# Application Note

## OpenVPN Client with pre-share key for RobustOS

| | |
|---|---|
| Doc Type: | **Application Note** |
| Version: | **v.1.0.0** |
| Date: | **2016-12-26** |
| Status: | **Confidential** |
| Doc ID: | **RT_AN006_OpenVPN Client with pre-share key for RobustOS_v.1.0.0** |
| Author: | **Singson Chen** |

# Contents

Chapter 1 Introduction ..... 2
1.1 Overview ..... 2
1.2 Assumptions ..... 2
1.3 Rectifications ..... 2
1.4 Version ..... 3
Chapter 2 Topology ..... 4
Chapter 3 Configuration ..... 5
3.1 OpenVPN Installation on Windows ..... 5
3.2 Initialize Environment for OpenVPN ..... 9
3.2.1 Generate the pre-shared key for OpenVPN ..... 9
3.3 Configuration for Windows OpenVPN Server ..... 10
3.3.1 Open and Edit server.ovpn File ..... 10
3.4 R2000 Configuration ..... 15
3.4.1 Configure Link Management ..... 15
3.4.2 Configure Cellular WAN ..... 16
3.4.3 Configure IP Address of LAN ..... 19
3.4.4 Configure OpenVPN Client ..... 20
Chapter 4 Testing ..... 26
4.1 Network Status ..... 26
4.2 Running the OpenVPN Software in Windows OS ..... 27
4.3 VPN Status and Communication ..... 28
4.4 Testing at OpenVPN Server ..... 29
4.5 Event/Log ..... 30
Chapter 5 Appendix ..... 33
5.1 Firmware Version ..... 33

# 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. The configuration web interface of the ROS is a little different from the existing old platform of R3000 series.

OpenVPN is an open-source project with GPL license agreement, completing solution characteristics of SSL VPN and providing solutions which contain site-to-site subnet, WIFI security and enterprise remote access. OpenVPN permits to establish VPN by using pre-shared key, third party certificate or username/password for authentication.

This application note has been written for customer with a good understanding of Robustel products and a basic experience of OpenVPN. It shows customer how to configure and test the OpenVPN between the R2000 and Windows OpenVPN server 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 OpenVPN have been fully tested and 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
- Required Software: OpenVPN 2.2.2
- 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.

  R2000’s cellular WAN could be dynamic or static, public or “private with NAT” IP address. OpenVPN is based on certificate, here we use pre-share key for authentication. It needs to install an OpenVPN Easy-RSA certificate created & signed by certificate authority on your PC. Any Easy-RSA is free and easy-to-use.

## 1.3 Rectifications

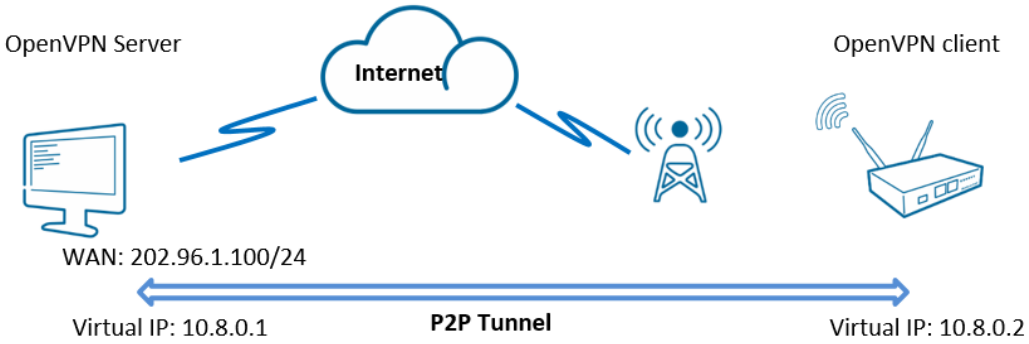
Appreciate for corrections or rectifications to this application note, and if there are any request for new application notes please email to: support@robustel.com.

## 1.4 Version

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

| Release Date | Document Version | Change Description |
|---|---|---|
| 2016-12-26 | v.1.0.0 | Initial Release |

# Chapter 2 Topology




1. The PC runs as OpenVPN server with a fixed public IP address and opens the specify port of OpenVPN.
2. Another R2000 works on wireless network with any kind of IP which can access internet and ping the WAN IP address of OpenVPN server successfully.
3. OpenVPN tunnel is established between server and client. It is a typical application for Point-to-Point connection.

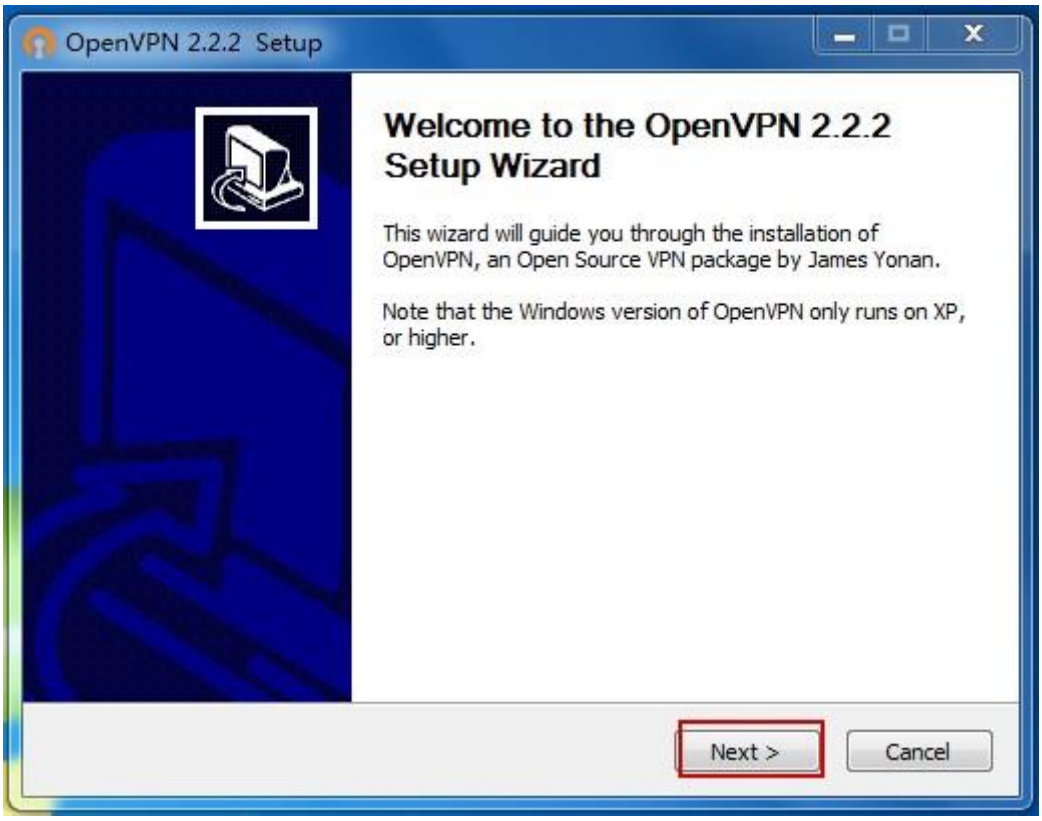
***Note:*** *If OpenVPN server behind a Gateway Router, the Router must open the 1194 port and set up port forwarding to the internal server. 1194 is the default port number for OpenVPN negotiation.*

# Chapter 3 Configuration

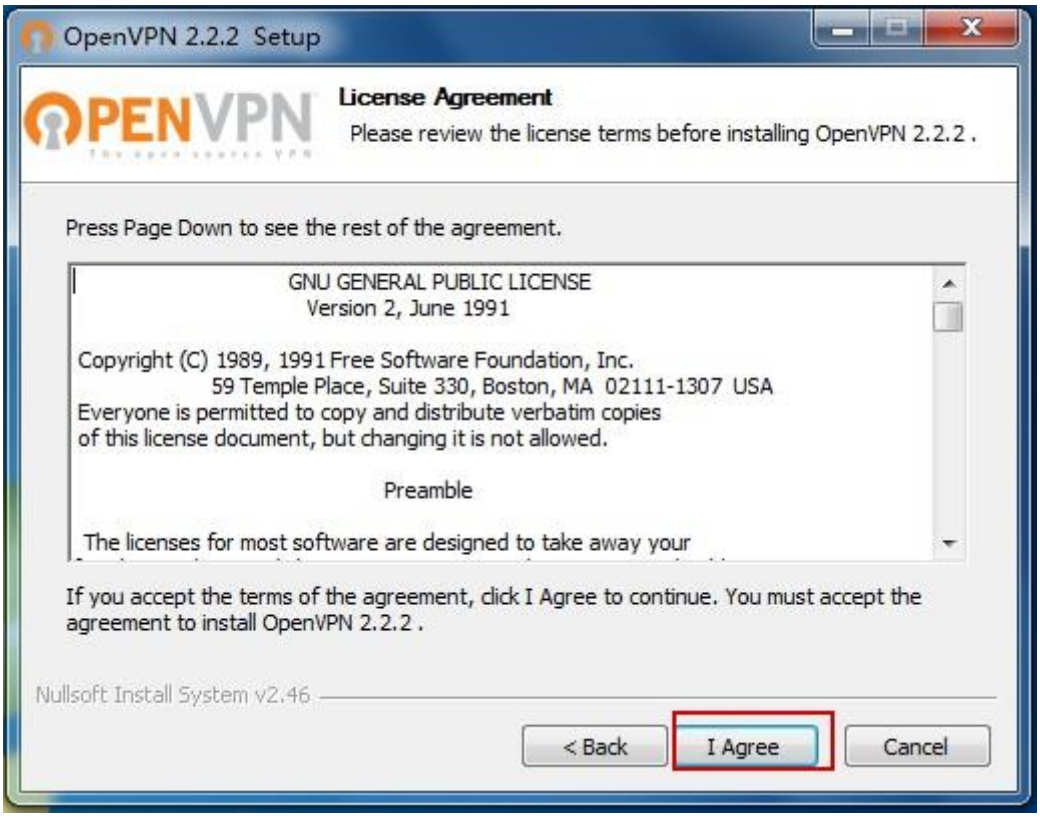
## 3.1 OpenVPN Installation on Windows

This step should be done on the PC which used to create certificates (the PC also can be an OpenVPN server).
Go to **http://openvpn.net/index.php** for download.

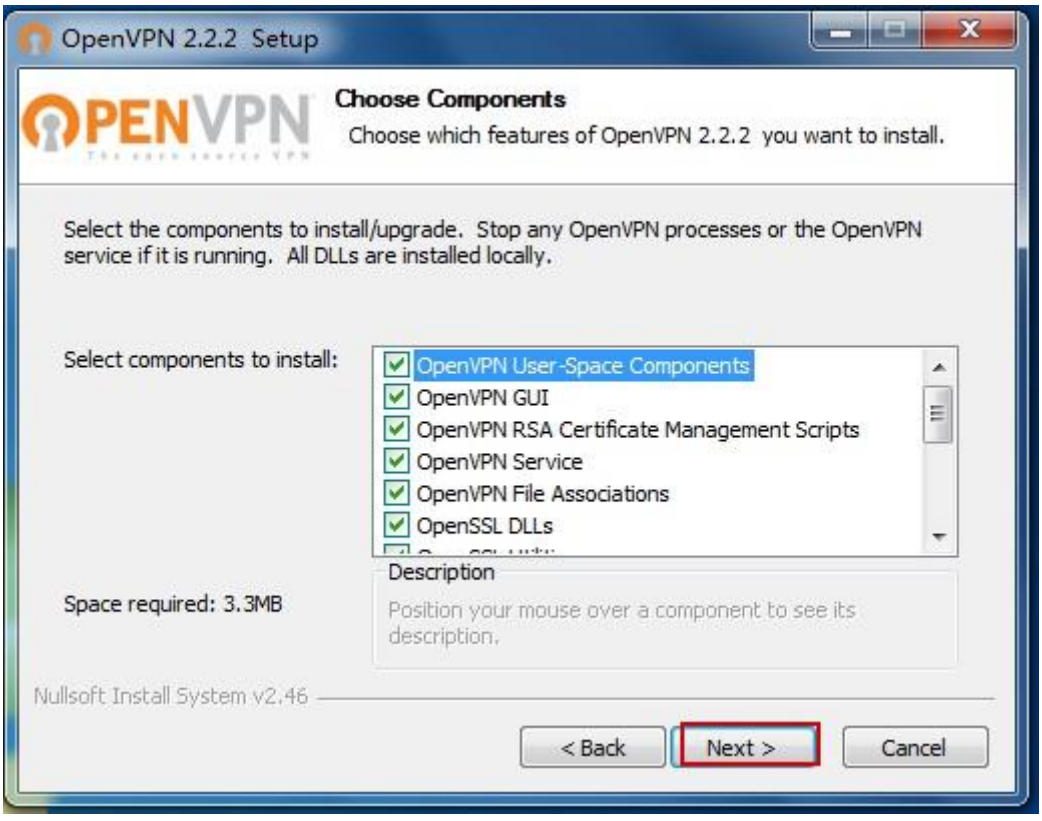
1. Download the release of Windows installer, and run the installation program.



