

M2M CDMA Router



GRE Configuration Guide

Copyright

Copyright© 2013 NetComm Wireless Limited. All rights reserved.

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



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

DOCUMENT VERSION	DATE
Initial document release	November 2013

Table 1 - 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://www.netcommwireless.com/product/m2m/nwl-11> 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.



Table of contents

Introduction	4
Configuring a GRE VPN Connection.....	5
GRE VPN Example Configuration	7
Verifying the GRE VPN Connection Status.....	8

Introduction

A VPN (Virtual private network) is a secure connection between two or more endpoints over a public network such as the Internet. It can also be seen as an extension of 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 is 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.

Generic Routing Encapsulation (GRE) is an example of a remote access VPN. It is a tunneling protocol developed by Cisco that allows the encapsulation of a wide variety of network layer protocols inside point-to-point links. When sending packets between endpoints connected over the Internet, a GRE virtual tunnel between them is created and is used to facilitate the transport of the packets.

An important difference between a GRE tunnel and the other VPN protocols available on the MachineLink 3G Router is that the GRE tunnel is not encrypted and only provides encapsulation. If you require data protection, you should configure IPSec for data confidentiality. Please refer to the **IPSec Configuration Guide** available at <http://www.netcommwireless.com/product/m2m/nwl-11> for further details.

Configuring a GRE VPN Connection

The following instructions describe a real world example of how to configure a GRE VPN connection:

1. Click on the **Internet** menu, click the **VPN** menu on the left, and then click the **GRE** menu item. The GRE client list appears.

