

NR500 Series Industrial Cellular VPN Router

Application Note 056

GRE VPN Redundancy Between NR500 and CISCO

Version: V1.0.0
Date: Aug 2020
Status: Confidential



Directory

1. Introduction.....	3
1.1 Overview.....	3
1.2 Compatibility.....	3
1.3 Version.....	3
1.4 Corrections.....	3
2. Topology.....	4
3. Configuration.....	5
3.1 NR500 Router Configuration.....	5
3.2 CISCO Router 1 Configuration.....	8
3.3 CISCO Router 2 Configuration.....	9
4. Test.....	11

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of GRE VPN redundancy between NR500 router and CISCO.

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

1.2 Compatibility

This application note applies to:

Models Shown: NR500 series.

Firmware Version: V1.1.5 (19adafb) or newer

Other Compatible Models: None

1.3 Version

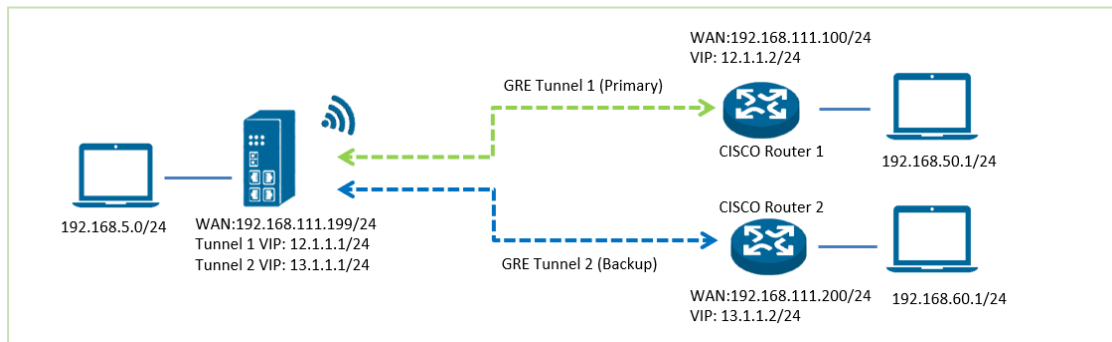
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2020/08/24	V1.0.0	V1.1.5 (19adafb)	First released

1.4 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: **support@navigateworx.com**

2. Topology



1. NR500 Pro establish two GRE VPN tunnels with remote two CISCO routers.
2. Enable VPN redundancy and set GRE Tunnel 1 as primary tunnel and it work well. The subnets between NR500 and remote CISCO router 1 can communicate with each other. At this moment, the GRE VPN tunnel 2 as backup and tunnel down.
3. When the GRE tunnel 1 down, the GRE Tunnel 2 will be up automatically and work well.
4. If the GRE tunnel 1 up again, then the router will switch back from GRE tunnel 2 to GRE tunnel 1 automatically and work well.

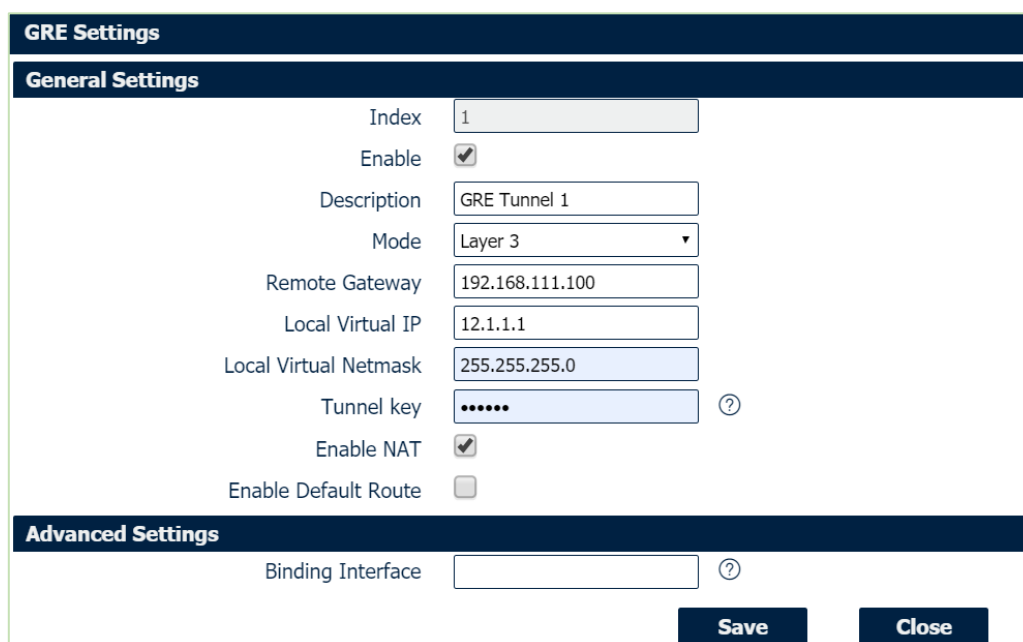
3. Configuration

3.1 NR500 Router Configuration

1. Go to **VPN>GRE>GRE**, Click the Edit button of GRE, like below:



2. Configure **GRE Tunnel 1** like below:



GRE Settings

General Settings

Index: 1

Enable:

Description: GRE Tunnel 1

Mode: Layer 3

Remote Gateway: 192.168.111.100

Local Virtual IP: 12.1.1.1

Local Virtual Netmask: 255.255.255.0

Tunnel key:

Enable NAT:

Enable Default Route:

Advanced Settings

Binding Interface:

Save **Close**

3. Click Save>Apply.

4. Follow step 1 and configure GRE Tunnel 2 like below:

GRE Settings

General Settings

Index	<input type="text" value="2"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text" value="GRE Tunnel 2"/>
Mode	<input type="text" value="Layer 3"/>
Remote Gateway	<input type="text" value="192.168.111.200"/>
Local Virtual IP	<input type="text" value="13.1.1.1"/>
Local Virtual Netmask	<input type="text" value="255.255.255.0"/>
Tunnel key	<input type="text" value="....."/> ?
Enable NAT	<input checked="" type="checkbox"/>
Enable Default Route	<input type="checkbox"/>

Advanced Settings

Binding Interface	<input type="text"/> ?
-------------------	------------------------

5. Click Save>Apply.

6. Go to **Network>Route>Route**, to configure two static routes to the subnet of cisco1 and cisco2, to make sure that the subnet can reach each other.


Login: admin

Overview
 Link Management
 Industrial Interface
 Network

Status

Route

Static Route Settings

Index	Description	IP Address	Netmask	Gateway	Interface
1	Tunnel 1 to remote subnet	192.168.50.0	255.255.255.0		

7. The static route to make **tunnel 1 to remote subnet of cisco 1**:

Static Route Settings

Static Route Settings

Index	<input type="text" value="1"/>
Description	<input type="text" value="Tunnel 1 to remote subnet"/>
IP Address	<input type="text" value="192.168.50.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text"/>
Metric	<input type="text" value="0"/> ?
Interface	<input type="text" value="gretun1"/> ?

8. The static route to make **tunnel 2 to remote subnet of cisco 2:**

Static Route Settings

Static Route Settings

Index	<input type="text" value="2"/>
Description	<input type="text" value="Tunnel 2 to remote subnet"/>
IP Address	<input type="text" value="192.168.60.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text"/>
Metric	<input type="text" value="0"/> ?
Interface	<input type="text" value="gretun2"/> ?

9. Click Save>Apply.

10. After that, we can see the route table:

Route Table Information					
Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	100	wan
2	12.1.1.0	255.255.255.0	0.0.0.0	0	gretun1
3	13.1.1.0	255.255.255.0	0.0.0.0	0	gretun2
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.50.0	255.255.255.0	0.0.0.0	0	gretun1
6	192.168.60.0	255.255.255.0	0.0.0.0	0	gretun2
7	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

10. Go to **VPN>VPN Redundancy** to enable VPN Redundancy feature, like below:

VPN Redundancy

General Settings

Enable	<input checked="" type="checkbox"/>
VPN Type	<input type="text" value="GRE"/>
Switch Mode	<input type="text" value="Primary"/>
Primary VPN Index	<input type="text" value="1"/>
Enable Verbose Log	<input checked="" type="checkbox"/>

ICMP Detection Settings

Connection 1 Remote Virtual IP	<input type="text" value="12.1.1.2"/>
Connection 2 Remote Virtual IP	<input type="text" value="13.1.1.2"/>
Connection 3 Remote Virtual IP	<input type="text"/>
Connection 4 Remote Virtual IP	<input type="text"/>
Connection 5 Remote Virtual IP	<input type="text"/>
Interval	<input type="text" value="30"/> ?
Retry Interval	<input type="text" value="5"/> ?
Timeout	<input type="text" value="3"/> ?
Retry Times	<input type="text" value="3"/> ?

10. Click Save>Apply.

3.2 CISCO Router 1 Configuration

1. Telnet to cisco route and configure cisco router 1 GRE VPN like below:

```
=====
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
  log config
  hidekeys
!
interface Loopback0
  ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
  ip address 12.1.1.2 255.255.255.0
  tunnel source 192.168.111.100
  tunnel destination 192.168.111.199
  tunnel key 123456
!
interface FastEthernet0/0
ip address 192.168.111.100 255.255.255.0
ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
speed auto
no mop enabled

interface FastEthernet0/1
ip address 192.168.0.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
```



```
duplex auto
speed auto
ip route 192.168.5.0 255.255.255.0 12.1.1.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0 overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
!
end
=====
```