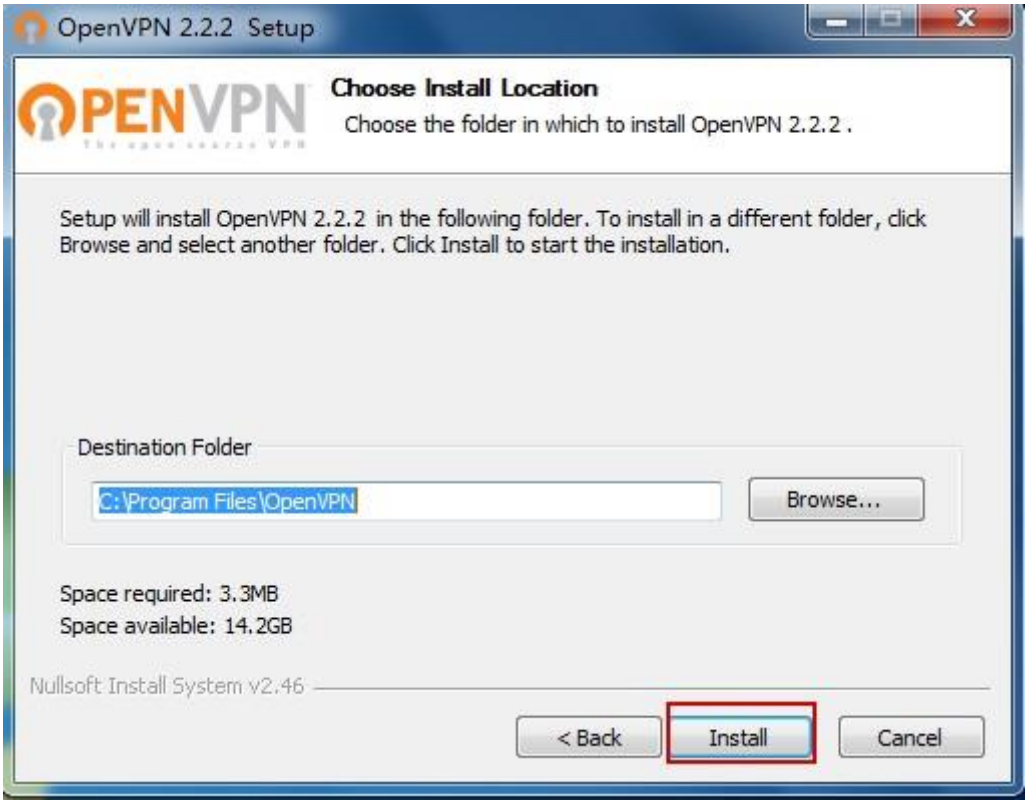
2. Agree the **License Agreement** as below.



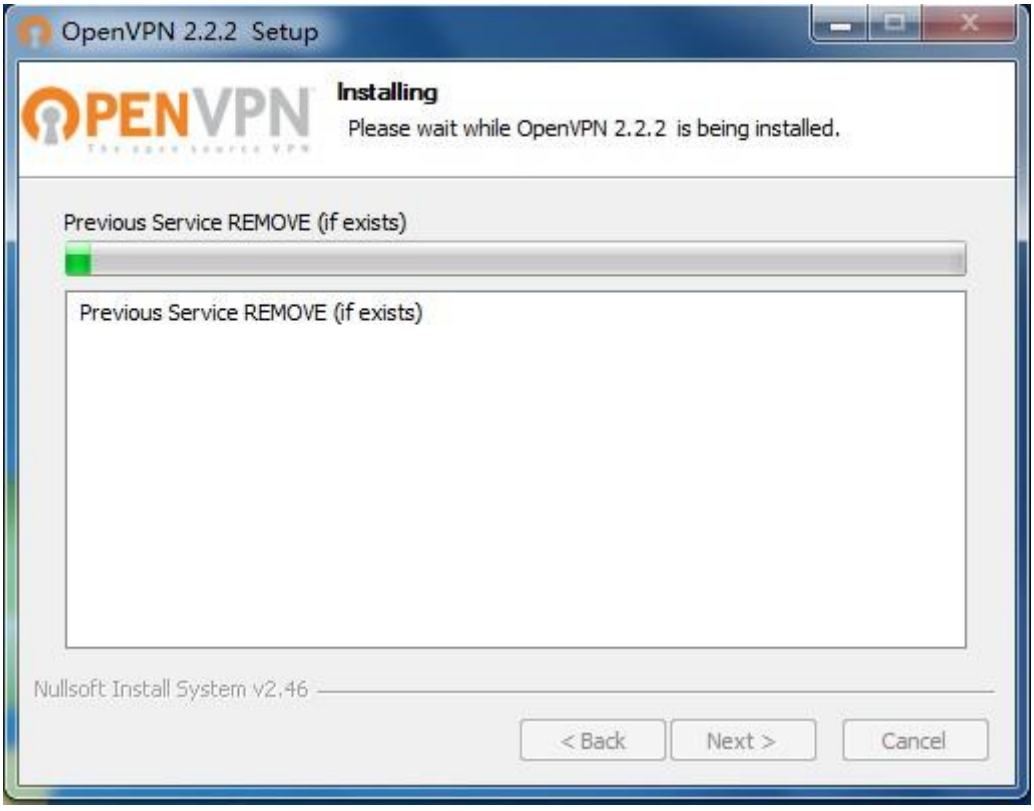

3. Select all options by default.



4. Select the installation path or save in default Destination Folder.

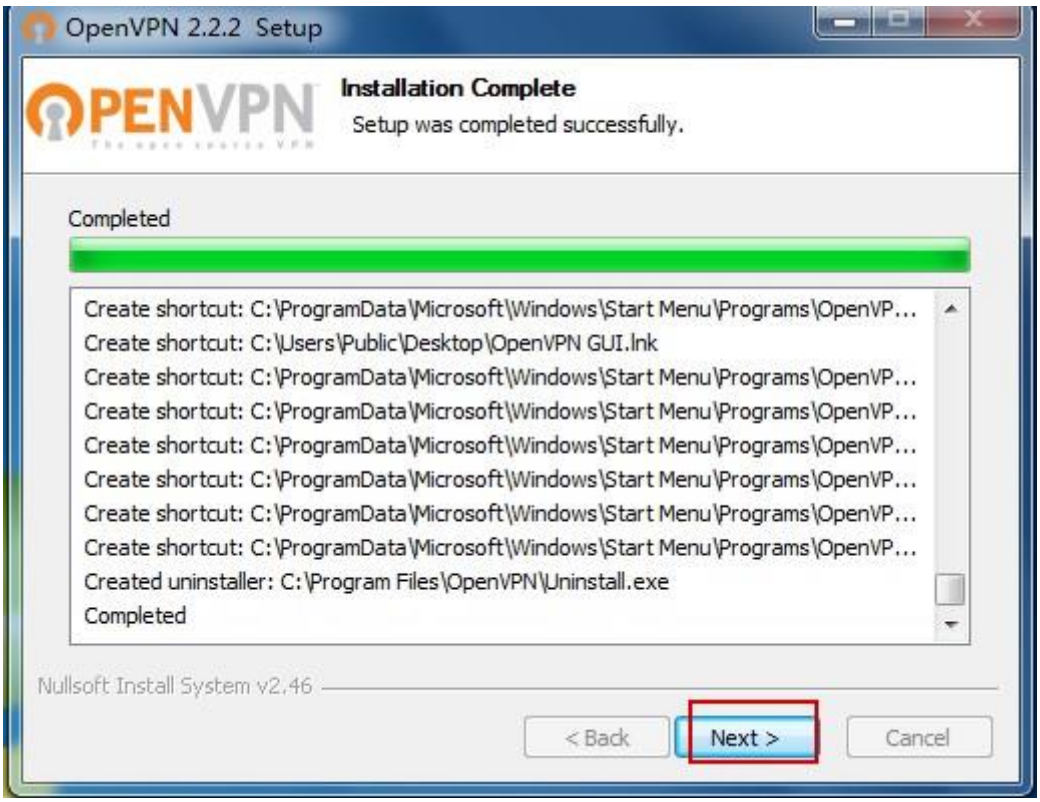



5. Wait while OpenVPN 2.2.2 is being installed.



6. Agree to install the TAP-Win32 network adapter.

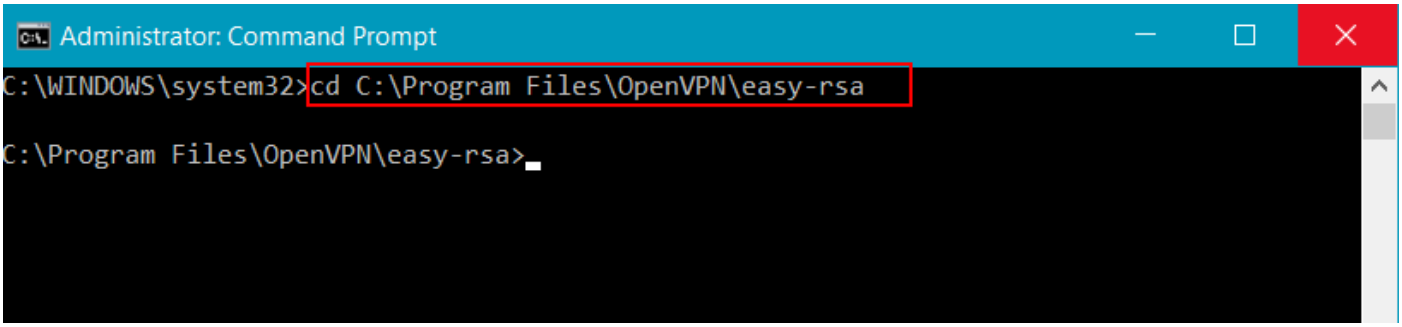

7. Complete the setup.



8. Click **Finish** to complete all installation.


## 3.2 Initialize Environment for OpenVPN

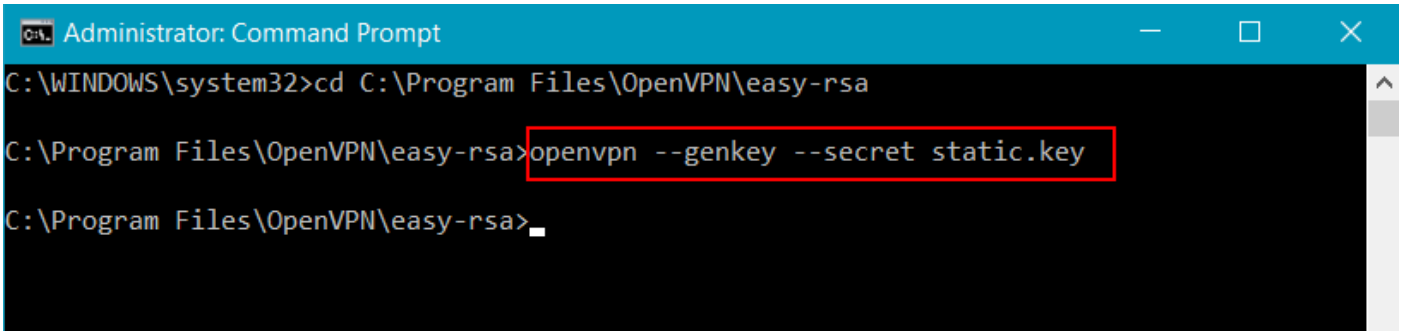
On Windows, open up a command line interface and **cd** to **C:\Program Files\OpenVPN\easy-rsa**.




