Vodafone MachineLink

PPTP Configuration Guide

Document history

This guide covers the following products:

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

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

Table i - Document revision history

Note – Before performing the instructions in this guide, please ensure that you have the latest firmware version installed on your router.

Visit http://vodafone.netcommwireless.com to download the latest firmware.

Note – The functions described in this document require that the router is assigned with a publicly routable IP address.

Please ensure that your mobile carrier has provided you with a publicly routable IP address before performing the instructions in this document.

Copyright

Copyright© 2016 NetComm Wireless Limited. All rights reserved.

Copyright© 2016 Vodafone Group Plc. All rights reserved.

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

Trademarks and registered trademarks are the property of NetComm Wireless Limited or Vodafone Group or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

Note – This document is subject to change without notice.

Contents

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

Site-to-site 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.

Remote Access VPN

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

PPTP is a popular choice when selecting a VPN type, mainly due to the large number of clients supporting it. Windows® Servers may be configured to function as PPTP VPN Servers. Owing to its popularity, the Vodafone MachineLink router has a PPTP client built-in enabling you to utilise this method of securing your data connection.

This document describes how to configure the PPTP client on the Vodafone MachineLink M2M IP Router.

PPTP Overview

The following diagram illustrates a typical PPTP usage scenario:

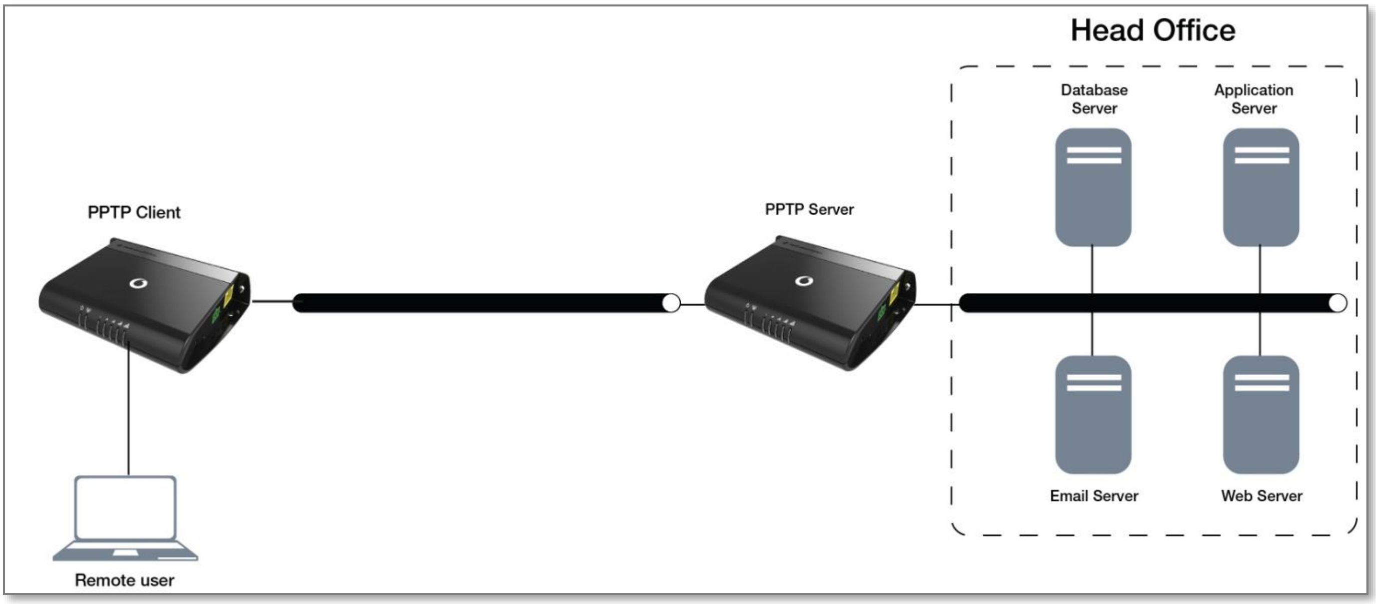


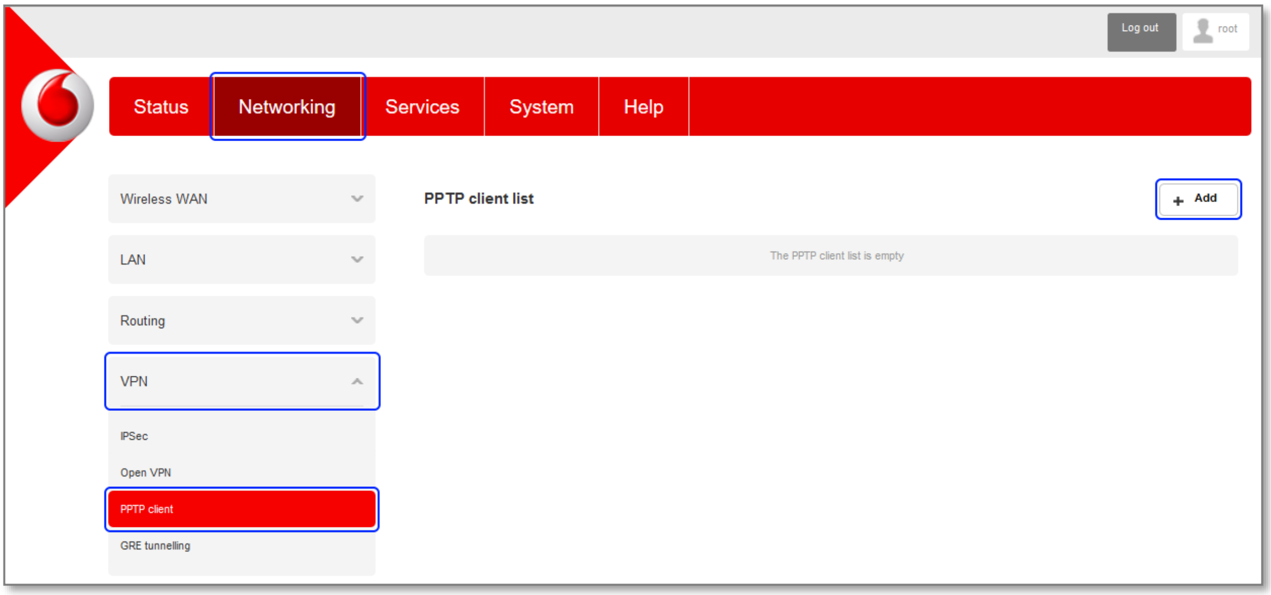
Figure 1 - PPTP Diagram

Configuring the PPTP Client

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

2 Click on **Networking**, then click on the **VPN** menu on the left, then the **PPTP client** item.

3 The PPTP VPN List is displayed.

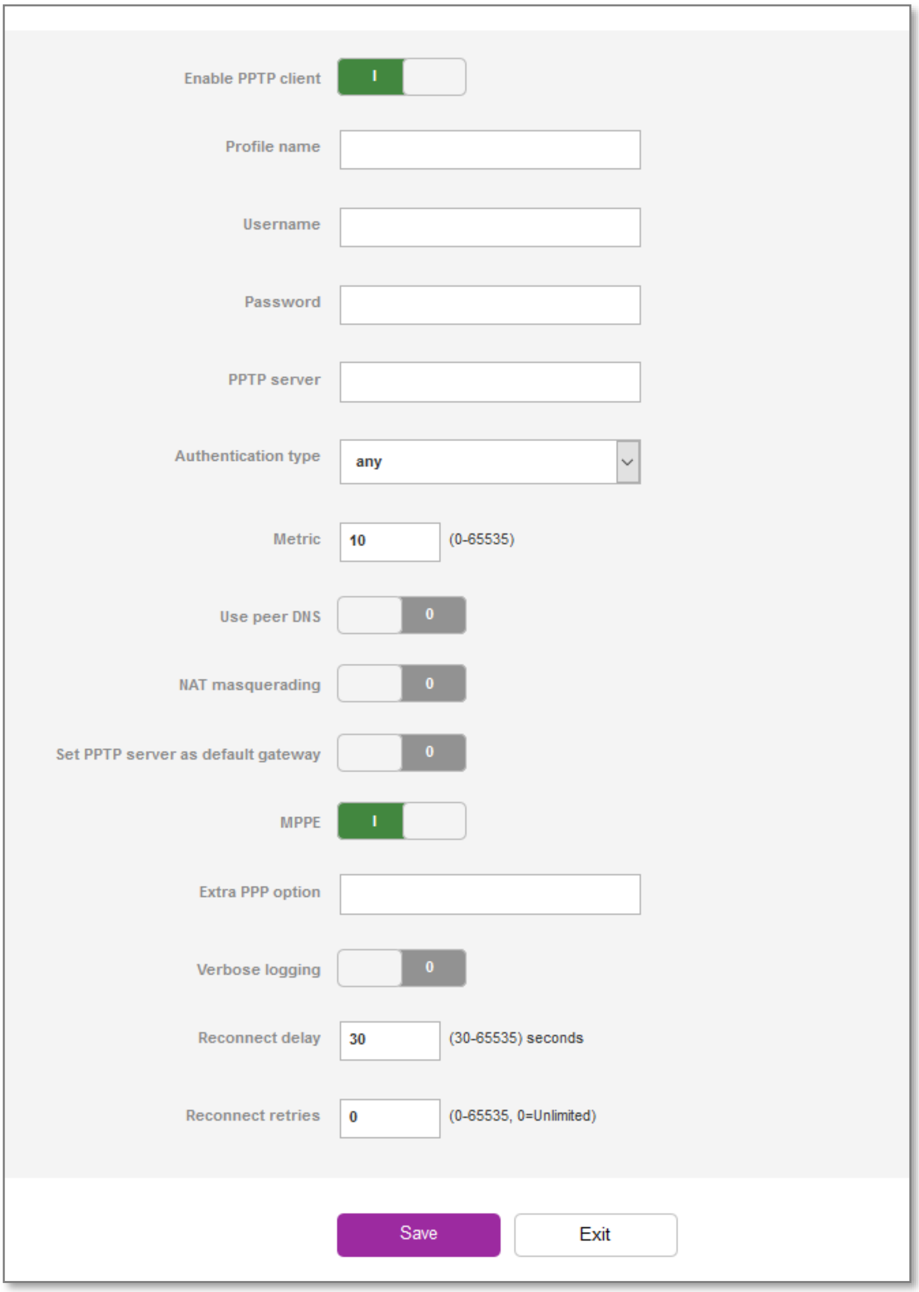


PPTP client list

The PPTP client list is empty

Figure 2 - PPTP Client List

4 Click the **+Add** button to begin configuring a new PPTP client profile. The PPTP client edit screen is displayed.



