Application Note

DMVPN Spoke with Cisco Router

Version:	**v.1.0.0**
Date:	**2017-03-10**
Status:	**Confidential**
Doc ID:	**RT_AN010_ROS_DMVPN Spoke with Cisco Router_v.1.0.0**
Author:	**Singson Chen**

www.robustel.com

Contents

Chapter 1 Introduction

1.1 Overview

RobustOS (hereinafter referred to as “the ROS”) is a new operating system for Robustel's IoT gateway released in 2015. It is a modular and open software platform which could support third party development based on SDK/API. Meanwhile, it supports different routing and VPN protocols for different application scenarios. This newer platform provides a different web configuration interface than the existing platform.

Dynamic Multipoint VPN (DMVPN) is a VPN solution for building scalable IPsec Virtual Private Networks (VPNs). DMVPN uses a centralized architecture to provide easier implementation and management for deployments that require granular access controls for diverse user communities, including mobile workers, telecommuters, and extranet users.

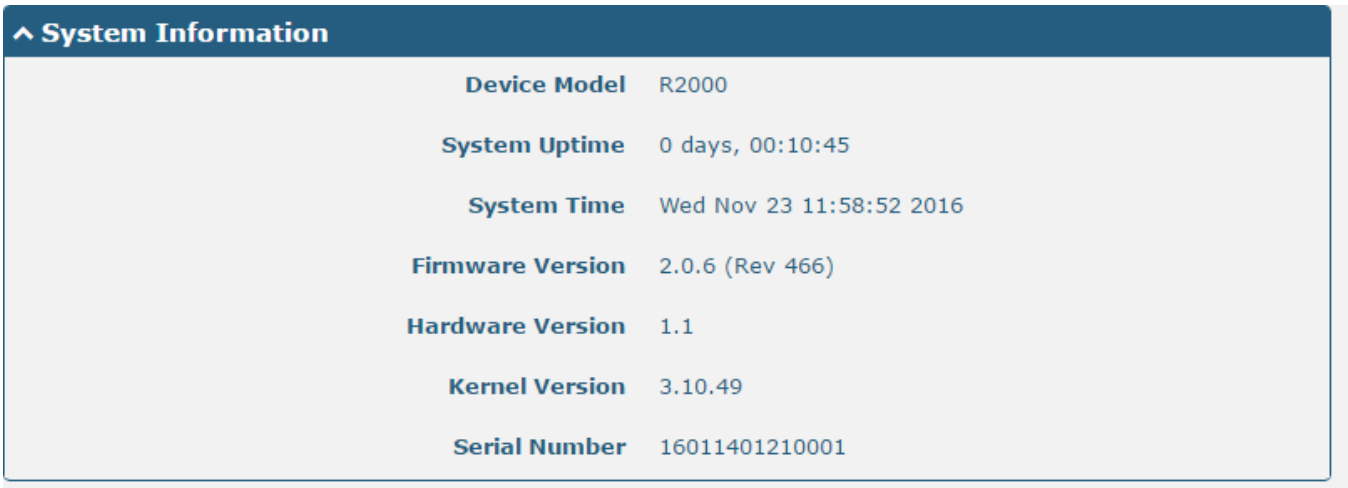
This application note has been written for customer with a good understanding of Robustel products and a basic experience of VPN. It shows customer how to configure and test the DMVPN between the ROS and a Cisco router through the cellular network.

This application note applies to the ROS firmware of R2000 and R3000. However, the followings will take R2000 as an example

1.2 Assumptions

The features of DMVPN have been fully tested. This application note has been written by technically competent engineer who is familiar with the Robustel products and the application requirements.
This application note is based on:

- Product model: Robustel GoRugged R2000, an industrial cellular VPN router
- Firmware version: R2000_ROS_V2.0.6.fs
- Configuration: This application note assumes the Robustel products are set to factory default. Most of configuration steps are only shown if they are different from the factory default settings.



The ROS's cellular WAN could be dynamic or static, and its IP address can be public or private with NAT. The configuration will be valid but depend on the capabilities and IOS version of the Cisco router. The ROS working with dynamic private IP address could still work for the DMVPN, but the central Cisco router must support NAT traversal feature and the ROS should also fully support NAT traversal by default.

It must assign a public IP address to the WAN port of the central Cisco router. This public IP address can be dynamic or static. If the central Cisco router working with dynamic public IP address, a DNS service must be used to park dynamic public IP address to a static domain.

- **Note about Cisco NAT Traversal:**
  NAT Traversal is a feature automatically detected by VPN devices. There are no configuration steps for a router running Cisco IOS Release 12.2(13)T. If both VPN devices are NAT-T capable, the NAT Traversal can auto detect and auto negotiate.

1.3 Rectifications

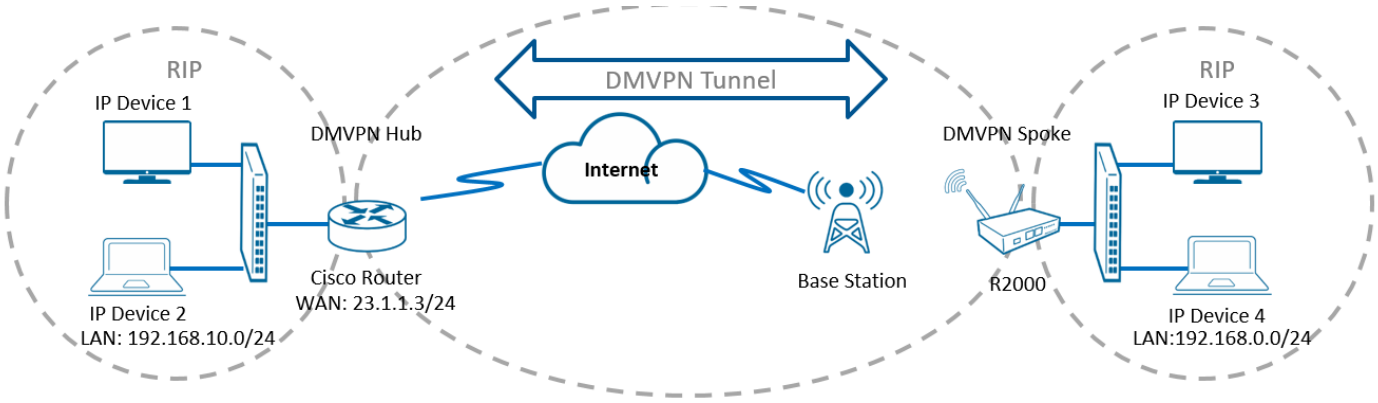
Requests for corrections or rectifications to this application note will be appreciated, and if there are any request for new application notes please email to: support@robustel.com.

1.4 Version

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	Doc Version	Change Description
2017-03-10	v.1.0.0	Initial Release

Chapter 2 Topology



1. The Cisco router has a fixed public network IP address.
2. The R2000 works on wireless network with any kind of IP which can access the Internet and ping the WAN IP address of the Cisco router successfully.
3. DMVPN will be established between the R2000 and the Cisco router, and the RIPV2 will be enabled between their local networks. The Cisco router works as a Hub, and the R2000 works as a Spoke. R2000 and Cisco router need to declare the route connecting to the tunnel and the route of their own local network.

