

# NR500 Series Industrial Cellular VPN Router

## Application Note 030

### DMVPN with OSPF

**Version:** V1.0.1  
**Date:** Jun 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 HUB Configuration .....	5
3.2 Spoke Configuration .....	7
4. Route Table .....	9
5. Testing.....	10

# 1. Introduction

## 1.1 Overview

This document contains information regarding the configuration and use of DMVPN with OSPF.

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:** devel(baba6c2) or newer

**Other Compatible Models:** None

## 1.3 Version

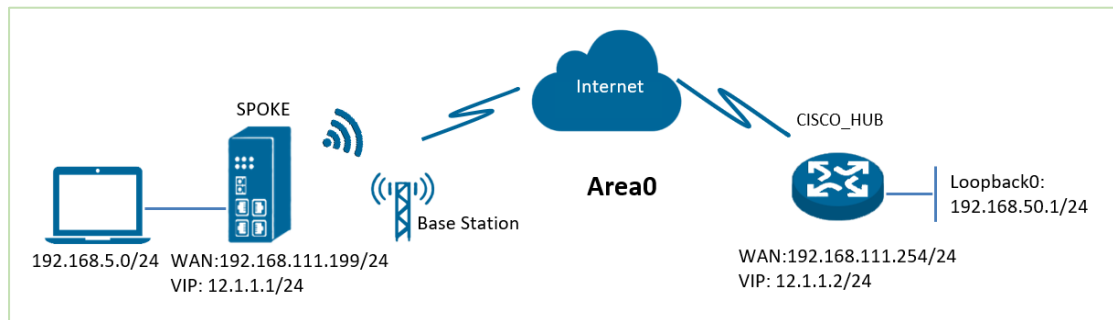
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/12/15	V1.0.0	devel(baba6c2)	First released
2020/06/23	V1.0.1	V1.1.2(3be6e5a)	

## 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](mailto:support@navigateworx.com)

## 2. Topology



1. NR500 Pro runs as DMVPN spoke with any kind of IP, which can ping DMVPN hub successfully.
2. CISCO router runs as DMVPN hub with a static public IP.
3. The tunnel is established between spoke and hub, the subnet can PING each other successfully.
4. Both NR500 Pro and CISCO run OSPF within a same Area0.

## 3. Configuration

### 3.1 HUB Configuration

1. The configuration of **Hub on CISCO** like below:

=====

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
!
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key 6 cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set DMVPN esp-3des esp-sha-hmac
  mode transport
!
crypto ipsec profile DMVPN-PROFILE
  set transform-set DMVPN

interface Loopback0
  ip address 192.168.50.1 255.255.255.0
!