Enable PPTP client	I
Profile name	
Username	
Password	
PPTP server	
Authentication type	any
Metric	10 (0-65535)
Use peer DNS	0
NAT masquerading	0
Set PPTP server as default gateway	0
MPPE	I
Extra PPP option	
Verbose logging	0
Reconnect delay	30 (30-65535) seconds
Reconnect retries	0 (0-65535, 0=Unlimited)

Figure 3 - VPN PPTP client edit

5 Click the **Enable PPTP client** toggle key to switch it to the **ON** position.

6 In the **Profile name list,** enter a profile name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.

7 Use the **Username** and **Password** fields to enter the username and password for the PPTP account.

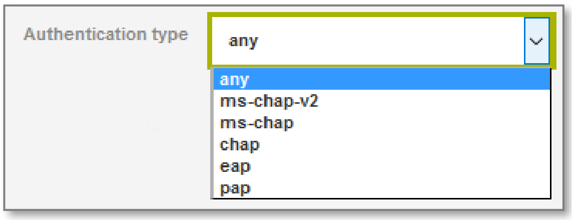
8 In the **PPTP server** field, enter the IP address of the PPTP server.

9 From the **Authentication type** drop down list, select the Authentication type used on the server.

There are 5 authentication types you can choose from:

a **Any –** Select if you do not know the authentication method to use and the router will attempt to determine the correct authentication type for you.

b **MS-CHAP v2** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol which was introduced in Windows® NT 4.0 and is still supported today.