### 3.2.1 Generate the pre-shared key for OpenVPN

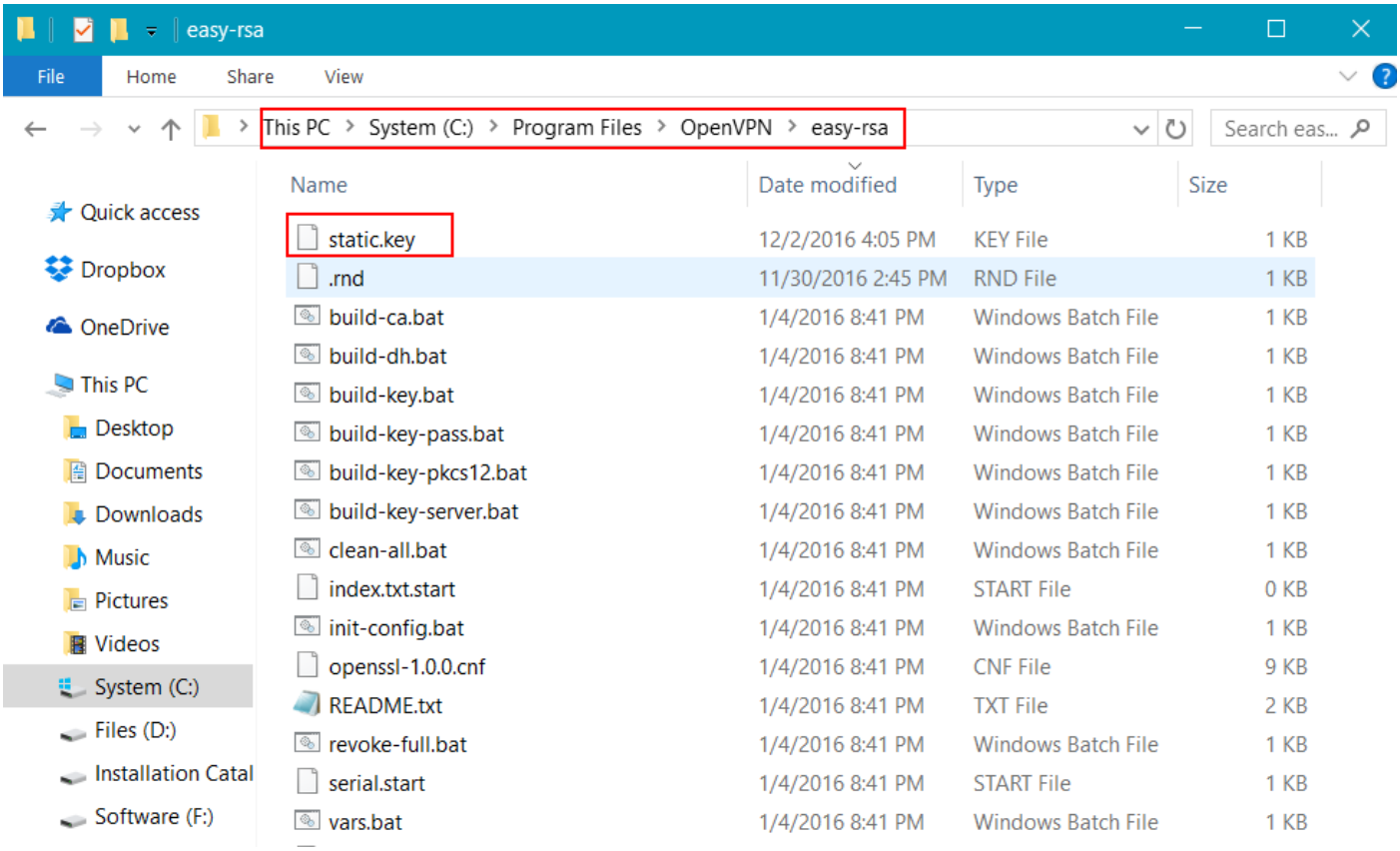
1. Generate the static pre-shared key on Windows.

**>openvpn --genkey --secret static.key**




2. Check the status of static.key.

*Path: C:\Program Files\OpenVPN\easy-rsa*

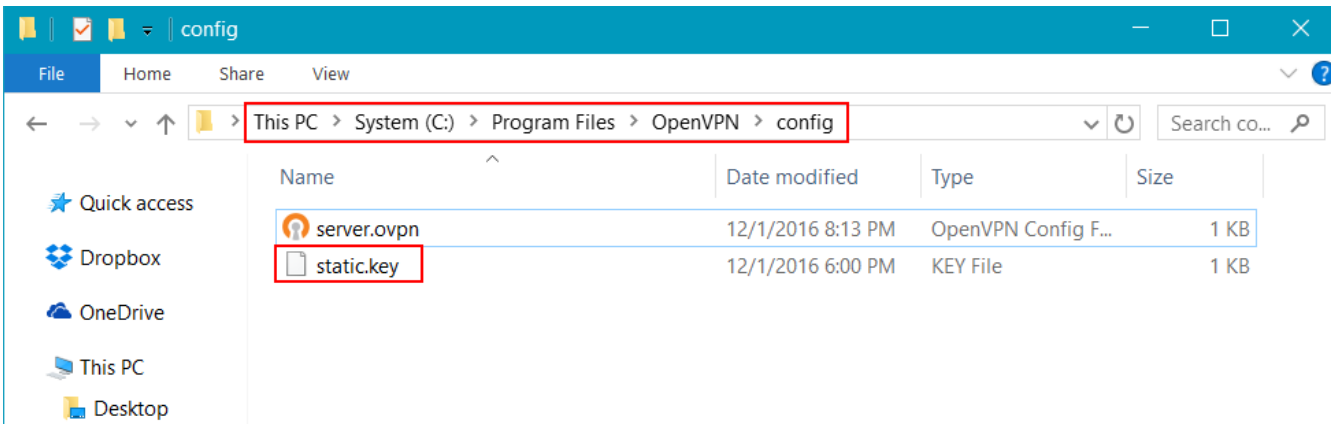



## 3.3 Configuration for Windows OpenVPN Server

The following steps explain the configuration that needs to be done on the Windows OpenVPN Server.

### 3.3.1 Open and Edit server.ovpn File

1. Place the static.key in the OpenVPN\config directory.
   *Path: C:\Program Files\OpenVPN\config*




2. The configuration of the server.

**Note:** The following contents marked as red have been changed from the sample configure defaults, and the extra comments are in blue.

```
#############################################
# Sample OpenVPN 2.0 config file for        #
# multi-client server.                      #
#                                           #
# This file is for the server side          #
# of a many-clients <-> one-server          #
# OpenVPN configuration.                    #
#                                           #
# OpenVPN also supports                     #
# single-machine <-> single-machine         #
# configurations (See the Examples page     #
# on the web site for more info).           #
#                                           #
# This config should work on Windows        #
# or Linux/BSD systems.    Remember on      #
# Windows to quote pathnames and use        #
# double backslashes, e.g.:                 #
# "C:\\Program Files\\OpenVPN\\config\\foo.key"  #
#                                           #
# Comments are preceded with '#' or ';'     #
#############################################

# Which local IP address should OpenVPN
# listen on? (optional)
local 202.96.1.100

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on the same machine, use a different port
# number for each one.    You will need to
```

```
# open up this port on your firewall.
port 1194

# TCP or UDP server?
;proto tcp
proto udp

# "dev tun" will create a routed IP tunnel,
# "dev tap" will create an ethernet tunnel.
# Use "dev tap0" if you are ethernet bridging
# and have precreated a tap0 virtual interface
# and bridged it with your ethernet interface.
# If you want to control access policies
# over the VPN, you must create firewall
# rules for the the TUN/TAP interface.
# On non-Windows systems, you can give
# an explicit unit number, such as tun0.
# On Windows, use "dev-node" for this.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun

# Maximum Transmission Unit for OpenVPN tunnel.
# It is the identifier of the maximum size of packet,
# which is possible to transfer in a given environment.
tun-mtu 1500

# set the fragment length for OpenVPN tunnel.
fragment 1500

# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1. Comment this line out if you are
# ethernet bridging. See the man page for more info.
;server 10.8.0.0 255.255.255.0

# ifconfig is different with VPN subnet under server mode.
# It is the Point-to-Point IP address settings.
ifconfig 10.8.0.1    10.8.0.2
```

```
# Push routes to the client to allow it
# to reach other private subnets behind
# the server.    Remember that these
# private subnets will also need
# to know to route the OpenVPN client
# address pool (10.8.0.0/255.255.255.0)
# back to the OpenVPN server.
;push "route 192.168.10.0 255.255.255.0"
;push "route 192.168.20.0 255.255.255.0"

# EXAMPLE: Suppose the client
# having the certificate common name "Thelonious"
# also has a small subnet behind his connecting
# machine, such as 192.168.40.128/255.255.255.248.
# First, uncomment out these lines:
;client-config-dir ccd
;route 192.168.1.0 255.255.255.0

# If enabled, this directive will configure
# all clients to redirect their default
# network gateway through the VPN, causing
# all IP traffic such as web browsing and
# and DNS lookups to go through the VPN
# (The OpenVPN server machine may need to NAT
# or bridge the TUN/TAP interface to the internet
# in order for this to work properly).
;push "redirect-gateway def1 bypass-dhcp"

# Certain Windows-specific network settings
# can be pushed to clients, such as DNS
# or WINS server addresses.    CAVEAT:
# http://openvpn.net/faq.html#dhcpcaveats
# The addresses below refer to the public
# DNS servers provided by opendns.com.
;push "dhcp-option DNS 208.67.222.222"
;push "dhcp-option DNS 208.67.220.220"

# The keepalive directive causes ping-like
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120
```

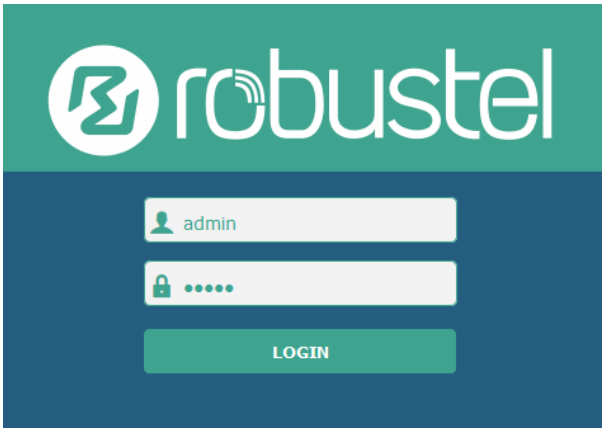
```
# For extra security beyond that provided
# by SSL/TLS, create an "HMAC firewall"
# to help block DoS attacks and UDP port flooding.
#
# Generate with:
#      openvpn --genkey --secret ta.key
#
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
;tls-auth ta.key 0 # This file is secret

# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
cipher BF-CBC               # Blowfish (default)
;cipher AES-128-CBC      # AES
;cipher DES-EDE3-CBC    # Triple-DES

# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo

# Generate with:
#      openvpn --genkey --secret static.key
secret static.key

# The maximum number of concurrently connected
# clients we want to allow.
max-clients 100

# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
#
# You can uncomment this out on
# non-Windows systems.
;user nobody
;group nobody

# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
```

```
persist-key
persist-tun

# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log

# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3

# Silence repeating messages.    At most 20
# sequential messages of the same message
# category will be output to the log.
;mute 20
```

## 3.4 R2000 Configuration

### 3.4.1 Configure Link Management

1. Install the antenna, insert the SIM cards, connect the power supply, and log-in the Web GUI of R2000.

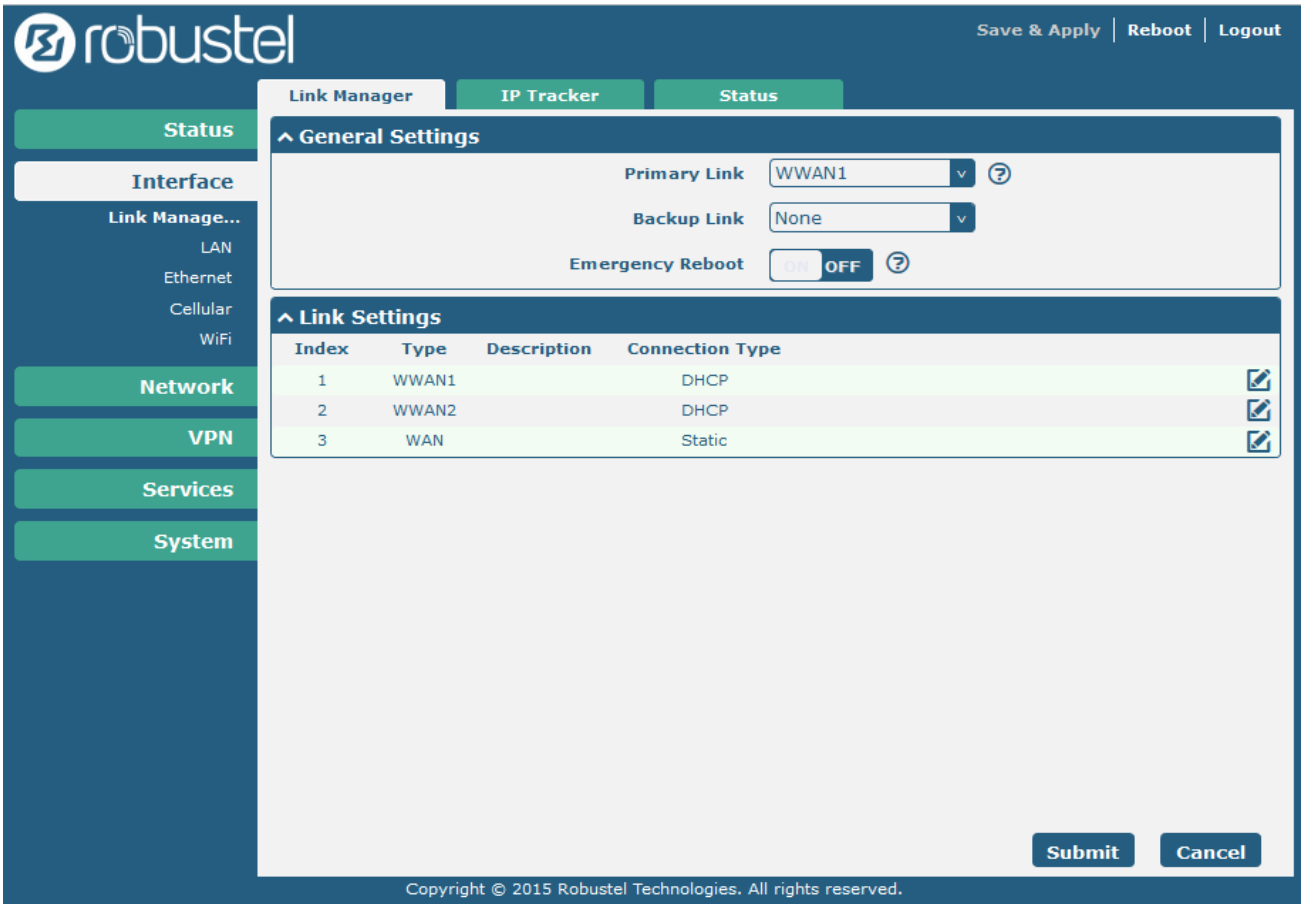


**Note:** You need to know the following factory settings before you have logged in the Web GUI.

| 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 Interface > Link Management.

