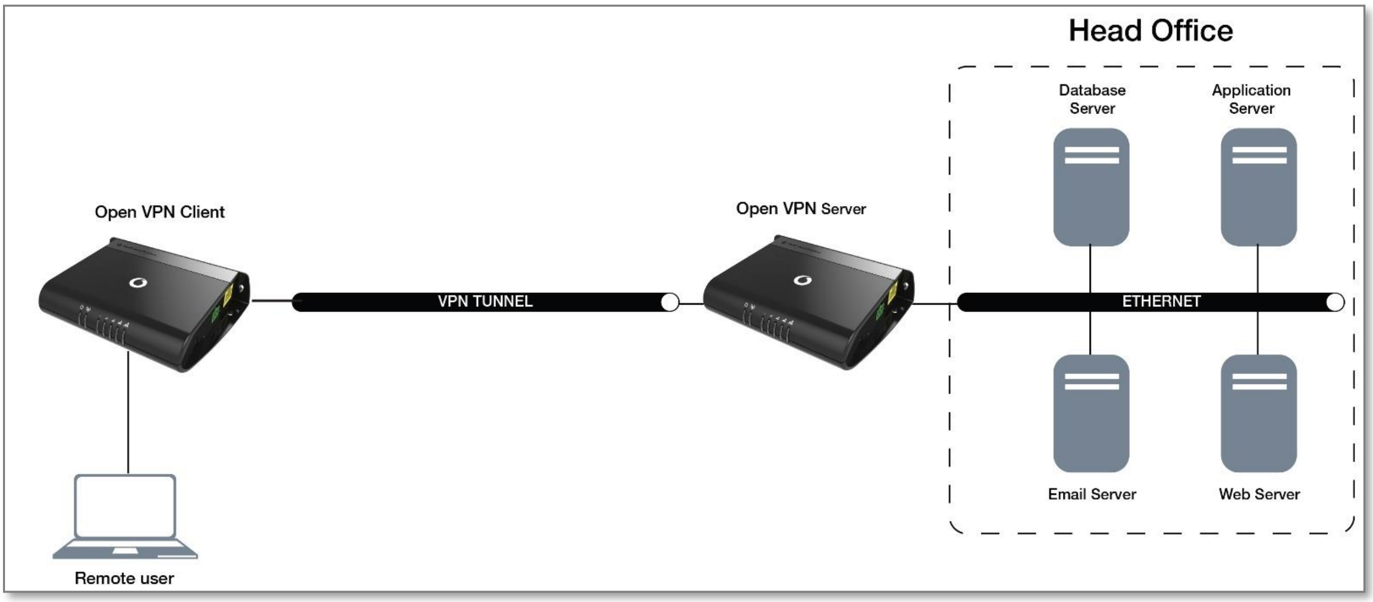


*Figure 9 - OpenVPN Client mode diagram*

## Certificate Files

When using two MachineLink 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 MachineLink router will expect a tar archive compressed using GZip. There are three files that the OpenVPN client in the MachineLink 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 MachineLink 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 Vodafone MachineLink router using the “root” account.

2 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **OpenVPN** item**.**

3 The OpenVPN lists are displayed.

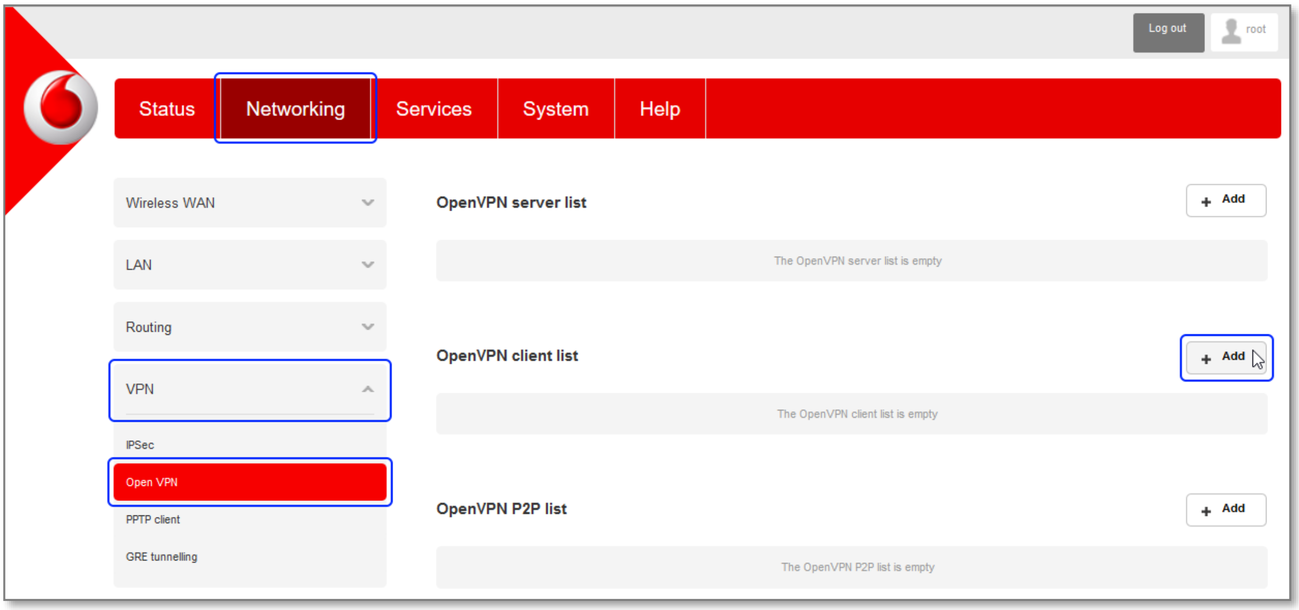
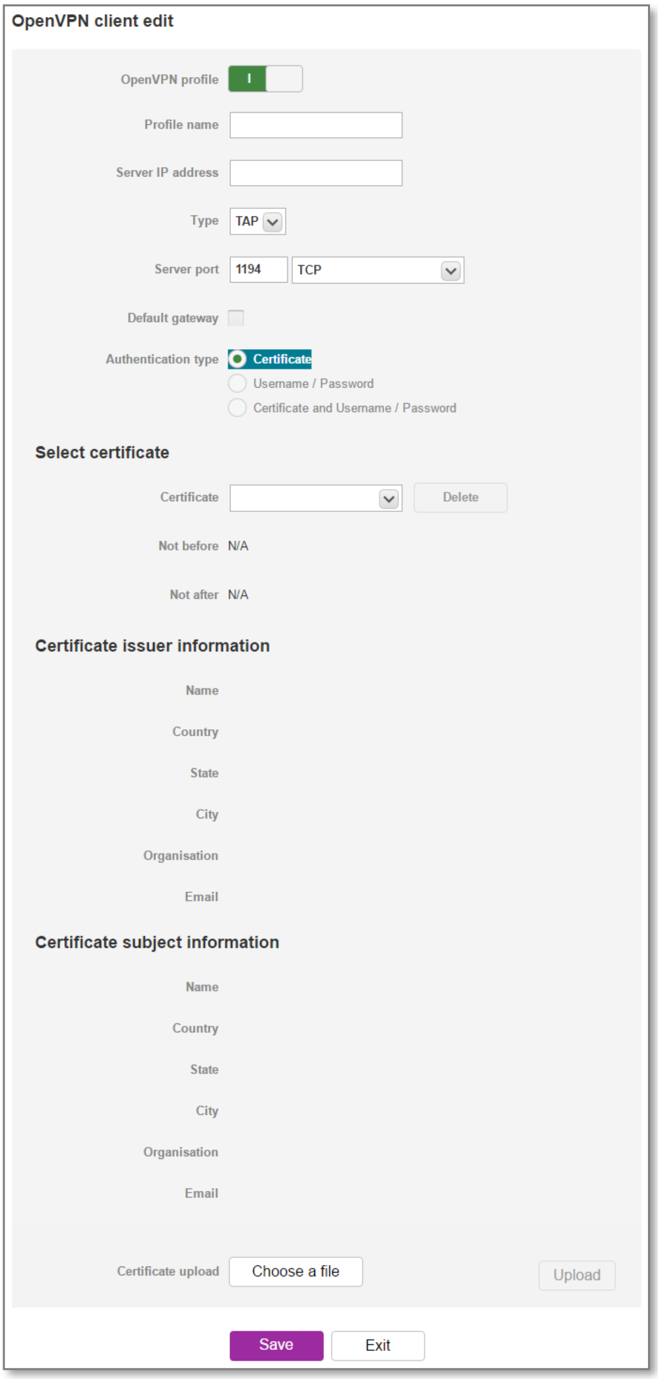


