PPTP 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	November 2012

Table 1 - Document Revision History

ℹ 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 Series routers support 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, NetComm Wireless M2M Series Routers have 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 NetComm Wireless M2M Series Routers.

PPTP Overview

The following diagram illustrates a typical PPTP usage scenario:

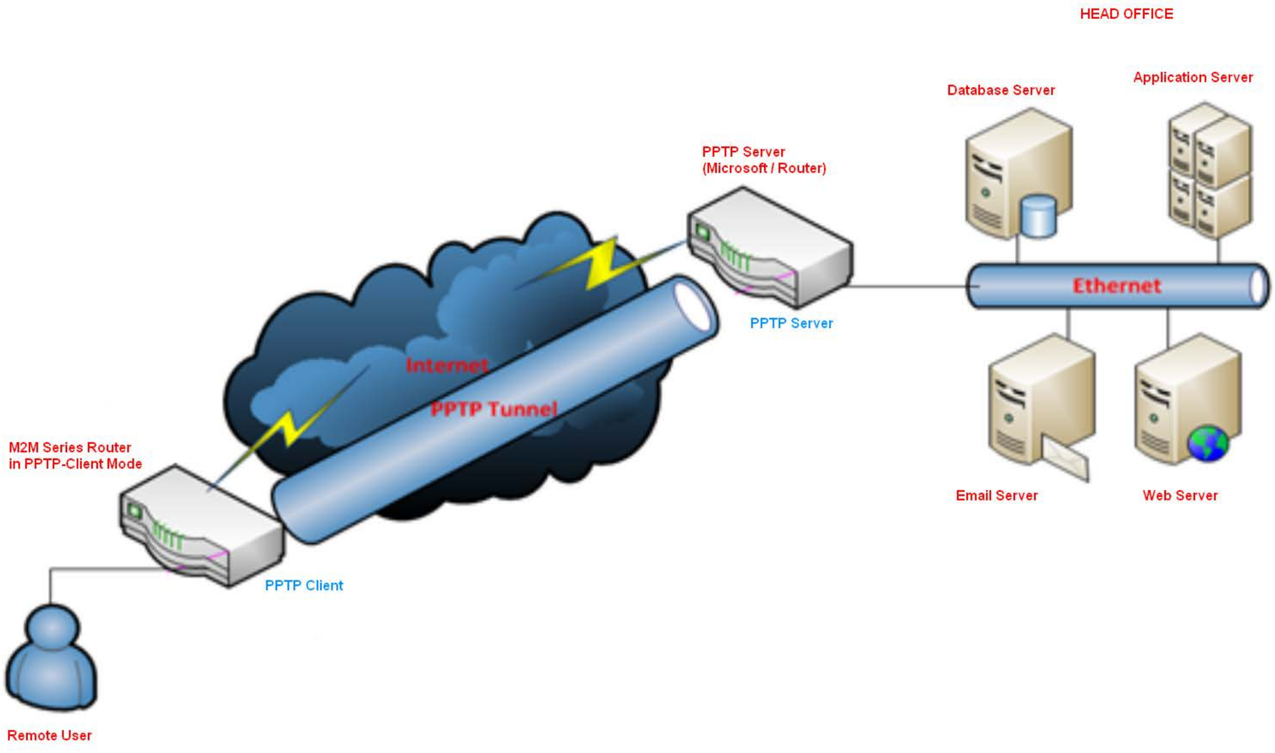
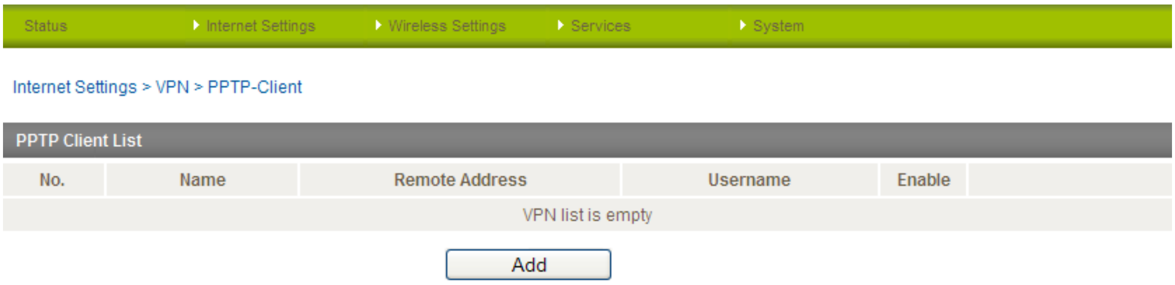


Figure 1 - PPTP Diagram

Configuring the PPTP Client

1. Log in to your NetComm Wireless M2M Series Router using the "root" account.
2. Click on **Internet Settings**, **VPN**, then **PPTP**. The PPTP VPN List is displayed.