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



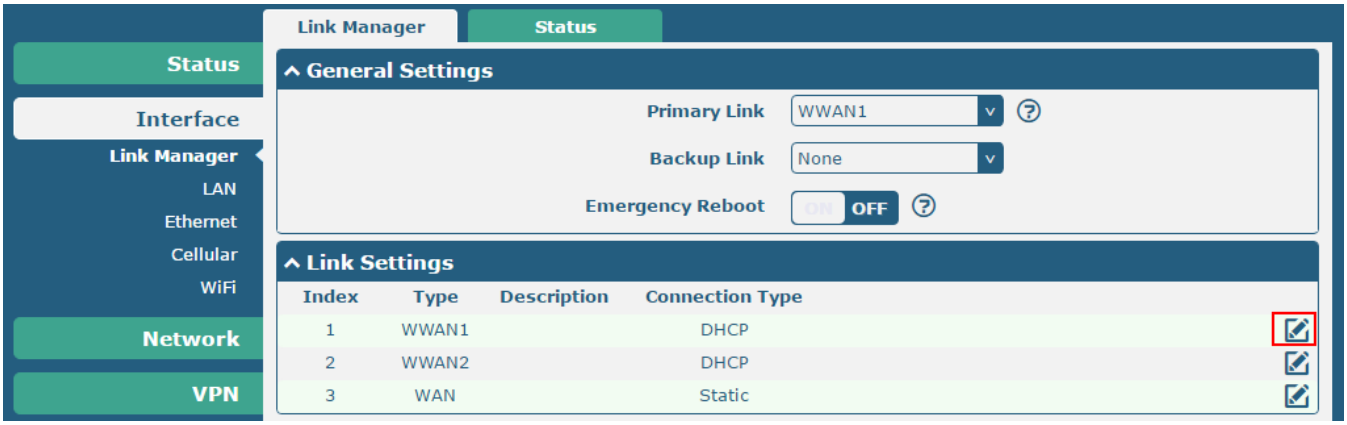

| Item | Description | Setting |
|---|---|---|
| Primary Link | Select “WWAN1”, “WWAN2” or “WAN” as the primary connecting interface. | WWAN1 |

## 3.4.2 Configure Cellular WAN

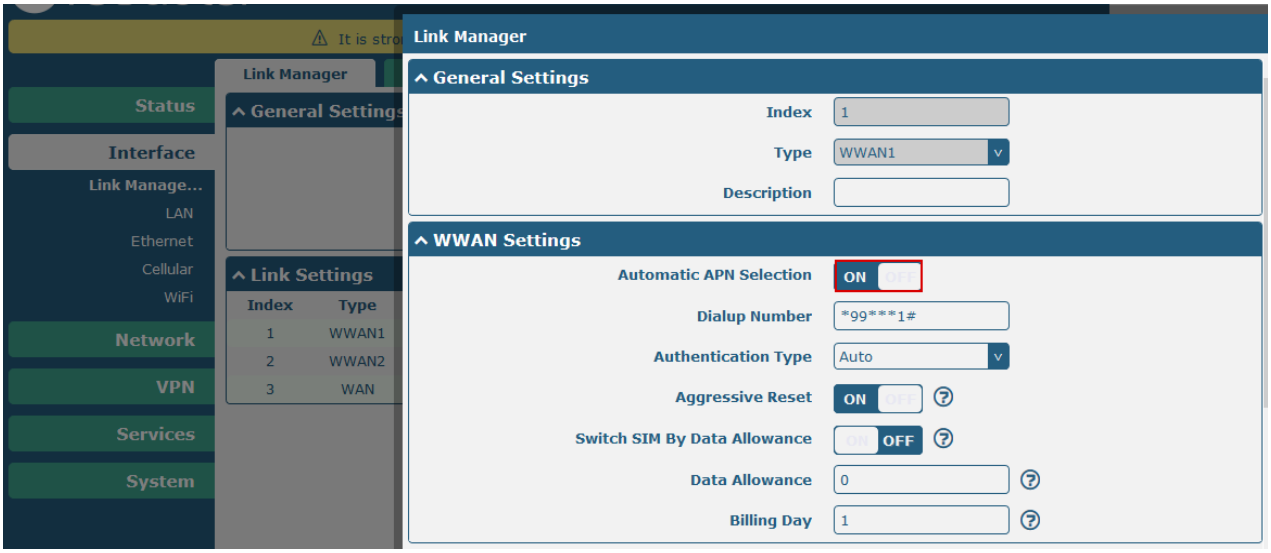
1. Browse **Interface > Link Management > Link Settings**.

- Click the edit button of **WWAN1**.

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

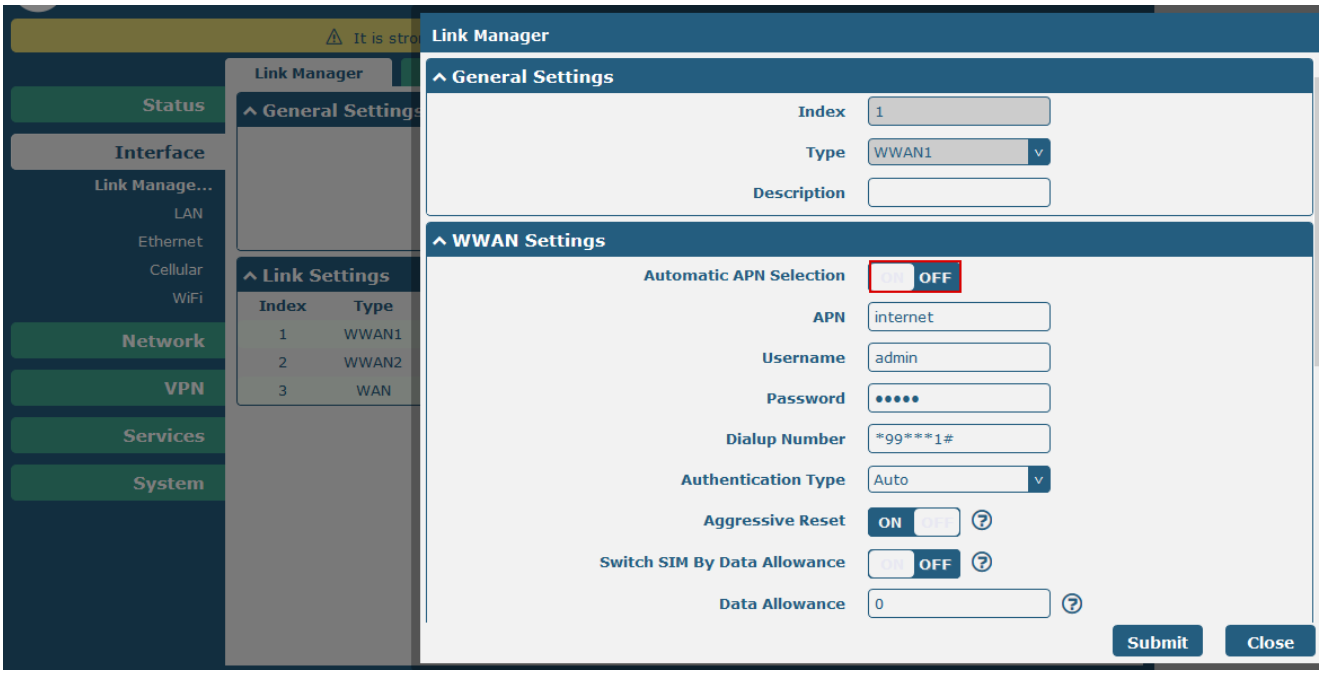



The window is displayed as below when enabling the **Automatic APN Selection**.

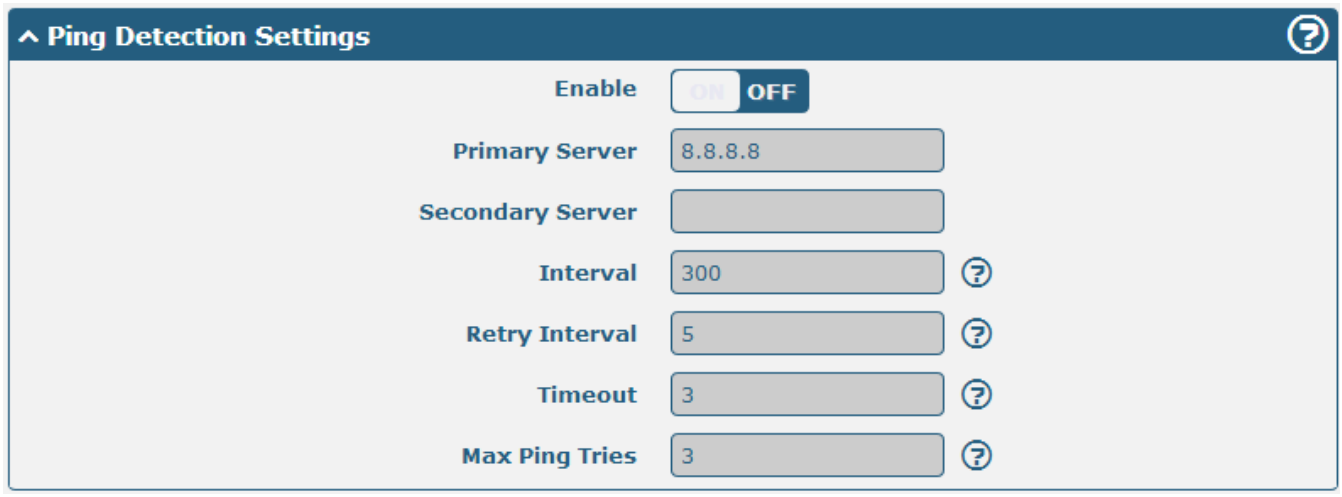



| Item | Description | Setting |
|---|---|---|
| Dialup Number | Set the dialup number for cellular dial-up connection, provided by local ISP. | *99***1# |
| Data Allowance | Set the monthly data traffic limitation. | 0 |
| Billing Day | Specify the monthly billing day, and the data traffic statistics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

The window is displayed as below when disabling the **Automatic APN Selection**.




| Item | Description | Setting |
|---|---|---|
| APN | Access Point Name for cellular dial-up connection, provided by local ISP. | Internet |
| Username | Username for cellular dial-up connection, provided by local ISP | Null |
| Password | Password for cellular dial-up connection, provided by local ISP | Null |