interface Tunnel1
  ip address 12.1.1.2 255.255.255.0
  no ip redirects
  ip mtu 1438
  ip nhrp authentication cisco
  ip nhrp map multicast dynamic
  ip nhrp network-id 3
  ip nhrp holdtime 120
  ip nhrp redirect
```

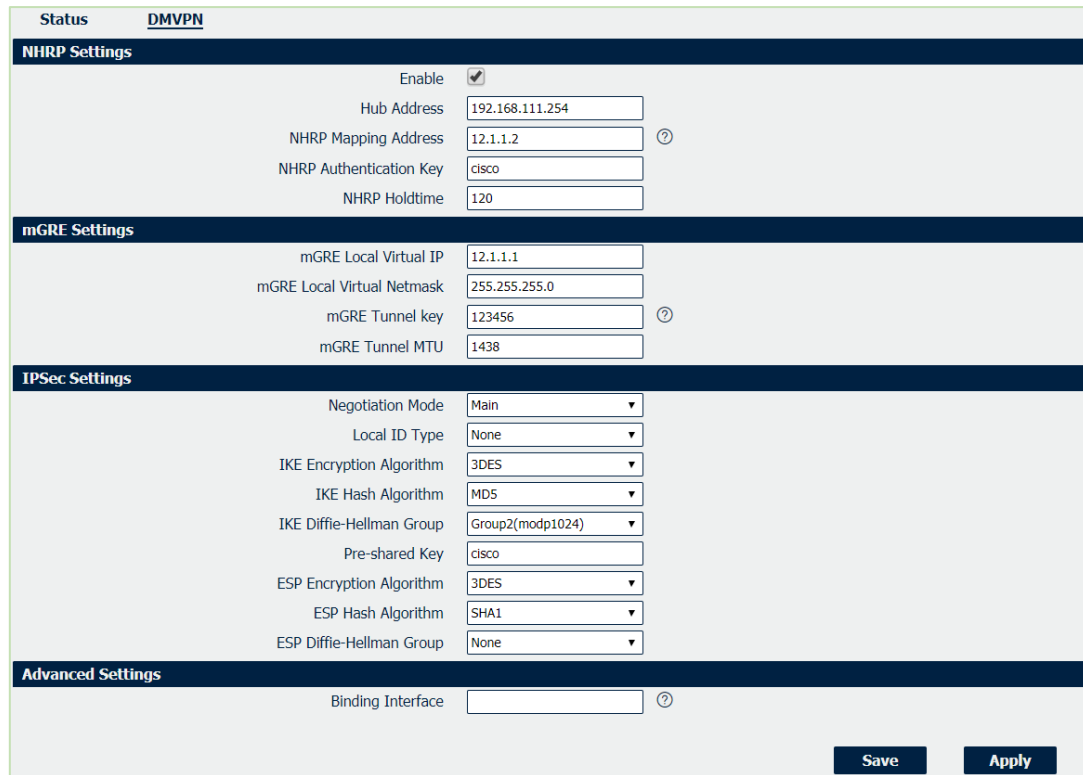
```
no ip split-horizon
ip ospf network non-broadcast
//Only support "non-broadcast" due to the limitation of protocol
tunnel source 192.168.111.254
tunnel mode gre multipoint
tunnel key 123456
tunnel protection ipsec profile DMVPN-PROFILE
!
interface FastEthernet0/0
  ip address 192.168.111.254 255.255.255.0
  ip nat outside
  ip nat enable
  ip virtual-reassembly
  duplex full
  speed auto
  no mop enabled
!
interface FastEthernet0/1
  ip address 192.168.6.3 255.255.255.0
  ip nat inside
  ip nat enable
  ip virtual-reassembly
  duplex auto
  speed auto
!
router ospf 110
  router-id 9.9.9.9
  log-adjacency-changes
  network 12.1.1.0 0.0.0.255 area 0
  network 192.168.50.0 0.0.0.255 area 0
  neighbor 12.1.1.1

ip forward-protocol nd
no ip http server
no ip http secure-server
!