*Figure 10 - OpenVPN profile list*

4 Click the **+Add** button next to the **OpenVPN client list**. The configuration window is displayed.



OpenVPN client edit

OpenVPN profile: I

Profile name:

Server IP address:

Type: TAP

Server port: 1194 TCP

Default gateway: □

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

**Select certificate**

Certificate: Delete

Not before: N/A

Not after: N/A

**Certificate issuer information**

Name

Country

State

City

Organisation

Email

**Certificate subject information**

Name

Country

State

City

Organisation

Email

Certificate upload: Choose a file Upload

Save Exit

*Figure 9 - OpenVPN Client - Configuration page*

5 Set the **OpenVPN profile** option to **ON.**

6 In the **Profile name** field type a name for the OpenVPN Client profile you are creating.

7 In the **Server IP address** field type the WAN IP address of the OpenVPN Server.

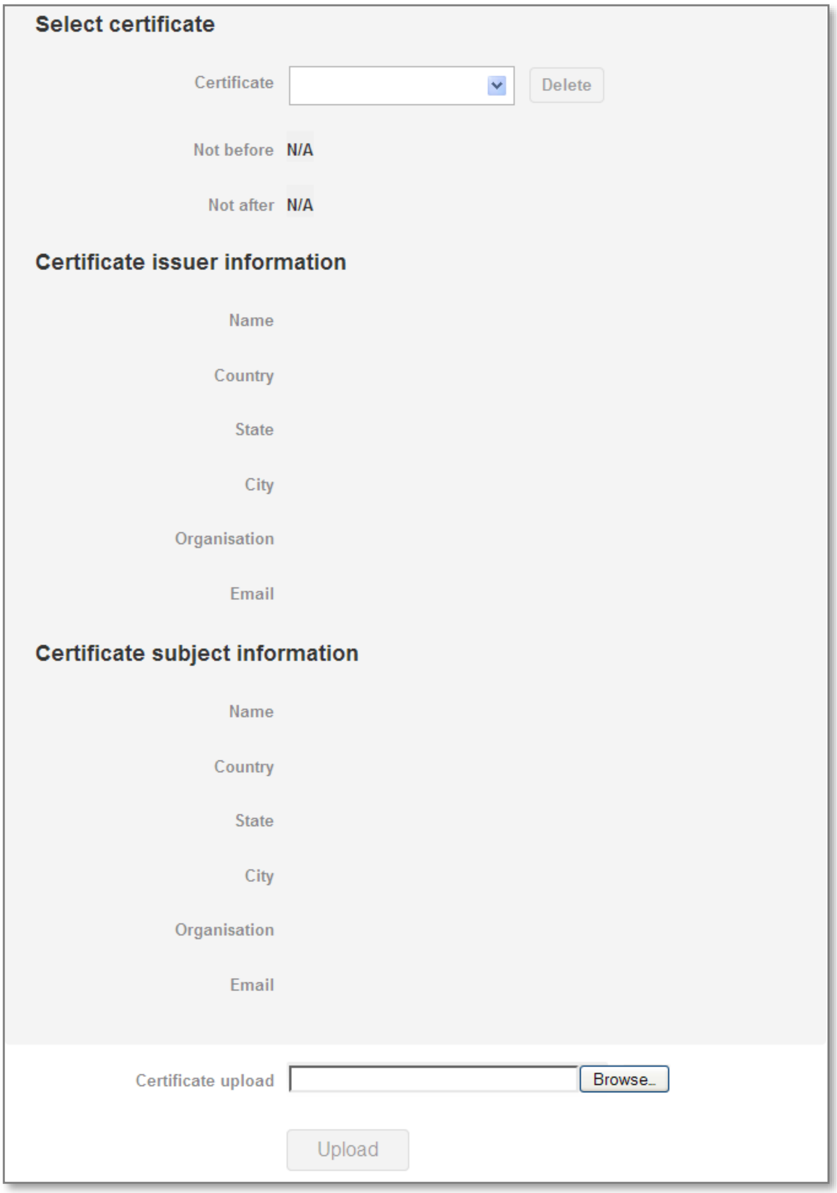
8 In the **Server port** fields enter the Server Port and packet type (UDP or TCP) to use for the connection.

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 For the **Authentication type** option, select the authentication type that you would like to use for the OpenVPN Client.

