GRE 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	February 2013

Table 1 - Document Revision History

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 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 NetComm M2M 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 VPN Configuration Whitepaper** available on the NetComm Wireless website 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. Log in to the router and navigate to **Internet Settings > VPN > GRE**. The GRE Client List appears.

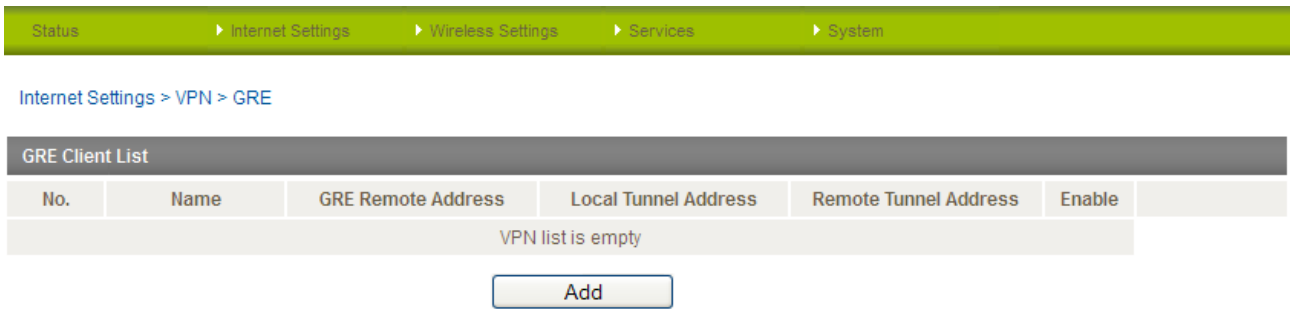

Figure 1 - GRE Client List

2. Click the **Add** button to begin configuring a GRE profile. The GRE Client Edit page appears.

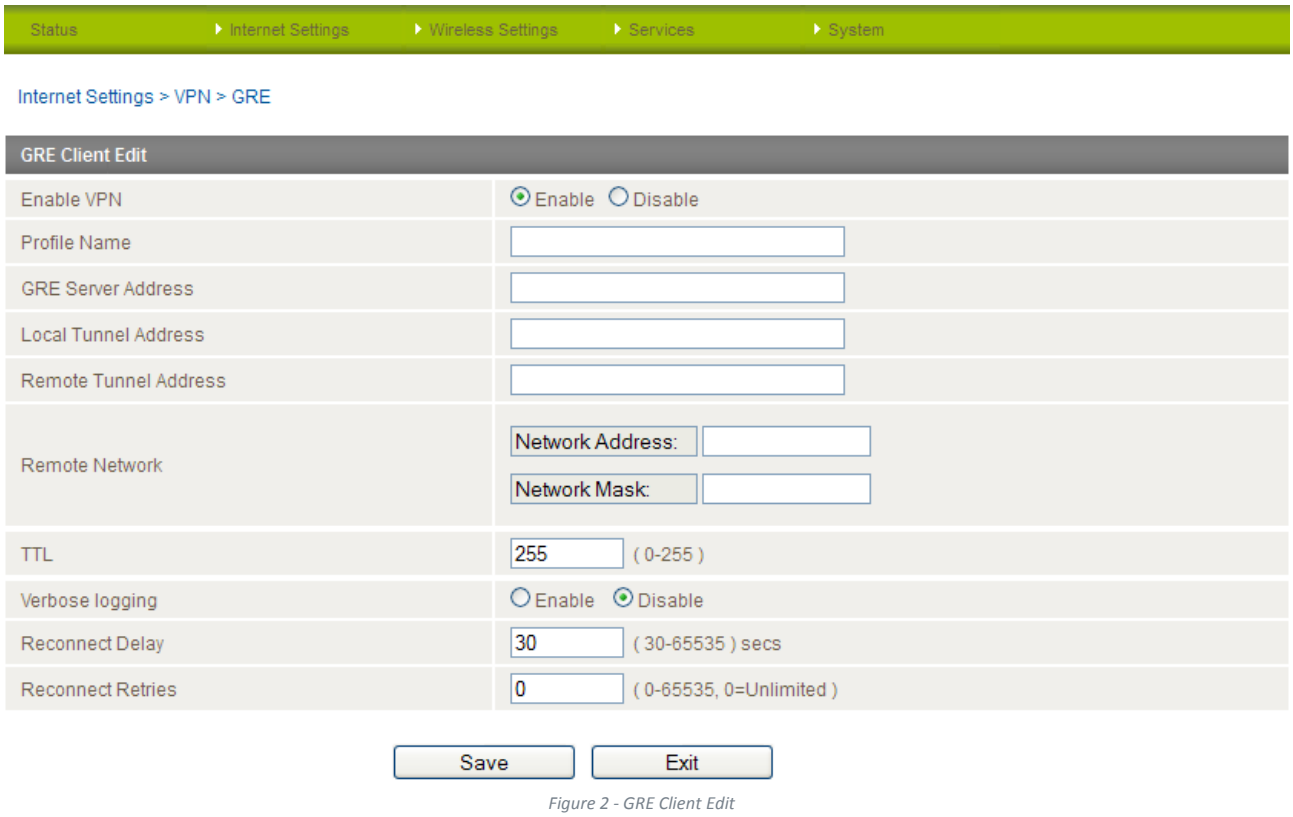

Figure 2 - GRE Client Edit

3. Set **Enable VPN** to **Enable**.

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

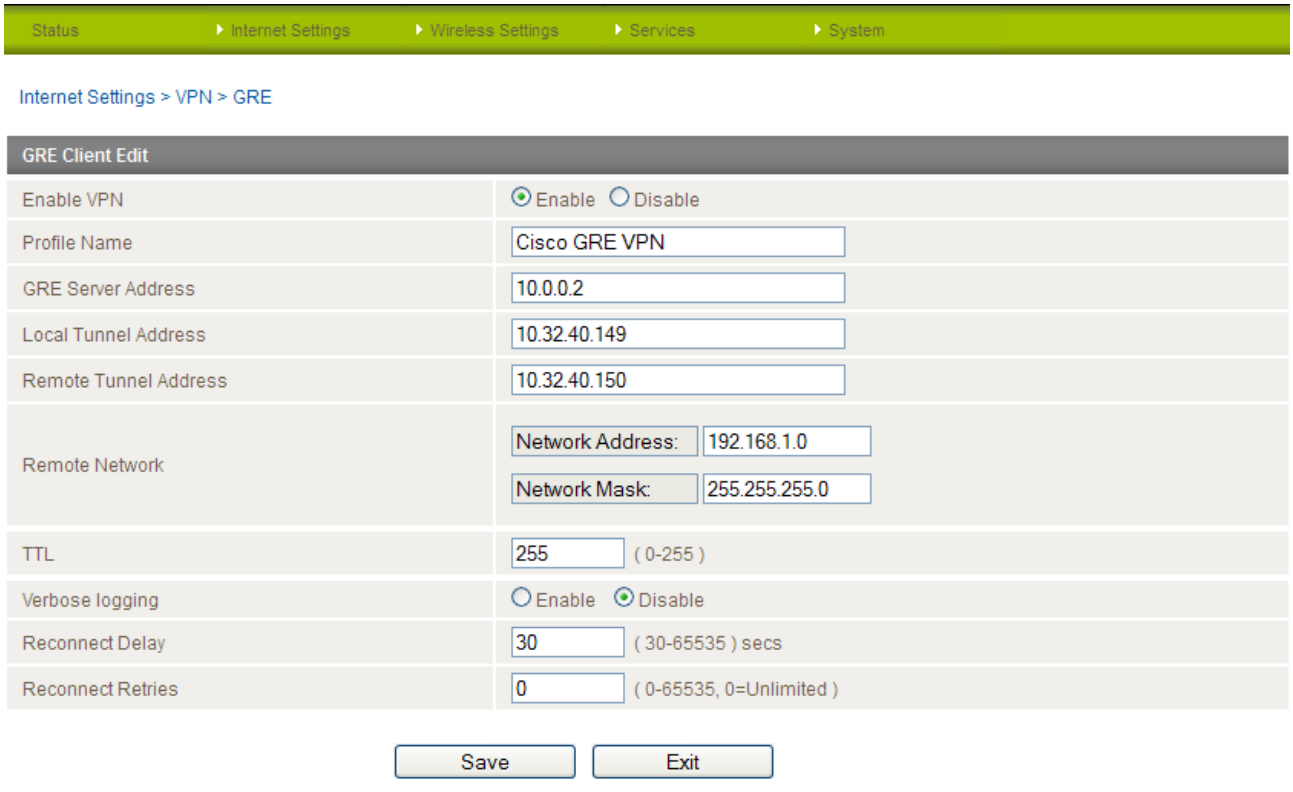

Figure 3 – NetComm Wireless M2M Router GRE VPN Example Configuration

Cisco Router Configuration

The following is a real world example of a Cisco Router configured for GRE.

```
Current configuration : 2931 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB
!
boot-start-marker
boot-end-marker
!
!
username netcomm privilege 15 password 0 netcomm