ip nat inside source list 10 interface FastEthernet0/0 overload
!
access-list 10 permit 192.168.6.0 0.0.0.255
snmp-server community public RO
cisco2811#
=====
```

## 3.2 Spoke Configuration

1. Go to **VPN>DMVPN**, enable DMVPN and configure DMVPN as below picture.



**Status** **DMVPN**

**NHRP Settings**

Enable

Hub Address

NHRP Mapping Address  ⓘ

NHRP Authentication Key

NHRP Holdtime

**mGRE Settings**

mGRE Local Virtual IP

mGRE Local Virtual Netmask

mGRE Tunnel key  ⓘ

mGRE Tunnel MTU

**IPSec Settings**

Negotiation Mode

Local ID Type

IKE Encryption Algorithm

IKE Hash Algorithm

IKE Diffie-Hellman Group

Pre-shared Key

ESP Encryption Algorithm

ESP Hash Algorithm

ESP Diffie-Hellman Group

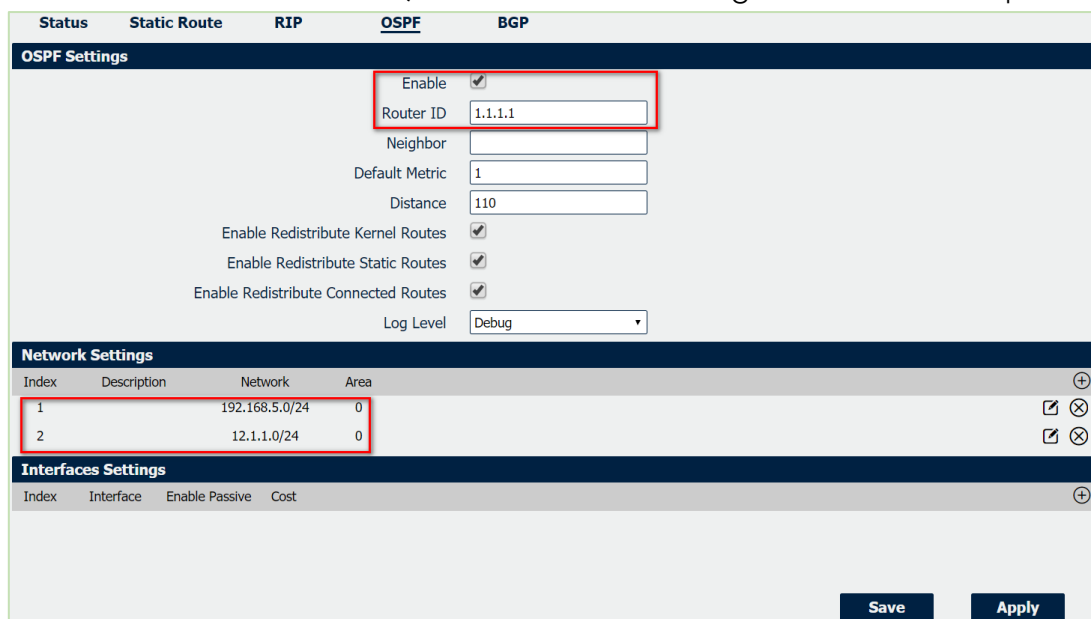
**Advanced Settings**

Binding Interface  ⓘ

**Save** **Apply**

2. Click Save>Apply.

3. Go to **Network>Route>OSPF**, enable OSPF and configure OSPF as below picture.



**Status** **Static Route** **RIP** **OSPF** **BGP**

**OSPF Settings**

Enable

Router ID

Neighbor

Default Metric

Distance

Enable Redistribute Kernel Routes

Enable Redistribute Static Routes

Enable Redistribute Connected Routes

Log Level

**Network Settings**

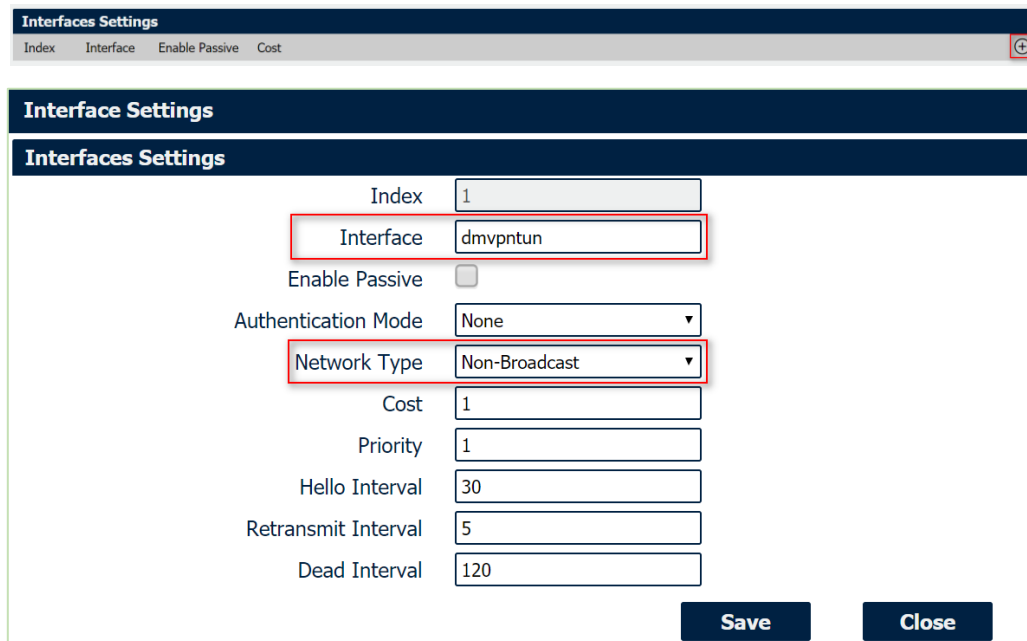
Index	Description	Network	Area	
1		192.168.5.0/24	0	<input checked="" type="checkbox"/> <input type="checkbox"/>
2		12.1.1.0/24	0	<input checked="" type="checkbox"/> <input type="checkbox"/>

**Interfaces Settings**

Index	Interface	Enable Passive	Cost	
-------	-----------	----------------	------	--

**Save** **Apply**

4. Go to **Network>Route>OSPF>Interface Settings**, to specify the Interface Network Type as “**Non-Broadcast**” as below picture.



**Interface Settings**

Index: 1

Interface: dmpntun

Enable Passive:

Authentication Mode: None

Network Type: Non-Broadcast

Cost: 1

Priority: 1

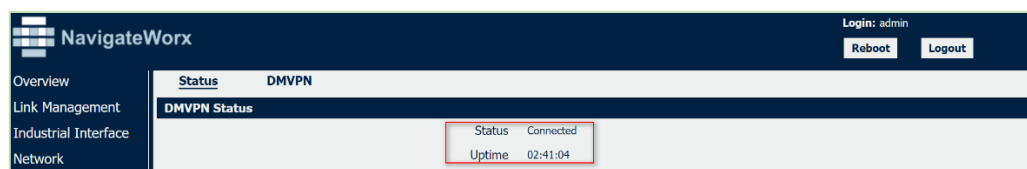
Hello Interval: 30

Retransmit Interval: 5

Dead Interval: 120

Save Close

5. Route had connected to CISCO HUB. Go to **VPN>DMVPN>Status** to check the connection status.



**Status DMVPN**

DMVPN Status

Status: Connected

Uptime: 02:41:04

Reboot Logout



## 4. Route Table

1. Route Table on CISCO HUB for reference.