3.3 CISCO Router 2 Configuration

1. Telnet to cisco route and configure cisco router 2 GRE VPN like below:

```
=====
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
  log config
  hidekeys
!
interface Loopback0
  ip address 192.168.60.1 255.255.255.0
!
interface Tunnel1
  ip address 13.1.1.2 255.255.255.0
  tunnel source 192.168.111.200
```

tunnel destination 192.168.111.199

tunnel key 123456

!

interface FastEthernet0/0

ip address 192.168.111.200 255.255.255.0

ip nat outside

ip nat enable

ip virtual-reassembly

duplex full

speed auto

no mop enabled

interface FastEthernet0/1

ip address 192.168.0.1 255.255.255.0

ip nat inside

ip nat enable

ip virtual-reassembly

duplex auto

speed auto

ip route 192.168.5.0 255.255.255.0 13.1.1.1

no ip http server

no ip http secure-server

!

ip nat inside source list 10 interface FastEthernet0/0 overload

!

access-list 10 permit 192.168.5.0 0.0.0.255

!

end

=====

4. Test

1. Go to VPN>VPN Redundancy, the primary tunnel is connected, and the secondary tunnel is standby:

Status		VPN Redundancy	
VPN Redundancy Status			
Enable	True		
VPN Type	Gre		
Primary VPN Status	Connection 1 Connected		
Secondary VPN Status	Connection 2 Standby		

2. Ping subnet of **cisco router 1** from NR500 and **successful**:

Ping	Traceroute	AT Debug	Sniffer
Ping Settings			
Host Address	192.168.50.1		
Ping Count	5		
Local IP Address			
PING 192.168.50.1 (192.168.50.1): 56 data bytes 64 bytes from 192.168.50.1: seq=0 ttl=255 time=27.286 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=23.112 ms 64 bytes from 192.168.50.1: seq=2 ttl=255 time=24.963 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=23.224 ms 64 bytes from 192.168.50.1: seq=4 ttl=255 time=22.390 ms --- 192.168.50.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 22.390/24.195/27.286 ms			

3. Ping subnet of **cisco router 2** from NR500 and **fail**, because GRE Tunnel 2 is standby:

Ping	Traceroute	AT Debug	Sniffer
Ping Settings			
Host Address	192.168.60.1		
Ping Count	5		
Local IP Address			
PING 192.168.60.1 (192.168.60.1): 56 data bytes --- 192.168.60.1 ping statistics --- 5 packets transmitted, 0 packets received, 100% packet loss			

4. Shut down GRE VPN Tunnel 1 on CISCO side, the Tunnel 2 will be up automatically:

Status		VPN Redundancy	
VPN Redundancy Status			
Enable	True		
VPN Type	Gre		
Primary VPN Status	Connection 1 Disconnected		
Secondary VPN Status	Connection 2 Connected		

5. Ping subnet of **cisco router 2** from NR500 and **successful**:

Ping	Traceroute	AT Debug	Sniffer
Ping Settings			
Host Address	192.168.60.1		
Ping Count	5		
Local IP Address			
<pre> PING 192.168.60.1 (192.168.60.1): 56 data bytes 64 bytes from 192.168.60.1: seq=0 ttl=255 time=14.550 ms 64 bytes from 192.168.60.1: seq=1 ttl=255 time=26.281 ms 64 bytes from 192.168.60.1: seq=2 ttl=255 time=28.431 ms 64 bytes from 192.168.60.1: seq=3 ttl=255 time=29.668 ms 64 bytes from 192.168.60.1: seq=4 ttl=255 time=22.890 ms --- 192.168.60.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 14.550/24.364/29.668 ms </pre>			

6. Ping subnet of **cisco router 1** from NR500 and **fail**, because GRE Tunnel 1 is disconnected:

Ping	Traceroute	AT Debug	Sniffer
Ping Settings			
Host Address	192.168.50.1		
Ping Count	5		
Local IP Address			
<pre> PING 192.168.50.1 (192.168.50.1): 56 data bytes --- 192.168.50.1 ping statistics --- 5 packets transmitted, 0 packets received, 100% packet loss </pre>			

7. Turn on the GRE VPN Tunnel 1 on CISCO side, it will switch back from Tunnel 2 to Tunnel 1 automatically and ping subnet of cisco router 1 successful:

Status	VPN Redundancy
VPN Redundancy Status	
Enable	True
VPN Type	Gre
Primary VPN Status	Connection 1 Connected
Secondary VPN Status	Connection 2 Standby

Ping	Traceroute	AT Debug	Sniffer
Ping Settings			
Host Address	192.168.50.1		
Ping Count	5		
Local IP Address			
<pre> PING 192.168.50.1 (192.168.50.1): 56 data bytes 64 bytes from 192.168.50.1: seq=0 ttl=255 time=27.286 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=23.112 ms 64 bytes from 192.168.50.1: seq=2 ttl=255 time=24.963 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=23.224 ms 64 bytes from 192.168.50.1: seq=4 ttl=255 time=22.390 ms --- 192.168.50.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 22.390/24.195/27.286 ms </pre>			

8. Test successfully.