Authentication type: any

c **MS-CHAP** – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.

d **CHAP** – uses a three-way handshake to authenticate the identity of a client.

e **EAP** – The Extensible Authentication Protocol is an authentication protocol commonly used in wireless networks.

f **PAP** – The Password Authentication Protocol uses a password as a means of authentication and as such, is commonly supported. PAP is not recommended because it transmits passwords unencrypted and is not secure.

10 The **metric** value helps the router to prioritise routes and must be a number between 0 and 65535. The default value is 30 and should not be modified unless you are aware of the effect your changes will have.

11 The **Use peer DNS** option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Click the toggle key to set this to ON or OFF as required.

12 **NAT masquerading** allows the router to modify the packets sent and received to inform remote computers on the internet that packets originating from a machine behind the router actually originated from the WAN IP address of the router's internal NAT IP address. Click the toggle key to switch this to the ON position if you want to use this feature.

13 **Set PPTP server as default gateway** sets all outbound data packets to go out through the PPTP tunnel. Click the toggle key to switch this to the ON position if you want to use this feature.

14 The **MPPE** toggle key turns the Microsoft Point-to-Point Encryption feature on or off. This is used to secure transmissions.

15 In the **Extra PPP option** field, specify any extra commands or parameters that you wish to use when the PPP connection is established.

16 The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System Log** section of the router interface.

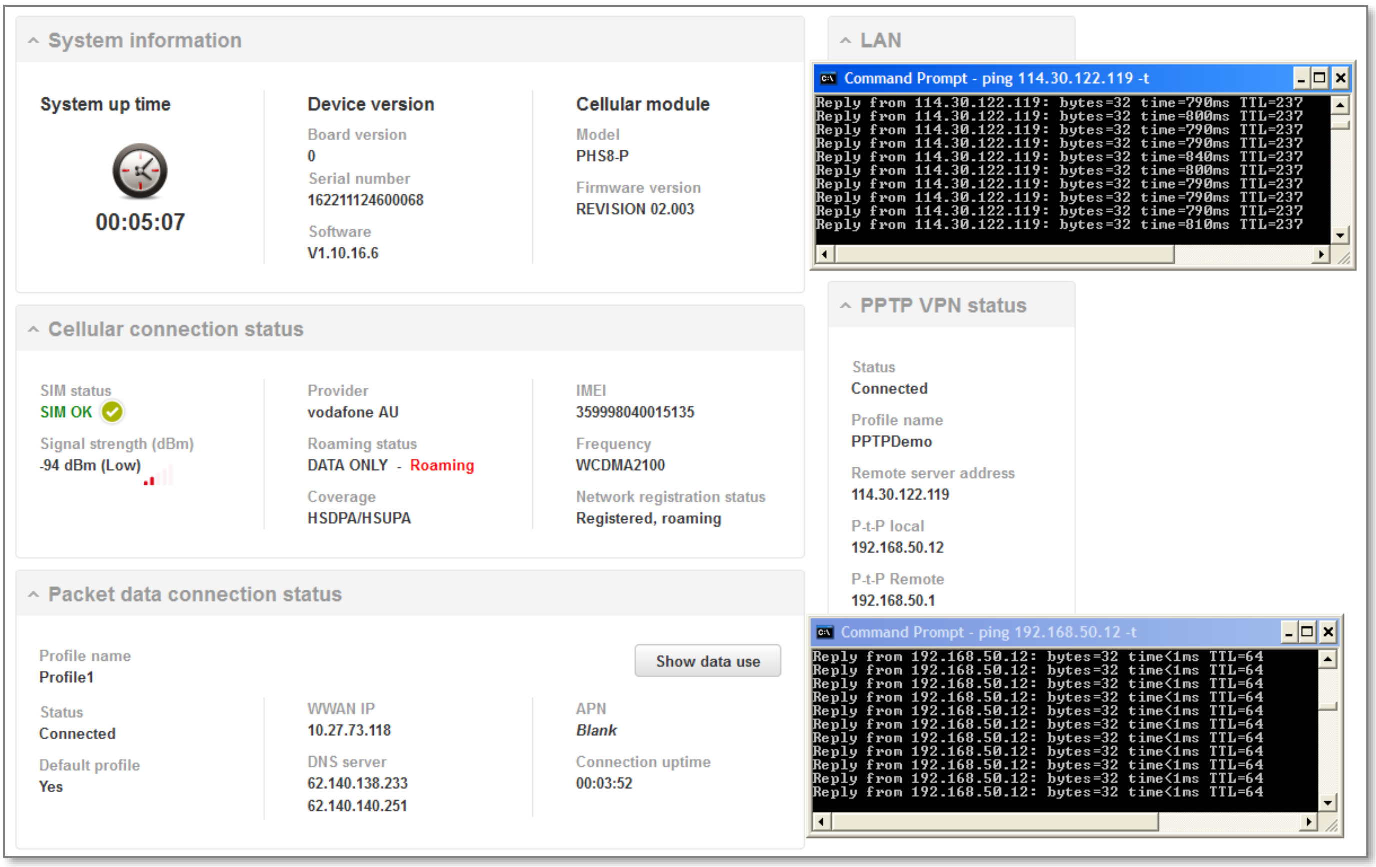
17 The **Reconnect delay** is the time in seconds that the router will wait before attempting to connect to the PPTP server in the event that the connection is broken. The minimum time to wait is 30 seconds so as to not flood the PPTP server with connection requests, while the maximum time to wait is 65335 seconds.