## Certificate Authentication

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

Not before N/A

Not after N/A

Certificate issuer information

Name

Country

State

City

Organisation

Email

Certificate subject information

Name

Country

State

City

Organisation

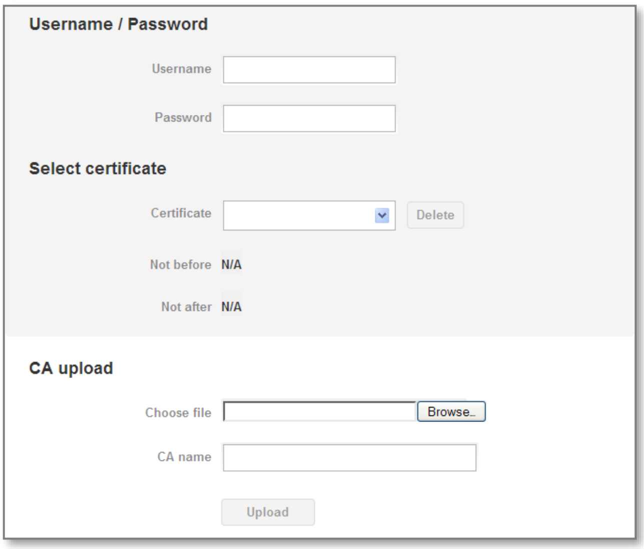
Email

Certificate 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

Password

**Select certificate**

Certificate

Not before N/A

Not after N/A

**CA upload**

Choose file

CA name

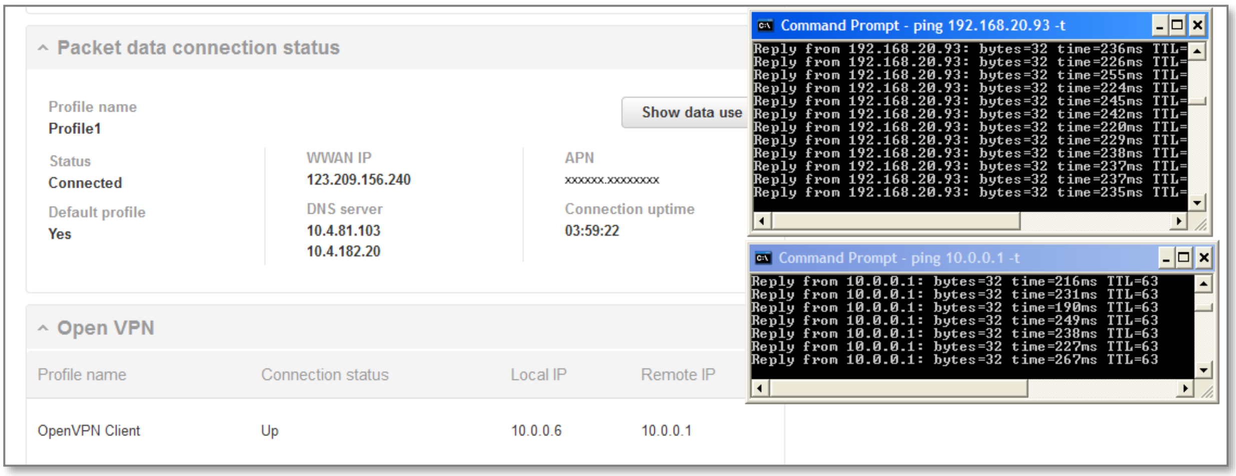
*Figure 12 - OpenVPN Client - Username/Password section*

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.



**Packet data connection status**

Profile name
Profile1

| | | |
|---|---|---|
| Status<br>Connected | WWAN IP<br>123.209.156.240 | APN<br>xxxxxx.xxxxxxxx |
| Default profile<br>Yes | DNS server<br>10.4.81.103<br>10.4.182.20 | Connection uptime<br>03:59:22 |

**Open VPN**

| Profile name | Connection status | Local IP | Remote IP |
|---|---|---|---|
| OpenVPN Client | Up | 10.0.0.6 | 10.0.0.1 |

Command Prompt - ping 192.168.20.93 -t

```
Reply from 192.168.20.93: bytes=32 time=236ms TTL=
Reply from 192.168.20.93: bytes=32 time=226ms TTL=
Reply from 192.168.20.93: bytes=32 time=255ms TTL=
Reply from 192.168.20.93: bytes=32 time=224ms TTL=
Reply from 192.168.20.93: bytes=32 time=245ms TTL=
Reply from 192.168.20.93: bytes=32 time=242ms TTL=
Reply from 192.168.20.93: bytes=32 time=220ms TTL=
Reply from 192.168.20.93: bytes=32 time=229ms TTL=
Reply from 192.168.20.93: bytes=32 time=238ms TTL=
Reply from 192.168.20.93: bytes=32 time=237ms TTL=
Reply from 192.168.20.93: bytes=32 time=237ms TTL=
Reply from 192.168.20.93: bytes=32 time=235ms TTL=
```

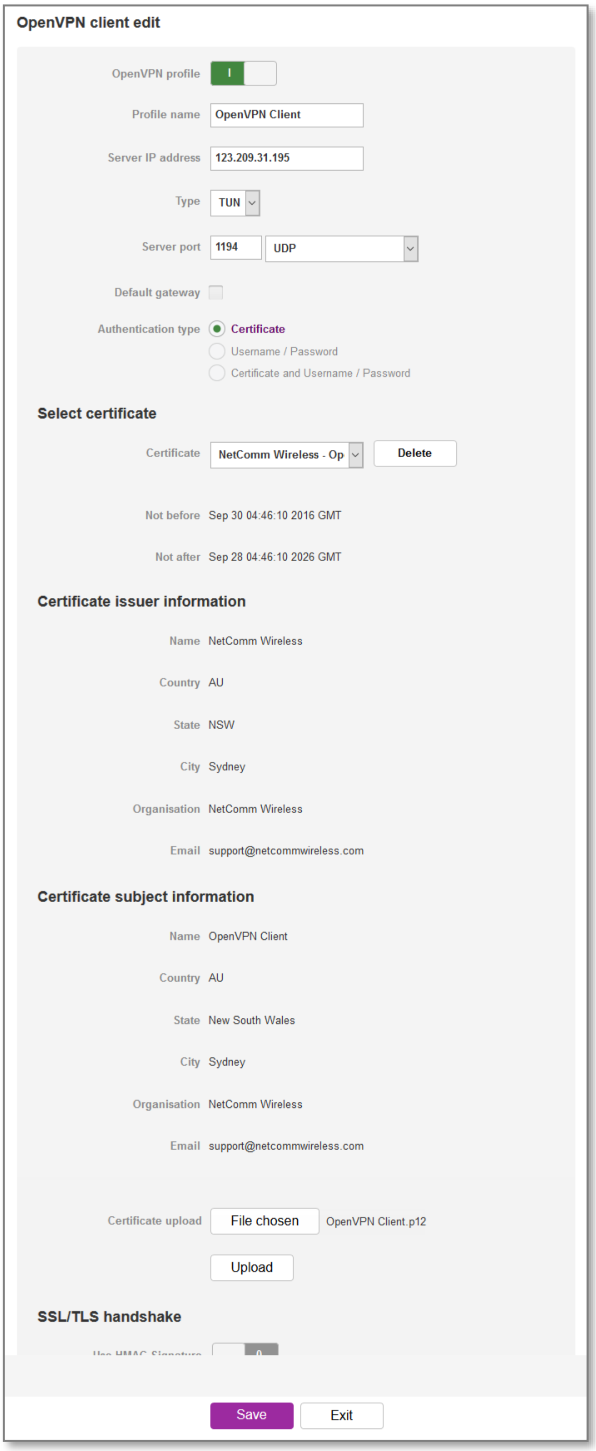
Command Prompt - ping 10.0.0.1 -t

```
Reply from 10.0.0.1: bytes=32 time=216ms TTL=63
Reply from 10.0.0.1: bytes=32 time=231ms TTL=63
Reply from 10.0.0.1: bytes=32 time=190ms TTL=63
Reply from 10.0.0.1: bytes=32 time=249ms TTL=63
Reply from 10.0.0.1: bytes=32 time=238ms TTL=63
Reply from 10.0.0.1: bytes=32 time=227ms TTL=63
Reply from 10.0.0.1: bytes=32 time=267ms TTL=63
```

*Figure 13 - OpenVPN Client verification of connection*

# OpenVPN Client Example

## OpenVPN Client – Certificate Authentication



**OpenVPN client edit**

| | |
|---|---|
| OpenVPN profile | I |
| Profile name | OpenVPN Client |
| Server IP address | 123.209.31.195 |
| Type | TUN |
| Server port | 1194 UDP |
| Default gateway | □ |
| Authentication type | ● Certificate<br>○ Username / Password<br>○ Certificate and Username / Password |

**Select certificate**

| | |
|---|---|
| Certificate | NetComm Wireless - Op |
| Not before | Sep 30 04:46:10 2016 GMT |
| Not after | Sep 28 04:46:10 2026 GMT |

**Certificate issuer information**

| | |
|---|---|
| Name | NetComm Wireless |
| Country | AU |
| State | NSW |
| City | Sydney |
| Organisation | NetComm Wireless |
| Email | support@netcommwireless.com |