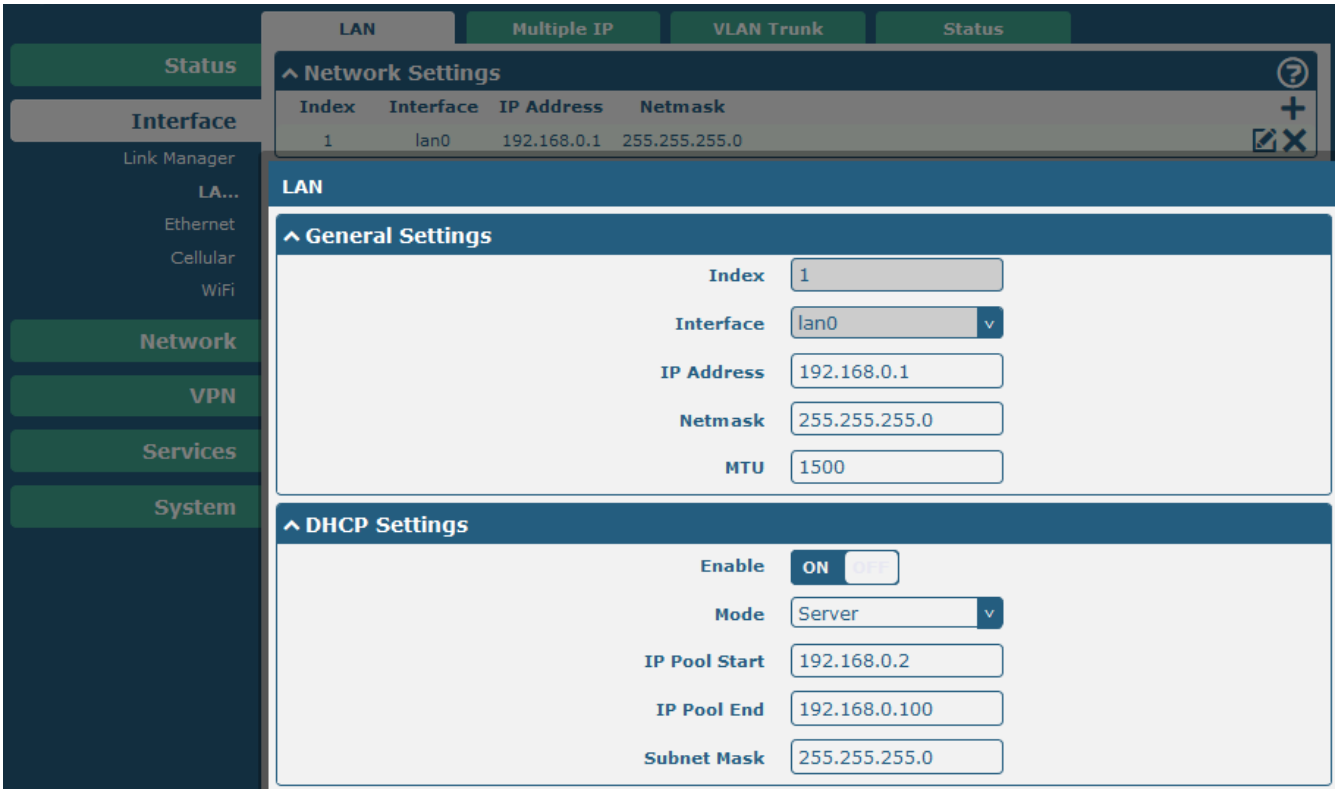

| Item | Description | Setting |
|---|---|---|
| Enable | Click to enable the ping detection, a keepalive policy of R2000 router. | OFF |
| Primary Server | Router will ping this primary address/domain name to check if the current connectivity is active. | 8.8.8.8 |
| Secondary Server | Router will ping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

### 3.4.3 Configure IP Address of LAN

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

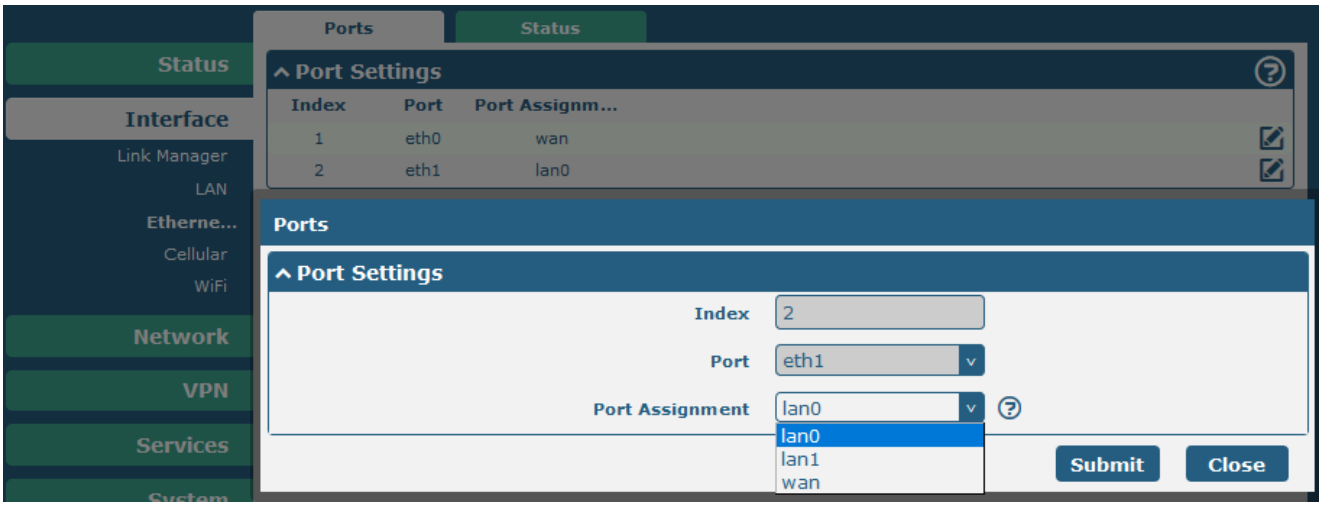
- Click the edit button of **lan0**.
- Set its **IP address** and **Netmask**, and the parameters of **DHCP Settings** are set accordingly.
- Click **Submit**.
- Click **Save & Apply**.




| 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 |

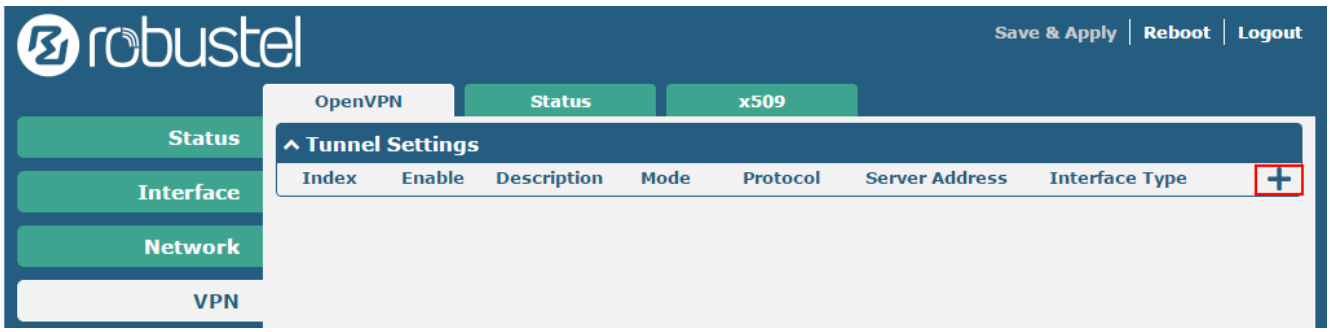
2. Browse **Interface > Ethernet > Ports**.

- Click the edit button of **eth1**.
- Assign **lan0** to the eth1 port.
- Click **Submit**.
- Click **Save & Apply**.

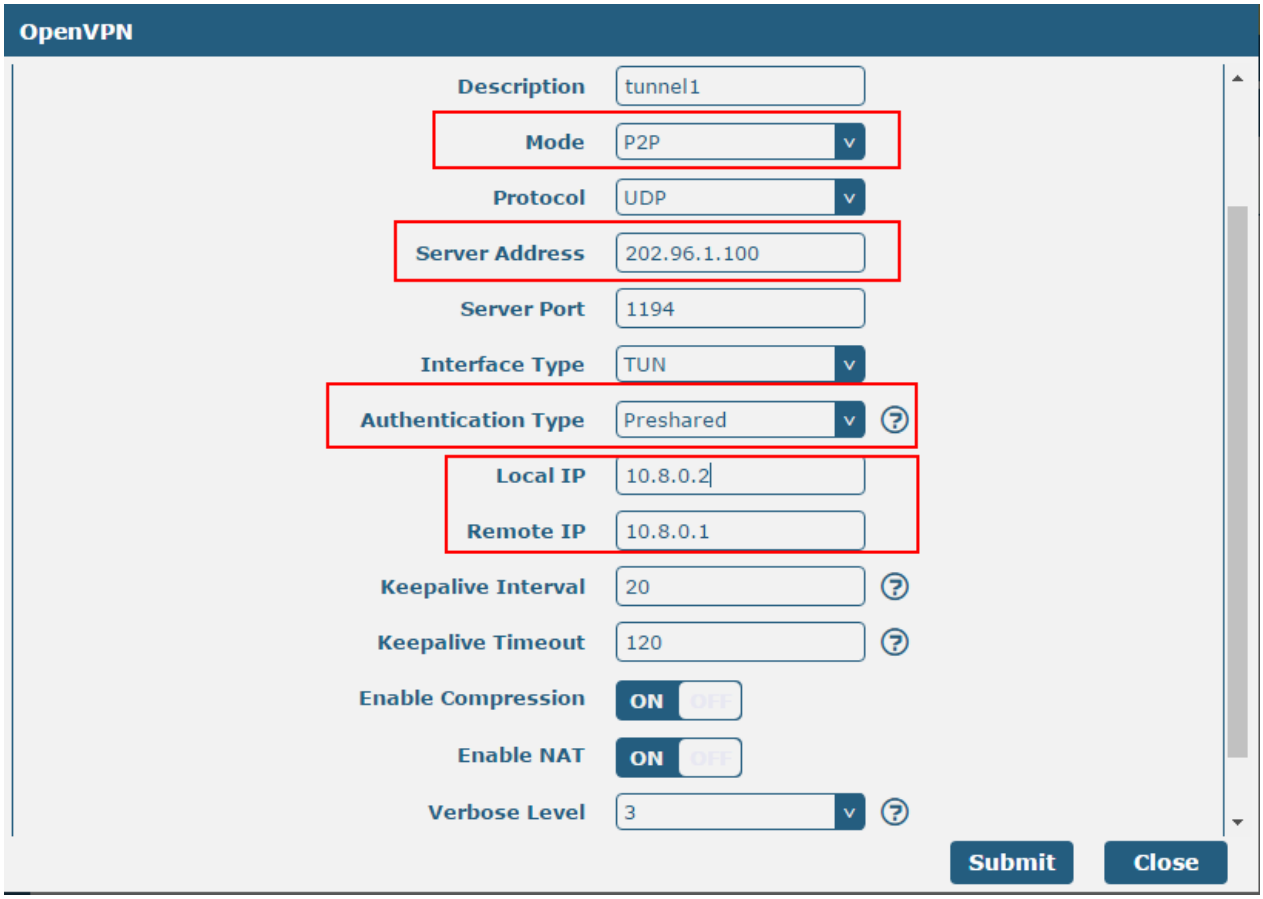



## 3.4.4 Configure OpenVPN Client

1. Browse **VPN > OpenVPN**, and click the add button.



2. Configure the parameters that matched with OpenVPN server side, and click **Submit**.




| Item | Description | Default |
|---|---|---|
| Index | Show the index of the tunnel. | 1 |
| Enable | Click to enable OpenVPN tunnel. | ON |
| Description | Enter some simple words about the OpenVPN Tunnel. | Null |
| Mode | Select from “P2P” or “Client”. | Client |
| Protocol | Select from “UDP” or “TCP-Client”. | UDP |
| Server Address | Enter the server address of OpenVPN. | Null |
| Server Port | Enter the server port of OpenVPN. | 1194 |
| Interface Type | Select from “TUN” or “TAP”, which are two different kinds of device interface for OpenVPN.<br>The difference between TUN and TAP device: a TUN device is a virtual IP point-to-point device and a TAP device is a virtual Ethernet device. | TUN |
| Authentication Type | Select from “None”, “Preshared”, “Password”, “X509CA” or “X509CA Password”.<br>“None” and “Preshared” type is only working in P2P mode. | None |
| Local IP | Define the local IP address of OpenVPN tunnel when setting P2P as the mode. | Null |
| Remote IP | Define the remote IP address of OpenVPN tunnel when setting P2P as the mode. | Null |

| Item | Description | Default |
|---|---|---|
| Username | Username used for Authentication Type “Password” or “X509CA Password”. | Null |
| Password | Password used for Authentication Type “Password” or “X509CA Password”. | Null |
| Encrypt Algorithm | Select from “BF”, “DES”, “DES-EDE3”, “AES128”, “AES192” or “AES256”.<br>BF: Use the BF algorithm in CBC mode and 128-bit key<br>DES: Use the DES algorithm in CBC mode and 64-bit key<br>DES-EDE3: Use the 3DES algorithm in CBC mode and 192-bit key<br>AES128: Use the AES algorithm in CBC mode and 128-bit key<br>AES192: Use the AES algorithm in CBC mode and 192-bit key<br>AES256: Use the AES algorithm in CBC mode and 256-bit key | BF |
| Keepalive Interval | Set keepalive (ping) interval to check if the tunnel is active. | 20 |
| Keepalive Timeout | Trigger OpenVPN to restart after n seconds if not receiving a ping or other packets from remote. | 120 |
| Private Key Password | Password of Private Key for Authentication Type “X509CA”. | Null |
| Enable Compression | Enable to compress the data stream. | ON |
| Enable NAT | Click to enable NAT for OpenVPN.<br>The source IP address of host behind R2000 will be disguised before accessing the remote OpenVPN client. | OFF |
| Verbose Level | Select the level of the output log. Values range from 0 to 11.<br>0 -- No output except fatal errors<br>1 to 4 -- Normal usage range<br>5 -- Output R and W characters to the console for each packet read and write<br>6 to 11 -- Debug info range | 0 |