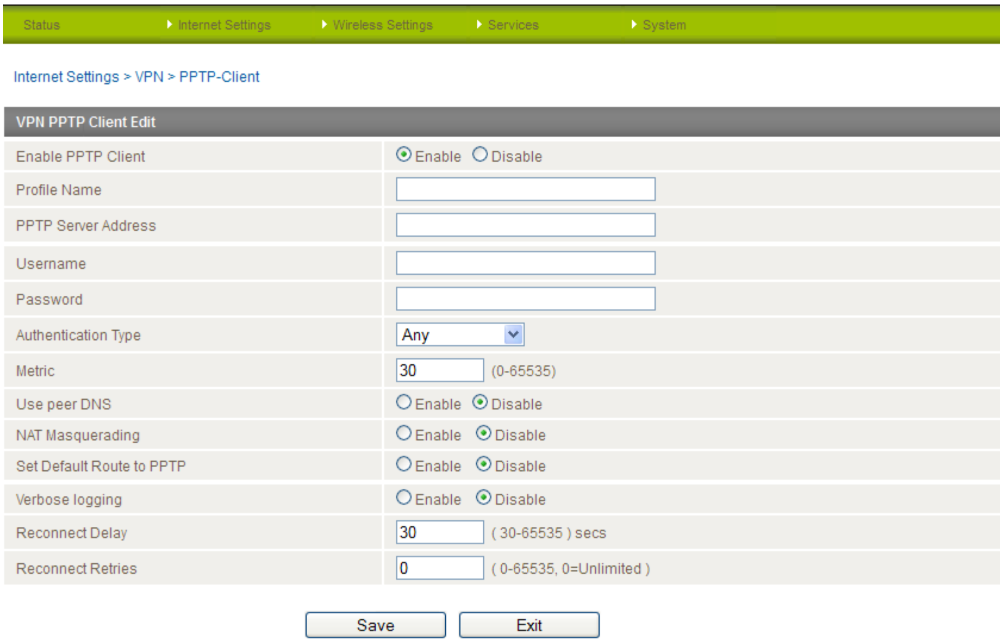


PPTP Client List

No.	Name	Remote Address	Username	Enable	
VPN list is empty					

Figure 2 - PPTP Client List

3. Click the **Add** button. The Configuration screen is displayed.



VPN PPTP Client Edit

Enable PPTP Client	● Enable ○ Disable
Profile Name	
PPTP Server Address	
Username	
Password	
Authentication Type	Any
Metric	30 (0-65535)
Use peer DNS	○ Enable ● Disable
NAT Masquerading	○ Enable ● Disable
Set Default Route to PPTP	○ Enable ● Disable
Verbose logging	○ Enable ● Disable
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)

Figure 3 - PPTP Configuration screen

4. Set the PPTP Client to **Enable**.
5. Enter a Profile Name for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
6. Enter the PPTP Server Address.