**Certificate subject information**

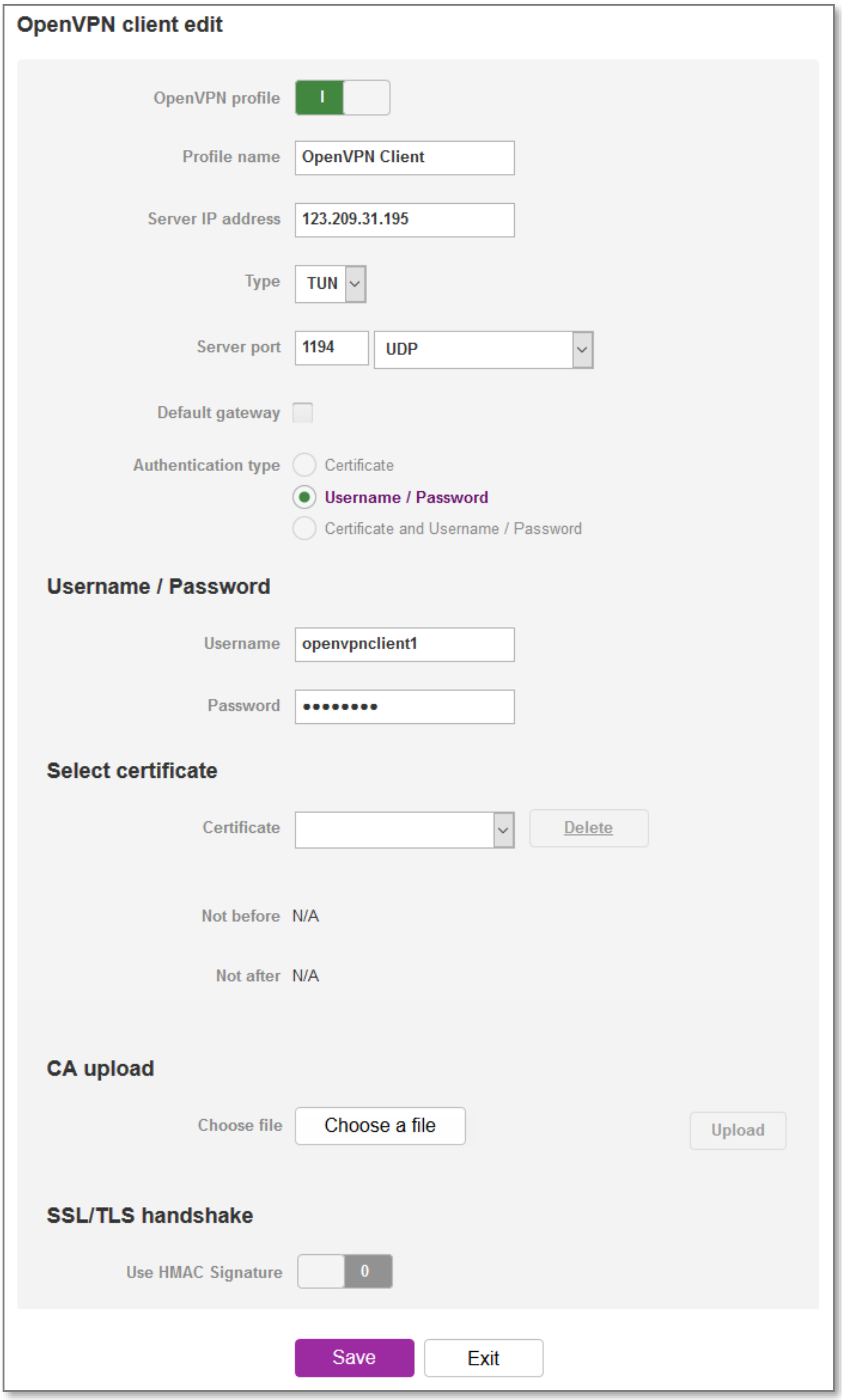
| | |
|---|---|
| Name | OpenVPN Client |
| Country | AU |
| State | New South Wales |
| City | Sydney |
| Organisation | NetComm Wireless |
| Email | support@netcommwireless.com |
| Certificate upload | File chosen OpenVPN Client.p12 |

**SSL/TLS handshake**

| | |
|---|---|
| Use HMAC Signature | 0 |

*Figure 14 - OpenVPN Client Mode - Certificate Authentication Example*

## OpenVPN Client – Username / Password Authentication



### OpenVPN client edit

| | |
|---|---|
| OpenVPN profile | I (on) |
| Profile name | OpenVPN Client |
| Server IP address | 123.209.31.195 |
| Type | TUN |
| Server port | 1194 UDP |
| Default gateway | □ |
| Authentication type | ○ Certificate<br>● Username / Password<br>○ Certificate and Username / Password |

**Username / Password**

| | |
|---|---|
| Username | openvpnclient1 |
| Password | •••••••• |

**Select certificate**

| | |
|---|---|
| Certificate | |
| Not before | N/A |
| Not after | N/A |

**CA upload**

**SSL/TLS handshake**

| | |
|---|---|
| Use HMAC Signature | 0 |

*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.

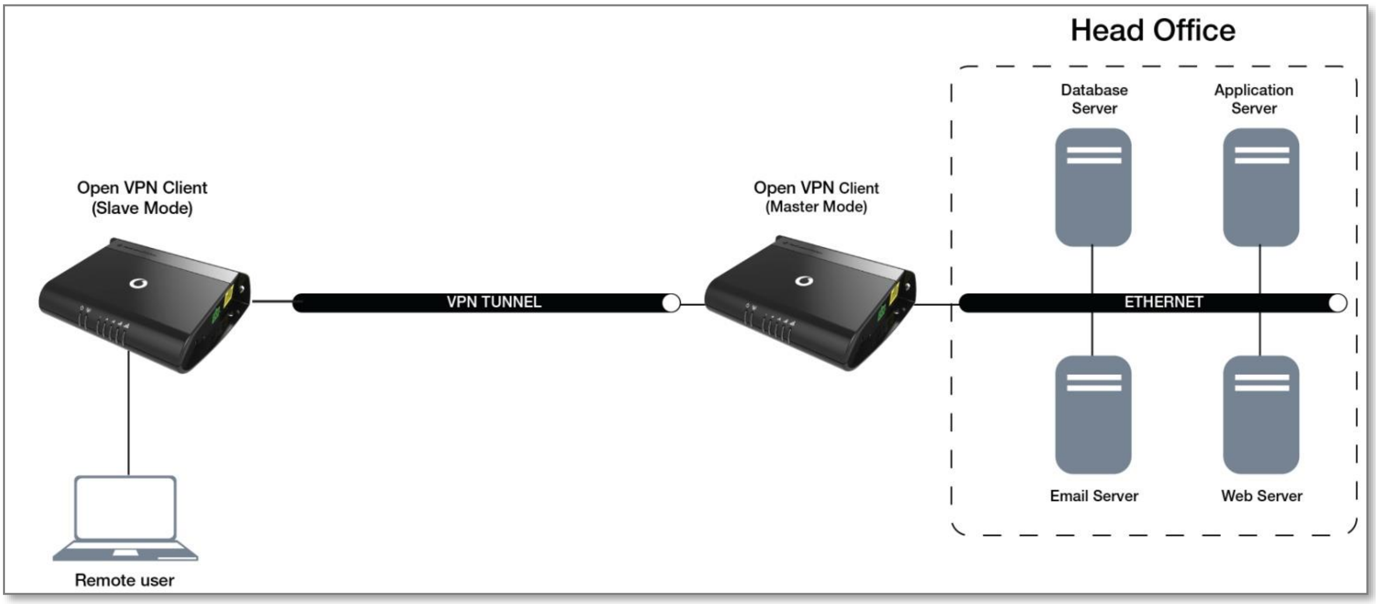


*Figure 16 - OpenVPN Peer-To-Peer mode diagram*

## Configuring an OpenVPN Peer-To-Peer Connection

Perform the following steps on two Vodafone MachineLink routers:

1 Login to your MachineLink routers using the “root” account.

2 Click on the **Networking** menu, click the **VPN** menu on the left, and then click the **OpenVPN** item**.** The OpenVPN lists are displayed.