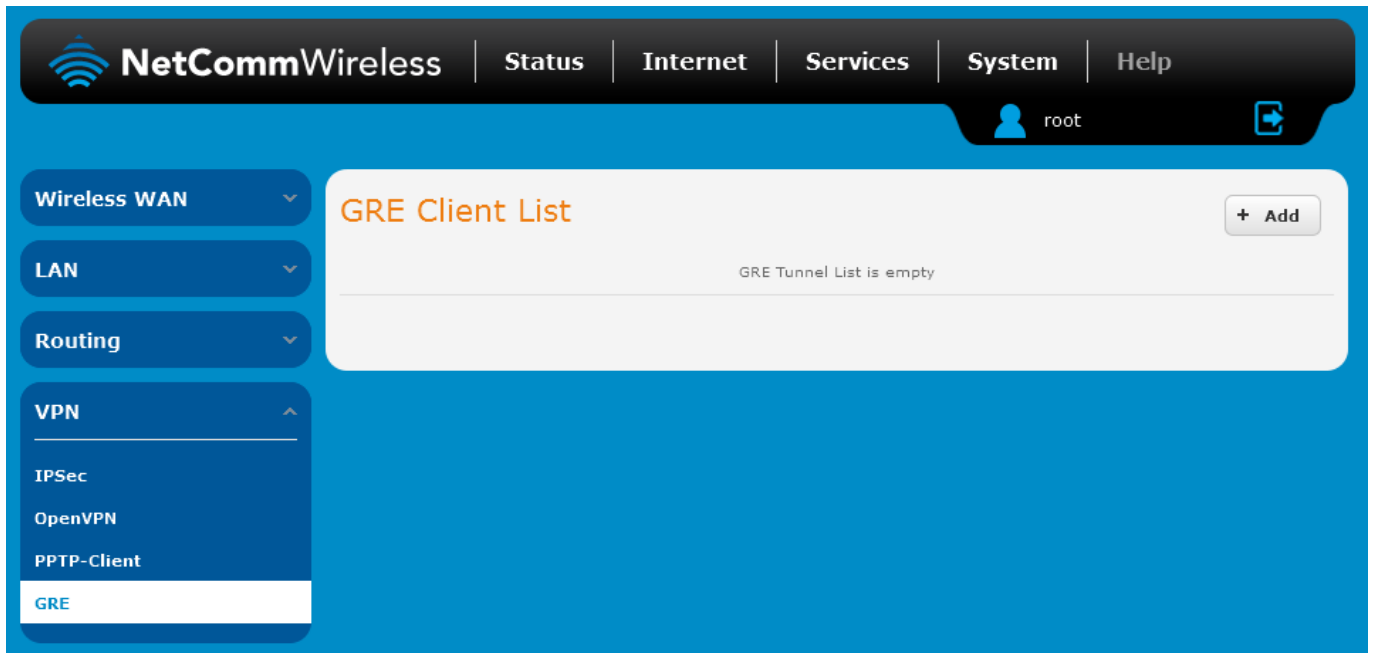


Figure 1 - GRE Client List

2. Click the **+Add** button to begin configuring a GRE profile. The GRE client edit page appears.

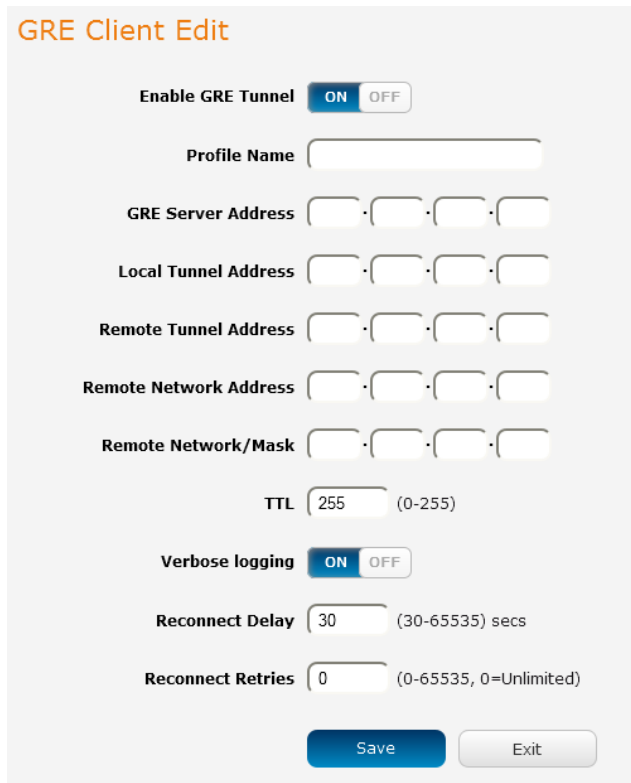
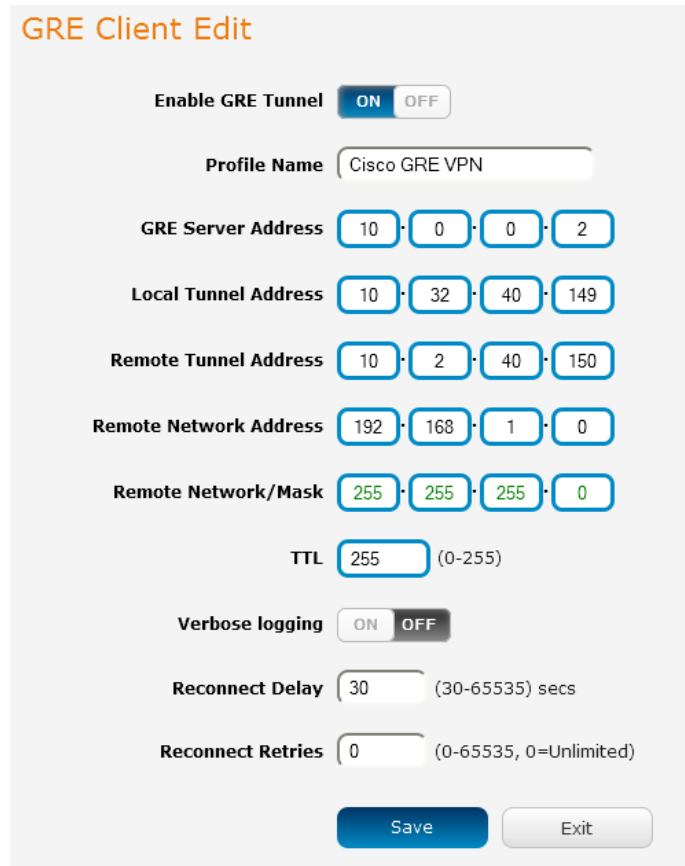


Figure 2 - GRE Client Edit

3. Click the **Enable GRE Tunnel** toggle key to set it to the **ON** position.
4. In the **Profile name** field, enter a name for the profile. This is just a name to identify the profile on the router.
5. In the **GRE Server Address** field, enter the GRE Server Address. This is the destination of the GRE VPN tunnel, for example, the remote Cisco router.
6. In the **Local Tunnel Address** field, enter the local IP address of the virtual GRE tunnel.
7. In the **Remote Tunnel Address** field, enter the remote IP address of the virtual GRE tunnel.
8. The **Remote Network/Mask** fields add a static route to the remote side's subnet so that the remote network is known to the local network. Enter the remote network address and mask.
9. The **TTL** (Time To Live) value indicates the number of hops that a packet may take during its life on the network. Each router that receives the packet subtracts a count from the number of hops. When the TTL for a packet reaches 0, the receiving router discards the packet and sends the originating host an ICMP message. The maximum value is 255. In most cases you will not need to change the TTL value but if you wish to change it, enter a value between 0 and 255 in the TTL field.
10. **Verbose logging** creates larger and more detailed logs and is therefore best used for troubleshooting problems with the VPN. For this reason, we recommend that you leave Verbose logging disabled unless you performing troubleshooting.
11. The **Reconnect delay** option specifies the time that the router should wait before trying to re-establish a connection in the event that a connection is broken.
12. The **Reconnect retries** option specifies the number of attempts that should be made to re-establish the VPN connection in the event that a connection is broken.