Chapter 3 Configuration

3.1 Cisco Router Configuration

Following is the configuration reference for Cisco router which works as a DMVPN Hub.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
crypto isakmp policy 1          #Configurate the policy of IKE (ISAKMP)#
 encr 3des
 authentication pre-share
 group 2


crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0    #The PSK key for authentication, 0.0.0.0 means
                                                        accepting any connection outside#
!
!
crypto ipsec transform-set ccie esp-3des esp-sha-hmac      #IPsec transform#
 mode transport
!
crypto ipsec profile cisco                      #IPsec profile#
 set transform-set ccie
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Tunnel1                       #Establish the GRE tunnel#
 bandwidth 100
 ip address 100.1.1.1 255.255.255.0        #Tunnel IP of DMVPN Hub#
 no ip redirects
 ip nhrp authentication ccie123           #Authentication password for all the spokes and Hub in a mGRE#
 ip nhrp map multicast dynamic            #Add the IP of spokes into the broadcast map automatically, otherwise the
                                           use of multicast routing protocol within spokes can not run normally#

 ip nhrp network-id 1                      #The unique network ID for for all the spokes and Hub in a Mgre#
```

```
 no ip split-horizon                    # Close the horizon split, or the route learned dynamically from a spoke
                                          can not be sent to another spoke#

 tunnel source FastEthernet0/1    #Define the source interface of Mgre#
 tunnel mode gre multipoint        #Define the type of GRE interface to be mGRE, and the type on the Hub must
                                          be mGRE#

 tunnel key 10000        # Define of the Tunnel interface ID. This step is not necessary, all the spokes and Hub in a
                              mGRE if defined#
tunnel protection ipsec profile cisco      # The IPsec profile is associated to the mGRE interface to protect the flow
                                          of the mGRE interface#
!
interface FastEthernet0/0
 ip address 192.168.10.3 255.255.255.0      #Lan IP of Cisco router#
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 23.1.1.3 255.255.255.0          #Wan IP of Cisco router#
 duplex auto
 speed auto
!
router rip                          #Enable RIPv2#
 version 2
 network 100.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 23.1.1.2
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
```

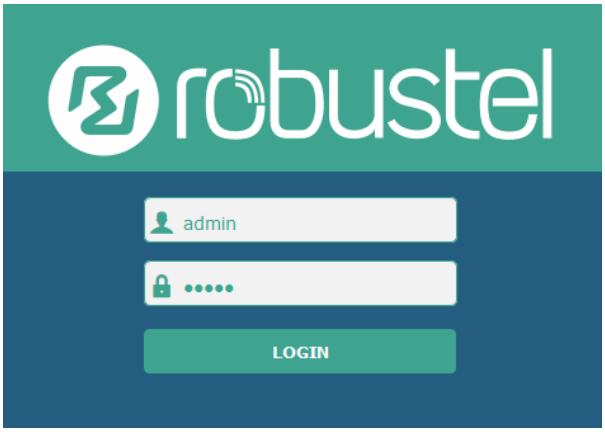
```
!
!
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

3.2 R2000 Configuration

3.2.1 Configure Link Manager

1. Follow these steps before configuring the router:

- Attach the external antenna to the router's connector and twist tightly
- Insert the SIM card into the router
- Connect the power supply correctly
- Log in the Web GUI of the router

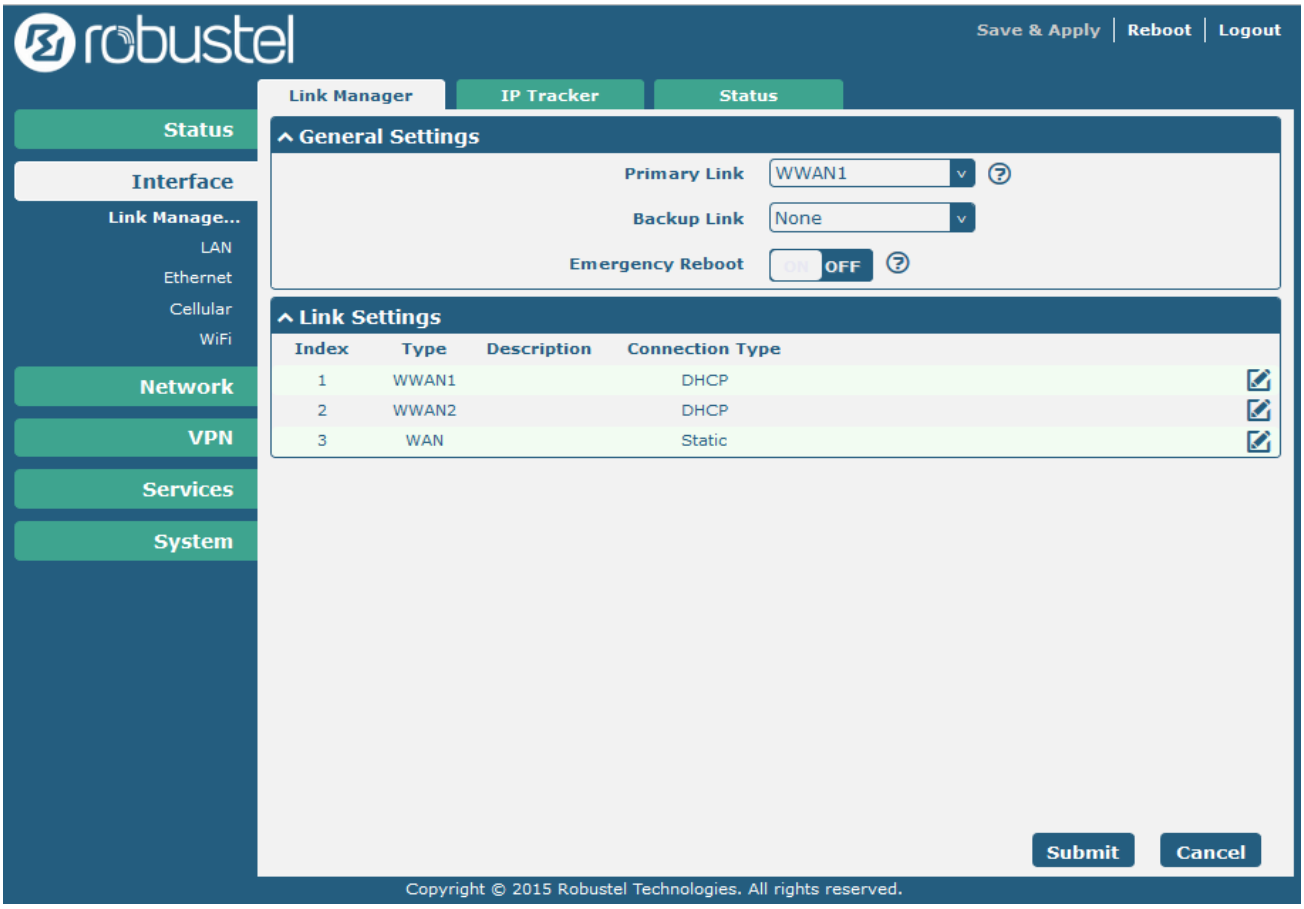


You need to know the following factory settings before you have logged in the Web GUI.

Item	Description
Username	Admin
Password	Admin
Eth0	192.168.0.1/255.255.255.0, LAN Mode
Eth1	192.168.0.1/255.255.255.0, LAN Mode
DHCP Server	Enabled

2. Browse to **Interface > Link Manager**.

- Click the drop-down list of “Primary Link” and select “WWAN1”.
- Click “Submit”.
- Click “Save & Apply”.