username abc privilege 15 password 0 xyz
no aaa new-model
ip subnet-zero
!
!
ip dhcp excluded-address 10.0.0.1 10.0.0.100
!
ip dhcp pool 10_0_0_0
   network 10.0.0.0 255.0.0.0
   dns-server 10.0.0.5
   default-router 10.0.0.5
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
!
!
crypto keyring RKEY
  pre-shared-key address 10.0.0.5 key CDCS
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 28880
!
crypto isakmp policy 2
 encr aes 256
 hash md5
 authentication pre-share
 group 2
 lifetime 3600
!
crypto isakmp policy 3
 encr aes 256
 authentication pre-share
 group 2
 lifetime 28880
!
crypto isakmp policy 4
 encr aes
 hash md5
 authentication rsa-encr
 group 2
 lifetime 28880
crypto isakmp identity hostname
crypto isakmp profile NTC
   keyring RKEY
   match identity address 10.0.0.5 255.255.255.255
```

```
   match identity user localntc
!
!
crypto ipsec transform-set 6908set esp-3des esp-md5-hmac
crypto ipsec transform-set richardset esp-aes 256 esp-md5-hmac
crypto ipsec transform-set richardset2 esp-aes 256 esp-sha-hmac
!
crypto dynamic-map dynmap6908 1
 description NTC6908
 set transform-set 6908set richardset richardset2
 set pfs group2
 set isakmp-profile NTC
 match address 101
 reverse-route
!
!
crypto map mymap 1 ipsec-isakmp dynamic dynmap6908
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
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 Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 ip address 192.168.1.80 255.255.255.0
 no ip redirects
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 no cdp enable
 ppp authentication chap callin
 ppp chap hostname xyz@call-direct.com.au
 ppp chap password 0 test
 ppp ipcp dns request accept
 ppp ipcp address accept
 crypto map mymap
!
ip http server
no ip http secure-server
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 10.0.0.14 255.255.255.255 Dialer1 permanent
ip route 192.168.20.0 255.255.255.0 Tunnel0
!
!
access-list 101 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 172.16.0.0 0.1.255.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 172.16.0.0 0.1.255.255 172.16.1.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login local
line aux 0
line vty 0 4
 login local
!
!
end
```

Verifying the GRE VPN Connection Status

Perform a ping test from the Cisco router to a PC behind the NetComm M2M 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 NetComm router

Perform a ping test from a PC behind the NetComm 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