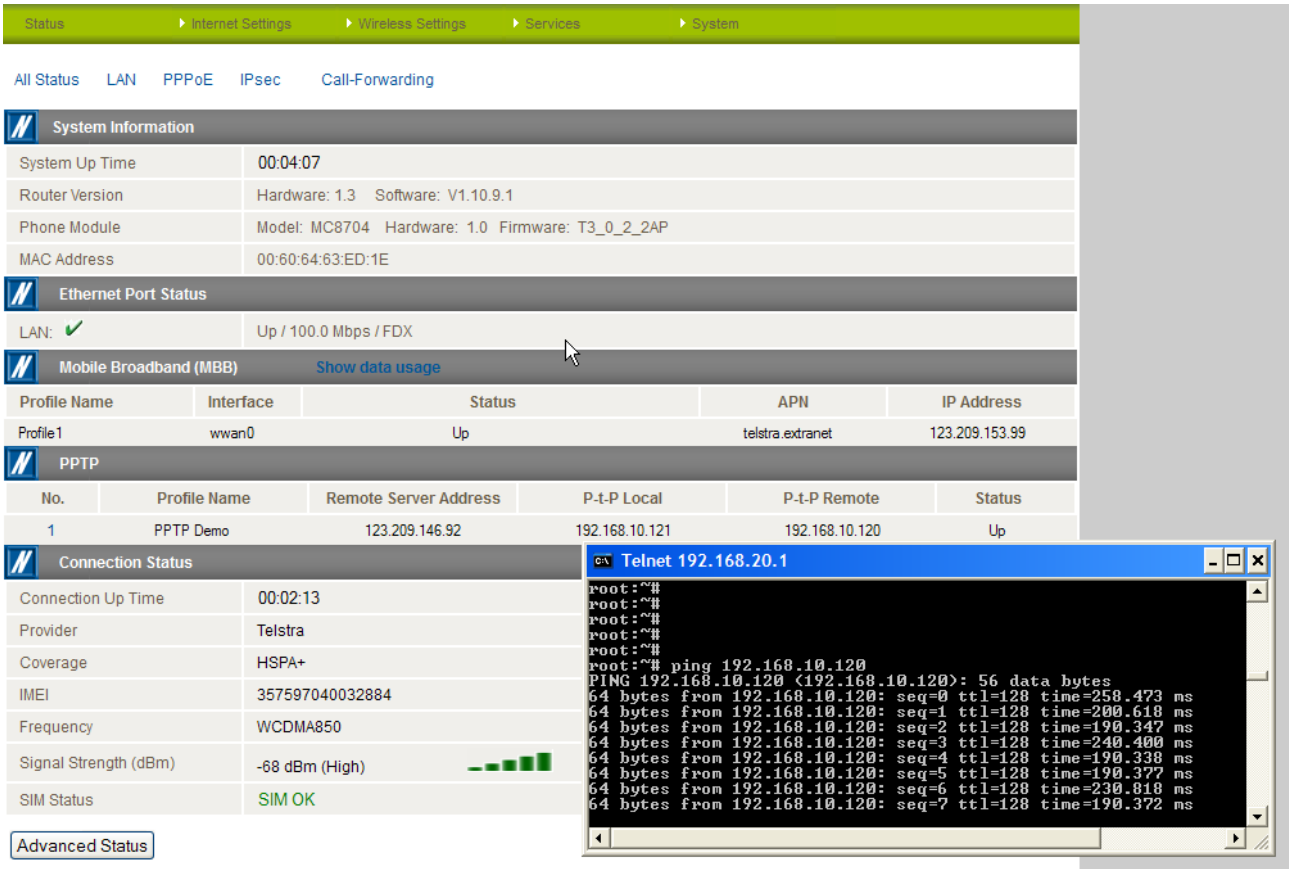
Note: The PPTP Server Address must be an IP Address. Domain names are not supported.

7. Enter the username and password for the PPTP account.

8. Select the Authentication Type used on the server from the drop down list. If you do not know the authentication method used, select **Any** and the router will attempt to determine the correct authentication type for you. There are 5 authentication types you can choose from:
    a) CHAP – uses a three way handshake to authenticate the identity of a client.
    b) MS-CHAP v1 – This is the Microsoft implementation of the Challenge Handshake Authentication Protocol for which support was dropped in Windows® Vista.
    c) 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.
    d) 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.
    e) EAP – Extensible Authentication Protocol. An Authentication protocol commonly used in wireless networks.
9. Enter the Metric for the tunnel. 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.
10. The Use peer DNS option allows you to select whether the remote clients will use the Domain Name Server of the PPTP server. Set this to Enable or Disable as required.
11. 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. Select Enable if you want to use this feature.
12. Set Default Route to PPTP sets all outbound data packets to go out through the PPTP tunnel. Use the radio buttons to Enable or Disable this option.
13. The Verbose Logging option sets the router to output detailed logs regarding the PPTP connection in the **System > Log** section of the router.
14. Set the Reconnect Delay. 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.
15. Set the number of Reconnect Retries that the router will make in the event that the PPTP connection goes down. If set to 0, the server will retry the connection indefinitely, otherwise the maximum number of times to retry must not be greater than 65335.
16. 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: `bovine`) and ping the **P-t-P Remote** IP address. See the screenshots below for an example.