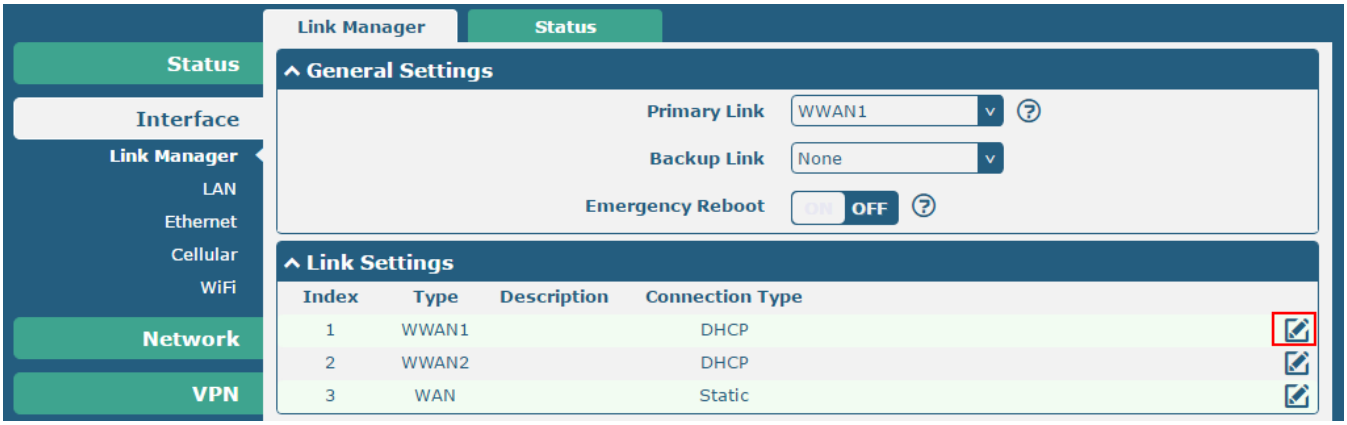
Item	Description	Setting
Primary Link	Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface.	WWAN1

3.2.2 Configure Cellular WAN

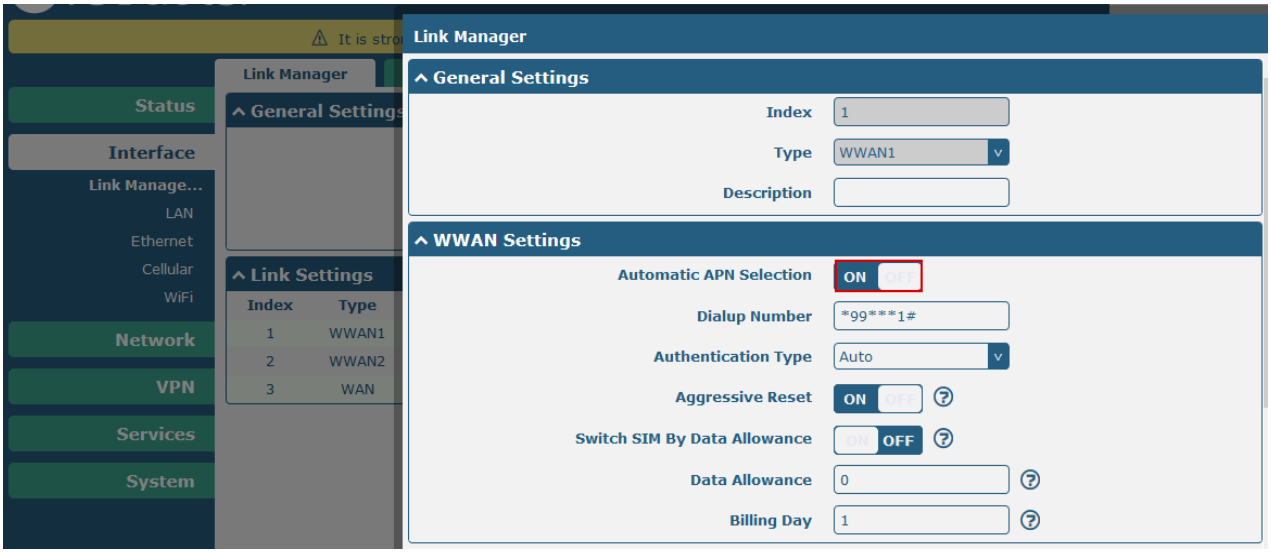
1 Browse to **Interface > Link Manager> Link Settings**.

- Click the edit button of “WWAN1”.

- Enter the related parameters in the “WWAN Settings” window.
- Enter the related parameters in the “Ping Detection Settings” window.
- Click “Submit”.
- Click “Save & Apply”.

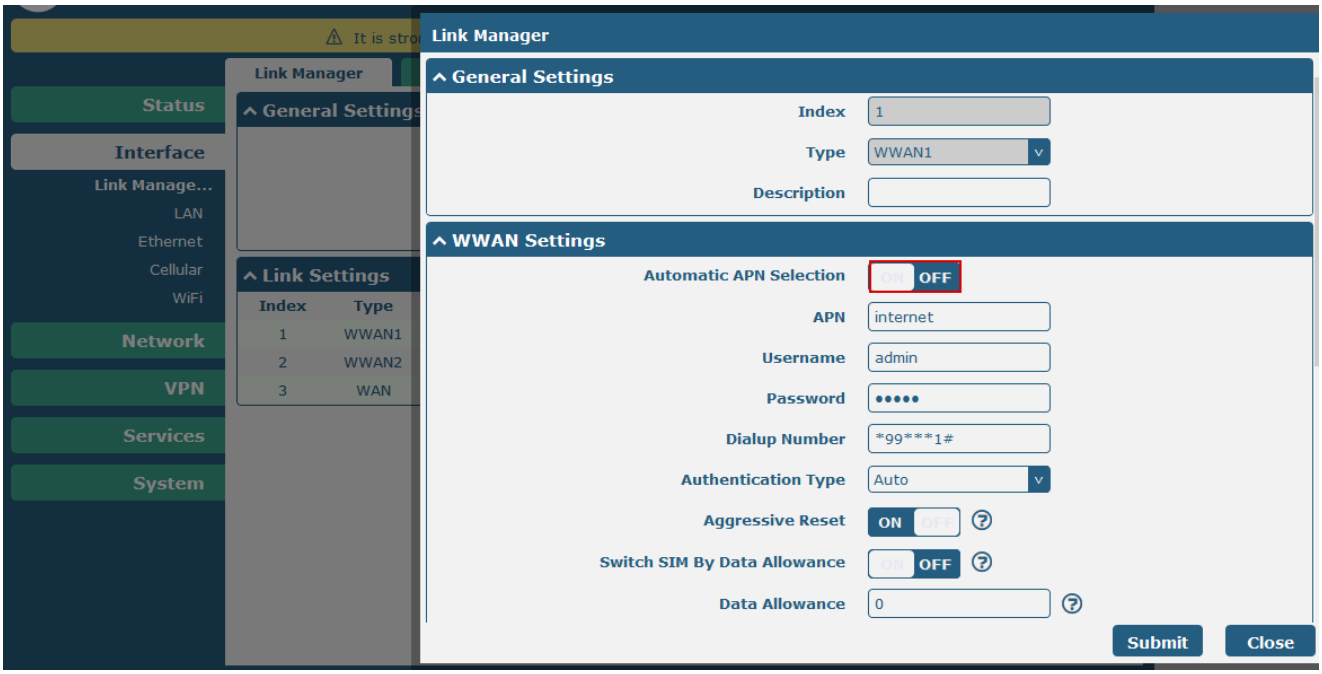


2 The window is displayed as below when enabling the “Automatic APN Selection” option.

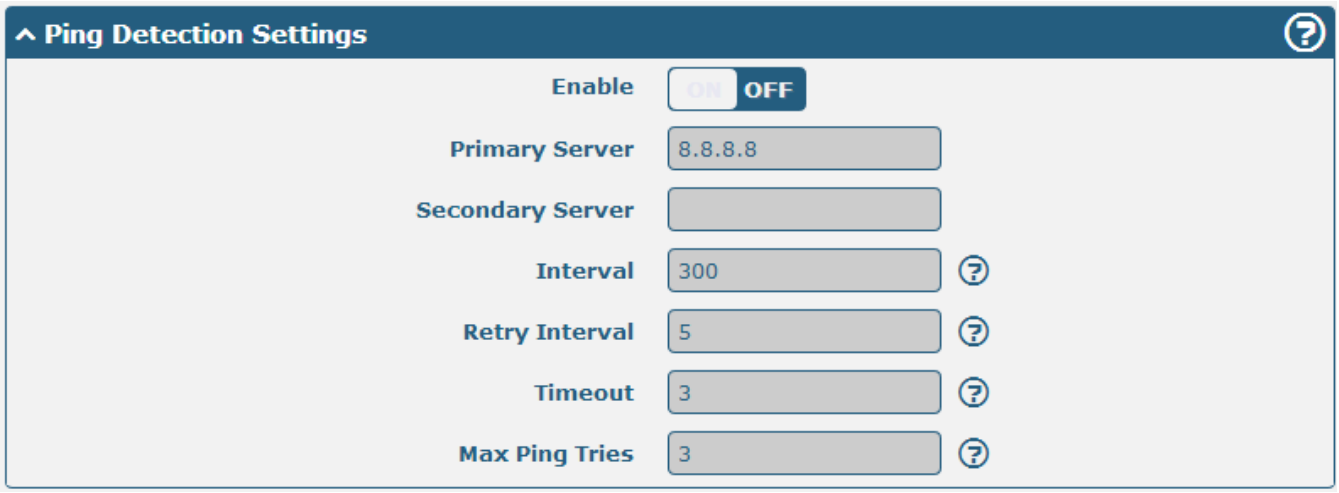


Item	Description	Setting
Dialup Number	Set the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Data Allowance	Set the monthly data traffic limitation.	0
Billing Day	Specify the monthly billing day, and the data traffic statistics will be recalculated from this day.	1

