NetCommWireless

# PPTP
# Technical Support Guide

Copyright

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

| DOCUMENT VERSION | DATE |
|---|---|
| 1.0 - Initial document release | 15 March 2016 |

*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

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 routers have a PPTP client built-in allowing you to use this method of securing your data connection.

This document describes how to configure the PPTP client on NetComm Wireless M2M routers.

# PPTP Overview

The following diagram illustrates a typical PPTP usage scenario:

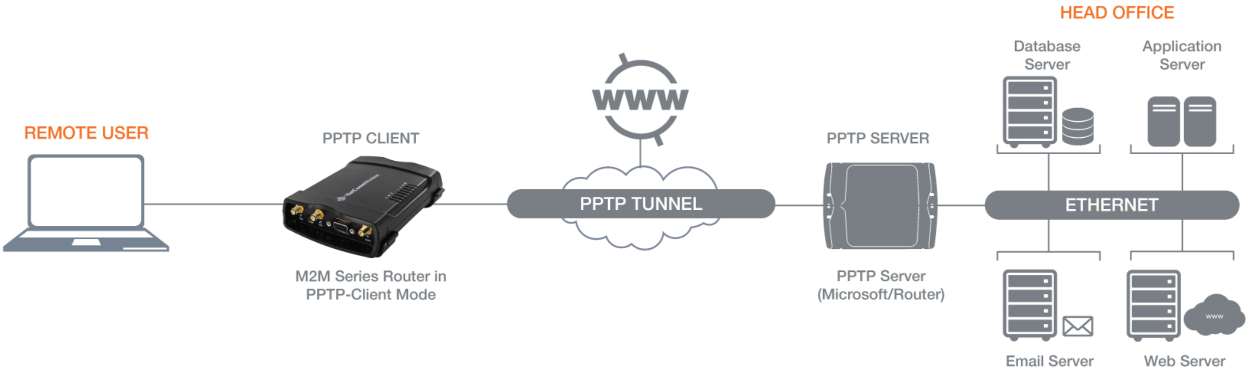
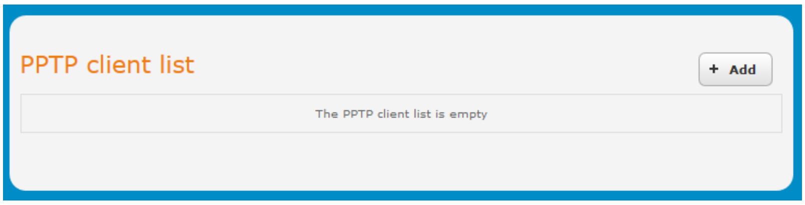


*Figure 1 - PPTP Diagram*

## Configuring the PPTP Client

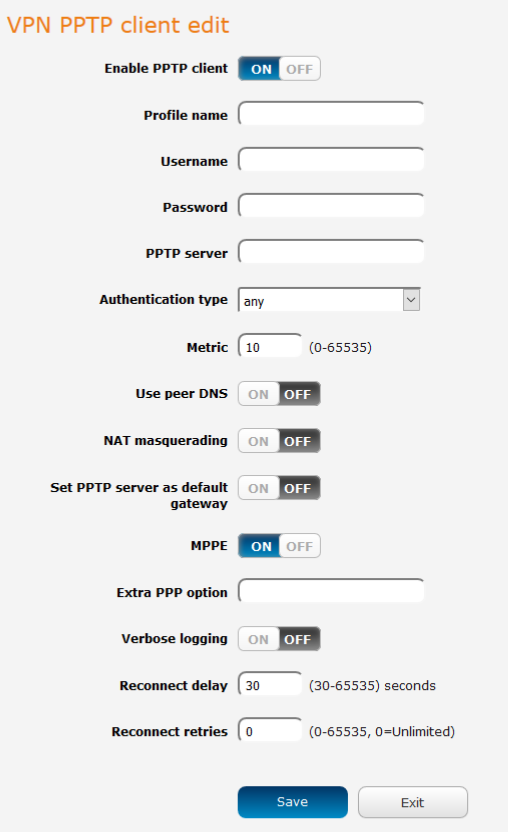
1. Log in to your NetComm Wireless M2M router using the “root” account.
2. Click on Networking, VPN, then PPTP client. The PPTP client list is displayed.