System Information

System Up Time	00:04:07
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

PPTP

No.	Profile Name	Remote Server Address	P-t-P Local	P-t-P Remote	Status
1	PPTP Demo	123.209.146.92	192.168.10.121	192.168.10.120	Up

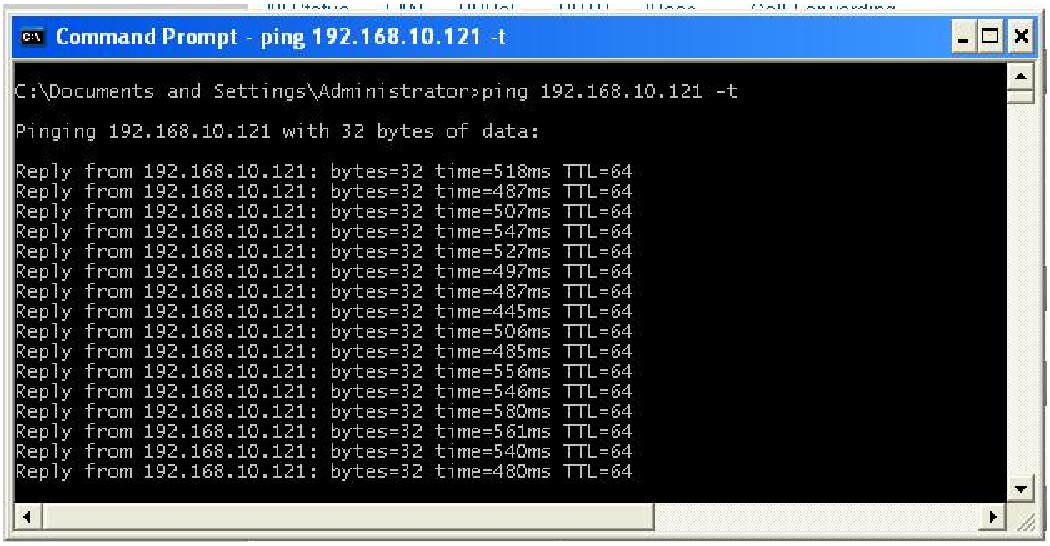
Connection Status

Connection Up Time	00:02:13
Provider	Telstra
Coverage	HSPA+
IMEI	357597040032884
Frequency	WCDMA850
Signal Strength (dBm)	-68 dBm (High)
SIM Status	SIM OK

Telnet 192.168.20.1

```
root:~#
root:~#
root:~#
root:~#
root:~#
root:~# ping 192.168.10.120
PING 192.168.10.120 (192.168.10.120): 56 data bytes
64 bytes from 192.168.10.120: seq=0 ttl=128 time=258.473 ms
64 bytes from 192.168.10.120: seq=1 ttl=128 time=200.618 ms
64 bytes from 192.168.10.120: seq=2 ttl=128 time=190.347 ms
64 bytes from 192.168.10.120: seq=3 ttl=128 time=240.400 ms
64 bytes from 192.168.10.120: seq=4 ttl=128 time=190.338 ms
64 bytes from 192.168.10.120: seq=5 ttl=128 time=190.377 ms
64 bytes from 192.168.10.120: seq=6 ttl=128 time=230.818 ms
64 bytes from 192.168.10.120: seq=7 ttl=128 time=190.372 ms
```