3 The window is displayed as below when disabling the “Automatic APN Selection” option.



Item	Description	Setting
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null



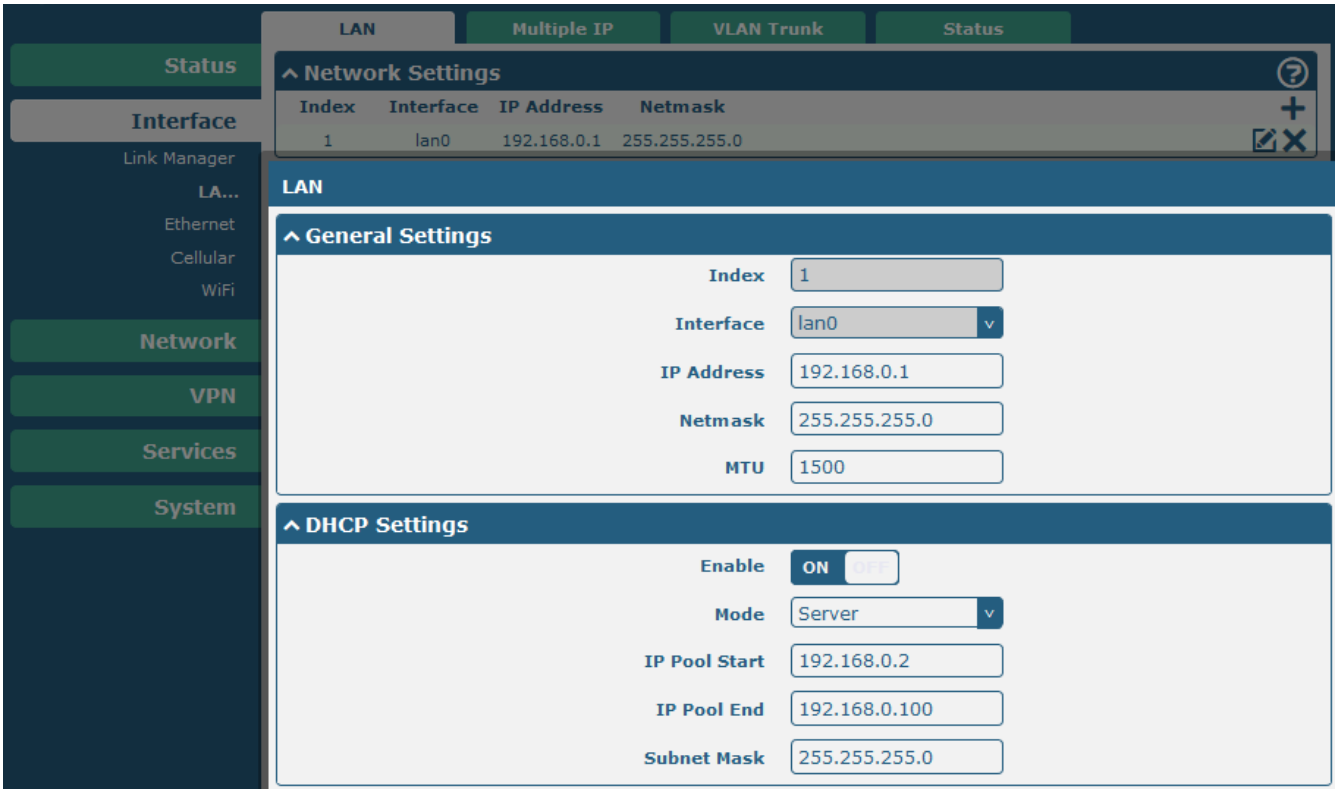
Item	Description	Setting
Enable	Click the toggle button to enable the Ping detection, a keepalive policy of R2000 router.	OFF
Primary Server	Router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check if	Null

	the current connectivity is active.	
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3

3.2.3 Configure IP Address of LAN

1. Browse to **Interface > LAN > LAN**.

- Click the edit button of lan0.
- Set its IP address and Netmask, and the parameters in “DHCP Settings” window are set accordingly.
- Click “Submit”.
- Click “Save & Apply”.

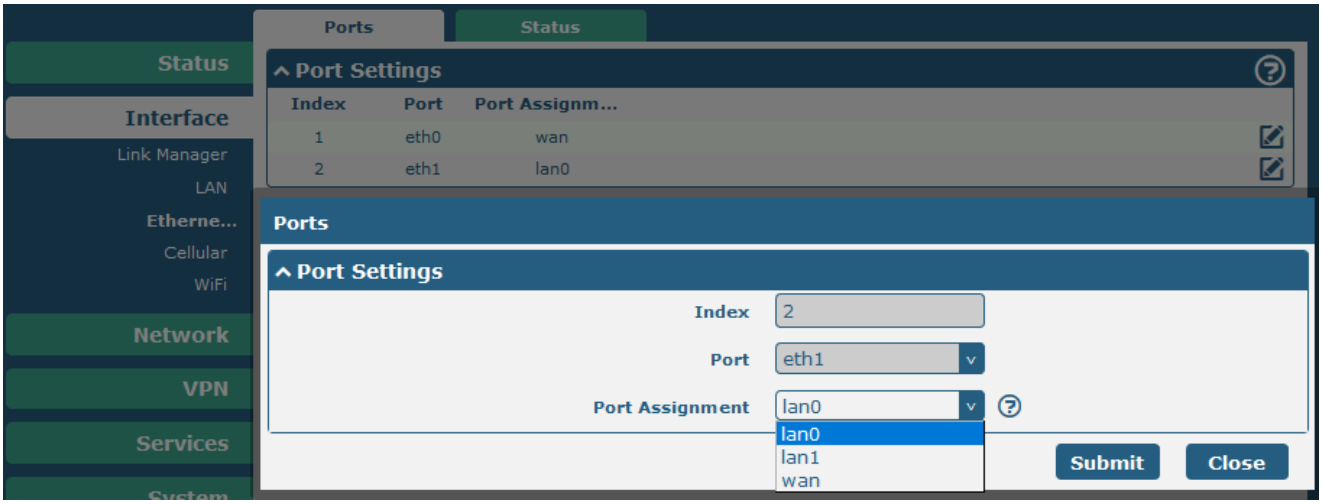


Item	Description	Setting
IP Address	Set the IP address of lan0.	Enter accordingly
Netmask	Set the Netmask of lan0.	Enter accordingly
MTU	Set the MTU of lan0.	1500

2. Browse to **Interface > Ethernet > Ports**.

- Click the edit button of eth1.
- Assign lan0 to the eth1 port.
- Click “Submit”.

- Click “Save & Apply”.



3.2.4 Configure DMVPN

This section allows you to set the related parameters of DMVPN.

1. DMVPN needs to be installed first in the APP Center since the DMVPN is not the default setting in the ROS. Kindly contact us when you need this function.