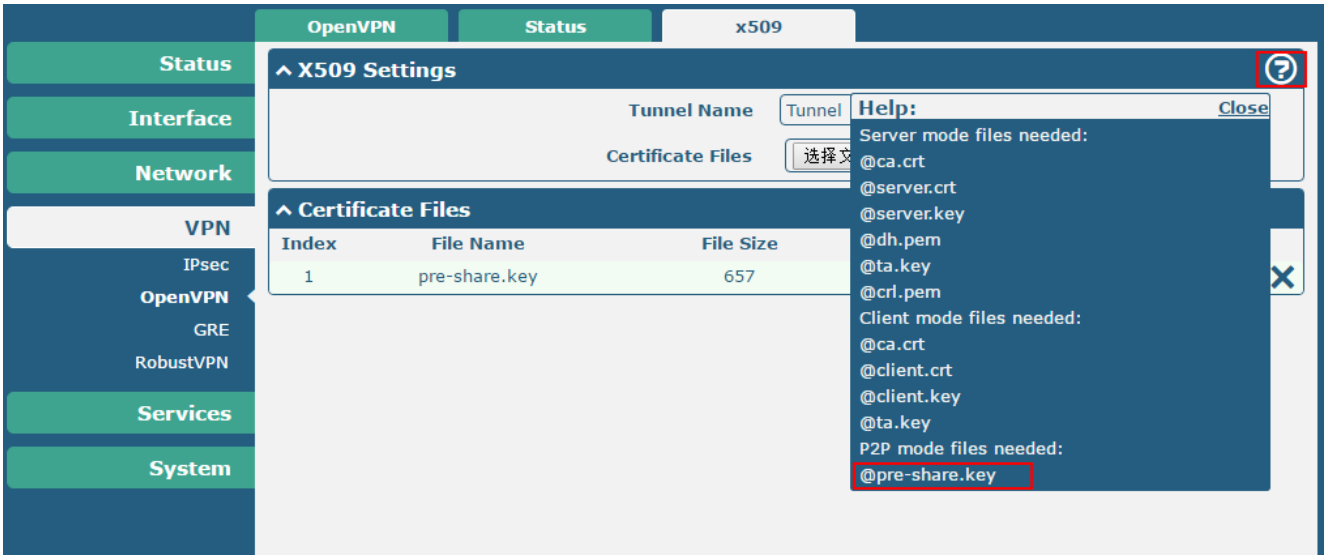

**Note:** For Expert Options, we suggest inputting “**fragment 1500; persist-tun; persist-key**” to establish a correct P2P tunnel with server.

| Item | Description | Default |
|---|---|---|
| Enable HMAC Firewall | Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks. | OFF |
| Enable PKCS#12 | Enable the PKCS#12 certificate.<br>It is an exchange of digital certificate encryption standard, used to describe personal identity information. | OFF |
| Enable nsCertType | Require that peer certificate was signed with an explicit nsCertType designation of "server". | OFF |

| | | |
|---|---|---|
| Expert Options | Enter some other options of OpenVPN in this field. Each expression can be separated by a semicolon (;). | Null |

3. Import the pre-share key for OpenVPN.

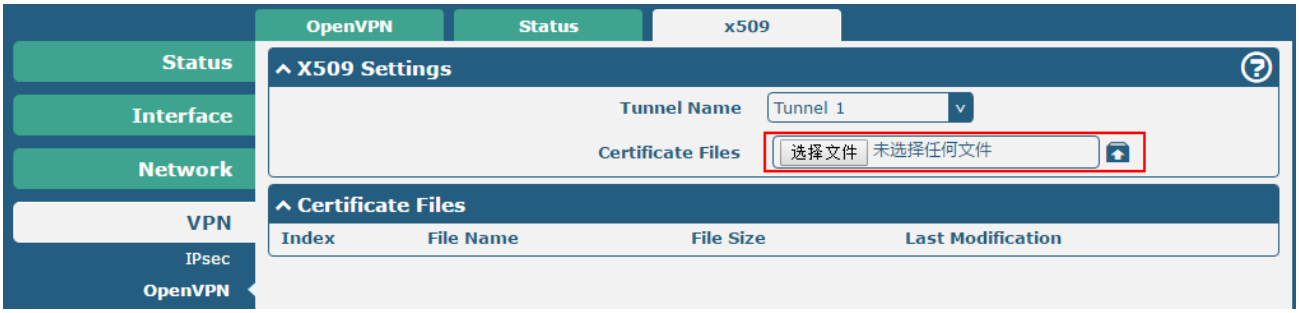
- Browse **VPN > OpenVPN > X509**.




| Item | Description | Setting |
|---|---|---|
| Select Cert Type | Select the OpenVPN client or server which the certificate used for. | Select accordingly |
| CA | Click “Browse” to select the correct CA file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the CA file from the router to your PC. | Select accordingly |
| Public Key | Click “Browse” to select the correct Public Key file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the Public Key A file from the router to your PC. | Select accordingly |
| Private Key | Click “Browse” to select the correct Private Key file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the Private Key file from the router to your PC. | Select accordingly |
| DH | Click “Browse” to select the correct DH A file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the DH file from the router to your PC. | Null |
| TA | Click “Browse” to select the correct TA file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the TA file from the router to your PC. | Null |
| CRL | Click “Browse” to select the correct CRL file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the CRL file from the router to your PC. | Null |
| Pre-Share Static Key | Click “Browse” to select the correct Pre-Share Static Key file from your PC, and click “Import” to import it to the router.<br>Click “Export” to export the Pre-Share Static Key file from the | Null |

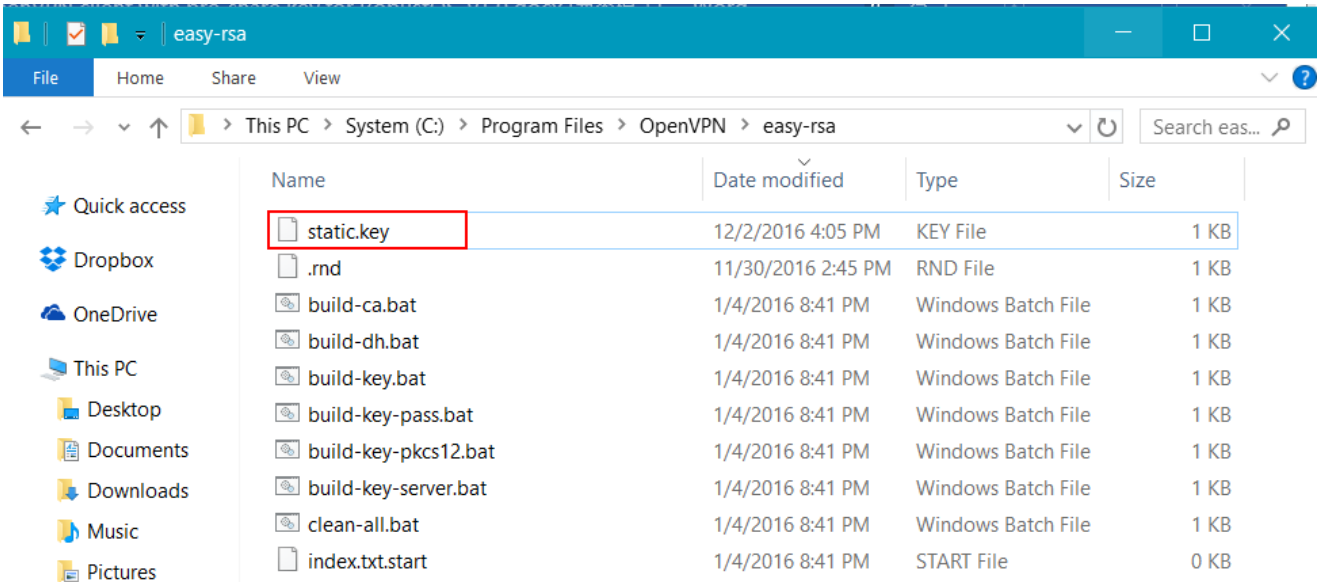
| | | |
|---|---|---|
| | router to your PC. | |

4. Import the certificate, select the Tunnel Name for **Client** and click **Choose File**.

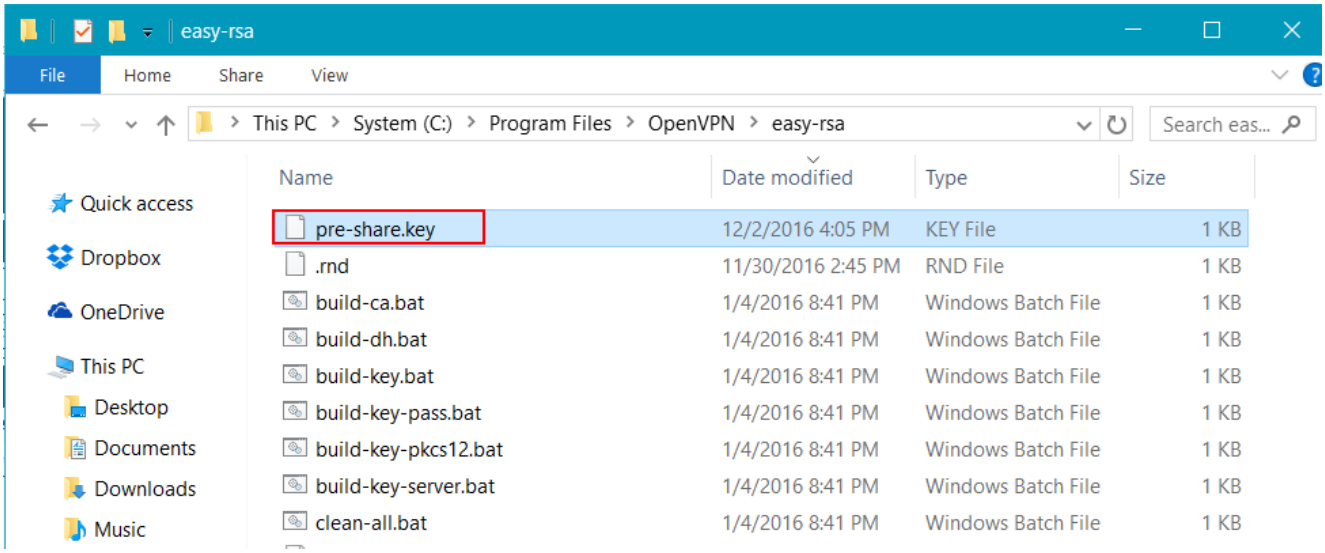



5. Rename the **static.key** to **pre-share.key** in path C:\Program Files\OpenVPN\easy-rsa\keys, regarding the rule of file name in R2000. Then import the **pre-share.key.**

- Original files:




- Renamed files which should be imported:

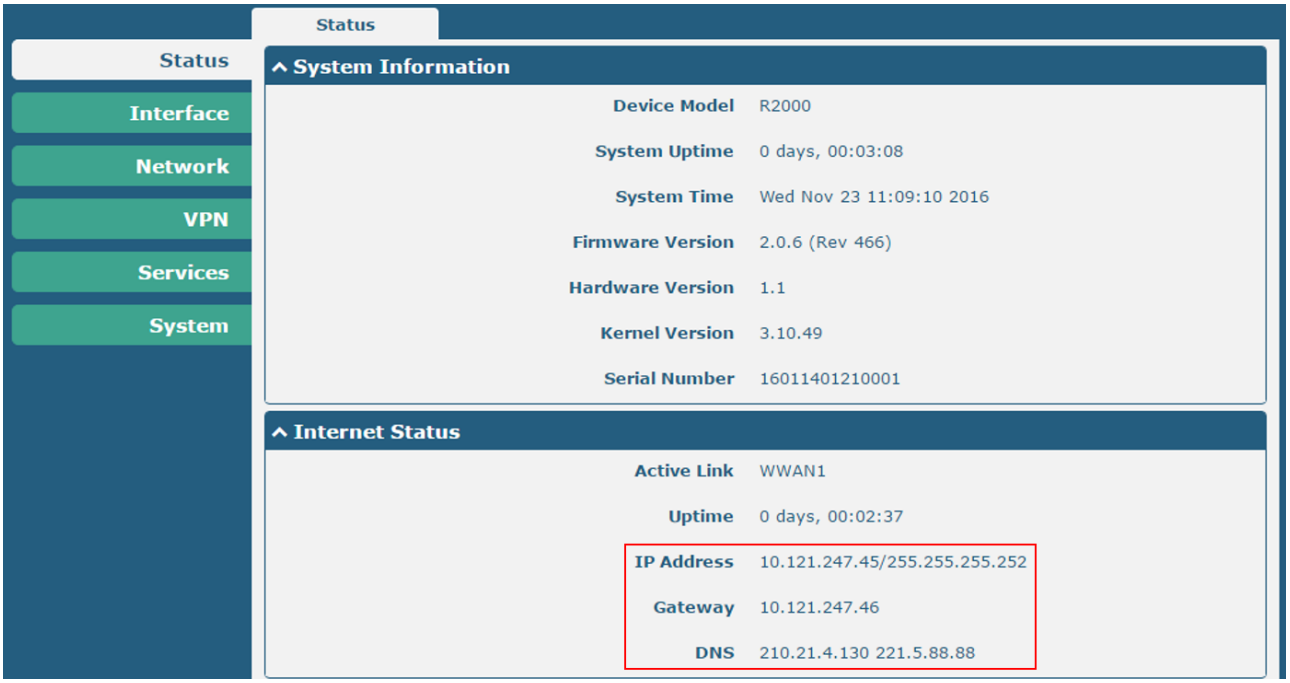


6. Click the **Save & Apply** and check the x509 status.

# Chapter 4 Testing

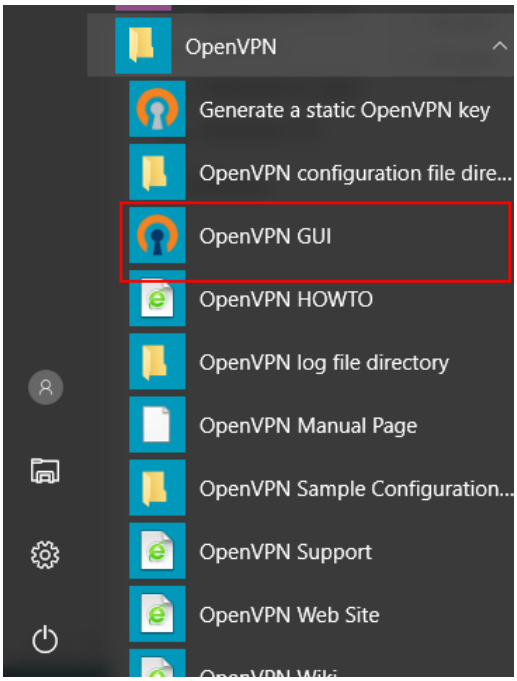
## 4.1 Network Status

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



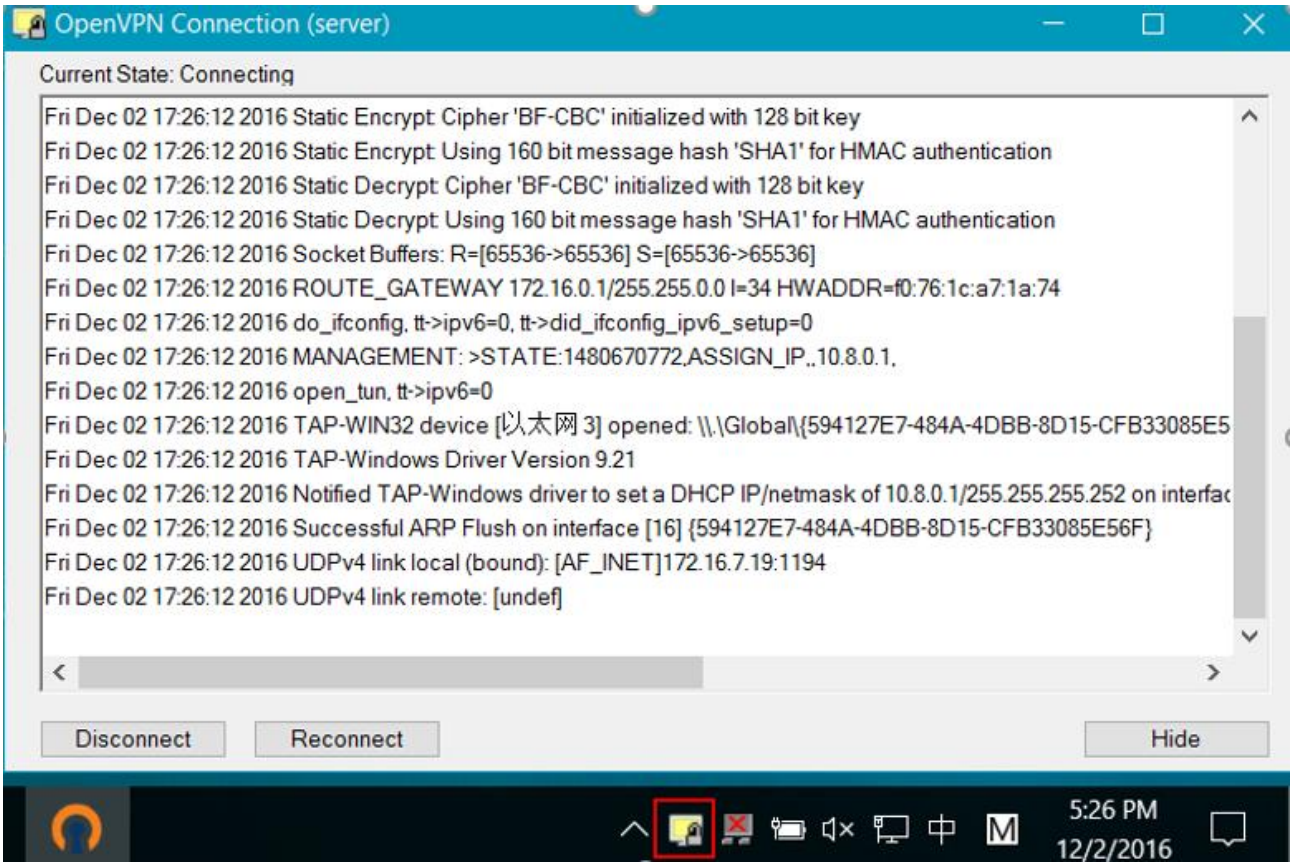
## 4.2 Running the OpenVPN Software in Windows OS

1. Run the OpenVPN software.

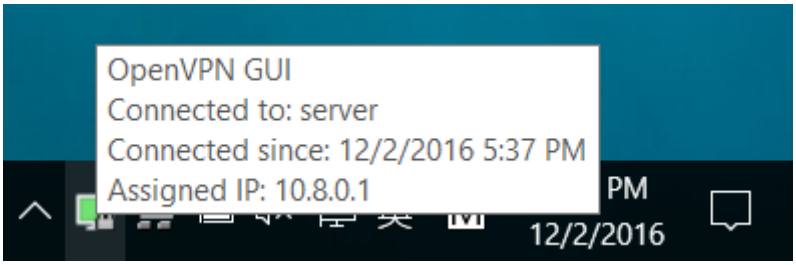



2. Check the OpenVPN icon in the system tray.


3. Right-click the icon and connect the Openvpn Server, then the icon will turn yellow and the Server run up to wait for the connection from peer outsides.



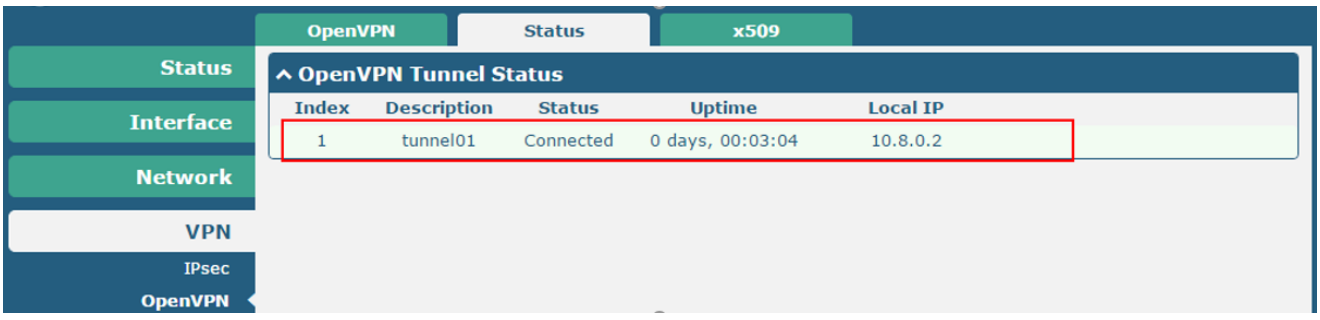

4. The icon will turn green and prompt a notification with the assigned IP address once the peer has connected and the tunnel establishes successfully.



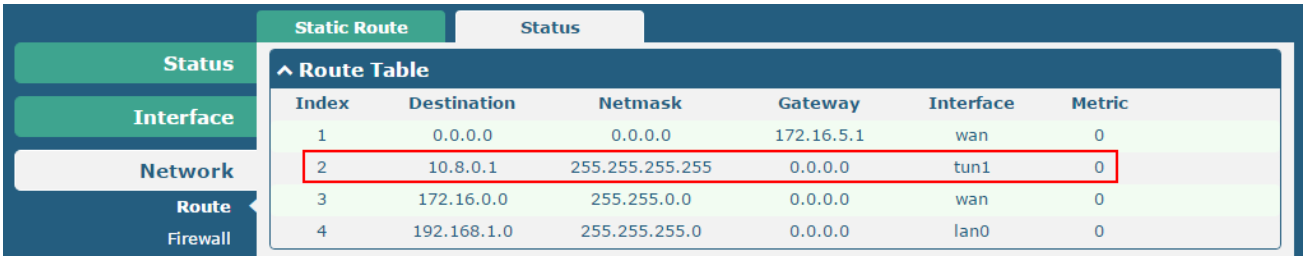

## 4.3 VPN Status and Communication

Browse **VPN > OpenVPN > Status**.

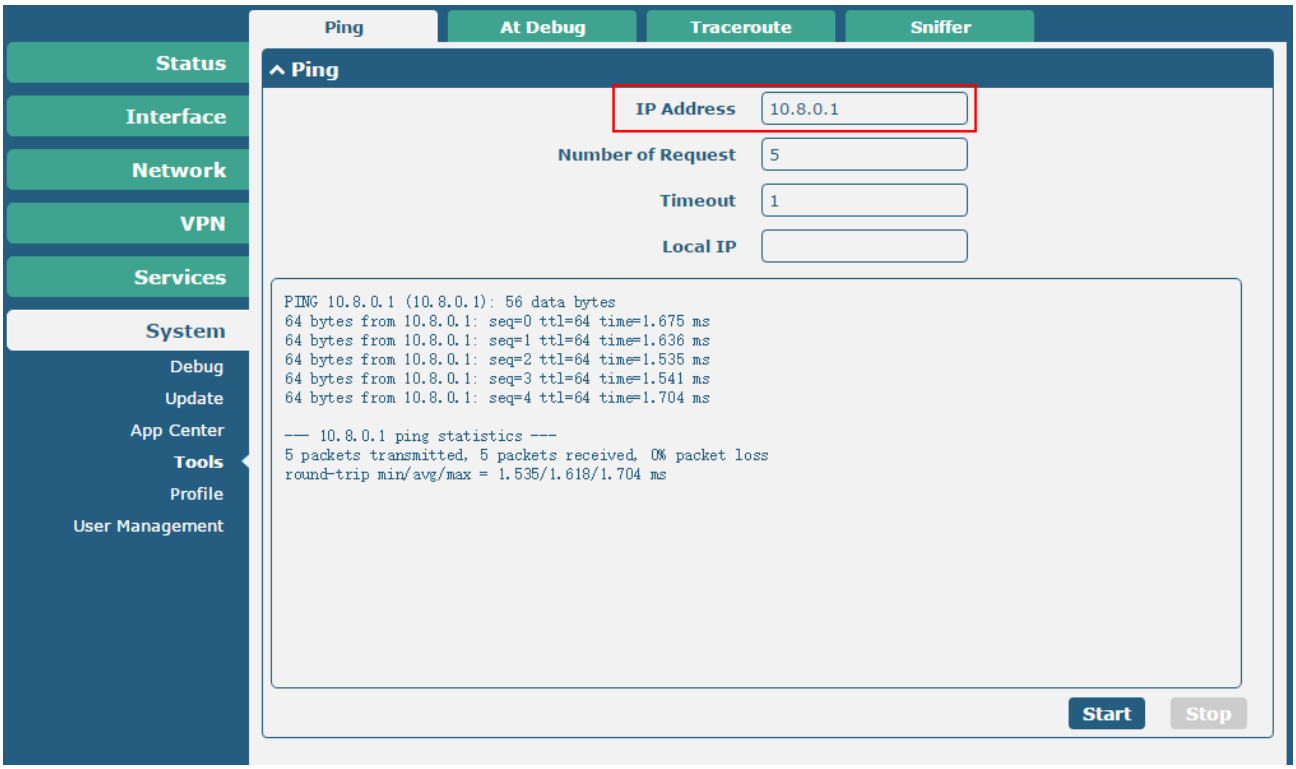
- Check whether R2000 has established OpenVPN tunnel with Server side.