18 The **Reconnect retries** is the number of connection attempts that the router will make in the event that the PPTP connection goes down. If set to 0, the router will retry the connection indefinitely, otherwise the maximum number of retries cannot be greater than 65335.

19 Click the **Save** button to save the changes. The VPN will attempt to connect after your click Save. Click the **Status** button at the top left of the interface to return to the status window and monitor the VPN's connection state.

Verifying the PPTP Connection Status

Perform a ping test in both directions. On the server, open a command prompt and ping the client IP address (shown under **P-t-P Local**). To test the tunnel in the other direction, telnet to the client router (username: `root` password: `admin`) and ping the **P-t-P Remote** IP address. See the screenshots below for an example.



System information

System up time
00:05:07

Device version
Board version
0
Serial number
162211124600068
Software
V1.10.16.6

Cellular module
Model
PHS8-P
Firmware version
REVISION 02.003

Cellular connection status

SIM status
SIM OK ✓
Signal strength (dBm)
-94 dBm (Low)

Provider
vodafone AU
Roaming status
DATA ONLY - Roaming
Coverage
HSDPA/HSUPA

IMEI
359998040015135
Frequency
WCDMA2100
Network registration status
Registered, roaming

Packet data connection status

Profile name
Profile1
Status
Connected
Default profile
Yes

WWAN IP
10.27.73.118
DNS server
62.140.138.233
62.140.140.251

Show data use

APN
Blank
Connection uptime
00:03:52

LAN

Command Prompt - ping 114.30.122.119 -t

```
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=800ms TTL=237
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=840ms TTL=237
Reply from 114.30.122.119: bytes=32 time=800ms TTL=237
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=790ms TTL=237
Reply from 114.30.122.119: bytes=32 time=810ms TTL=237
```