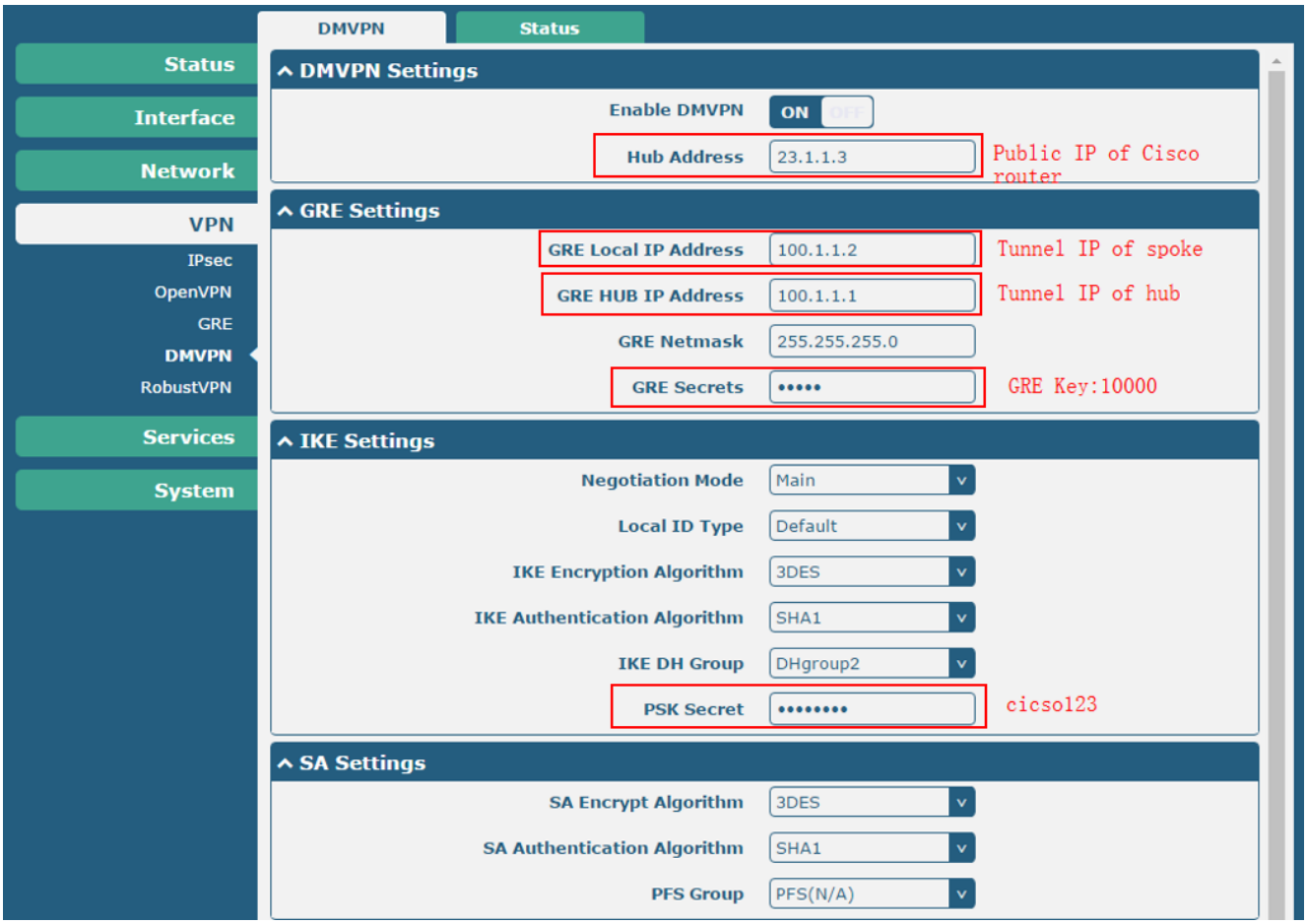
- APP:

- Path of installation:

- Installed:

2. Browse to **VPN > DMVPN**, and enable the DMVPN.

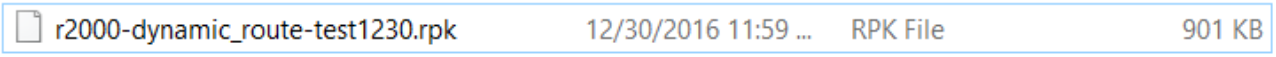
3. Configure the related parameters to match the DMVPN Hub side (following is just for reference), and click **Submit > Save & Apply**.



3.2.5 Configure RIP

1. RIP needs to be installed first in the APP Center since the RIP is not the default setting in the ROS. Kindly contact us when you need this function.

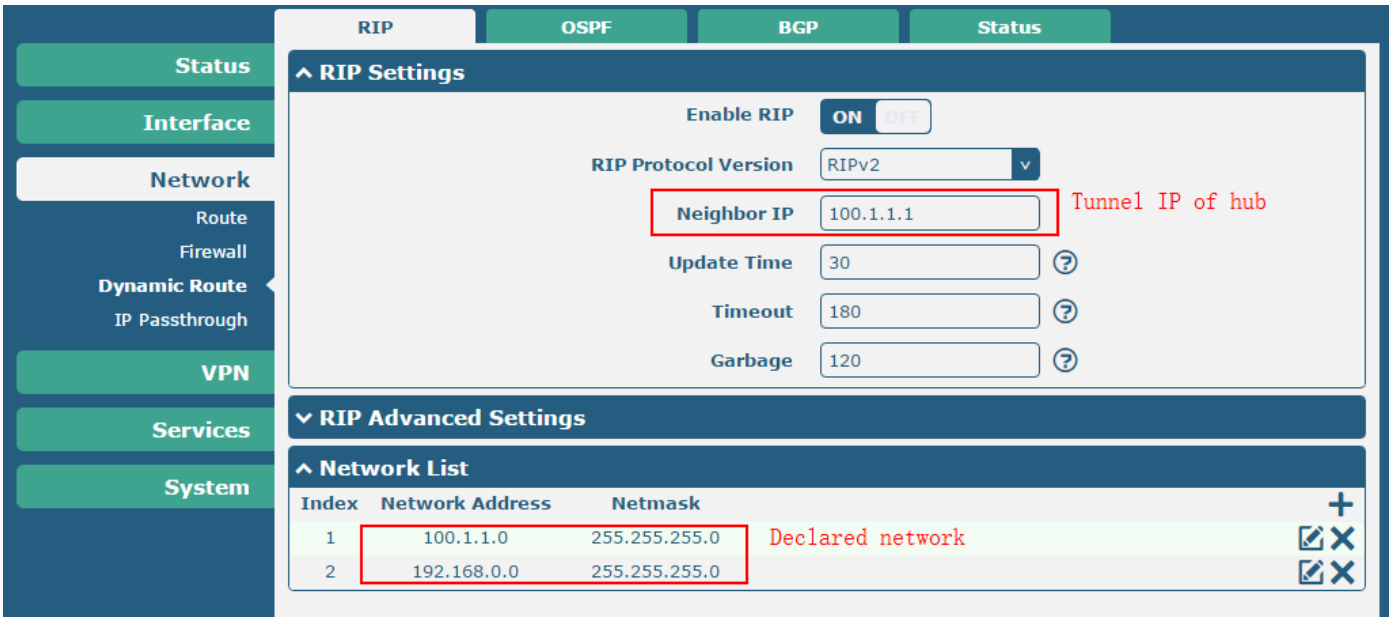
- APP:



- Path of installation:

- Installed:

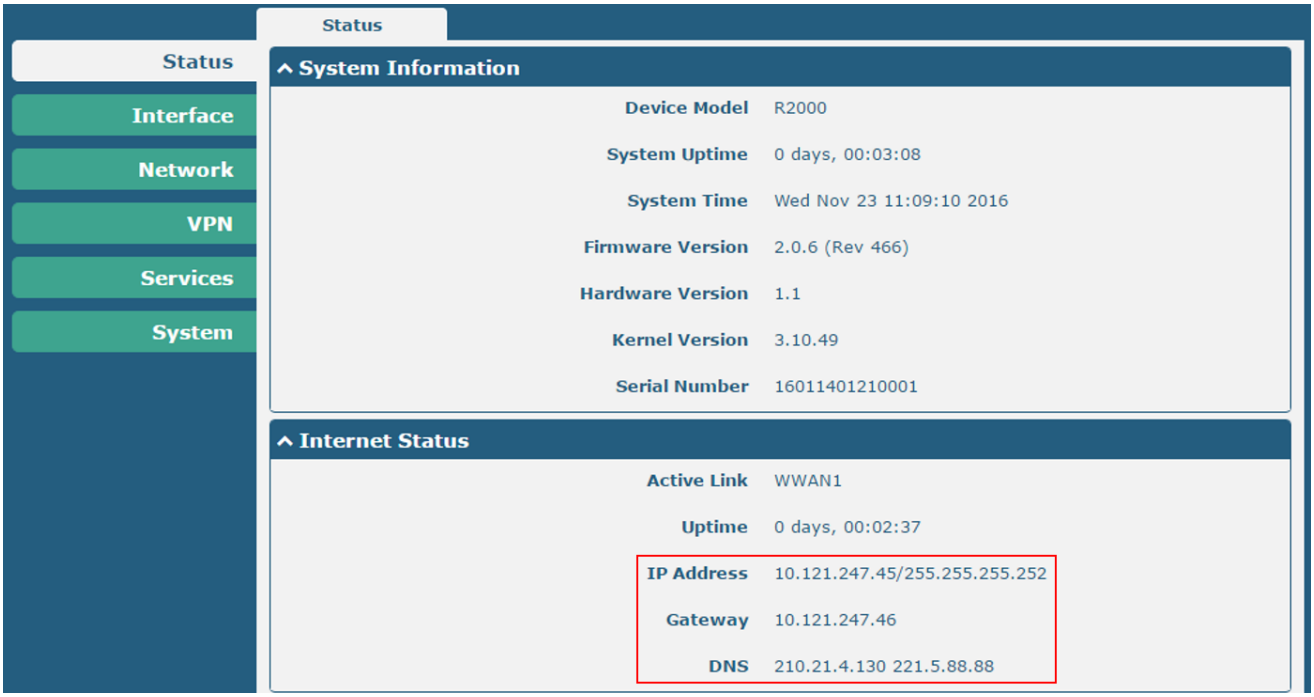
2. Browse to **Interface > Dynamic Route**, configure the related network in RIP, and click **Submit > Save & Apply.**


RIP
OSPF
BGP
Status
Status
Interface
Network
Route
Firewall
Dynamic Route
IP Passthrough
VPN
Services
System
RIP Settings
Enable RIP
ON
OFF
RIP Protocol Version
RIPv2
Neighbor IP
100.1.1.1
Tunnel IP of hub
Update Time
30
Timeout
180
Garbage
120
RIP Advanced Settings
Network List
Index
Network Address
Netmask
1
100.1.1.0
255.255.255.0
Declared network
2
192.168.0.0
255.255.255.0

Chapter 4 Testing

4.1 Network Status

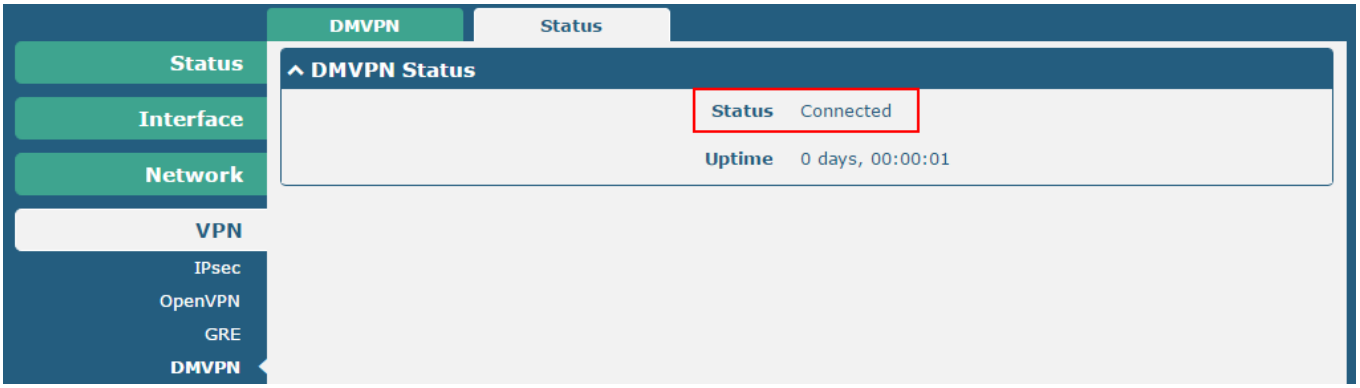
1. Click “Status” bar.
2. Check whether R2000 has obtained the assigned static IP address (the following IP is just for reference).
3. Check whether R2000 has used SIM card to register to network, dial up to get IP address and get access to the Internet.

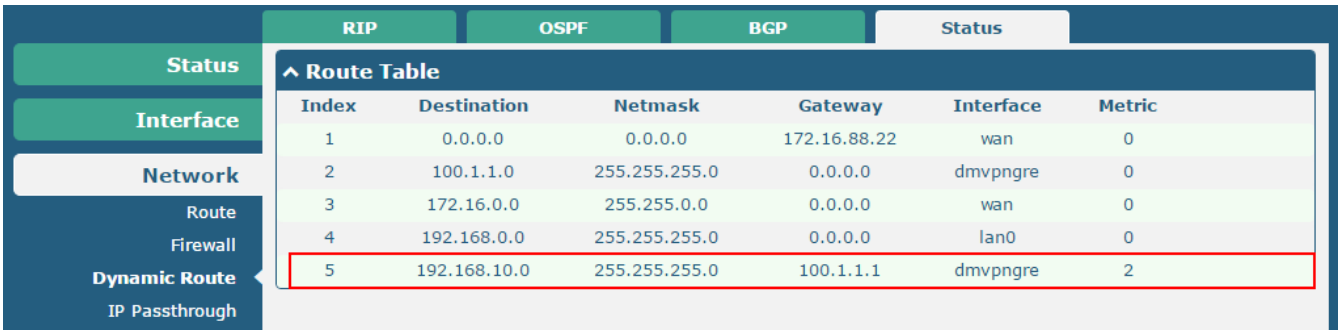


4.2 VPN Status and Communication

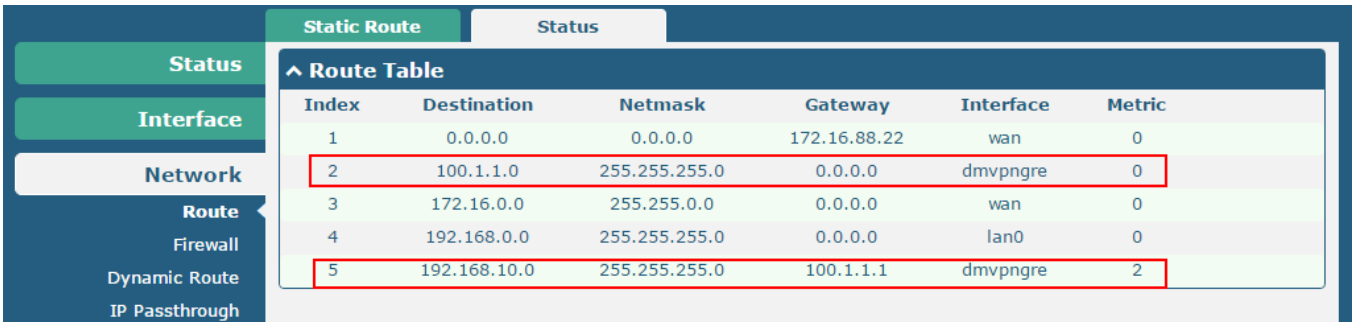
1. Browse to **VPN > DMVPN > Status**.