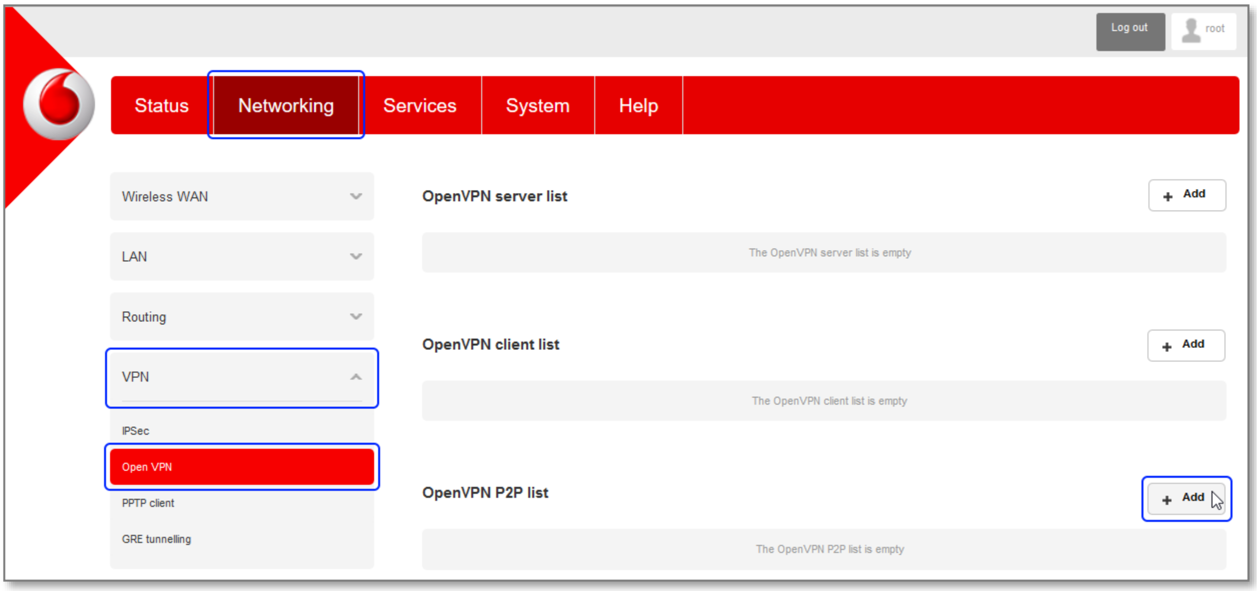
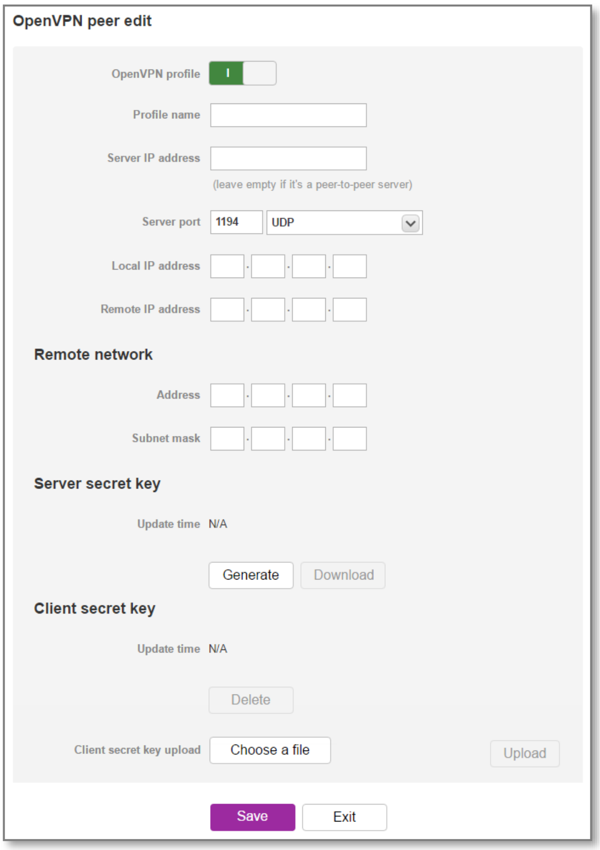


*Figure 17 - OpenVPN profile list*

3 Click the **+Add** button next to the **OpenVPN P2P list**. The configuration window is displayed.


OpenVPN peer edit

OpenVPN profile: I

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

Client secret key

Update time: N/A

*Figure 9 - OpenVPN Peer-To-Peer Mode*

4 Set the **OpenVPN profile** option to **ON.**

5 In the **Profile name** field, 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 In the **Server port** field, enter the Server Port and packet type to use for the connection.

8 In the **Local IP address** and **Remote IP address** fields, enter the local and remote IP addresses 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 network mask. The Network Address and Network Mask fields inform the Master node of the LAN address scheme of the Slave.

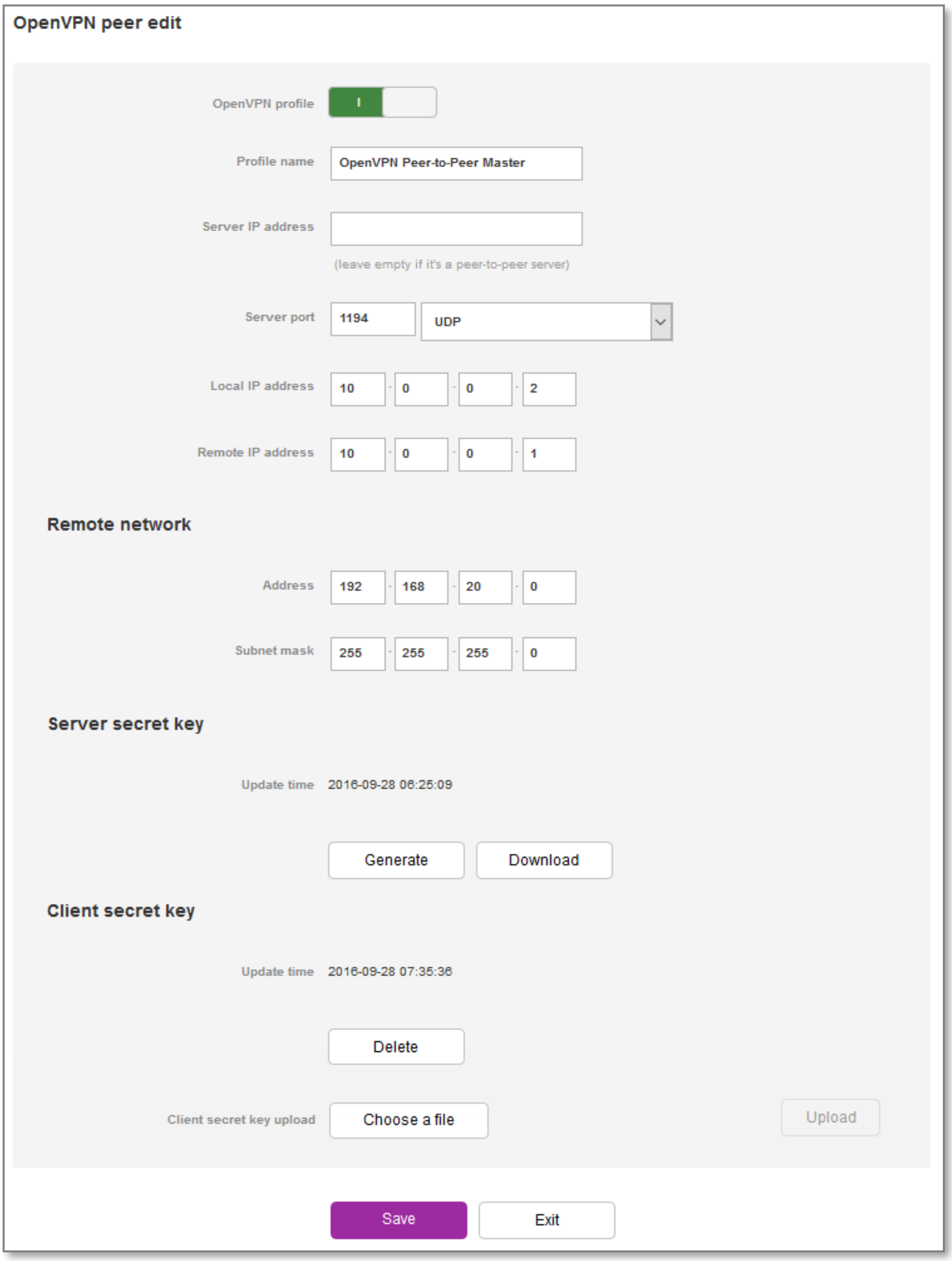
10 Press the **Generate** button to create a secret key to be shared with the slave. When the timestamp appears, you can click the **Download** button to save the file to exchange with the other router.