GRE VPN Example Configuration

The M2M CDMA Router configuration below is a real world example of a GRE VPN. In this example, the M2M CDMA Router has a WAN IP address of 10.0.0.5 and a Local LAN IP address of 192.168.20.1.



GRE Client Edit

Enable GRE Tunnel ON OFF

Profile Name Cisco GRE VPN

GRE Server Address 10 · 0 · 0 · 2

Local Tunnel Address 10 · 32 · 40 · 149

Remote Tunnel Address 10 · 2 · 40 · 150

Remote Network Address 192 · 168 · 1 · 0

Remote Network/Mask 255 · 255 · 255 · 0

TTL 255 (0-255)

Verbose logging ON OFF

Reconnect Delay 30 (30-65535) secs

Reconnect Retries 0 (0-65535, 0=Unlimited)

Save **Exit**

Figure 3 – M2M CDMA Router GRE VPN example configuration

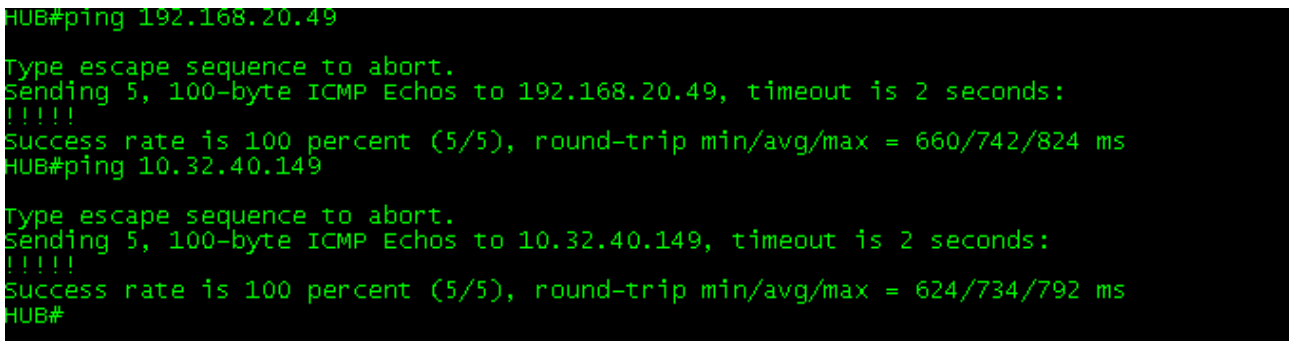
Cisco Router Configuration

The following is an excerpt of the configuration from a Cisco Router configured for GRE.

```
interface Tunnel0
  ip address 10.32.40.150 255.255.255.252
  ip mtu 1476
  tunnel source Dialer1
  tunnel destination 10.0.0.5
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
  pppoe enable
  pppoe-client dial-pool-number 1
  no cdp enable
!
interface FastEthernet0/1
  ip address 192.168.1.80 255.255.255.0
  no ip redirects
  duplex auto
  speed auto
```

Verifying the GRE VPN Connection Status

Perform a ping test from the Cisco router to a PC behind the M2M CDMA Router.



```
HUB#ping 192.168.20.49
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.49, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 660/742/824 ms
HUB#ping 10.32.40.149
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.32.40.149, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 624/734/792 ms
HUB#
```

Figure 4 - Ping from Cisco router to PC behind the M2M CDMA Router

Perform a ping test from a PC behind the M2M CDMA Router to the IP address of the Cisco router and then the VPN tunnel address of the Cisco router.

```
C:\Documents and Settings\congh>ping 192.168.1.80 -t
Pinging 192.168.1.80 with 32 bytes of data:
Reply from 192.168.1.80: bytes=32 time=20ms TTL=254
Reply from 192.168.1.80: bytes=32 time=23ms TTL=254
Reply from 192.168.1.80: bytes=32 time=23ms TTL=254
Reply from 192.168.1.80: bytes=32 time=35ms TTL=254
Reply from 192.168.1.80: bytes=32 time=23ms TTL=254
Reply from 192.168.1.80: bytes=32 time=24ms TTL=254

Ping statistics for 192.168.1.80:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 35ms, Average = 24ms
Control-C
^C
C:\Documents and Settings\congh>ping 10.32.40.150 -t
Pinging 10.32.40.150 with 32 bytes of data:
Reply from 10.32.40.150: bytes=32 time=35ms TTL=254
Reply from 10.32.40.150: bytes=32 time=22ms TTL=254

Ping statistics for 10.32.40.150:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 35ms, Average = 28ms
Control-C
^C
C:\Documents and Settings\congh>
```

Figure 5 - Ping from PC to tunnel address of Cisco router