2. Check whether R2000 has established a DMVPN tunnel with Hub side and exchanged the RIP route.

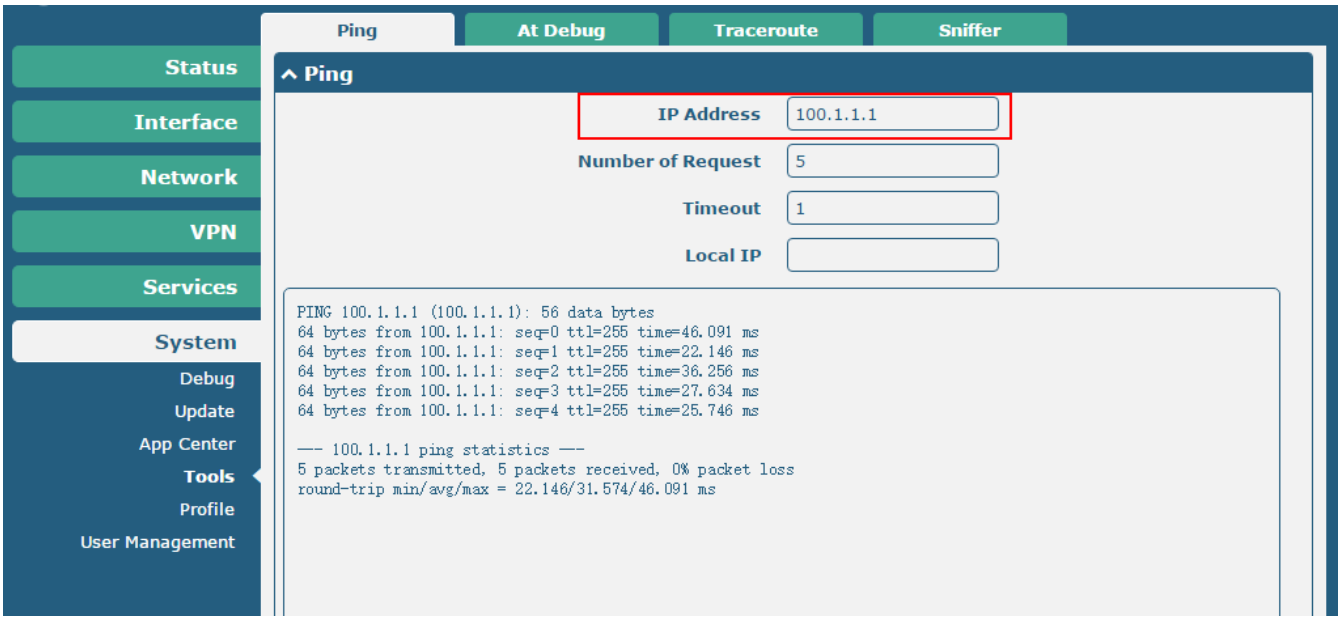


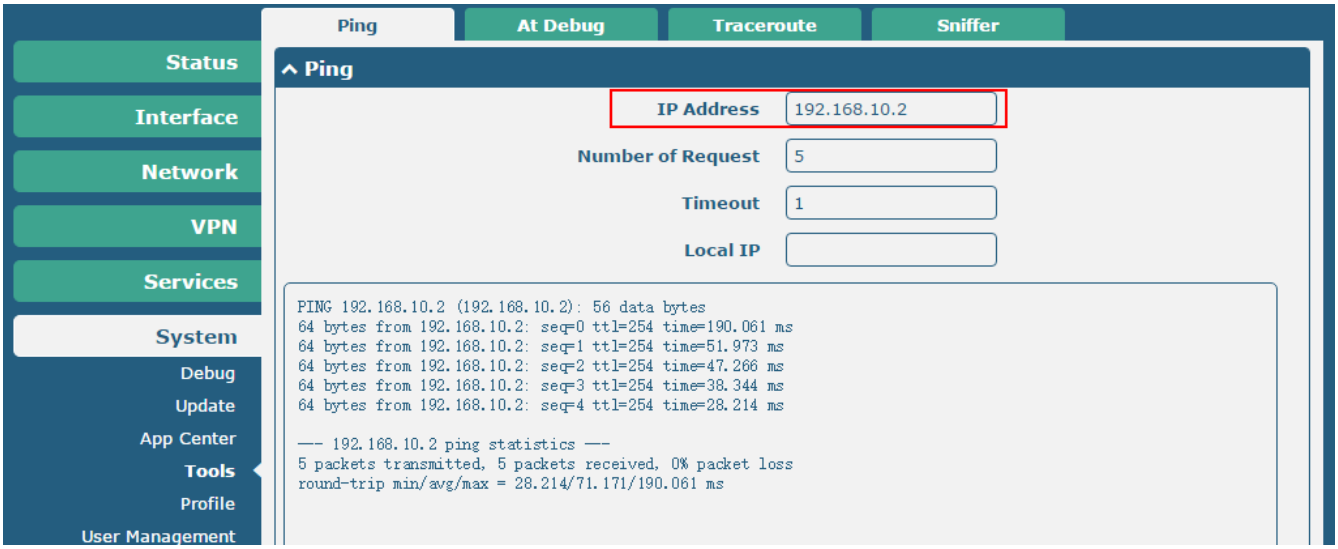


3. Browse to **Network > Route > Status**, and check the virtual tunnel on Route table.



4. Browse to **System > Tools > Ping**.
   Ping the virtual IP of DMVPN Hub and LAN IP address behind Hub, and get ICMP reply from remote end.





4.3 Testing at Cisco router

1. Run console terminal and input “show ip route” command to check the route-table in Cisco router.

```
*Mar  1 06:28:45.646: %SYS-5-CONFIG_I: Configured from console by console
cisco#sho ip route
cisco#sho 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 23.1.1.2 to network 0.0.0.0

     100.0.0.0/24 is subnetted, 1 subnets
C       100.1.1.0 is directly connected, Tunnel1
C    192.168.10.0/24 is directly connected, FastEthernet0/0
     23.0.0.0/24 is subnetted, 1 subnets
C       23.1.1.0 is directly connected, FastEthernet0/1
R    192.168.0.0/24 [120/1] via 100.1.1.2, 00:00:11, Tunnel1
S*   0.0.0.0/0 [1/0] via 23.1.1.2
cisco#
```