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: I

Profile name: OpenVPN Peer-to-Peer Master

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 . 20 . 0

Subnet mask: 255 . 255 . 255 . 0

**Server secret key**

Update time: 2016-09-28 06:25:09

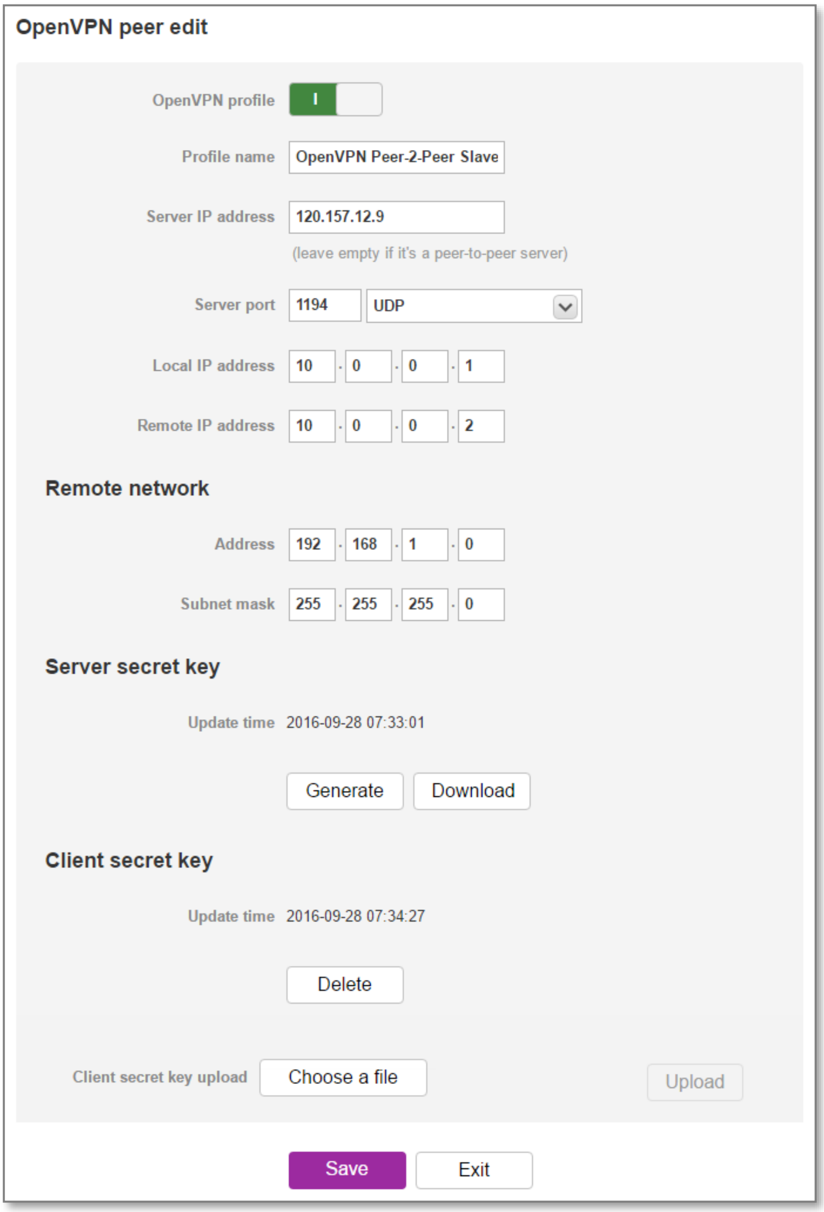
**Client secret key**

Update time: 2016-09-28 07:35:36

Client secret key upload

*Figure 18 - OpenVPN Peer-To-Peer Master example*

## OpenVPN Peer-To-Peer Slave



OpenVPN peer edit

| | |
|---|---|
| OpenVPN profile | I |
| Profile name | OpenVPN Peer-2-Peer Slave |
| Server IP address | 120.157.12.9<br>(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 . 1 . 0 |
| Subnet mask | 255 . 255 . 255 . 0 |