PPTP client list

The PPTP client list is empty

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

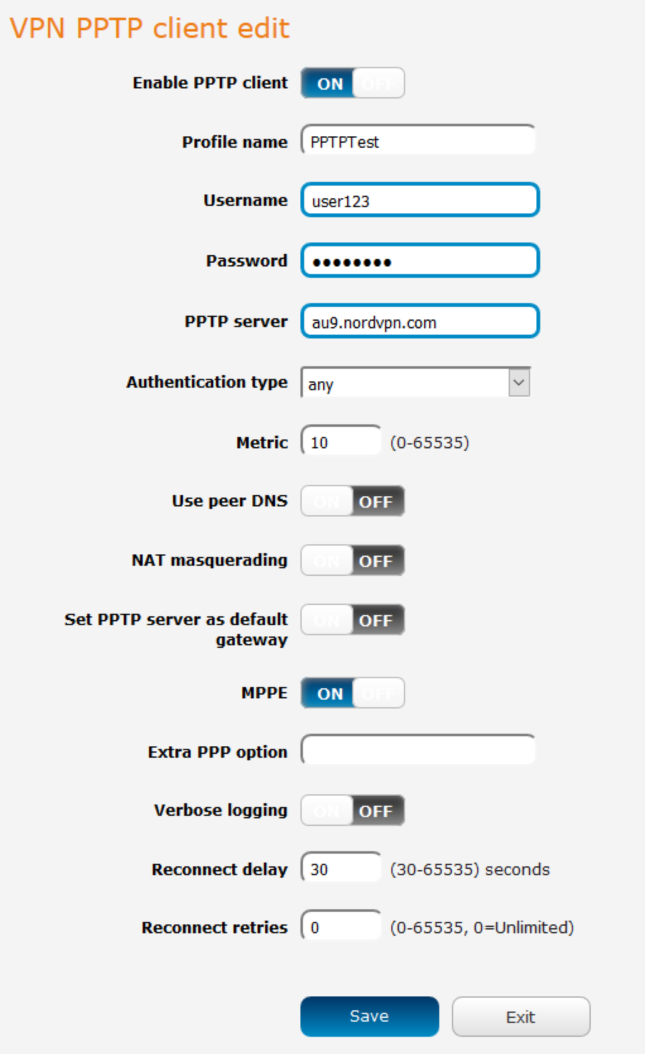


VPN PPTP client edit

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

4. Enter a **Profile name** for the tunnel. This may be anything you like and is used to identify the tunnel on the router.
5. Enter the **Username** and **Password** for the PPTP account.
6. Enter the **PPTP server** address.
7. 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.
8. 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.
9. 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.
10. **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.
11. **Set PPTP server as default gateway** sets all outbound data packets to go out through the PPTP tunnel. Use the radio buttons to Enable or Disable this option.
12. By default, **MPPE**, or Microsoft Point-to-Point Encryption, is on. This provides data security for the PPTP connection between the client and server. If you wish to disable this, click the toggle key so that it is in the OFF position.
13. You can use the **Extra PPP option** field to specify any parameters that you may wish to use for the tunnel.
14. The **Verbose logging** option sets the router to output detailed logs regarding the PPTP connection in the **System > Log** section of the router.
15. 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.
16. 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.
17. 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.

The screenshot below displays an example of the settings that were used to configure the PPTP client for this document.



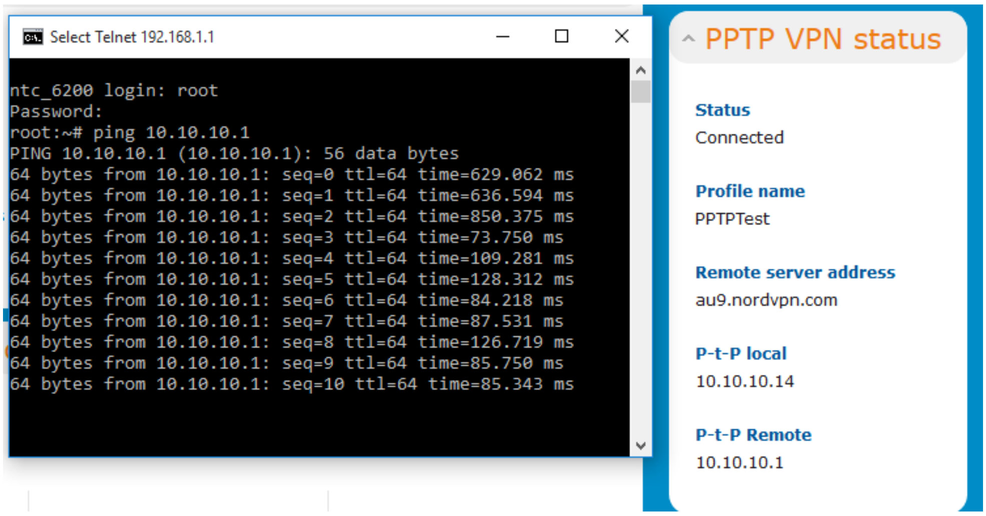
VPN PPTP client edit

| | |
|---|---|
| Enable PPTP client | ON |
| Profile name | PPTPTest |
| Username | user123 |
| Password | •••••••• |
| PPTP server | au9.nordvpn.com |
| Authentication type | any |
| Metric | 10 (0-65535) |
| Use peer DNS | OFF |
| NAT masquerading | OFF |
| Set PPTP server as default gateway | OFF |
| MPPE | ON |
| Extra PPP option | |
| Verbose logging | OFF |
| Reconnect delay | 30 (30-65535) seconds |
| Reconnect retries | 0 (0-65535, 0=Unlimited) |

*Figure 2 - Example configuration of the PPTP client*

## Verifying the PPTP Connection Status

Perform a ping test from the client to the server. Telnet to the client router (username: `root` password: `admin`) and ping the **P-t-P Remote** IP address. See the screenshot below for an example.



```
ntc_6200 login: root
Password:
root:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1): 56 data bytes
64 bytes from 10.10.10.1: seq=0 ttl=64 time=629.062 ms
64 bytes from 10.10.10.1: seq=1 ttl=64 time=636.594 ms
64 bytes from 10.10.10.1: seq=2 ttl=64 time=850.375 ms
64 bytes from 10.10.10.1: seq=3 ttl=64 time=73.750 ms
64 bytes from 10.10.10.1: seq=4 ttl=64 time=109.281 ms
64 bytes from 10.10.10.1: seq=5 ttl=64 time=128.312 ms
64 bytes from 10.10.10.1: seq=6 ttl=64 time=84.218 ms
64 bytes from 10.10.10.1: seq=7 ttl=64 time=87.531 ms
64 bytes from 10.10.10.1: seq=8 ttl=64 time=126.719 ms
64 bytes from 10.10.10.1: seq=9 ttl=64 time=85.750 ms
64 bytes from 10.10.10.1: seq=10 ttl=64 time=85.343 ms
```

PPTP VPN status

Status
Connected

Profile name
PPTPTest

Remote server address
au9.nordvpn.com

P-t-P local
10.10.10.14

P-t-P Remote
10.10.10.1

*Figure 3 – PPTP connection verification*