2. There is a new remote subnet 192.168.0.0/24 passed through the DMVPN tunnel.

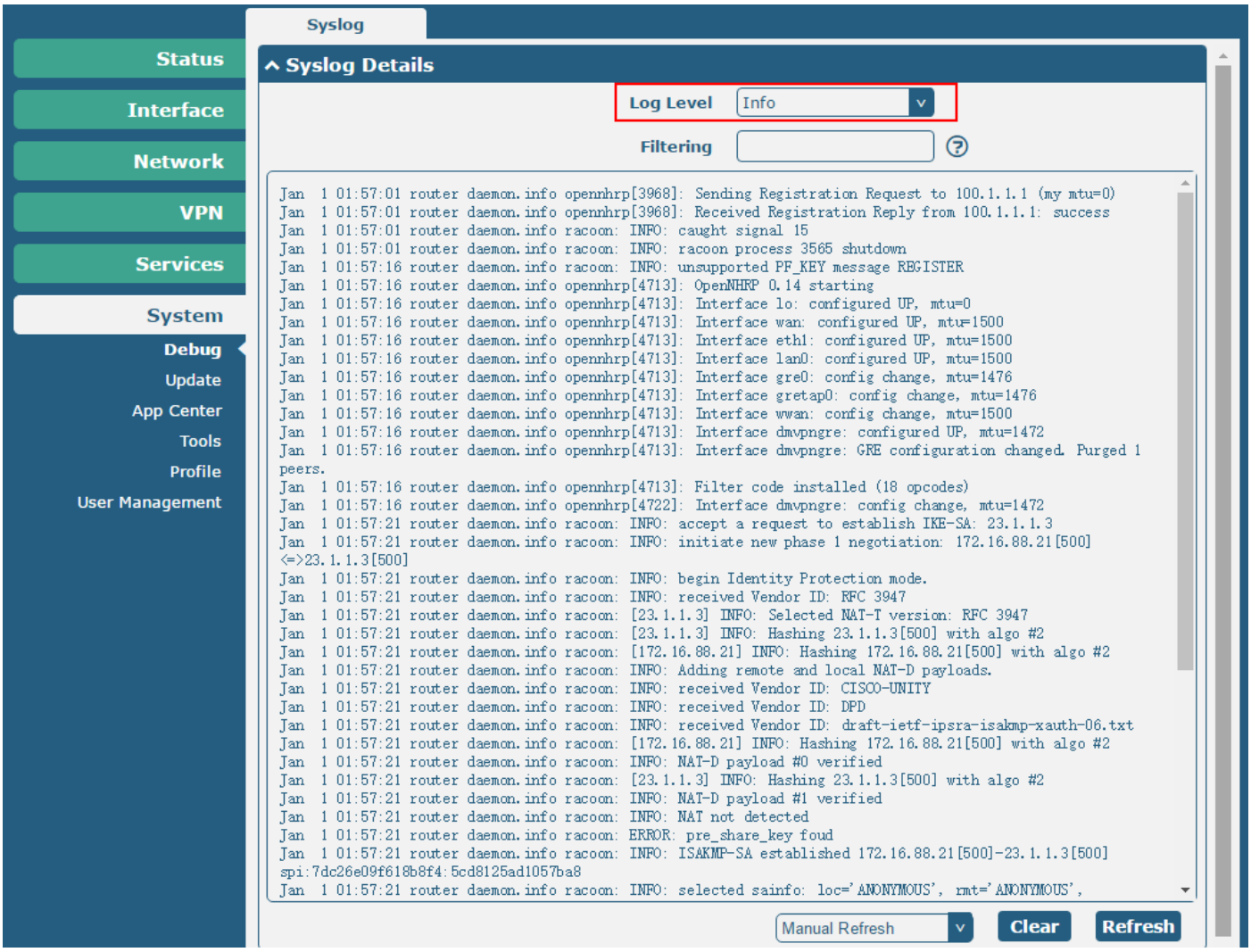
3. Ping the virtual IP of DMVPN spoke and LAN IP address behind R2000, and get ICMP reply from remote end.

```
cisco#ping 100.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/36 ms
cisco#
```

```
cisco#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/32 ms
```

4.4 Event/Log

Debug shows the running process and the status of R2000. Only the information that specifically relate to the configuration above will be explained below.




```
……
Jan  1 01:57:16 router daemon.info opennhrp[4713]: OpenNHRP 0.14 starting
Jan  1 01:57:16 router daemon.info opennhrp[4713]: Interface lo: configured UP, mtu=0
Jan  1 01:57:16 router daemon.info opennhrp[4713]: Interface wan: configured UP, mtu=1500
Jan  1 01:57:16 router daemon.info opennhrp[4713]: Interface eth1: configured UP, mtu=1500
Jan  1 01:57:16 router daemon.info opennhrp[4713]: Interface lan0: configured UP, mtu=1500
Jan  1 01:57:16 router daemon.info opennhrp[4713]: Interface gre0: config change, mtu=1476
```

Jan 1 01:57:16 router daemon.info opennhrp[4713]: Interface gretap0: config change, mtu=1476
Jan 1 01:57:16 router daemon.info opennhrp[4713]: Interface wwan: config change, mtu=1500
Jan 1 01:57:16 router daemon.info opennhrp[4713]: Interface dmvpngre: configured UP, mtu=1472
Jan 1 01:57:16 router daemon.info opennhrp[4713]: Interface dmvpngre: GRE configuration changed. Purged 1 peers.
Jan 1 01:57:16 router daemon.info opennhrp[4713]: Filter code installed (18 opcodes)
Jan 1 01:57:16 router daemon.info opennhrp[4722]: Interface dmvpngre: config change, mtu=1472
Jan 1 01:57:21 router daemon.info racoon: INFO: accept a request to establish IKE-SA: 23.1.1.3
Jan 1 01:57:21 router daemon.info racoon: INFO: initiate new phase 1 negotiation: 172.16.88.21[500]<=>23.1.1.3[500]
Jan 1 01:57:21 router daemon.info racoon: INFO: begin Identity Protection mode.
Jan 1 01:57:21 router daemon.info racoon: INFO: received Vendor ID: RFC 3947
Jan 1 01:57:21 router daemon.info racoon: [23.1.1.3] INFO: Selected NAT-T version: RFC 3947
Jan 1 01:57:21 router daemon.info racoon: [23.1.1.3] INFO: Hashing 23.1.1.3[500] with algo #2
Jan 1 01:57:21 router daemon.info racoon: [172.16.88.21] INFO: Hashing 172.16.88.21[500] with algo #2
Jan 1 01:57:21 router daemon.info racoon: INFO: Adding remote and local NAT-D payloads.
Jan 1 01:57:21 router daemon.info racoon: INFO: received Vendor ID: CISCO-UNITY
Jan 1 01:57:21 router daemon.info racoon: INFO: received Vendor ID: DPD
Jan 1 01:57:21 router daemon.info racoon: INFO: received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt
Jan 1 01:57:21 router daemon.info racoon: [172.16.88.21] INFO: Hashing 172.16.88.21[500] with algo #2
Jan 1 01:57:21 router daemon.info racoon: INFO: NAT-D payload #0 verified
Jan 1 01:57:21 router daemon.info racoon: [23.1.1.3] INFO: Hashing 23.1.1.3[500] with algo #2
Jan 1 01:57:21 router daemon.info racoon: INFO: NAT-D payload #1 verified
Jan 1 01:57:21 router daemon.info racoon: INFO: NAT not detected
Jan 1 01:57:21 router daemon.info racoon: ERROR: pre_share_key foud
Jan 1 01:57:21 router daemon.info racoon: INFO: ISAKMP-SA established 172.16.88.21[500]-23.1.1.3[500] spi:7dc26e09f618b8f4:5cd8125ad1057ba8
Jan 1 01:57:21 router daemon.info racoon: INFO: selected sainfo: loc='ANONYMOUS', rmt='ANONYMOUS', peer='ANY', id=0
Jan 1 01:57:21 router daemon.info racoon: INFO: initiate new phase 2 negotiation: 172.16.88.21[500]<=>23.1.1.3[500]
Jan 1 01:57:21 router daemon.info racoon: INFO: received RESPONDER-LIFETIME: 3600 seconds
Jan 1 01:57:21 router daemon.info racoon: INFO: received RESPONDER-LIFETIME: 4608000 kbytes
Jan 1 01:57:21 router daemon.info racoon: WARNING: attribute has been modified.
Jan 1 01:57:21 router daemon.info racoon: INFO: IPsec-SA established: ESP/Transport 172.16.88.21[500]->23.1.1.3[500] spi=205865745(0xc454311)
Jan 1 01:57:21 router daemon.info opennhrp[4722]: Sending Registration Request to 100.1.1.1 (my mtu=0)
Jan 1 01:57:21 router daemon.info racoon: INFO: IPsec-SA established: ESP/Transport 172.16.88.21[500]->23.1.1.3[500] spi=1016032307(0x3c8f6c33)
Jan 1 01:57:21 router daemon.info opennhrp[4722]: Received Registration Reply from 100.1.1.1: success
Jan 1 01:57:21 router daemon.info opennhrp[4722]: Sending Purge Request (of local routes) to 100.1.1.1
……