Server secret key

Update time 2016-09-28 07:33:01

Client secret key

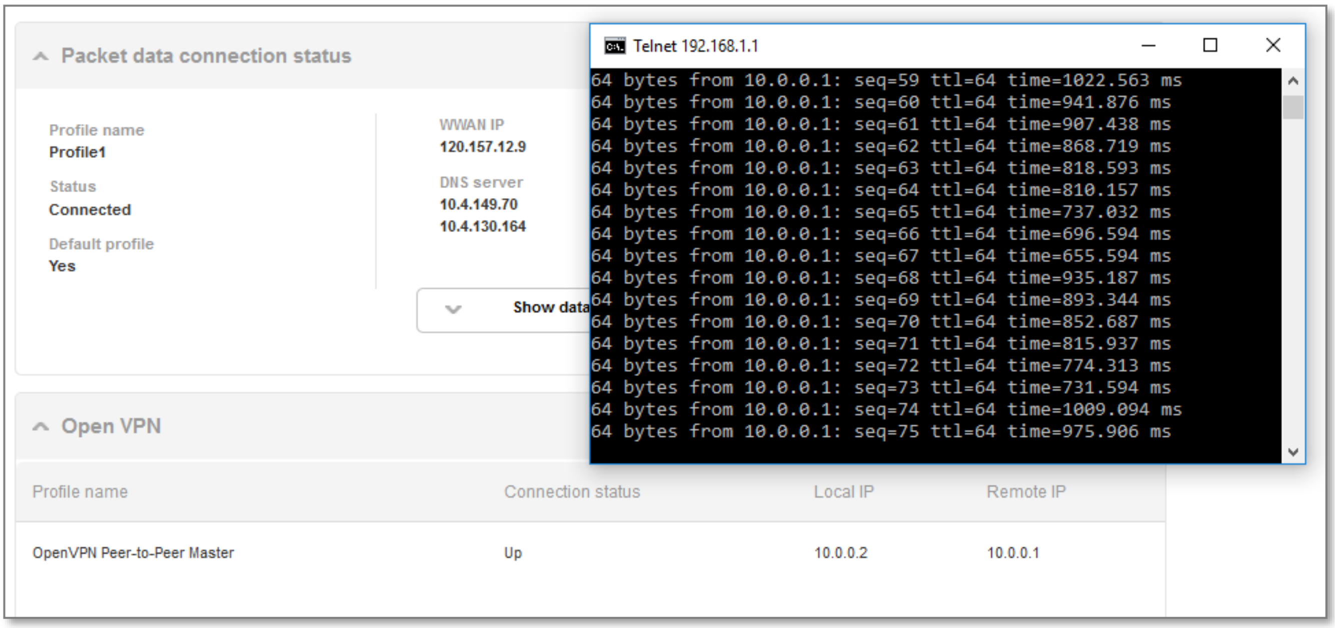
Update time 2016-09-28 07:34:27

*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



Profile name
Profile1

Status
Connected

Default profile
Yes

WWAN IP
120.157.12.9

DNS server
10.4.149.70
10.4.130.164

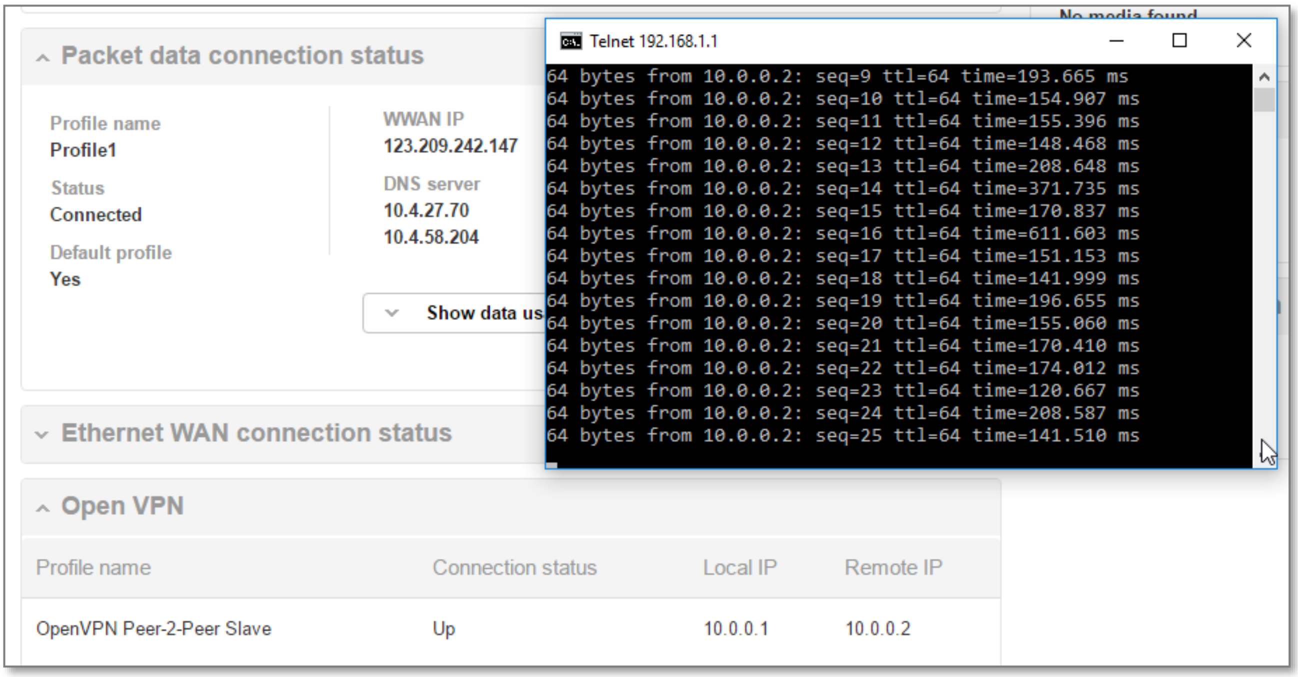
| Profile name | Connection status | Local IP | Remote IP |
|---|---|---|---|
| OpenVPN Peer-to-Peer Master | Up | 10.0.0.2 | 10.0.0.1 |

Telnet 192.168.1.1

```
64 bytes from 10.0.0.1: seq=59 ttl=64 time=1022.563 ms
64 bytes from 10.0.0.1: seq=60 ttl=64 time=941.876 ms
64 bytes from 10.0.0.1: seq=61 ttl=64 time=907.438 ms
64 bytes from 10.0.0.1: seq=62 ttl=64 time=868.719 ms
64 bytes from 10.0.0.1: seq=63 ttl=64 time=818.593 ms
64 bytes from 10.0.0.1: seq=64 ttl=64 time=810.157 ms
64 bytes from 10.0.0.1: seq=65 ttl=64 time=737.032 ms
64 bytes from 10.0.0.1: seq=66 ttl=64 time=696.594 ms
64 bytes from 10.0.0.1: seq=67 ttl=64 time=655.594 ms
64 bytes from 10.0.0.1: seq=68 ttl=64 time=935.187 ms
64 bytes from 10.0.0.1: seq=69 ttl=64 time=893.344 ms
64 bytes from 10.0.0.1: seq=70 ttl=64 time=852.687 ms
64 bytes from 10.0.0.1: seq=71 ttl=64 time=815.937 ms
64 bytes from 10.0.0.1: seq=72 ttl=64 time=774.313 ms
64 bytes from 10.0.0.1: seq=73 ttl=64 time=731.594 ms
64 bytes from 10.0.0.1: seq=74 ttl=64 time=1009.094 ms
64 bytes from 10.0.0.1: seq=75 ttl=64 time=975.906 ms
```

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

## OpenVPN Peer-To-Peer Slave



Profile name
Profile1

Status
Connected

Default profile
Yes

WWAN IP
123.209.242.147

DNS server
10.4.27.70
10.4.58.204

| Profile name | Connection status | Local IP | Remote IP |
|---|---|---|---|
| OpenVPN Peer-2-Peer Slave | Up | 10.0.0.1 | 10.0.0.2 |

Telnet 192.168.1.1

```
64 bytes from 10.0.0.2: seq=9 ttl=64 time=193.665 ms
64 bytes from 10.0.0.2: seq=10 ttl=64 time=154.907 ms
64 bytes from 10.0.0.2: seq=11 ttl=64 time=155.396 ms
64 bytes from 10.0.0.2: seq=12 ttl=64 time=148.468 ms
64 bytes from 10.0.0.2: seq=13 ttl=64 time=208.648 ms
64 bytes from 10.0.0.2: seq=14 ttl=64 time=371.735 ms
64 bytes from 10.0.0.2: seq=15 ttl=64 time=170.837 ms
64 bytes from 10.0.0.2: seq=16 ttl=64 time=611.603 ms
64 bytes from 10.0.0.2: seq=17 ttl=64 time=151.153 ms
64 bytes from 10.0.0.2: seq=18 ttl=64 time=141.999 ms
64 bytes from 10.0.0.2: seq=19 ttl=64 time=196.655 ms
64 bytes from 10.0.0.2: seq=20 ttl=64 time=155.060 ms
64 bytes from 10.0.0.2: seq=21 ttl=64 time=170.410 ms
64 bytes from 10.0.0.2: seq=22 ttl=64 time=174.012 ms
64 bytes from 10.0.0.2: seq=23 ttl=64 time=120.667 ms
64 bytes from 10.0.0.2: seq=24 ttl=64 time=208.587 ms
64 bytes from 10.0.0.2: seq=25 ttl=64 time=141.510 ms
```