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

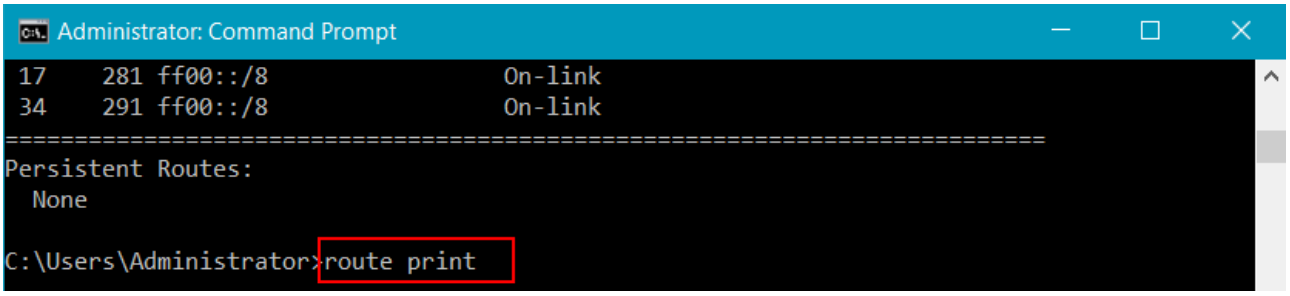



- Browse **System > Tools > Ping**.
  Ping virtual IP of OpenVPN tunnel and get ICMP reply from OpenVPN server.

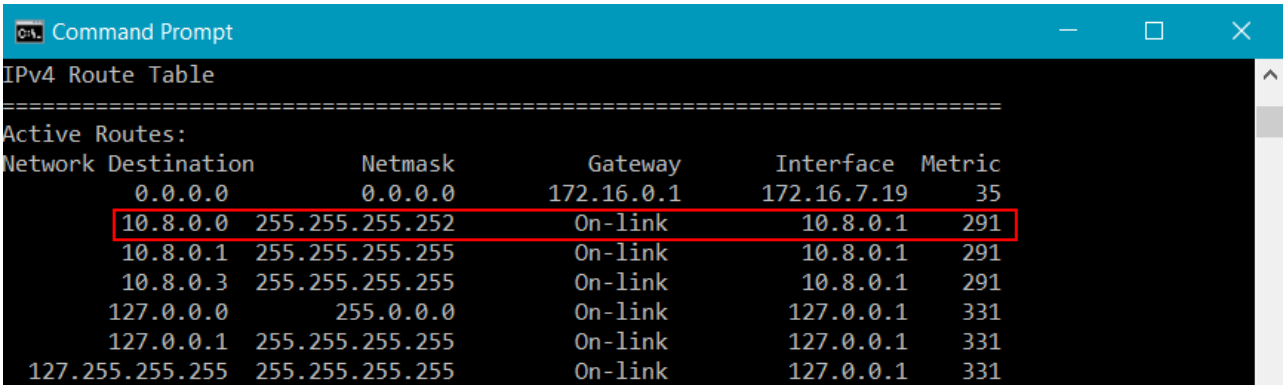



## 4.4 Testing at OpenVPN Server

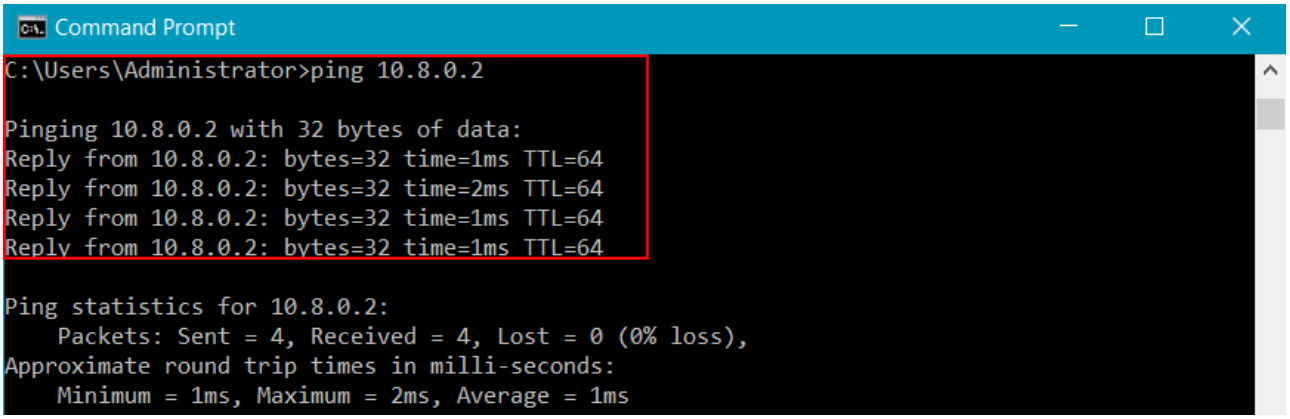
1. Run the CLI and input “route print” command to check the route-table in Windows 7.



2. There is a remote subnet 192.168.1.0/24 passing through the OpenVPN tunnel.

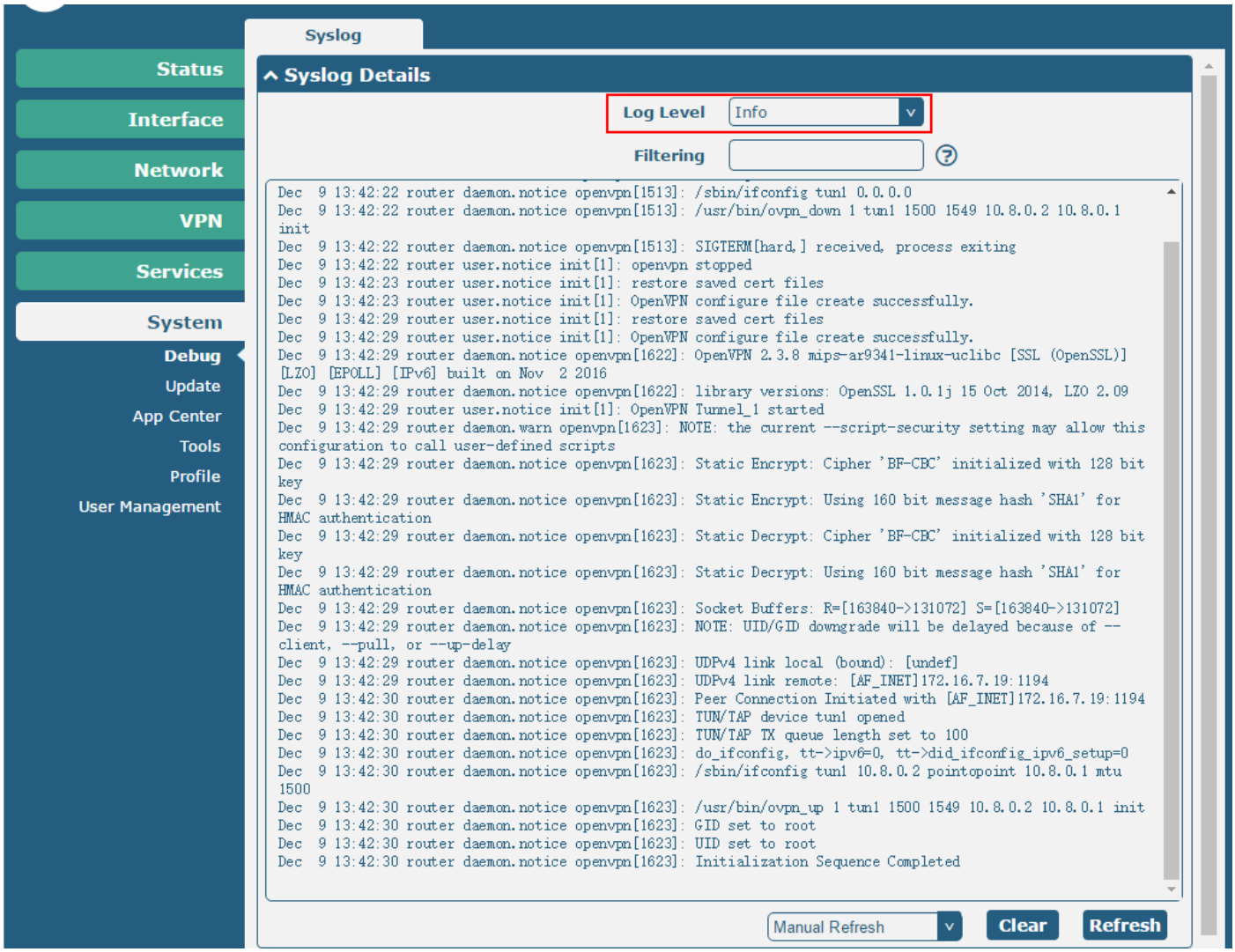



3. Ping the virtual IP of OpenVPN client and LAN IP address behind R2000, got ICMP reply from remote end.




## 4.5 Event/Log

Debug shows the running process and the status of R2000. Only the information is relevant to the configuration above will be explained below:




……

Dec 9 13:42:29 router user.notice init[1]: OpenVPN configure file create successfully.

Dec 9 13:42:29 router daemon.notice openvpn[1622]: OpenVPN 2.3.8 mips-ar9341-linux-uclibc [SSL (OpenSSL)] [LZO] [EPOLL] [IPv6] built on Nov 2 2016

Dec 9 13:42:29 router daemon.notice openvpn[1622]: library versions: OpenSSL 1.0.1j 15 Oct 2014, LZO 2.09

**Dec 9 13:42:29 router user.notice init[1]: OpenVPN Tunnel_1 started**

Dec 9 13:42:29 router daemon.warn openvpn[1623]: NOTE: the current --script-security setting may allow this configuration to call user-defined scripts

Dec 9 13:42:29 router daemon.notice openvpn[1623]: Static Encrypt: Cipher 'BF-CBC' initialized with 128 bit key

Dec 9 13:42:29 router daemon.notice openvpn[1623]: Static Encrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Dec 9 13:42:29 router daemon.notice openvpn[1623]: Static Decrypt: Cipher 'BF-CBC' initialized with 128 bit key

Dec 9 13:42:29 router daemon.notice openvpn[1623]: Static Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication

Dec 9 13:42:29 router daemon.notice openvpn[1623]: Socket Buffers: R=[163840->131072] S=[163840->131072]

Dec 9 13:42:29 router daemon.notice openvpn[1623]: NOTE: UID/GID downgrade will be delayed because of --client, --pull, or --up-delay

Dec 9 13:42:29 router daemon.notice openvpn[1623]: UDPv4 link local (bound): [undef]

**Dec 9 13:42:29 router daemon.notice openvpn[1623]: UDPv4 link remote: [AF_INET]172.16.7.19:1194**
**Dec 9 13:42:30 router daemon.notice openvpn[1623]: Peer Connection Initiated with [AF_INET]172.16.7.19:1194**
Dec 9 13:42:30 router daemon.notice openvpn[1623]: TUN/TAP device tun1 opened
Dec 9 13:42:30 router daemon.notice openvpn[1623]: TUN/TAP TX queue length set to 100
Dec 9 13:42:30 router daemon.notice openvpn[1623]: do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
**Dec 9 13:42:30 router daemon.notice openvpn[1623]: /sbin/ifconfig tun1 10.8.0.2 pointopoint 10.8.0.1 mtu 1500**
**Dec 9 13:42:30 router daemon.notice openvpn[1623]: /usr/bin/ovpn_up 1 tun1 1500 1549 10.8.0.2 10.8.0.1 init**
Dec 9 13:42:30 router daemon.notice openvpn[1623]: GID set to root
Dec 9 13:42:30 router daemon.notice openvpn[1623]: UID set to root
**Dec 9 13:42:30 router daemon.notice openvpn[1623]: Initialization Sequence Completed**
**……**

# Chapter 5 Appendix

## 5.1 Firmware Version

The configuration above was tested on R2000 with firmware version 2.0.6.