Figure 4 – PPTP connection verification



Command Prompt - ping 192.168.10.121 -t

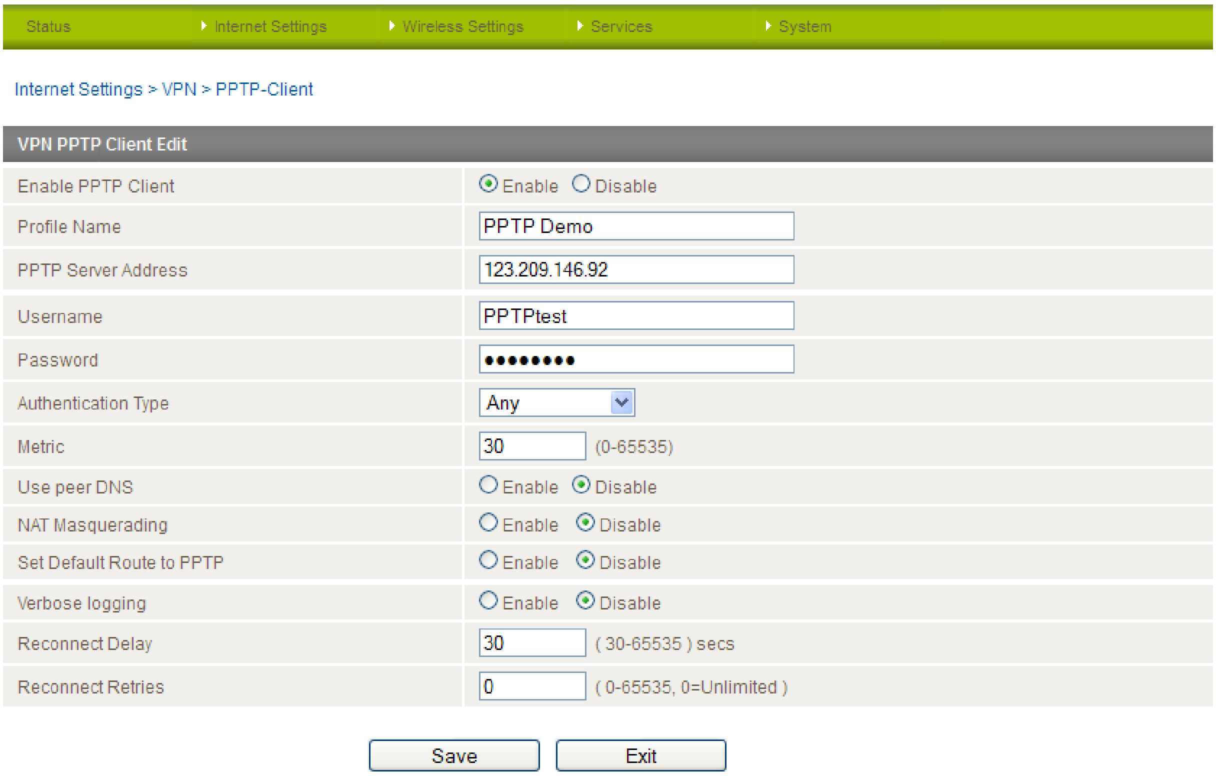
```
C:\Documents and Settings\Administrator>ping 192.168.10.121 -t

Pinging 192.168.10.121 with 32 bytes of data:

Reply from 192.168.10.121: bytes=32 time=518ms TTL=64
Reply from 192.168.10.121: bytes=32 time=487ms TTL=64
Reply from 192.168.10.121: bytes=32 time=507ms TTL=64
Reply from 192.168.10.121: bytes=32 time=547ms TTL=64
Reply from 192.168.10.121: bytes=32 time=527ms TTL=64
Reply from 192.168.10.121: bytes=32 time=497ms TTL=64
Reply from 192.168.10.121: bytes=32 time=487ms TTL=64
Reply from 192.168.10.121: bytes=32 time=445ms TTL=64
Reply from 192.168.10.121: bytes=32 time=506ms TTL=64
Reply from 192.168.10.121: bytes=32 time=485ms TTL=64
Reply from 192.168.10.121: bytes=32 time=556ms TTL=64
Reply from 192.168.10.121: bytes=32 time=546ms TTL=64
Reply from 192.168.10.121: bytes=32 time=580ms TTL=64
Reply from 192.168.10.121: bytes=32 time=561ms TTL=64
Reply from 192.168.10.121: bytes=32 time=540ms TTL=64
Reply from 192.168.10.121: bytes=32 time=480ms TTL=64
```

Figure 5 - Ping from Server to Client

PPTP Configuration Example



Internet Settings > VPN > PPTP-Client

VPN PPTP Client Edit

Enable PPTP Client	● Enable ○ Disable
Profile Name	PPTP Demo
PPTP Server Address	123.209.146.92
Username	PPTPtest
Password	••••••••
Authentication Type	Any
Metric	30 (0-65535)
Use peer DNS	○ Enable ● Disable
NAT Masquerading	○ Enable ● Disable
Set Default Route to PPTP	○ Enable ● Disable
Verbose logging	○ Enable ● Disable
Reconnect Delay	30 (30-65535) secs
Reconnect Retries	0 (0-65535, 0=Unlimited)

Figure 6 – PPTP Client configuration example