PPTP VPN status

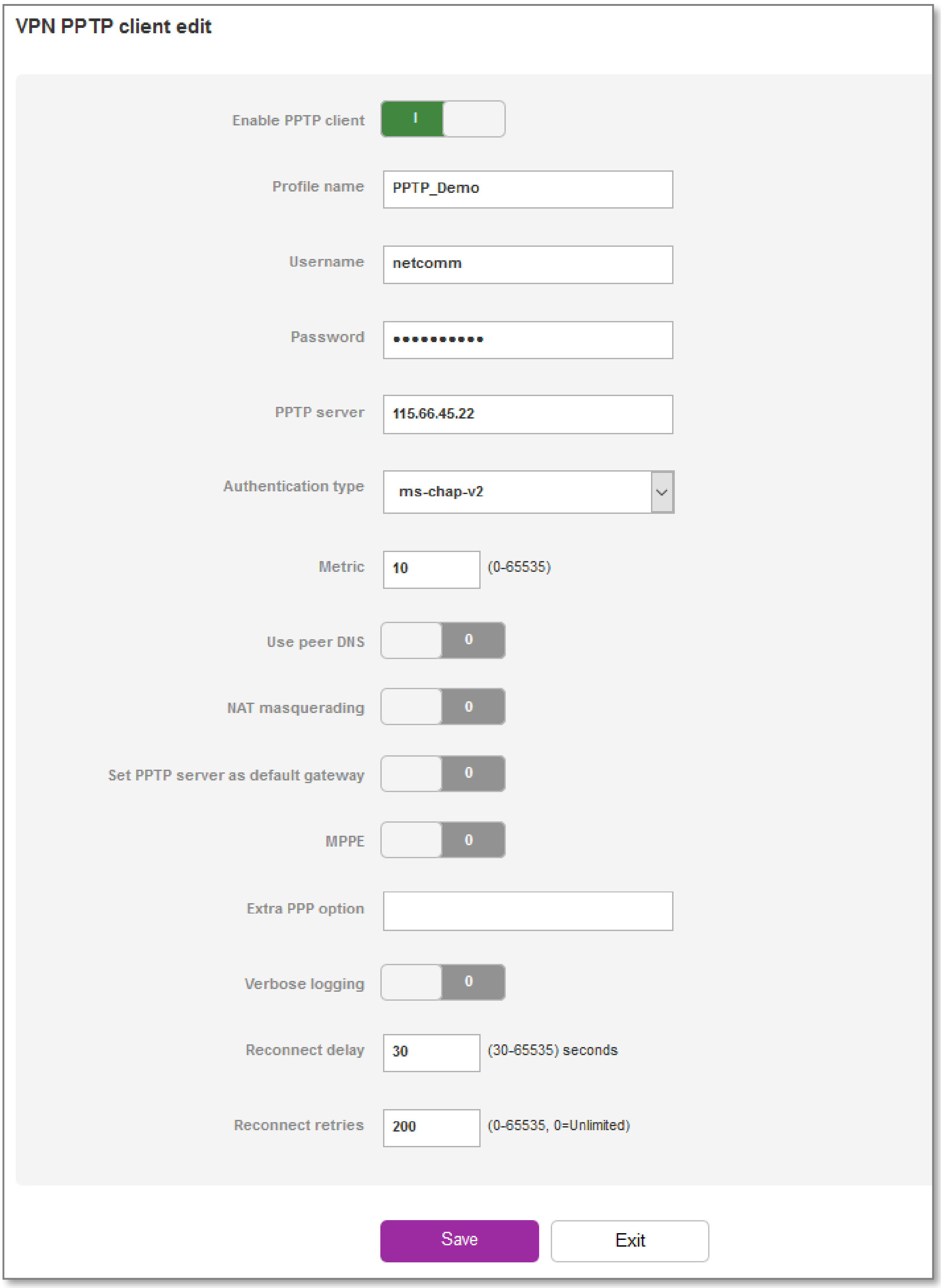
Status
Connected
Profile name
PPTPDemo
Remote server address
114.30.122.119
P-t-P local
192.168.50.12
P-t-P Remote
192.168.50.1

Command Prompt - ping 192.168.50.12 -t

```
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
Reply from 192.168.50.12: bytes=32 time<1ms TTL=64
```

Figure 4 – PPTP connection verification

PPTP Configuration Example



VPN PPTP client edit

Enable PPTP client	I
Profile name	PPTP_Demo
Username	netcomm
Password	•••••••••••
PPTP server	115.66.45.22
Authentication type	ms-chap-v2
Metric	10 (0-65535)
Use peer DNS	0
NAT masquerading	0
Set PPTP server as default gateway	0
MPPE	0
Extra PPP option	
Verbose logging	0
Reconnect delay	30 (30-65535) seconds
Reconnect retries	200 (0-65535, 0=Unlimited)

Figure 5 – PPTP Client configuration example