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

# Appendix: Country codes

| Code | Country | Code | Country | Code | Country | Code | Country |
|---|---|---|---|---|---|---|---|
| **AX** | Åland Islands | **DM** | Dominica | **KE** | Kenya | **OM** | Oman |
| **AD** | Andorra | **DO** | Dominican Republic | **KG** | Kyrgyzstan | **PA** | Panama |
| **AE** | United Arab Emirates | **DZ** | Algeria | **KH** | Cambodia | **PE** | Peru |
| **AF** | Afghanistan | **EC** | Ecuador | **KI** | Kiribati | **PF** | French Polynesia |
| **AG** | Antigua and Barbuda | **EE** | Estonia | **KM** | Comoros | **PG** | Papua New Guinea |
| **AI** | Anguilla | **EG** | Egypt | **KN** | Saint Kitts and Nevis | **PH** | Philippines |
| **AL** | Albania | **EH** | Western Sahara | **KR** | Korea (South) | **PK** | Pakistan |
| **AM** | Armenia | **ER** | Eritrea | **KW** | Kuwait | **PL** | Poland |
| **AN** | Netherlands Antilles | **ES** | Spain | **KY** | Cayman Islands | **PM** | St. Pierre and Miquelon |
| **AO** | Angola | **ET** | Ethiopia | **KZ** | Kazakhstan | **PN** | Pitcairn |
| **AQ** | Antarctica | **FI** | Finland | **LA** | Laos | **PR** | Puerto Rico |
| **AR** | Argentina | **FJ** | Fiji | **LC** | Saint Lucia | **PS** | Palestinian Territory |
| **AS** | American Samoa | **FK** | Falkland Islands (Malvinas) | **LI** | Liechtenstein | **PT** | Portugal |
| **AT** | Austria | **FM** | Micronesia | **LK** | Sri Lanka | **PW** | Palau |
| **AU** | Australia | **FO** | Faroe Islands | **LS** | Lesotho | **PY** | Paraguay |
| **AW** | Aruba | **FR** | France | **LT** | Lithuania | **QA** | Qatar |
| **AZ** | Azerbaijan | **FX** | France, Metropolitan | **LU** | Luxembourg | **RE** | Reunion |
| **BA** | Bosnia and Herzegovina | **GA** | Gabon | **LV** | Latvia | **RO** | Romania |
| **BB** | Barbados | **GB** | Great Britain (UK) | **LY** | Libya | **RS** | Serbia |
| **BD** | Bangladesh | **GD** | Grenada | **MA** | Morocco | **RU** | Russian Federation |
| **BE** | Belgium | **GE** | Georgia | **MC** | Monaco | **RW** | Rwanda |
| **BF** | Burkina Faso | **GF** | French Guiana | **MD** | Moldova | **SA** | Saudi Arabia |
| **BG** | Bulgaria | **GG** | Guernsey | **ME** | Montenegro | **SB** | Solomon Islands |
| **BH** | Bahrain | **GH** | Ghana | **MG** | Madagascar | **SC** | Seychelles |
| **BI** | Burundi | **GI** | Gibraltar | **MH** | Marshall Islands | **SE** | Sweden |
| **BJ** | Benin | **GL** | Greenland | **MK** | Macedonia | **SG** | Singapore |
| **BM** | Bermuda | **GM** | Gambia | **ML** | Mali | **SH** | St. Helena |
| **BN** | Brunei Darussalam | **GN** | Guinea | **MM** | Myanmar | **SI** | Slovenia |
| **BO** | Bolivia | **GP** | Guadeloupe | **MN** | Mongolia | **SJ** | Svalbard and Jan Mayen Islands |
| **BR** | Brazil | **GQ** | Equatorial Guinea | **MO** | Macau | **SK** | Slovak Republic |

| Code | Country | Code | Country | Code | Country | Code | Country |
|---|---|---|---|---|---|---|---|
| **BS** | Bahamas | **GR** | Greece | **MP** | Northern Mariana Islands | **SL** | Sierra Leone |
| **BT** | Bhutan | **GS** | S. Georgia and S. Sandwich Isls. | **MQ** | Martinique | **SM** | San Marino |
| **BV** | Bouvet Island | **GT** | Guatemala | **MR** | Mauritania | **SN** | Senegal |
| **BW** | Botswana | **GU** | Guam | **MS** | Montserrat | **SR** | Suriname |
| **BZ** | Belize | **GW** | Guinea-Bissau | **MT** | Malta | **ST** | Sao Tome and Principe |
| **CA** | Canada | **GY** | Guyana | **MU** | Mauritius | **SU** | USSR (former) |
| **CC** | Cocos (Keeling) Islands | **HK** | Hong Kong | **MV** | Maldives | **SV** | El Salvador |
| **CF** | Central African Republic | **HM** | Heard and McDonald Islands | **MW** | Malawi | **SZ** | Swaziland |
| **CH** | Switzerland | **HN** | Honduras | **MX** | Mexico | **TC** | Turks and Caicos Islands |
| **CI** | Cote D'Ivoire (Ivory Coast) | **HR** | Croatia (Hrvatska) | **MY** | Malaysia | **TD** | Chad |
| **CK** | Cook Islands | **HT** | Haiti | **MZ** | Mozambique | **TF** | French Southern Territories |
| **CL** | Chile | **HU** | Hungary | **NA** | Namibia | **TG** | Togo |
| **CM** | Cameroon | **ID** | Indonesia | **NC** | New Caledonia | **TH** | Thailand |
| **CN** | China | **IE** | Ireland | **NE** | Niger | **TJ** | Tajikistan |
| **CO** | Colombia | **IL** | Israel | **NF** | Norfolk Island | **TK** | Tokelau |
| **CR** | Costa Rica | **IM** | Isle of Man | **NG** | Nigeria | **TM** | Turkmenistan |
| **CS** | Czechoslovakia (former) | **IN** | India | **NI** | Nicaragua | **TN** | Tunisia |
| **CV** | Cape Verde | **IO** | British Indian Ocean Territory | **NL** | Netherlands | **TO** | Tonga |
| **CX** | Christmas Island | **IS** | Iceland | **NO** | Norway | **TP** | East Timor |
| **CY** | Cyprus | **IT** | Italy | **NP** | Nepal | **TR** | Turkey |
| **CZ** | Czech Republic | **JE** | Jersey | **NR** | Nauru | **TT** | Trinidad and Tobago |
| **DE** | Germany | **JM** | Jamaica | **NT** | Neutral Zone | **TV** | Tuvalu |
| **DJ** | Djibouti | **JO** | Jordan | **NU** | Niue | **TW** | Taiwan |
| **DK** | Denmark | **JP** | Japan | **NZ** | New Zealand (Aotearoa) | **TZ** | Tanzania |

| Code | Country |
|---|---|
| **UA** | Ukraine |
| **UG** | Uganda |
| **UM** | US Minor Outlying Islands |
| **US** | United States |

| Code | Country |
|---|---|
| **UY** | Uruguay |
| **UZ** | Uzbekistan |
| **VA** | Vatican City State (Holy See) |
| **VC** | Saint Vincent and the Grenadines |
| **VE** | Venezuela |
| **VG** | Virgin Islands (British) |
| **VI** | Virgin Islands (U.S.) |
| **VN** | Viet Nam |
| **VU** | Vanuatu |
| **WF** | Wallis and Futuna Islands |
| **WS** | Samoa |
| **YE** | Yemen |
| **YT** | Mayotte |
| **ZA** | South Africa |
| **ZM** | Zambia |
| **COM** | US Commercial |
| **EDU** | US Educational |
| **GOV** | US Government |
| **INT** | International |
| **MIL** | US Military |
| **NET** | Network |
| **ORG** | Non-Profit Organization |
| **ARPA** | Old style Arpanet |

*Table 1 - Country codes*