```

cisco2811#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

C    192.168.88.0/24 is directly connected, Loopback3
C    192.168.111.0/24 is directly connected, FastEthernet0/0
C    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.1.0 is directly connected, Loopback1
C      172.16.2.0 is directly connected, Loopback2
O    192.168.5.0/24 [110/1010] via 12.1.1.3, 00:19:30, Tunnel1
C    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.1.0 is directly connected, Loopback100
C    12.0.0.0/24 is subnetted, 1 subnets
C      12.1.1.0 is directly connected, Tunnel1
C    192.168.50.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#
  
```

2. Route Table on SPOKE for reference.



The screenshot shows the NavigateWorx web interface with a sidebar on the left containing navigation options like Overview, Link Management, Industrial Interface, Network, Firewall, Rotic, VRRP, and Applications. The main content area displays a table titled 'Route Table Information' with columns for Status, Static Route, RIP, OSPF, and BGP. The table contains five entries, with rows 2, 3, and 4 highlighted in red.

Status	Static Route	RIP	OSPF	BGP
1	0.0.0.0	0.0.0.0	192.168.111.11	0 wan
2	12.1.1.0	255.255.255.0	0.0.0.0	0 dmvptun
3	192.168.5.0	255.255.255.0	0.0.0.0	0 lan0
4	192.168.50.1	255.255.255.255	12.1.1.2	20 dmvptun
5	192.168.111.0	255.255.255.0	0.0.0.0	0 wan

## 5. Testing

1. Enable CMD and Ping from end device of SPOKE to subnet of CISCO HUB.

```
Administrator: Command Prompt
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\Administrator>
```

2. Ping from CISCO HUB to end device of SPOKE.

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
cisco2811#
```

3. Test successfully.